



**MEASUREMENT OF SYSTEM SECURITY ISSUES OF PRIVATE
COMPUTER NETWORKS FOR DIFFERENT TYPES OF ATTACKS**

Taha ALJADIR

August 2015

**MEASUREMENT OF SYSTEM SECURITY ISSUES OF PRIVATE
COMPUTER NETWORKS FOR DIFFERENT TYPES OF ATTACKS**

**A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY**

**BY
TAHA ALJADIR**

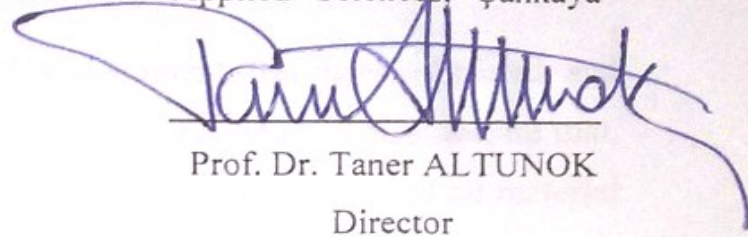
**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
COMPUTER ENGINEERING**

August 2015

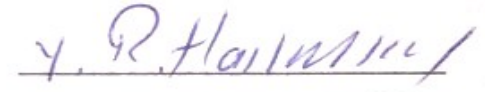
Title of the Thesis: **Measurement of System Security Issues of Private Computer Networks for Different Types of Attacks.**

Submitted by **Taha ALJADIR**

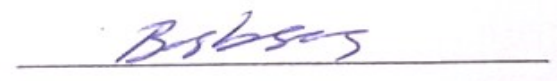
Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.


Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.


Prof. Dr. Müslim BOZYIĞIT
Head of Department

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


Assist. Prof. Dr. Barbaros Preveze
Supervisor

Examination Date: 12.08.2015

Examining Committee Members

Assist. Prof. Dr. Barbaros PREVEZE

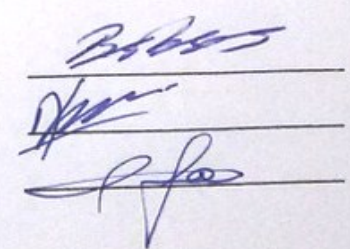
Assist. Prof. Dr. Abdül Kadir GÖRÜR

Assoc. Prof. Dr. Fahd JARAD

(Çankaya Univ.)

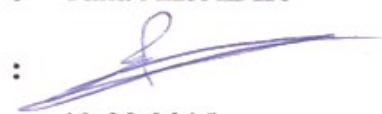
(Çankaya Univ.)

(UTAA)



STATEMENT OF NON-PLAGIARISM PAGE

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 : Taha ALJADIR
Signature : 
Date : 12.08.2015

ABSTRACT

MEASUREMENT OF SYSTEM SECURITY ISSUES OF PRIVATE COMPUTER NETWORKS FOR DIFFERENT TYPES OF ATTACKS

Taha ALJADIR

M.Sc., Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Barbaros PREVEZE

August 2015, 96 pages

In this thesis, two different types of Remote Access Virtual Private Network protocols (PPTP and SSL) have been established virtually using Virtual Lab. In addition, different types of security attacks have been applied to each protocol under the same conditions. For each attack, different tools were applied separately to each protocol. Moreover, the attacks were used to target different components for each VPN. The results were studied carefully, which led to obtaining a good security analysis used later to compare between those protocols under the test conditions and to give recommendations to use each of those protocols.

Keywords: Attack, VPN, Security, PPTP, SSL

ÖZ

SALDIRILAR FARKLI TIPLERİ İÇİN ÖZEL BİLGİSAYAR ŞEBEKELERİNİN SİSTEM GÜVENLİK KONULARI ÖLÇÜMÜ

ALJADIR, Taha

Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı

Tez Yöneticisi: Y. Doç Dr. Barbaros Preveze

Ağustos 2015, 96 sayfa

Bu tezde “GNS3” ve “VMWARE” kullanılarak iki farklı tipteki Uzaktan Erişimli Sanal Özel Ağ (PPTP ve SSL) bilgisayar ortamında sanal olarak kurulmuştur. Buna ek olarak, her bir protocol için, aynı koşullar altında farklı tiplerde güvenlik atakları uygulanmıştır. Her protokole uygulanan her atak türü için farklı araçlar kullanılmıştır. Bununla birlikte her bir VPN ağının farklı parçalarını hedef alan ataklar geliştirilerek, sonuçlar üzerinde dikkatli bir şekilde çalışılmış, ve daha sonra protokoller arasında test koşulları altında kıyaslama yapmak üzere etkin güvenlik analiz sonuçları elde edilmiş ve her bir protokolda kullanılmak üzere öneriler geliştirilmiştir.

Anahtar Kelimeler: Saldırı, VPN, güvenlik, PPTP, SSL.

ACKNOWLEDGEMENTS

First of all, I am thanking God for guiding me and helping me in all my life. Then I would like to express my sincere gratitude to assist. Prof. Dr. Barbaros PREVEZE for his supervision, special guidance, suggestions, and encouragement through the development of this thesis. A special thanks for my parents, words cannot express how grateful I am to my mother, and my father who tired a lot to make me what I am today. It is a pleasure to express my special thanks to my beloved wife for her valuable support and sacrifices, in addition to my brothers and sisters, and my friends who supported me and helped me to complete this work.

TABLE OF CONTENTS

STATEMENT OF NON PLAGIARISM.....	iii
ABSTRACT.....	iv
ÖZ.....	v
ACKNOWLEDGEMENTS.....	vi
TABLE OF CONTENTS.....	vii
LIST OF FIGURES.....	xi
LIST OF TABLES.....	xv
LIST OF ABBREVIATIONS.....	xvi

CHAPTERS:

1. INTRODUCTION.....	1
1.1 Background.....	1
1.2 Aim of the Work.....	3
1.3 Thesis Overview	4
2. VIRTUAL PRIVATE NETWORKS (VPN).....	5
2.1. What is a Virtual Private Network	5
2.2. Types of VPN.....	6
2.3. VPN Security.....	9
2.3.1. Cryptography	9
2.3.1.1. Encryption.....	9
2.3.1.2. Hashing or Message Digets	11
2.3.1.3. Digital Signature	12
2.3.1.4. The Digital Certificates	13
2.3.2. Authentication.....	13
2.3.3. Tunneling.....	13

2.4.	Summary and Notes.....	14
3.	VPN PROTOCOLS	15
3.1.	Jump Start	15
3.2.	IPsec Tunneling Protocol.....	15
3.2.1.	Encapsulating Security Payload	16
3.2.2.	Authentication Header	16
3.2.3.	IKE (Internet Key Exchange).....	17
3.3.	PPTP (Point To Point Tunneling Protocol).....	19
3.4.	L2TP (Layer 2 Tunneling Protocol).....	20
3.5.	SSL (Secure Socket Layer)/TLS (Transport Layer Security).....	20
3.6.	Summary and Notes.....	21
4.	SECURITY THREATS AND ATTACKS.....	22
4.1.	Overview	22
4.2.	DOS and DDOS Attack.....	22
4.3.	MITM (Man In The Middle) Attack.....	24
4.3.1.	Some MITM Attack Tools.....	25
4.4.	Access Attack (Password Recovery).....	26
4.5.	Encryption Defeating	27
4.5.1.	Defeating MS-CHAPv2 in PPTP.....	27
4.6.	SSL strip Attack.....	29
4.7.	Heart Bleed Attack.....	31
4.8.	Summary and Notes.....	31
5.	ESTABLISHING VPN NETWORKS USING VIRTUAL LAB.....	32
5.1.	Overview.....	32
5.2.	GNS3 And VMware.....	32
5.3.	Cisco ASA (Adaptive Security Appliance).....	33
5.4.	Initializing Work Environment.....	34
5.5.	Establishing PPTP VPN Network in Virtual lab.....	37
5.6.	Establishing an SSL VPN Network in Virtual lab.....	39

6.	APPLYING SECURITY ATTACKS AND GETTING THE RESULTS.....	42
6.1.	Applying DOS and DDOS Attacks.....	42
6.1.1.	Attacking PPTP VPN.....	42
6.1.1.1.	Attacking a PPTP VPN with Slowlori.....	42
6.1.1.2.	Attacking a PPTP VPN with Smurf6.....	44
6.1.1.3.	Attacking a PPTP VPN with LOIC.....	45
6.1.2.	Attacking SSL VPN.....	46
6.1.2.1	Attacking an SSL VPN with Slowloris.....	46
6.1.2.2.	Attacking an SSL VPN with Smurf6.....	48
6.1.2.3.	Attacking an SSL VPN with LOIC.....	50
6.2.	Applying MITM attack.....	51
6.2.1.	Applying MITM attack on PPTP VPN.....	51
6.2.1.1.	MITM attacking a PPTP VPN using ETTERCAP.....	52
6.2.1.2.	MITM attacking a PPTP VPN using Cain and Abel.....	54
6.2.1.3.	MITM attacking a PPTP VPN using Subterfuge.....	56
6.2.2.	Applying MITM attack on SSL VPN.....	57
6.2.2.1.	MITM attacking an SSL VPN using ETTERCAP.....	57
6.2.2.2.	MITM attacking an SSL VPN using Cain and Abel.....	58
6.2.2.3.	MITM attacking an SSL VPN using Subterfuge.....	59
6.3.	Attacking the Encryption.....	61
6.3.1.	Attacking PPTP VPN Encryption.....	61
6.3.1.1.	Dictionary Attacking PPTP to Obtain the Password.....	61
6.3.1.2.	Brute Force Attacking PPTP to Obtain the Password.....	62
6.3.2.	Attacking SSL VPN Encryption.....	63
6.3.2.1.	Attacking SSL VPN with SSLSTRIP.....	63
6.3.2.2.	Attacking SSL VPN with the HeartBleed Attack.....	66
7.	RESULTS, DISCUSSION AND COMPARISONS.....	67
7.1.	Overview.....	67
7.2.	Attacking VPN Protocols with a DOS Attack.....	67

7.2.1.	Attacking PPTP with DOS.....	67
7.2.2.	Attacking SSL with DOS.....	75
7.3.	Attacking VPN Protocols with MITM Attack.....	82
7.3.1.	Attacking PPTP with MITM.....	82
7.3.2.	Attacking SSL with MITM.....	83
7.4.	Attacking VPN Protocols Encryption.....	85
7.4.1.	Attacking PPTP VPN Encryption.....	85
7.4.2.	Attacking SSL VPN Encryption.....	86
7.5.	VPN Protocols Comparison (PPTP vs. SSL).....	86
8.	CONCLUSION, RECOMMENDATION AND FUTURE WORKS.....	93
8.1.	Conclusions.....	93
8.2.	Recommendations.....	95
8.3.	Future Works.....	96
	REFERENCES.....	R1
	APPENDICES.....	A1

LIST OF FIGURES

FIGURES

Figure 2.1	VPN Types	6
Figure 2.2	Intranet VPN	7
Figure 2.3	Extranet VPN	8
Figure 2.4	Remote Access VPN	8
Figure 2.5	Symmetric Encryption	10
Figure 2.6	Asymmetric Encryption	11
Figure 2.7	Message Digest	12
Figure 2.8	Digital signature	12
Figure 2.9	Digital Certificate	13
Figure 2.10	Tunneling Technology	14
Figure 3.1	ESP in Transport mode and Tunnel mode.....	16
Figure 3.2	AH in Transport mode and Tunnel mode	17
Figure 3.3	IKE phase 1.....	18
Figure 3.4	IKE phase 2.....	19
Figure 3.5	PPTP protocol packets	20
Figure 3.6	L2TP protocol packets	20
Figure 4.1	DDOS Attack	23
Figure 4.2	MITM Attack.....	25
Figure 4.3	Dictionary Attack flow chart.....	28
Figure 4.4	Brute Force Attack flow chart	29
Figure 4.5	SSL strip Attack	30
Figure 5.1	GNS3 with VMware	33
Figure 5.2	ASA and ASDM.....	34

FIGURES

Figure 5.3	Virtual Networks.....	35
Figure 5.4	The main Network diagram	36
Figure 5.5	PPTP VPN Network diagram.....	37
Figure 5.6	Users accounts and Network policy	38
Figure 5.7	DHCP Server and Windows Firewall.....	38
Figure 5.8	PPTP Client side connection.....	39
Figure 5.9	ASA Configuration for SSL.....	40
Figure 5.10	SSL Client side connection.....	41
Figure 6.1	DOS attack with Slowloris on PPTP.....	43
Figure 6.2	Client side under attack.....	43
Figure 6.3	Enhancing Slowloris DOS attack on PPTP.....	44
Figure 6.4	Smurf6 attack on PPTP.....	44
Figure 6.5	Enhanced Smurf6 DOS attack on PPTP.....	45
Figure 6.6	LOIC attack on PPTP.....	45
Figure 6.7	Effects of LOIC on VPN.....	46
Figure 6.8	Slowloris attack on SSL.....	47
Figure 6.9	Effects of Slowloris on SSL VPN.....	47
Figure 6.10	Enhanced Slowloris DOS attack on SSL.....	48
Figure 6.11	Smurf6 attack on SSL VPN.....	49
Figure 6.12	Enhanced Smurf6 DOS attack on SSL.....	50
Figure 6.13	LOIC attack on SSL VPN.....	50
Figure 6.14	Effects of LOIC attack on SSL.....	51
Figure 6.15	Applying MITM and waiting the VPN to be started.....	52
Figure 6.16	After PPTP client connected.....	53
Figure 6.17	Applying PPTP-Clear plug-in.....	53
Figure 6.18	Applying PPTP-chapms1 plug-in.....	54

FIGURES

Figure 6.19	Applying MITM on PPTP using Cain and Abel.....	55
Figure 6.20	Sniffing Korberos5 packets.....	56
Figure 6.21	Applying MIMT on PPTP with Subterfuge.....	56
Figure 6.22	MITM attacking SSL using Ettercap.....	58
Figure 6.23	MITM attacking SSL VPN using Cain and Abel.....	59
Figure 6.24	MITM attacking PPTP VPN using Subterfuge.....	60
Figure 6.25	Dictionary attacking PPTP VPN.....	62
Figure 6.26	Brute Force attacking PPTP.....	63
Figure 6.27	Attacking SSL VPN with SSLSTRIP and Ettercap.....	65
Figure 6.28	Attacking SSL VPN with Cain and Abel.....	65
Figure 6.29	Attacking SSL VPN with HeartBleed attack.....	66
Figure 7.1	Effects of attacking PPTP with Slowloris on connection time..	68
Figure 7.2	Effects of attacking PPTP with Smurf6 on connection time.....	69
Figure 7.3	Effects of attacking PPTP with LOIC on connection time.....	70
Figure 7.4	The effect of Slowloris on PPTP transfer rate through tunnel...	71
Figure 7.5	The effect of Smurf6 on PPTP transfer rate through tunnel.....	72
Figure 7.6	The effect of LOIC on PPTP transfer rate through tunnel.....	72
Figure 7.7	The effect of Slowloris on PPTP Round Trip Time.....	73
Figure 7.8	The effect of Smurf6 on PPTP Round Trip Time.....	73
Figure 7.9	The effect of LOIC on PPTP Round Trip Time	74
Figure 7.10	Effects of attacking SSL with Slowloris on connection time.....	75
Figure 7.11	Effects of attacking SSL with Smurf6 on connection time.....	76
Figure 7.12	Effects of attacking PPTP with LOIC on connection time.....	77
Figure 7.13	The effect of Slowloris on SSL transfer rate through tunnel....	78
Figure 7.14	The effect of Smurf6 on SSL transfer rate through tunnel.....	78
Figure 7.15	The effect of LOIC on SSL transfer rate through tunnel.....	79

FIGURES

Figure 7.16	The effect of Slowloris on SSL Round Trip Time.....	80
Figure 7.17	The effect of Smurf6 on SSL Round Trip Time.....	80
Figure 7.18	The effect of LOIC on SSL Round Trip Time.....	81
Figure 7.19	Effects of DOS using Slowloris on SSL and PPTP.....	88
Figure 7.20	Effects of DOS using Smurf6 on SSL and PPTP.....	89
Figure 7.21	Effects of DOS using LOIC on SSL and PPTP.....	89
Figure 7.22	Effects of Slowloris on transfer rate in SSL and PPTP.....	90
Figure 7.23	Effects of Smurf6 on transfer rate in SSL and PPTP.....	90
Figure 7.24	Effects of LOIC on transfer rate in SSL and PPTP.....	91
Figure 7.25	SSL VS. PPTP based on effect of Slowloris on RTT.....	91
Figure 7.26	SSL VS. PPTP based on effect of Smurf6 on RTT.....	92
Figure 7.27	SSL VS. PPTP based on effect of LOIC on RTT.....	92

LIST OF TABLES

TABLES

Table 5.1	Cisco ASA Configuration Table	35
Table 5.2	Cisco Router Configuration	36
Table 7.1	The Average Impact of DOS Attack on PPTP Connection Time.....	71
Table 7.2	The Average Impact of DOS Attack on PPTP VPN RTT.....	75
Table 7.3	The Average Impact of DOS Attack on SSL VPN	77
Table 7.4	The Average Impact of DOS Attack on SSL VPN RTT.....	81
Table 7.5	Attacking PPTP with MITM using Ettercap.....	82
Table 7.6	Attacking PPTP with MITM using Cain and Abel	83
Table 7.7	Attacking PPTP with MITM using Subterfuge.....	83
Table 7.8	Attacking SSL with MITM using Ettercap	84
Table 7.9	Attacking SSL with MITM using Cain and Abel.....	84
Table 7.10	Attacking SSL with MITM using Subterfuge	84
Table 7.11	Attacking PPTP VPN Encryption.....	85
Table 7.12	Attacking SSL VPN Encryption	86
Table 7.13	Average Vulnerability for Different Attacks on PPTP and SSL.....	87
Table 7.14	Average of DOS Attack Results for PPTP & SSL.....	87
Table 7.15	Average of MITM Attack Results for PPTP & SSL	88

LIST OF ABBREVIATIONS

AH	Authentication Header
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certificate Authority
DDOS	Distributed Denial Of Service
DES	Data Encryption Standard
DOS	Denial Of Service
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
L2Tp	Layer 2 Tunneling Protocol
MD5	Message Digest 5
MITM	Man In The Middle
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
PAP	Password Authentication protocol
PGP	Pretty Good Privacy
PPTP	Point To Point Tunneling Protocol
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm Version 1
SSL	Secure Socket Layer
TLS	Transport Layer Protocol
VPDN	Virtual Private Dial-up Network
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

1.1 Background

There is a clear division between public and private networks such that public networks are large collections of computers which are communicate with each other either freely or with some restrictions. Users who access public networks may or may not have commonalities, and each person on such networks may communicate with only a part of this network.

A private network is a group of computers owned by one foundation in which information is exchanged within the network only. They are the only computers that use this network and the information exchanged can be seen by computers of the same group (at worst). LAN and WAN are examples of private networks and public networks respectively [1]. To a limited extent, companies allow their branches or offices to acquire separate or isolated LANs where each office has a separate LAN, and each LAN may differ from another office's LAN in terms of protocol, domains and so on. For the most part, these LANs were incompatible with each other. These branch networks communicated with each other using leased lines (leased telephone lines), which ensured that connections were continuous and secure. However, this was very expensive, especially if a company has a branch office out of the country [2]. Private networks have another trouble with regard to handling travelling salespeople such that they needed to access company resources from time to time and were required to dial long distances, or even make international calls, which was extremely expensive [2]. It is no secret that the Internet has become the backbone for most fields of life starting with business, health, commerce and even governmental applications. Thus, the idea of virtual private networks started with the need for secure communications using low cost and available media.

There have been many developments on the Internet including QOS (Quality of Service), total performance, and low cost technologies such as DSL. However, the most important development was related to Virtual Private Networks [3]. Starting from here, VPN became one of the most attractive technologies of networking and communication, and was developed to cover the varying needs of secure communication. In parallel, security threats and attacks also developed and became more harmful and more powerful starting from stealing information or disturbing the users to the breakdown of an entire network [4]. Virtual Private Networks can be classified based on their architecture, such as Site-to-Site and Remote Access [1].

A scientific paper titled *Common VPN Security Flows* by Roy Hills mentions the security flaws which are, for the most part, unrelated to VPN protocol, such as misconfiguration, some manufacturing problems with Remote Access VPN, and a focus on IPsec protocol [5]. This was comprehensive and useful research; however, it did not cover other types of protocol which are variants commonly used worldwide, such as PPTP and SSL.

Debunking the Myths of SSL VPN Security is another study, written by Rainer Enders and Clint Stewart, which covers the SSL VPN protocol and some related issues that were most important and were not seen by many organizations or manufacturers [6]. This was a very strong and useful study based on the most famous references. However, again, it did not make comparisons with other protocols and only focused on one protocol.

The Master thesis for Koen Van Besien discussed establishing VPNs and their requirements. He presented a simple classification for VPNs and explained different protocols briefly and finally provided an example about building a VPN based on OPEN VPN [7]. He briefly discusses expected attacks, and did not make any comparisons that would help in detecting which protocol is better in a specific case and which in the other.

Martin Hack, EVP, NCP Engineering, in a scientific essay, discusses Remote Access challenges and a number of myths and incorrect ideas about using Remote Access VPN and its security [8]. Although it was a very nice work, it cannot be a reference alone unless it covers every other incorrect idea and user fault.

VPN Security is another published small study by the Special Administrative Region in Hong Kong [9], which aims to explain VPNs and their types with a brief demonstration of the threats that may face those VPNs. This was simple and good but did not provide a practical application to establish networks or apply the attacks.

On 29 January 2004, Steve Pitts submitted a study that explained the brute force attack on IPsec VPNs based on an aggressive mode pre-shared key [10]. He discussed practical applications for attacks on fixed IPsec-based VPNs. This was a very commendable work, but it did not make any comparisons with other protocols.

A good and new method has been covered by Kevin Benton and Ty Bross regarding timing analysis of SSL/TLS MITM attacks [11]. The work was very good and presented a new dimension to detecting security attacks depending on time analyses. Again, it covers one protocol with one attack.

Finally, the MITM attack was discussed clearly by Gopi Nath and Shefalika Ghosh [12], which were demonstrated with varying kinds of MITM attacks in a LAN. However, similarly to the others, it still focused on only one attack.

1.2 Aim of the work

Presented in this research is a study which aims to test the resistance of the two most commonly used protocols of VPN, namely PPTP and SSL, against the most famous and frequently used attacks. In addition, it aims to cover the points that other and past research has not covered, including testing more than one protocol, covering Remote Access as the most vulnerable protocol, establishing different kinds of Remote Access VPNs with different protocols and different appliances (Cisco ASA as hardware VPN gateway and Windows Server 2008 as Software VPN NAS), establishing networks and applying attacks in virtual environments using a single computer (which allows the researchers to work easily in their own virtual lab), using

emulation programs to connect network components to obtain more realistic results than simulations, such as (GNS3), making comparisons between two common VPN protocols from a security point of view, demonstrating the effects of each attack on each protocol separately and using different tools to apply each single attack (which gives more accuracy for results and wider covering for the most frequent attack). Finally, it aims to offer recommendations based on the results and comparisons that explain the best use for each protocol showing their respective weaknesses and strengths from a security point of view.

1.3 Thesis Overview

This thesis consists of eight chapters, the first of which is a brief description of Virtual Private Networks and how they developed, while the second chapter surveys the current Virtual Private Networks technologies and classifies them into two main types and then explains each type separately. Chapter 3 focuses on Virtual Private Network protocols and presents those most commonly used in the world.

Chapter 4 describes the security threats that face Virtual Private Networks in addition to demonstrating the most famous and most frequent attacks. Chapter 5 explains how to build a virtual lab and how to establish Virtual Private Networks using virtual machines and emulation programs. Applying attacks and obtaining the results are presented in Chapter 6, while result comparisons and discussion are presented in Chapter 7.

Finally, a conclusion, recommendations and future works are presented in Chapter 8.

CHAPTER 2

VIRTUAL PRIVATE NETWORKS

2.1 What is a Virtual Private Network?

A Virtual Private Network (VPN) simply refers to networks that are virtual (i.e., not real), but nevertheless do their job as one of the most widespread and most widely used types of network. Such networks use the Internet to connect between parties securely. They are designed to maintain privacy and security of information. The term VPN is also used to describe Frame Relay, ATM, MPLS and a number of other private networks. The main idea of VPN security is that any data transferred across such networks is protected by encryption and sent via the Internet to their destination, thereby keeping information free from tampering and/or manipulation. Moreover, they ensure that only the two authenticated users (sides) can access the data using authentication protocols. As Internet usage has grown, all businesses have come to use their own private networks, and due to the parallel growth of attacks on the Web, VPNs attract most of these businesses as a good solution to keep their networks safe [1], [3], [4]. A VPN transmits data based on tunneling, where packets are encapsulated in a new packet with new headers that provide routing information. They are then transmitted as new, normal Internet packets. The tunnel is the logical path through which packets travel after they are encapsulated. When encapsulated packets reach the end point of the tunnel, they are decapsulated and sent to their destinations. The two end points of the tunnel mostly support the same VPN protocols, otherwise VPN fails.

Tunneling protocols work in layer 2 or layer 3 of the OSI model depending on the protocol type. The most famous tunneling protocols are IPsec, L2TP, PPTP and SSL.

The packets with parameters that differ from Internet packets can be easily sent using VPN; therefore, it supports the idea of protocol forwarding through the Internet [9].

2.2 Types of VPN

VPNs can generally be classified into two types depending on their architectures, namely Site-To-Site and Remote Access VPN. Site-To-Site is used commonly to connect two branch offices of the same organization or two offices of different organizations. It consists of two main gateways at each side which respond to encapsulation-decapsulation of the packets. Remote Access is mostly used by employees to access the main office of their company or company resources remotely via the Internet [1].

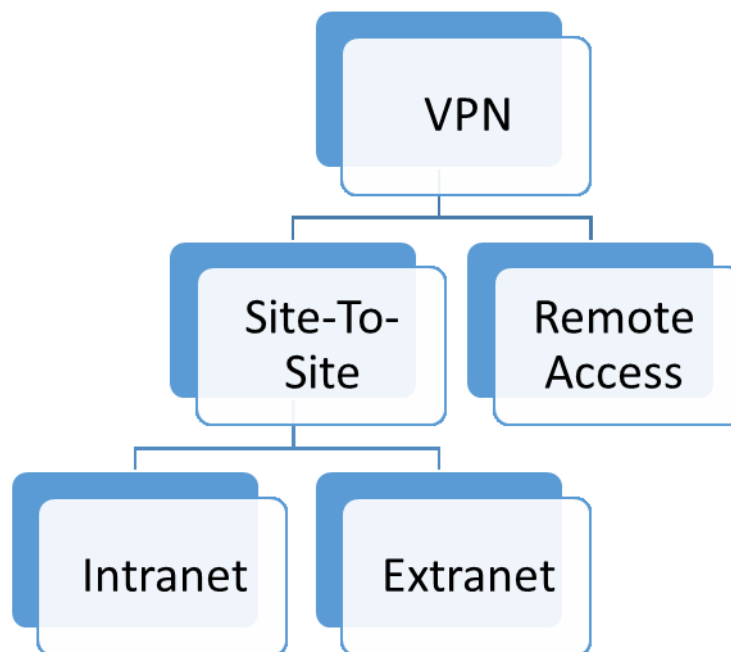


Figure 2.1 VPN Types

1. Site-To-Site VPN

As mentioned previously, Site-To-Site VPNs mainly have two common kinds of network architecture. One is used to connect different organizations, and the other is used to connect two different offices of the same organization. These are Intranets and Extranets:

- Intranet: Intranets are often used to connect company branch offices to headquarter offices or to remote employees in their homes. The cost of connection is expensive without the use the VPN; thus, companies have moved to use the Internet with a VPN.

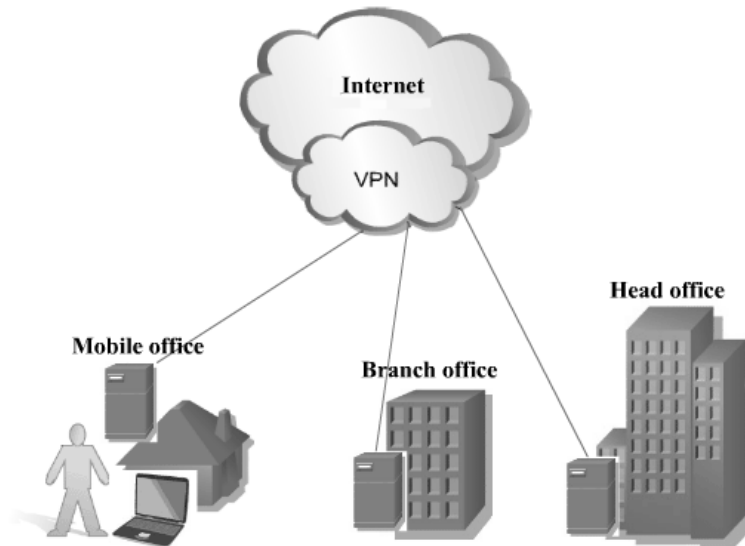


Figure 2.2 Intranet VPN ^[39]

Extranet: An extranet is used to connect the offices or LANs of cooperating companies that need to share information for secure communication or business purposes. An extranet has more limited access than an intranet.

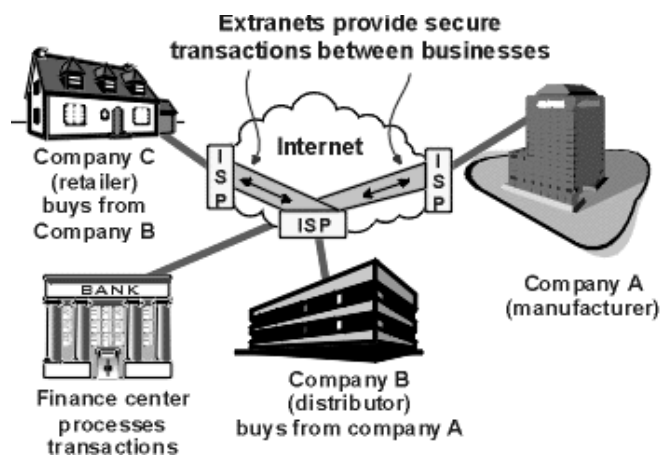


Figure 2.3 Extranet VPN ^[40]

2. Remote Access VPN

Also known as a Virtual Private Dial-up Network (VPDN), a Remote Access VPN connects a remote user to a LAN or site. It is mostly used by companies whose employees need to access the company's private network remotely. For example, a large firm with many salespeople needs to connect to the main LAN remotely for the salespeople to complete their tasks. The new application for this class of VPN is carried out using a mobile phone or tablet PC [1], [9].

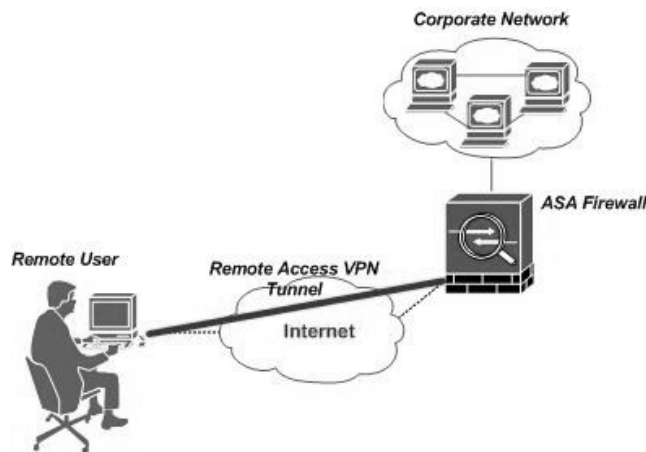


Figure 2.4 Remote Access VPN ^[41]

2.3 VPN Security

There are several requirements to acquire a secure network, and such requirements define how secure each network is depending on how many of them are available in addition to the level of each:

- **Confidentiality:** This refers to the privacy of the message so that nobody can read it except for the authorized two persons.
- **Integrity:** This is to ensure that a message is protected against manipulation or modification during transmission.
- **Authentication:** This is to ensure that the message is sent by the right person and is not tampered with by others (such as an attacker).

- **Availability:** This is to ensure that the path of a message is fixed and available from the sender until it is received.

VPN security depends on cryptography to provide data confidentiality packets that are sent through the network in an unreadable form. However, a header is added during encapsulation for routing purposes. Only the sender and receiver can read these packets. VPNs also provide data integrity using a message digest to protect data against modification. By default, a VPN provides strong user authentication using authentication protocols. Another important issue is that there is a reverse relation between security and performance on a VPN. More security means lower performance and vice versa since more security needs more computer and network resources and calculation processes [1], [7], [9].

2.3.1 Cryptography

2.3.1.1 Encryption

Encryption is the process of changing the form of the data to an unreadable form so that no one can read it except for the owner of the encryption key. The encryption concept is very old; it started as far back as 2000 years BC and was used in war, such as the (Caesar cipher). Later, a new encryption machine was released (Enigma machine). In the 1960s, IBM released (Lucifer) as a new developed encryption. In 1973, NIST (National Institute of Standards and Technology) created a new encryption method known as DES with one secret key for encryption and decryption and 56 bits. Later, RSA was developed by three academics. This system uses two keys, one of which is public and the other private. Decryption is the opposite process to change back the data into readable form using a suitable key and algorithm. Strong encryption is obtained with a strong algorithm and long encryption key.

- **Symmetric Encryption**

Known also as the secret key, this key is used for encryption and decryption. The two parties deal with the one shared secret key. An example of a symmetric encryption algorithm is DES. Another enhancement is added to this algorithm by using Triple DES or 3DES to increase the complexity of the encryption by applying DES three

times. The main drawback of this algorithm is exchanging the key through the Internet. Figure (2.5) explains the main idea of this type of encryption.

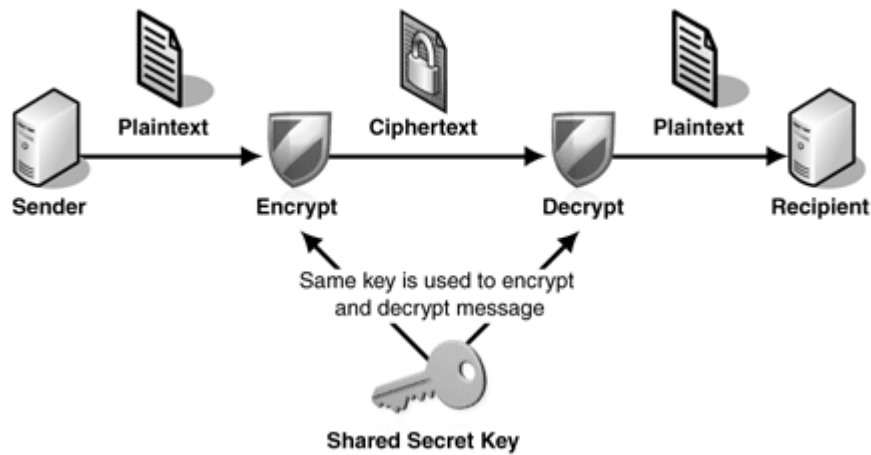


Figure 2.5 Symmetric encryption ^[42]

- **Asymmetric Encryption**

Two types of key are available in this method: one is called *public*, which can be used to encrypt data and can be available to the public since it cannot decrypt the data with which it is encrypted. The other type of key is called *private* and must be secret. The public key can decrypt data encrypted with the private key, but the private key cannot be derived from the public key. Data encrypted with the public key can only be decrypted using the private key. RSA is an example of an asymmetric encryption algorithm. It is stronger than DES and 3DES, but it is slower. A new method released recently, known as PGP, uses 128 bits and is a message digest. Figure (2.6) demonstrates the main concept of asymmetric encryption.

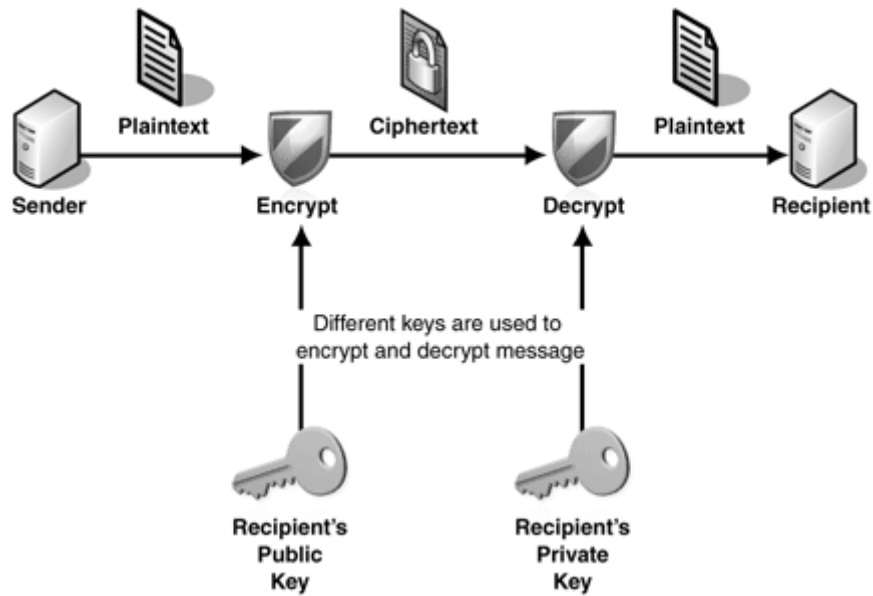


Figure 2.6 Asymmetric encryption ^[42]

2.3.1.2 Hashing or Message Digest

Hashing is the digital fingerprint of the message. It is a special algorithm to generate a fixed unique digest from the original message, no matter the size of the message. It cannot recover the original message and is used to check data integrity. Moreover, it can be used to check the original source of the message. MD5 and SHA-1 are examples of hashing algorithms.

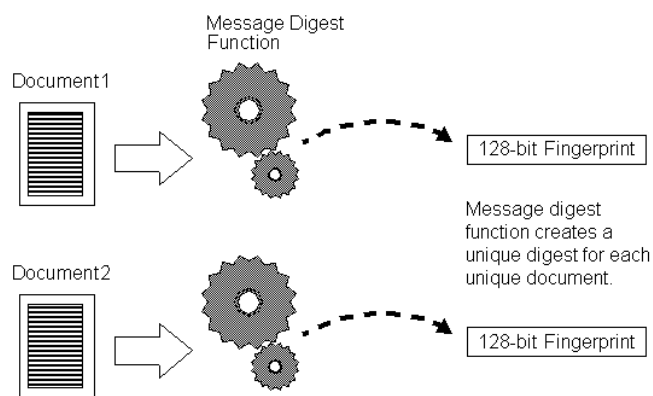


Figure 2.7 Message Digest ^[43]

2.3.1.3 Digital Signature

A digital signature used to ensure that this data is sent or received by the right person. It is carried out using one of the hashing algorithms. The first message digest creates it and then it is encrypted with a private key and sent in parallel with the message. The receiver can decrypt the digest that is encrypted by using a public key. Then the receiver calculates the digest for the message received using the same hashing algorithm. Finally, the receiver compares the new digest with the decrypted one; if they are identical, it means no modification has occurred during transmission [4], [7].

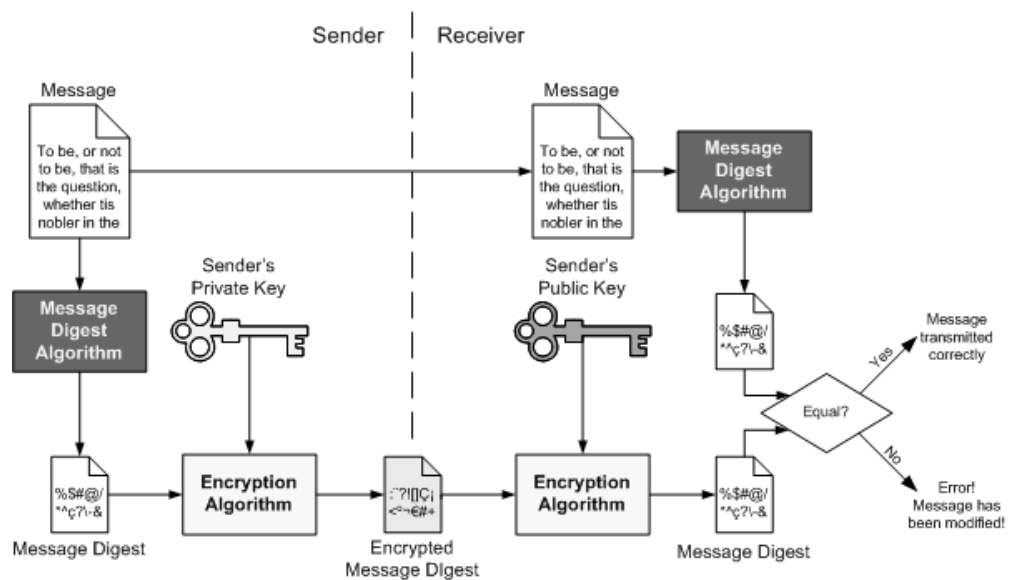


Figure 2.8 Digital Signature [44]

2.3.1.4 The Digital Certificates

The main drawback of the digital signature is that it cannot ensure that the public key has been received from the original sender. Moreover, it is not a hacker who puts himself in the middle and sends his public key and encrypts his digest generated after modifying the message. Certificates have come to solve this issue. A certificate is a message from a certified authority to prove that a key is the public key of the server [4]. The certificate authority (CA) is a well-known and trusted authority on the Web.



Figure 2.9 Digital certificate [45]

2.3.2 Authentication

Authentication is the approval of the origin of the message sent. It is carried out using a collection of encryption, hashing and digital signature techniques. The level of authentication depends on the complexity of an authentication algorithm which in turn depends on the security level of the message [4], [7].

2.3.3 Tunneling

The tunneling concept is based on forming a virtual network over a physical network. It encapsulates the packets and adds a new header containing routing information. In order to establish a tunnel, the two parties (sender and receiver) must use the same tunneling protocol. Tunneling protocols work on layer 3 or layer 2 in the OSI model. PPTP and IPSEC are examples of tunneling protocols as mentioned in Section 2.1.

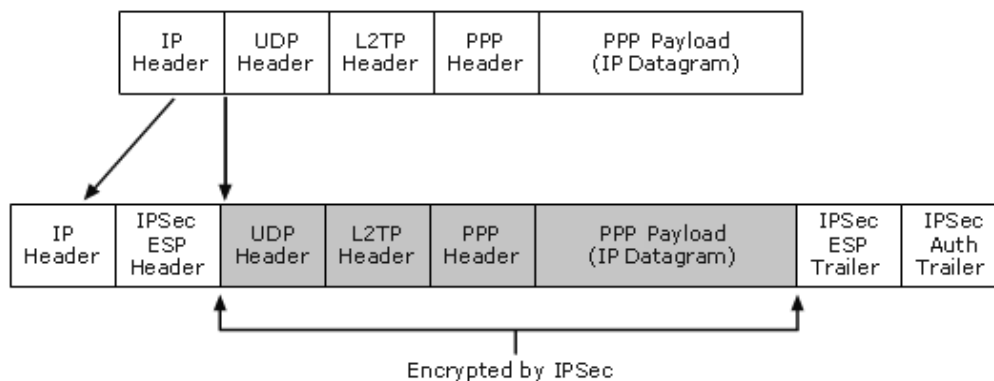


Figure 2.10 Tunneling Technology [46]

2.4 Summary and notes

A VPN is a group of computers owned by a single foundation. They can be classified into two kinds: Site-to-Site and Remote Access. Remote Access is more vulnerable to attacks [9]; therefore, it has been selected in this thesis to be the focus of the study. A VPN protects data using encryption, digital signatures, certificates and authentication algorithms.

CHAPTER 3

VPN PROTOCOLS

3.1 Jump Start

As mentioned in 2.3.3, Virtual Private Networks are based on a number of concepts, the most important being tunneling. To date, many tunneling protocols have been developed in various OSI layers. Each protocol is designed to work in specific parameters and in an OSI layer. For example, the IPsec protocol works based on layer 3 and has multiple sub-protocols such as DES for encryption, MD5 or SHA-1 for hashing, and so on. The most commonly used VPN protocols around the world are IPsec, PPTP, L2TP and SSL [2], [3].

3.2 IPsec Tunneling protocol

The Internet Security Protocol was designed by a group at the Internet Engineering Task Force (IETF). It was developed to support network security at the IP level. IPsec supports IPv4 and IPv6 and deals with three main areas: encryption, authentication and key management. IPsec is considered to be the most secure protocol available commercially [3] and works in two encryption modes: Tunnel mode and Transport mode. In Tunnel mode, it encrypts the whole IP packet (the header and the payload), while in Transport mode, only the data payload is encrypted. This protocol has three elements:

- ESP (Encapsulating Security Payload): This element provides confidentiality, authentication and integrity.
- AH (Authentication Header): provides authentication and integrity.

- IKE (Internet Key Exchange): provides key management and security association.

3.2.1 Encapsulating Security Payload

This element has been designed to keep data free from modification and/or tampering. It provides an adequate protection for message content. ESP supports the use of MD5 and SHA-1 hashing algorithms and IPsec uses a unique fingerprint for each packet, which allows the device to determine whether this packet has been modified. In addition, ESP is a response to all encryption services in IPsec, as referred to in 2.3.1.1. Encryption is to change the form of data into an unreadable form. ESP does not encrypt the ESP header or ESP authentication. Figure (3.1) demonstrates the ESP.

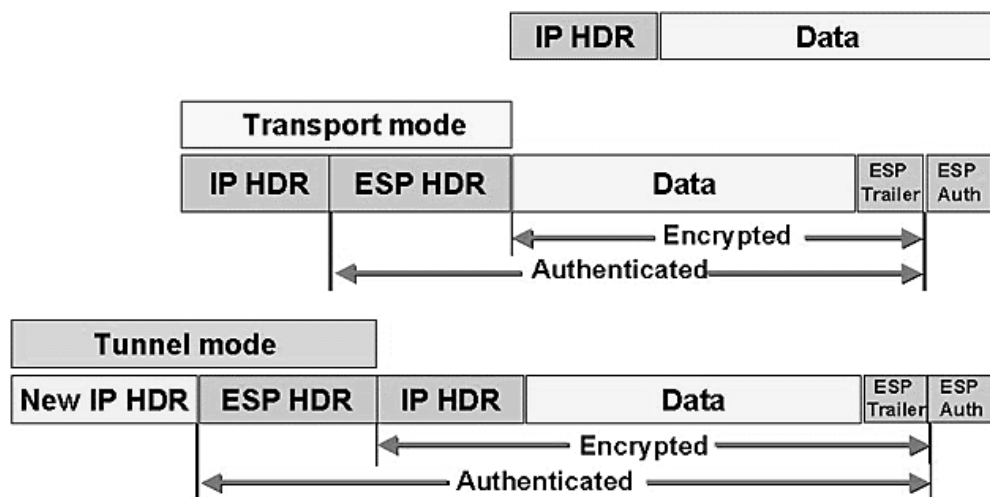


Figure 3.1 ESP in Transport mode and Tunnel mode ^[47]

3.2.2 Authentication Header

AH provides authentication and integrity to keep data safe from tampering by using the same algorithms as ESP. It also provides protection against a replay attack; however, this protection is optional (not mandatory), so here the payload is not involved in AH protection. Although AH protects the message's origin and contents, the identity is still known. Moreover, it does not provide confidentiality; therefore, if

packets are spoofed, the contents of the message are readable. To add more security, both ESP and AH can be used together [3].

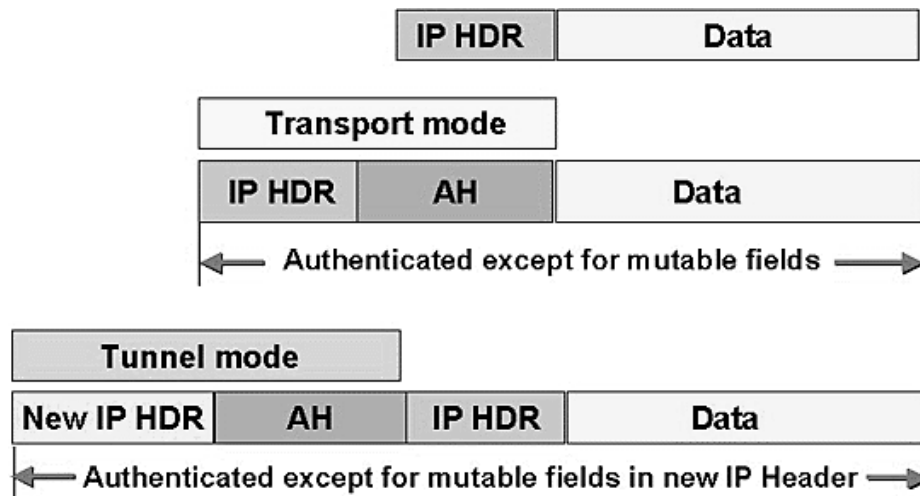


Figure 3.2 AH in Transport mode and Tunnel mode ^[47]

3.2.3 IKE (Internet Key Exchange)

The IKE protocol is used by IPsec to automate security sharing and the exchange of keys between the sender and receiver. IPsec needs keys to be refreshed or regenerated periodically to keep communication secure. IKE has the job such that the refresh rate can be controlled by the user, which improves the confidentiality of the communication. IKE has two phases of work.

IKE phase I:

- The two parties deal with the algorithms of encryption and authentication to be used in IKE.
- Each party authenticates the other using an authentication algorithm such as PSK (pre-shared key) or digital certificates.
- A shared secret key is generated using the Diffie-Hellman algorithm derived from the private key of one of the parties and the public of the other; the same occurs for the other party. This key will be used in the second IKE phase.

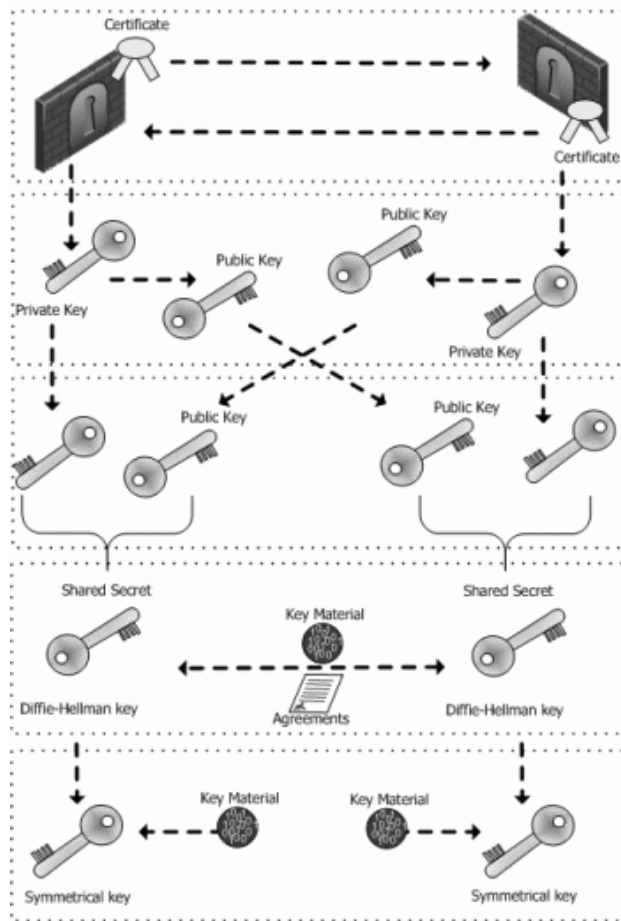


Figure 3.3 IKE phase 1 [48]

IKE phase II:

- The two parties in this phase deal with the encryption and authentication algorithms that will be used in the IPsec communication session.
- The IPsec key is derived from the shared secret key, which will be used to protect user data transmitted between the parties [3], [13].

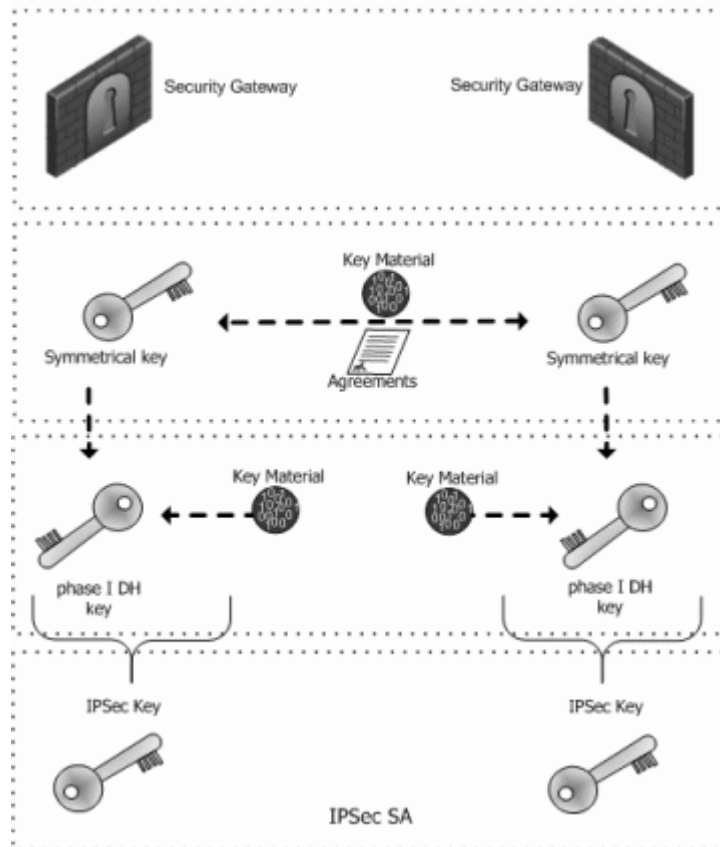


Figure 3.4 IKE phase 2 [48]

3.3 PPTP (Point To Point Tunneling Protocol)

The PPTP protocol is based on the standard PPP (Point To Point) protocol. The main tunneling service in this protocol rides on top of the IP, while the PPP underlies the IP. PPP is very suitable to apply to PPTP and all that it needs is the security that is provided by PPTP. It is mostly used as a host-to-host protocol, but it can also be used as a LAN-to-LAN [2]. Typically, PPTP encrypts packets and adds a new header using a modified version of GRE (Generic Routing Encapsulation). PPTP uses TCP port 1723, thus, its packets can pass through routers and firewalls. The Microsoft version of PPTP uses DES for encryption and this becomes vulnerable later by an attacker that can exploit this hole. This protocol makes it possible to route non-IP protocols through the Internet, such as AppleTalk, IPX and NetBIOS. PPP works on layer 2 in the OSI model and uses EAP (Extensible Authentication Protocol) MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) and PAP

(Password Authentication protocol) for encryption. PPTP is widely used and supported by most operating systems, which makes it famous [9].

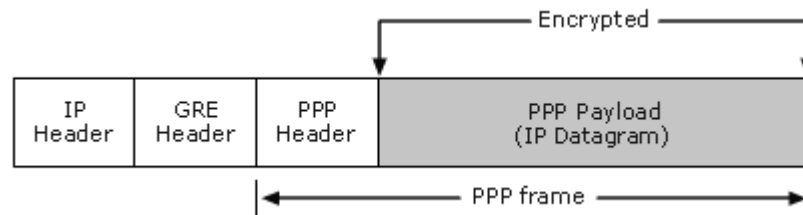


Figure 3.5 PPTP protocol packets ^[49]

3.4 L2TP (Layer 2 Tunneling Protocol)

This protocol is a combination of two protocols, namely Microsoft PPTP and Cisco L2F (Layer 2 Forwarding). It can be used with PPP as a tunneling protocol instead of GRE to make it sendable over IP, X.25, Frame Relay or ATM. L2TP is a layer 2 protocol and uses UDP port 1710. Moreover, the same encryption and authentication protocols are used in PPTP due to the lack of confidentiality of L2TP. It is often used with IPsec (L2TP/IPsec) [9].

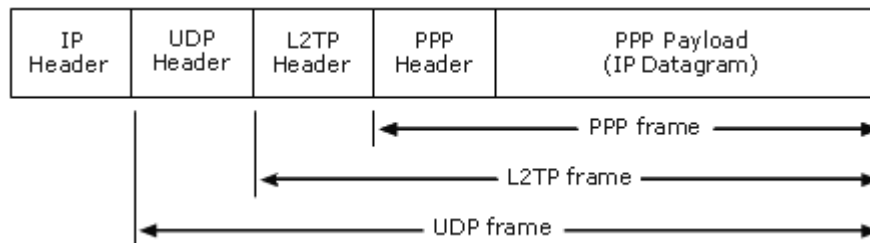


Figure 3.6 L2TP protocol packets ^[49]

3.5 SSL (Secure Socket Layer) / TLS (Transport Layer Security)

Secure Socket Layer (SSL) was developed by Netscape and IETF and later put under the name of TLS because it works in the Transport Layer in spite of the fact that there are some differences between SSLv3 and TLSv1. However, they are still

identical. SSL provides confidentiality, authentication and integrity at layer 4 using encryption, a digital signature and a certificate. It can provide security for any protocol with reliable connections such as TCP. SSL is used widely for secure HTTP connections on web (HTTPS) and it consists of three mechanisms or protocols:

- Handshake Protocol: each party has to authenticate himself to the other and mostly the server authenticates itself. During handshaking, parties negotiate the encryption algorithm. The handshake protocol uses symmetric encryption to protect data while asymmetric ones are used to negotiate the secret key.
- Record Protocol: after handshaking finishes and the shared secret key is generated, the parties deal with a data form and mostly a message digest that is used to insure data integrity, while symmetric encryption is used to encrypt the messages.
- Alert Protocol: if any party detects an error during transmission, it sends an alert containing the error. Three types of alert messages are available: warning, critical and fatal, and based on these messages, a session may be restricted or terminated [7].

3.6 Summary and notes

Different types of VPN protocols are available. IPsec, PPTP, L2TP and SSL are some of the most famous VPN protocols. A number of protocols encrypt data (payload) in packets only, while other types encrypt both the header and payload to provide more security for information. It is important to note that PPTP and SSL were chosen in this thesis to study as they are famous and widely used VPN protocols.

CHAPTER 4

SECURITY THREATS AND ATTACKS

4.1 Overview

The Internet is well known to be open to everybody. Both good and bad people are able to access it. For this reason, using the Internet as a communications medium has the drawback of being more vulnerable to security attacks. These attacks range from unauthorized access, eavesdropping, data tampering to even collapsing the network.

4.2 DOS and DDOS attacks:

DOS (Denial of Service) has been the most ever-growing attack on Internet services and is the most discussed in security and hacking forums. Hackers continue to develop DOS tools and techniques as this attack does not focus on data integrity or privacy. In fact, it focuses on service denial, so it does not need wide knowledge of target vulnerability. To increase the efficiency of a DOS attack, DDOS (distributed denial of service) was developed by applying DOS attacks by many attackers (zombies).

Various types of DOS and DDOS were developed to attack different network layers. Some of these attacks include:

1. IP (layer 3) DOS: which attacks network bandwidth.
2. TCP (layer 4) DOS: attacks a server's sockets.
3. HTTP (layer 7) DOS: attacks web server threads.
4. Web Application (layer 7) DOS: which attacks the CPU or resources.

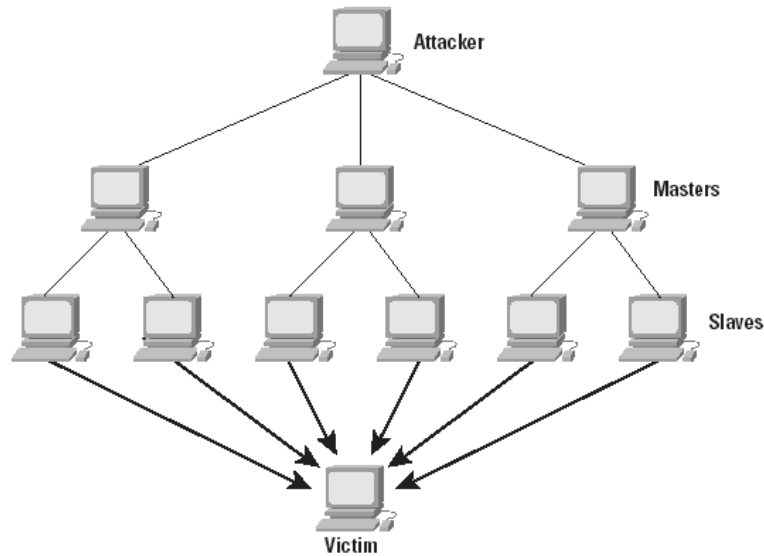


Figure 4.1 DDOS Attack ^[50]

The application layer DOS is a modern hacking technique which decreases the cost of an attack and becomes more efficient in order to avoid detection as most protection solutions focus on the lower layers. Some studies mention that DOS attacks are discussed at a rate of 22% on hacking forums, while SQL injection was discussed at a rate of only 19%. Some DOS and DDOS attack tools include:

- **Slowloris:** an open-source tool implementing an application layer DOS by draining the concurrent connection. It applies a low bandwidth attack by holding many connections open for a long time, thereby consuming resources.
- **LOIC:** Low Orbit Ion Canon is an open-source tool written in C#. It aims to attack the application layer.
- **Smurf6:** is an open-source tool which uses the POD (Ping of Death) methodology. It sends packets to networks using a broadcast address (misconfigured networks), thus the network will amplify an attack which is based on sending large ICMP packets (larger than 65500) with no acknowledgement of targeting the TCP protocol.

4.3 MITM (Man-In-The-Middle) Attack

The Man-In-The-Middle, or TCP hijacking, is one of the most famous security attacks used by attackers to sniff protocols or modify them or even insert other packets back into networks. The MITM attack is used mostly as preparation for other types of attack, such as Fishing and the SSL strip. The main idea of this attack is to put the attacker machine between the victim machine and the gateway (target machine). It mostly works on the LAN environment and it is strong enough to face VPNs and sniff secure information. Different types of MITM attack are available and can be classified based on spoofing methodology, including ARP spoofing, DNS spoofing and by using ICMP packets.

- ARP spoofing (ARP poisoning):

This type has been designed to work in LAN environments where data transfer is based on layer 2 (exactly on the MAC address). When packets are transferred across a network, it is necessary to convert the IP addresses to MAC addresses in order to complete data forwarding to their destination, the ARP (Address Resolution Protocol) which is the protocol in response to converting the IPs.

ARP spoofing is done by inserting fake information to the cache of the ARP protocol in the victims. Thus, it fools the victim that this MAC is for his gateway and does the same for the other party; however, it is in fact the MAC of the attacker machine, so the attacker creates two connections: one with the victim machine and the second is with the target. This is an MITM attack based on ARP poisoning.

- DNS spoofing (DNS poisoning):

This spoofing depends on the application of ARP spoofing, when the web browser requests the nearest DNS server in order to obtain the corresponding IP address for a web site name. The attacker fools the victim to think that it is the DNS server; however, in fact it is the attacker machine. The attacker sends a fake IP at the request of the victim.

For example, when the victim's browser makes a request to *google.com*, he receives a wrong IP or even an IP address of a fake page being used by the attacker for a FISHING attack.

- MITM through ICMP packets:

In this method, the attacker collects a sufficient number of MAC addresses from the network, including the MAC address of the gateway and the victim. Then he sends a ping (ICMP request) to the gateway using the IP address of the victim with its own MAC address and then does the same with the victim by sending a ping with the IP address of the gateway; thus, the ARP cache of the victim holds the MAC address of the attacker machine as the gateway MAC address and on the other side, the gateway ARP cache does the same by holding the attacker MAC address as the victim MAC address. Now all the traffic of the LAN from the victim will be sent to the attacker machine and then to the gateway, which can be easily sniffed.

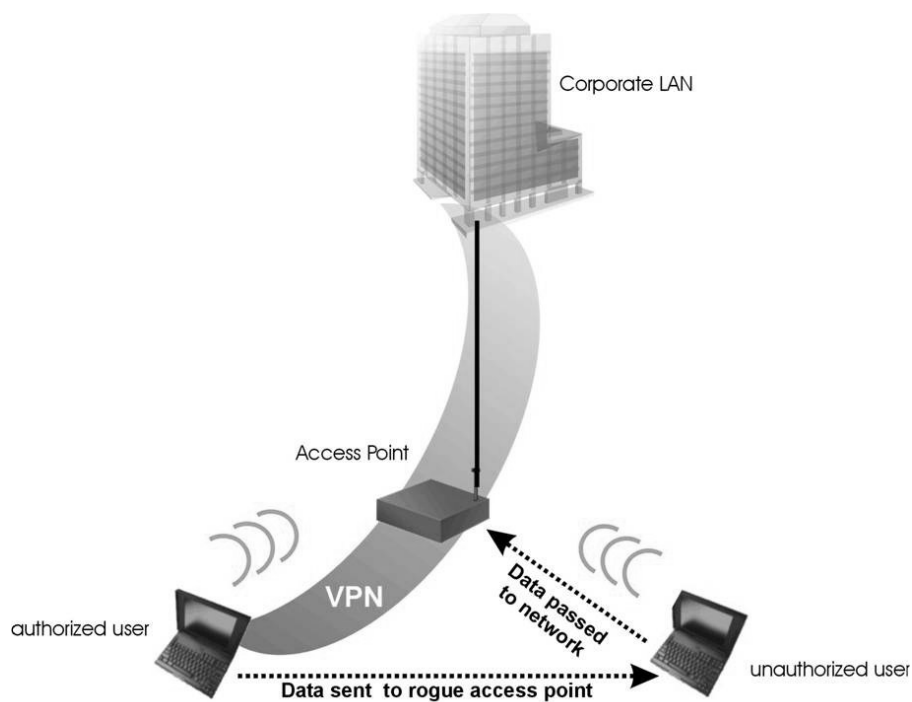


Figure 4.2 MITM Attack ^[51]

4.3.1 Some MITM attack tools:

- ETTERCAP:

These are some of the most famous and most powerful tools that are used to apply different types of MITM attack and penetration testing, and include open-source sniffers, interceptors and a logger for the LAN. They were developed to obtain a GUI version and they have different types of additions, known as plugins, which can be used to apply new attacks, including SSL strip, PPTP attacking plugins, and so on

- CAIN and ABEL:

This is a free tool used to crack passwords easily, for hashes and sniffing and which uses a dictionary and brute force attacking methodologies.

It has many functions for sniffing and applying MITM by ARP poisoning the network, dumping cached passwords, and so on.

- SUBTERFUGE:

This is a user-friendly, free, open-source tool. In fact, it is a framework where developers can add their new tools and test them using a subterfuge environment. Subterfuge attempts to use a paradigm popularized by Armitage, Fire sheep and other network security tools to construct a framework or environment for an MITM attack. It has a GUI that makes the work easier and more dynamic. For example, one can conduct a full network analysis with port scanning in one click.

4.4 Access Attack (Password recovery)

This attack is based on exploiting known vulnerabilities in authentication services so as to gain entry to VPNs, databases and other important information. It can be carried out using various methodologies such as the Brute force attack, the Dictionary attack and so on. In the Brute force attack, the attacker tool attempts every possibility for a password and user name. This attack can have a rate of success that exceeds 80 percent. However, it requires much time and a high-performance machine to be

carried out in addition to the drawback of a very long time when a password is too long or too complex. On the other hand, a dictionary attack is faster and based on lists of passwords collected to represent any possible password. The success of this attack depends on the list of passwords and attacker machine performance.

4.5 Encryption Defeating

This type of attack attacks the tunnel by attempting to decrypt (crack) any encrypted passwords. It can be applied using different methods, such as brute forcing and dictionary attacking the encrypted passwords sent through the tunnel. This type of attack depends on the protocol type and the vulnerabilities of that protocol. An example of this type of attack is the MS-CHAPv2 using the Chap2asleap script or Chapcrack that was released by Moxio Marlinspike on 29 July 2012 at the Defcon 20 conference. These two samples apply a dictionary attack and a brute force attack respectively.

4.5.1 Defeating MS-CHAPv2 in PPTP

- **Using the Dictionary attack:**

Firstly, it needs to acquire the challenge and response packets sent between a client and the NAS which contains the encrypted passwords. Hence, that user name is sent in clear text in PPTP. This can be carried out either by applying an MITM attack or by sniffing all of the traffic using Wireshark and then filtering the MS-CHAP packets. (Chapter 5 explains this in detail.) Secondly, by using the Chap2asleap script, the form of the challenge and response can be changed to be suitable as inputs for the (Asleap) dictionary attack tool. Finally, Asleap will apply a dictionary attack to guess the password. Figure (4.3) shows the flow chart of this attack.

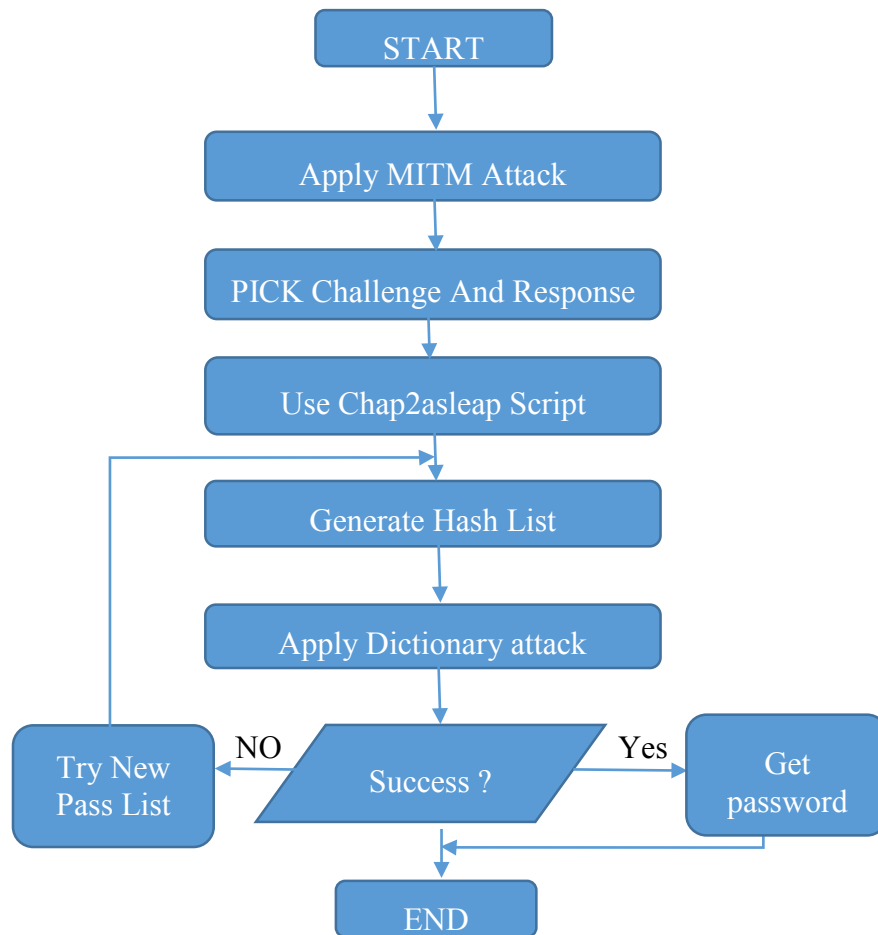


Figure 4.3 Dictionary attack flowchart

- **Using a Brute force attack**

This type of attack was released by Moxio Marlinspike on 29 July 2012 at the Defcon 20 conference. , It aims to simplify the 3DES encryption by removing the less useful parts that make it easy to decrypt. A simple tool known as Chapcrack was developed by Moxio to do this job. A later resulting hash will decrypt online using www.cloudcracker.com at a success rate of 100% and decryption time of maximum 24 hours. The following flow chart shows this method:

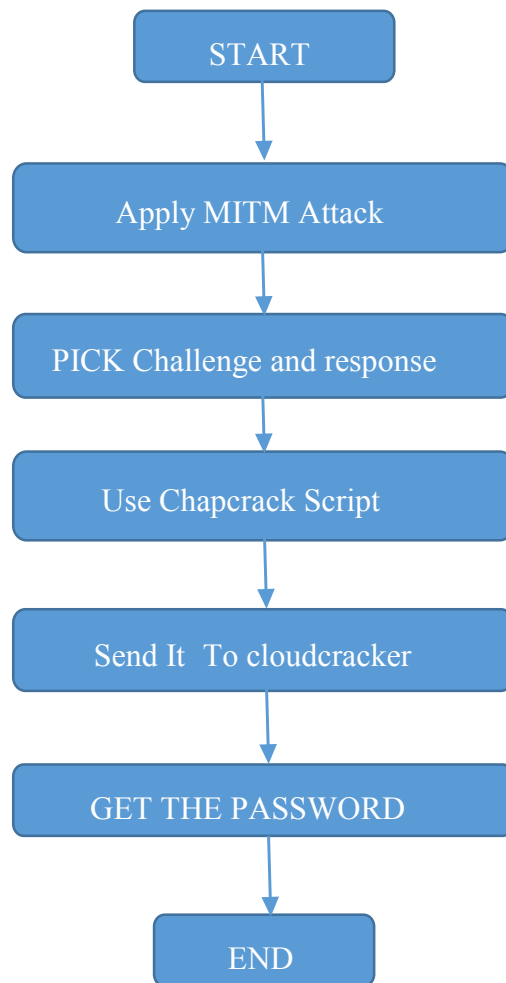


Figure 4.4 Brute force attack flow chart

4.6 SSL Strip attack

This attack is applied against HTTPS using an SSL stripping technique. First of all, it needs to apply an MITM attack to eavesdrop on the traffic. Secondly, packet forwarding needs to be carried out to complete the path of the tunnel. Finally, when the server responds to the request sent by the client, the SSL strip tool will change the HTTPS tunnel into normal HTTP and forward the packets to the client over HTTP, as shown in Figure (4.5). The SSL Strip attack has the following steps:

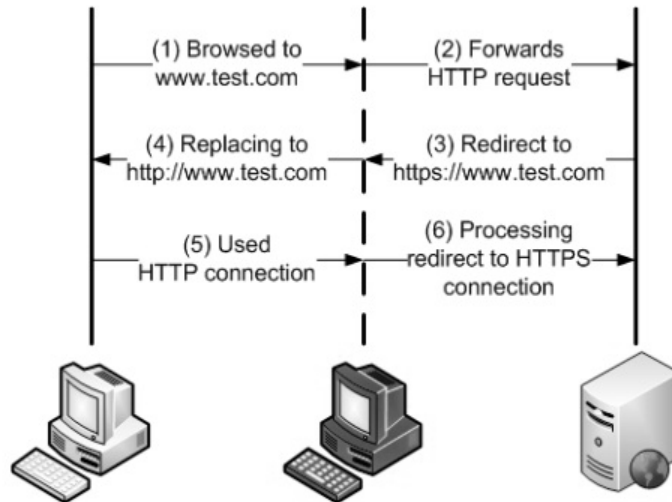


Figure 4.5 SSL Strip Attack ^[52]

- The attacker applies an MITM attack to be between the client and server.
- When the client requests the web page from server, the user usually types the URL directly without the HTTPS; for example, *www.test.com*.
- When request packets are sent to the server on an HTTP connection, the attacker forwards the first request to the web server.
- The server deals with the request and returns a redirection to an HTTPS connection.
- When the attacker in the middle receives response packets from the server, he replaces it with an HTTP connection; for example, *https://www.test.com* is replaced with *http://www.test.com* and sent to the victim.
- In the victim's browser, the HTTP is shown and all connections will be in clear text while the user does not notice.
- After the packets arrive at the attacker machine, he eavesdrops on the information easily as it is in clear text and then encrypts it and sends it back to the web server in the HTTPS connection.

4.7 Heart Bleed attack

The heart bleed bug was first discovered by Matti, Antti, Riku and Neel Metha. This threat enabled the attackers to sniff a large amount of important and secure information, including passwords, accounts and so on. The main problem was in the Open SSL library and this attack drops the information from the recent memory of the SSL server. Such a situation may actually be worse than expected as the heart bleed may leak all that secret information to the client side, and vice versa. This attack was discovered in version 1.0.1 of Open SSL and there are many web sites still infected with this bug to the present day [17].

4.8 Summary and notes

Different types of attacks can be applied to VPNs, ranging from slowing down a network to sniffing secret information and even service denial. DOS, MITM and Cryptanalysis are some of the more famous attacks against networks, especially against VPNs. For this reason, they are selected here. Some attacks may fail, implying that such protocols are immune to these types of attack.

CHAPTER 5

Establishing VPNs Using Virtual Lab

5.1 Overview

This thesis aims to test the two famous protocols (PPTP and SSL) in a virtual environment, as referred to in Section 1.2. The virtual lab here is built using the networks emulator GNS3 as it yields more realistic results and is a better working environment than a simulation. Moreover, this tool is widely used by the CCIE students. The second element is VMware Workstation, which is a virtual machine program that can be used to virtualize PCs. This tool is also trusted and widely used. The following sections explain in further detail how a virtual lab is built.

5.2 GNS3 and VMware

GNS3 is a network simulator that works graphically and has the ability to run multiple emulated systems such as Cisco routers, Vyatta routers in addition to host machines such as Linux virtual machines and Windows virtual machines. It is not always an easy task to do these simulations when one has GNS, especially if one wants to carry out some advanced or complicated networking. [15]. GNS3 has the ability to accept real router image files, which makes working on this tool more realistic. In addition, it can connect an emulated network and routers to virtual machines that can be built with VMware or Virtual Box. Moreover, VMware has the ability to virtualize PCs with real operating systems such as Linux, Windows and Mac OS; thus, we can build our virtual lab by connecting VMware machines with Cisco routers and network devices in GNS3. The following figure shows an example of using a virtual lab built with GNS3 and VMware:

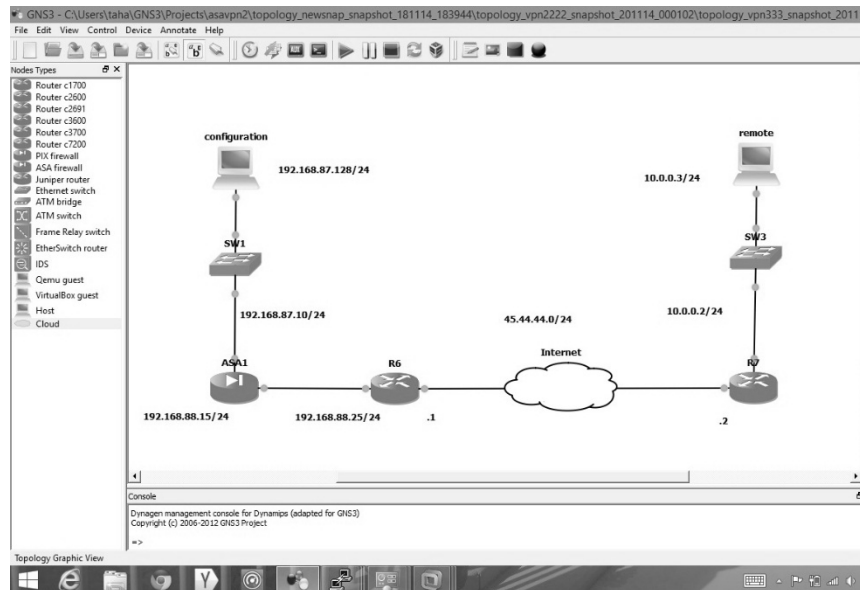


Figure 5.1 GNS3 with VMware

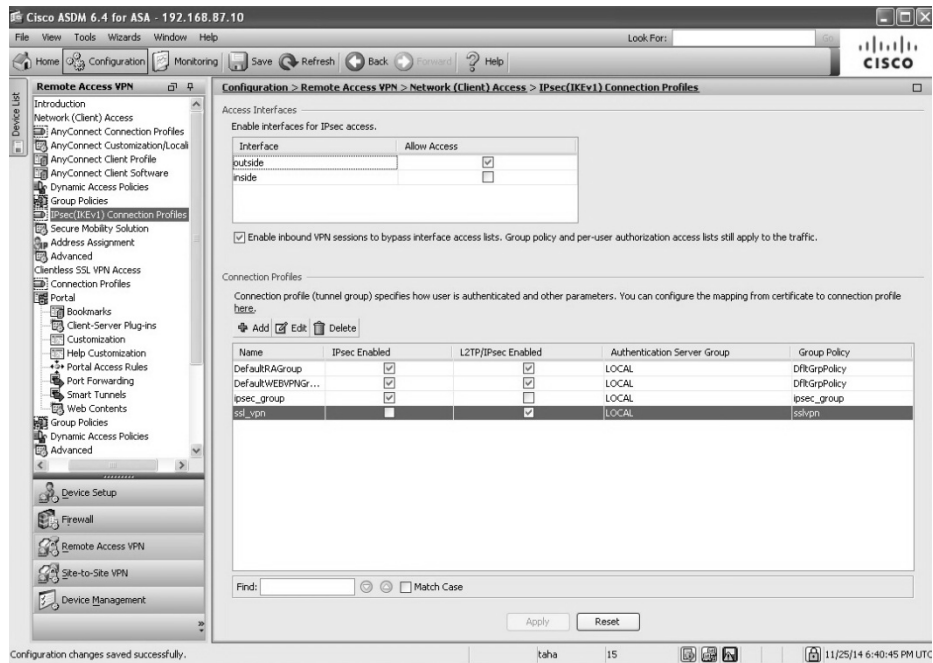
Here the client and remote PCs represent a Virtual machine, and it can be seen that they are connected to emulate a network represented with Cisco routers and a Cisco ASA VPN device. All in all, it represents a virtual lab with more realistic results. However, it needs more computer resources. The host computer used in this thesis has 4 GB of RAM and a Core i5 CPU, with the Windows operating system.

5.3 Cisco ASA (Adaptive Security Appliance)

This is a hardware solution from Cisco and is a firewall with many capabilities such as Route, IDS/IP, and VPN gateway, ASA supports IPsec and SSL for Site To Site and Remote Access VPN. It provides an easy way to establish, monitor and control VPNs using ASDM scripts which can be uploaded to the ASA from an FTP server and then installed using a line command. Figure (5.2) shows the ASA device and ASDM.



(A) Cisco ASA



(B) ASDM

Figure 5.2 ASA and ASDM

5.4 Initializing Work Environment

First of all, GNS3 and VMware are installed and later new virtual network adapters are established with VMware that will represent the different networks in a virtual environment. In this thesis, networks are initialized as follows:

Network 1	192.168.87.0/24	Vmnet1
Network 2	192.168.247.0/24	Vmnet2
Network 3	10.0.0.0 /24	Vmnet3

The following figure shows this clearly:

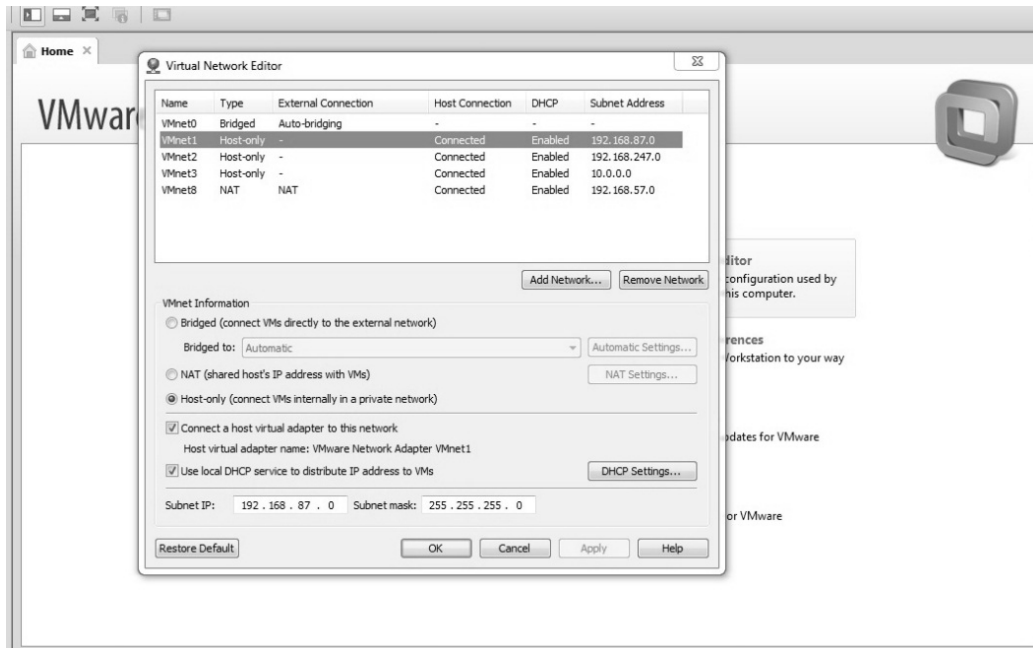


Figure 5.3: Virtual Networks

In addition, the Cisco ASA 5520 and Cisco 2700 routers are initialized with real images in GNS3 and are prepared to work typically. For example, the Cisco ASA is programmed and has its own inside and outside networks as follows:

Network	Name	Privilege	IP address
Inside Network	Inside	100	192.168.87.10/24
Outside Network	Outside	0	192.168.247.15/24

Table 5.1 Cisco ASA Configuration Table

While two Cisco routers are used to simulate the Internet as simply as possible, the following configurations are obtained:

Router	F1/0	F1/1	Routing Protocol
R1	192.168.247.10/24	40.40.40.1/24	Dynamic RIP
R2	40.40.40.2/24	10.0.0.2/24	Dynamic RIP

Table 5.2 Cisco Router Configuration

The following figure shows the main network diagram and the routers' IP addresses with connections:

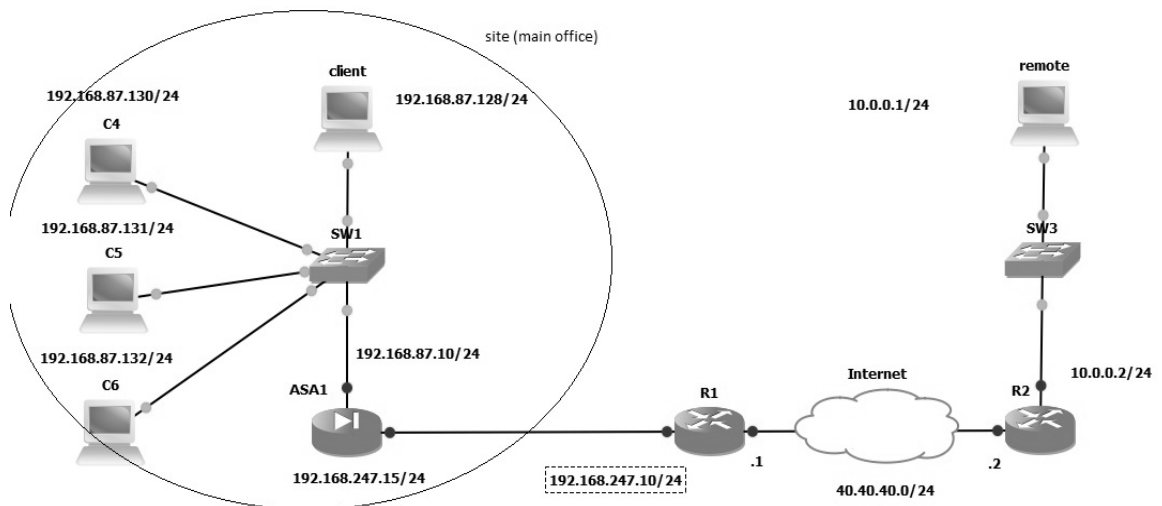


Figure 5.4 The Main Network Diagram

Here, the Cisco ASA is used as a VPN hardware gateway and a router to establish an SSL VPN network, while a Windows 2008 Server virtual PC is used instead for the PPTP VPN establishment. Further details can be found in Section 5.5.

5.5 Establishing PPTP VPN in Virtual Lab

This section explains the procedures to establish a PPTP VPN based on Windows 2008 Server as software, VPN NAS (Network Access Server) in a virtual environment using GNS3 as a network emulator and VMware as a virtual machine-creating tool.

Of note is the fact that the host PC has a Windows 7 environment and 4 GB of RAM as mentioned previously. The following figure shows the main diagram of the network.

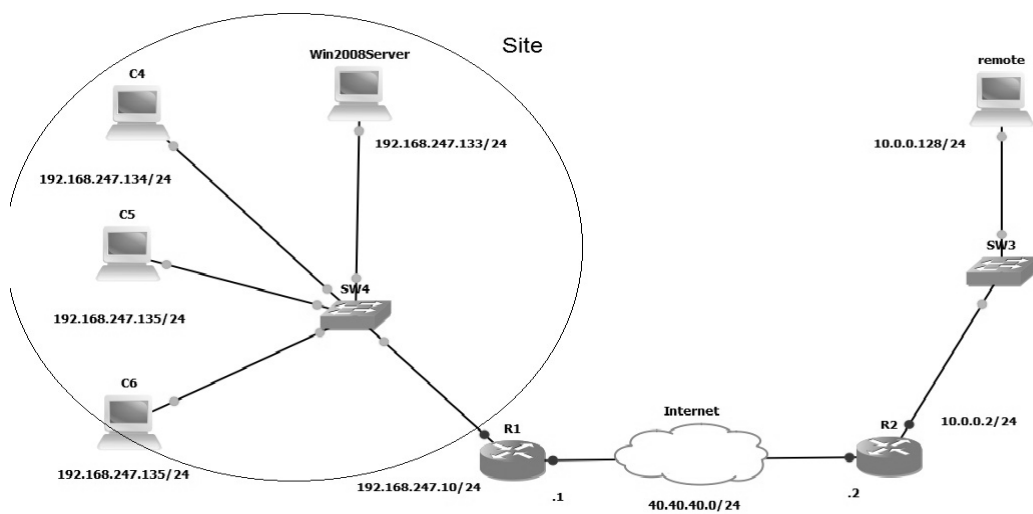


Figure 5.5 PPTP VPN network diagram

The procedures of establishing the network from the NAS side are as follows:

- Creating users' accounts with user names and passwords for each and enabling remote access.
- Configuring routing and remote access to accept connections from outside.
- Configuring new network policies to give access permissions to users from outside.

- Configuring a DHCP server to provide suitable IP addresses following connection.
- Configuring the Windows firewall to allow VPN requests.

The following figures show some of these configurations:

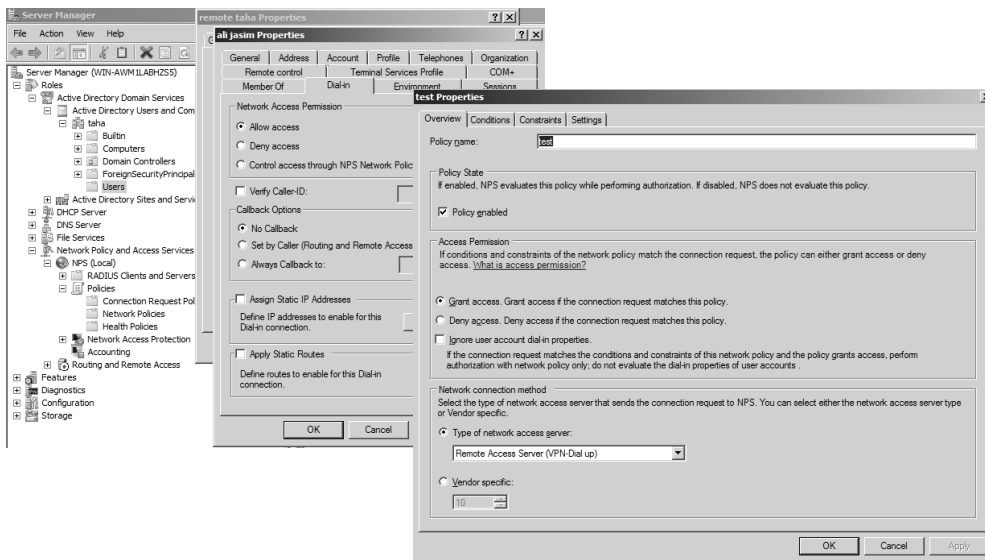


Figure 5.6 Users accounts and Network Policy

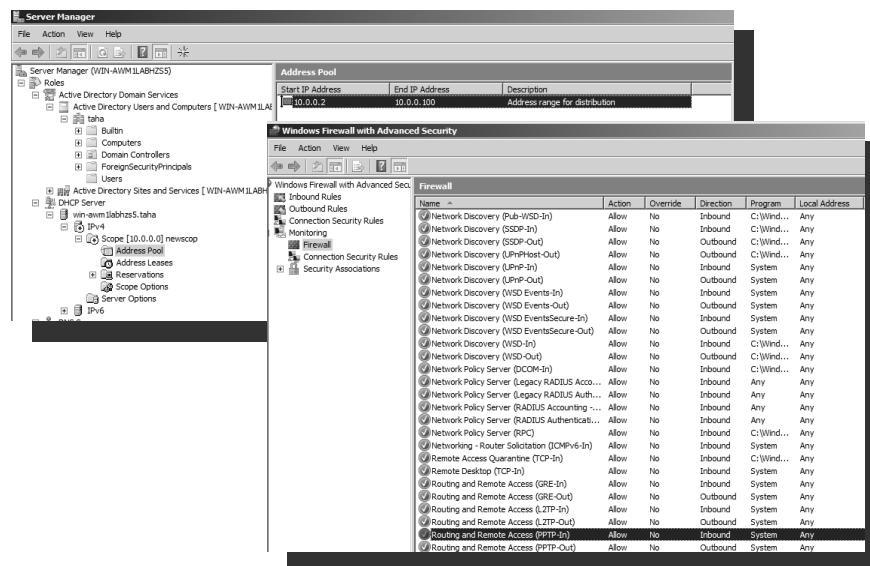


Figure 5.7 DHCP server and Windows Firewall

On the remote client side, a simple configuration has been carried out by creating new connections and selecting VPN and dialup connection, followed by giving a connection name and the server (NAS) IP address. When the user wants to connect, he only needs to enter the username and password. The following figure shows a simple explanation:

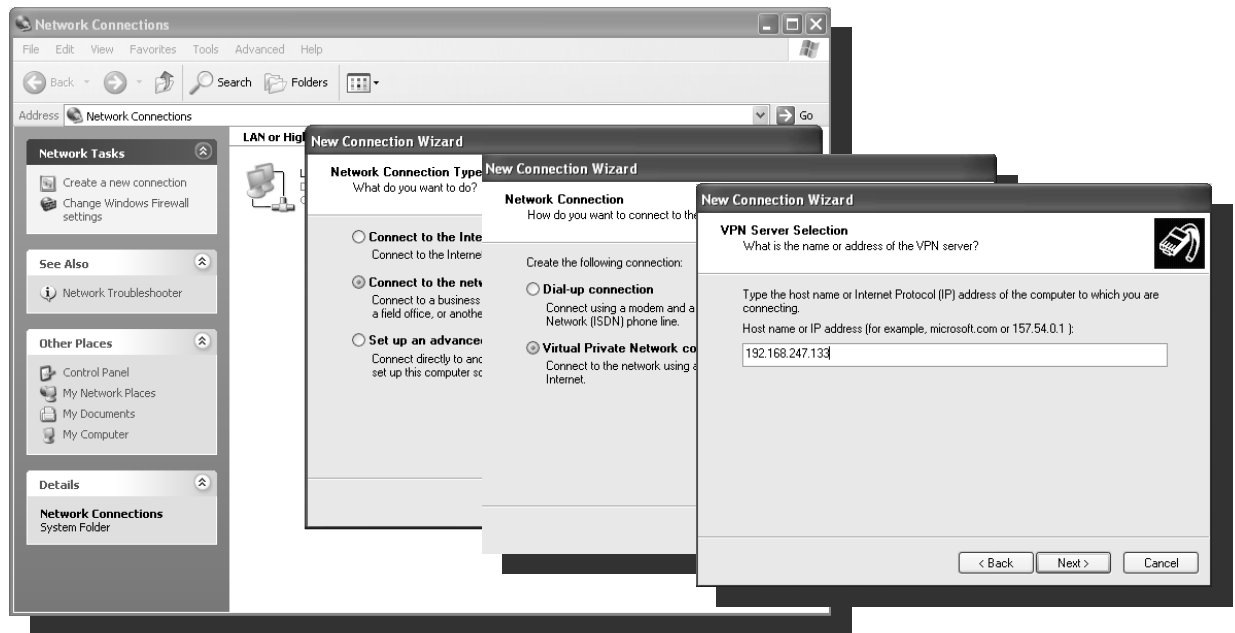


Figure 5.8 PPTP Client side connection

5.6 Establishing an SSL VPN in Virtual Lab

This section explains the procedures for establishing an SSL VPN based on Cisco ASA as a hardware VPN gateway in a virtual environment using GNS3 as a network emulator and VMware as a virtual machine virtualized tool. Of note is the fact that the host PC has Windows 7 environment and 4 GB of RAM as mentioned before. The ASA image is for an ASA 5520 device. Figure (5.4) in Section 5.4 shows the main diagram of this network. The procedures for establishing a network from the Cisco ASA side using an ASDM GUI are as follows:

- To specify the authentication method, ASA provides two methods, one of which uses an AAA server and the other using the local user database where new user accounts are created; here the second method is used.

- To specify the SSL connection interface, here the outside is selected and given a connection profile name.
- The group policy for user accounts are defined or a new group policy is created.
- To define device certificates if certificates are used for authentication, here a PSK (pre-shared key) used.

The following figures show some of these configurations:

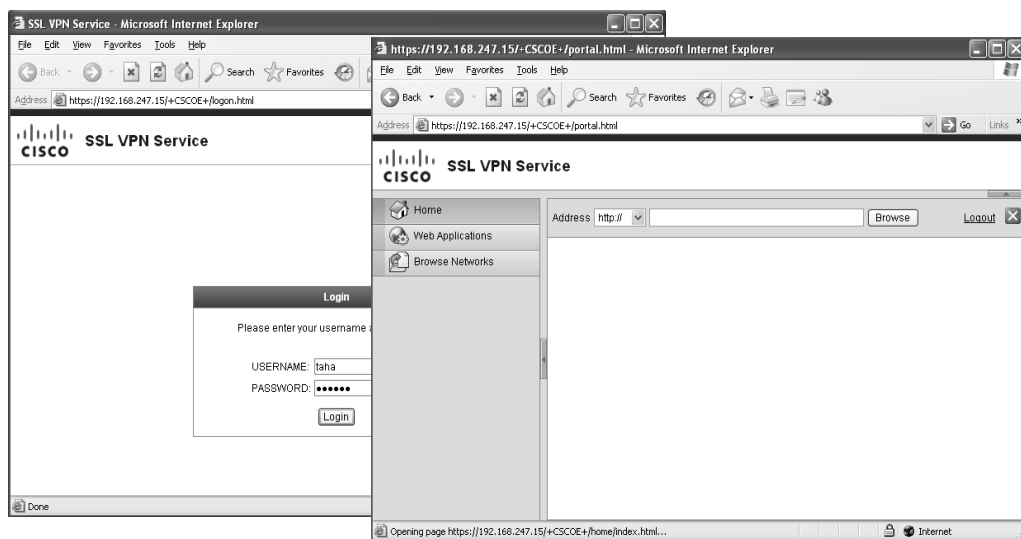


Figure 5.9 ASA configuration for SSL

On the remote client side, a simple web browser can be used for the connection with ASA SSL by writing the IP address of the ASA outside the interface, and then entering the user name and the password for authorized users, as shown in the following figure.

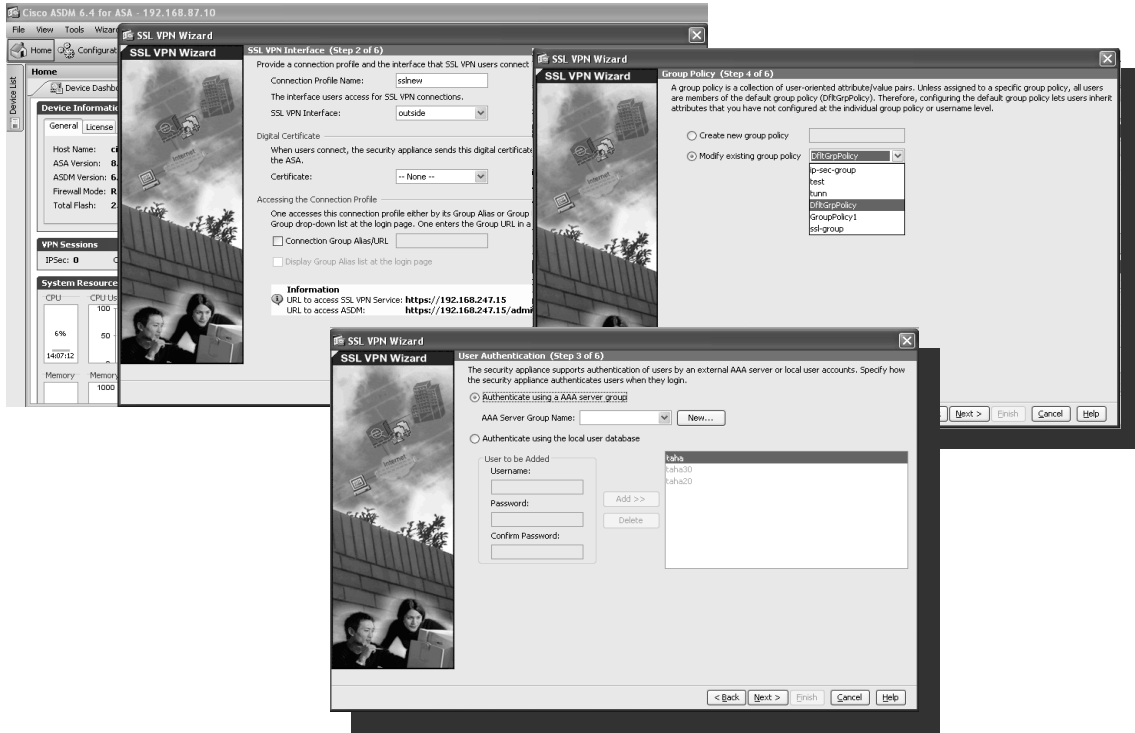


Figure 5.10 SSL Client Side Connection

CHAPTER 6

Applying Security Attacks and Getting the Results

6.1 Applying DOS and DDOS Attacks

6.1.1 Attacking PPTP VPN

As mentioned previously in this thesis, PPTP VPN was implemented using Windows Server 2008 as an NAS (VPN gateway), and Windows XP client as a remote user. Here, the hacker machine was Backtrack5 Linux or Windows XP.

6.1.1.1 Attacking a PPTP VPN with Slowloris:

In this attack, the hacker machine was Backtrack5 Linux. Starting the attack was carried out by an open console terminal and the following command was written:

```
Perl ./slowloris.pl -dns 192.168.247.132 -port 1723 -timeout 1 -num 1000 -cache
```

It can be seen that 192.168.247.132 is the IP address of Windows Server 2008 and 1723 is the open port for the PPTP protocol. The time-out is the time between sending a packet, while *num* is the number of packets in each transmission. Further details are found in Figure (6.1).

```

Desktop : bash
File Edit View Bookmarks Settings Help
root@bt:~# cd Desktop
root@bt:~/Desktop# chmod +x slowloris.pl
No command 'chmod' found, did you mean:
  Command 'chmod' from package 'coreutils' (main)
chmod: command not found
root@bt:~/Desktop# chmod +x slowloris.pl
root@bt:~/Desktop# perl ./slowloris.pl -dns 192.168.247.132 -port 1723 -timeout 1 -num 1000 -cache
Desktop : perl
File Edit View Bookmarks Settings Help
Building sockets.
Sending data.
Install
BackTrack Sending data.
Current stats: Slowloris has now sent 157885 packets successfully.
This thread now sleeping for 1 seconds...
Sending data.
Current stats: Slowloris has now sent 157985 packets successfully.
This thread now sleeping for 1 seconds...
test
Current stats: Slowloris has now sent 157935 packets successfully.
This thread now sleeping for 1 seconds...

```

Figure 6.1 Dos attack with Slowloris on PPTP

After a number of minutes, the client cannot connect to the server using a PPTP connection. A slow connection may be reached as shown in Figure (6.2).

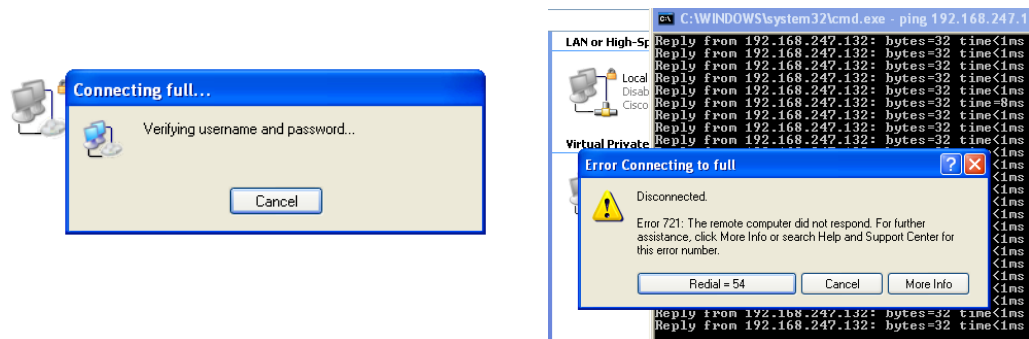


Figure 6.2 Client side under attack

The DOS attack has been improved by opening more terminals and applying Slowloris in each terminal to simulate DOS Slowloris and obtain better results, as shown in Figure (6.3).

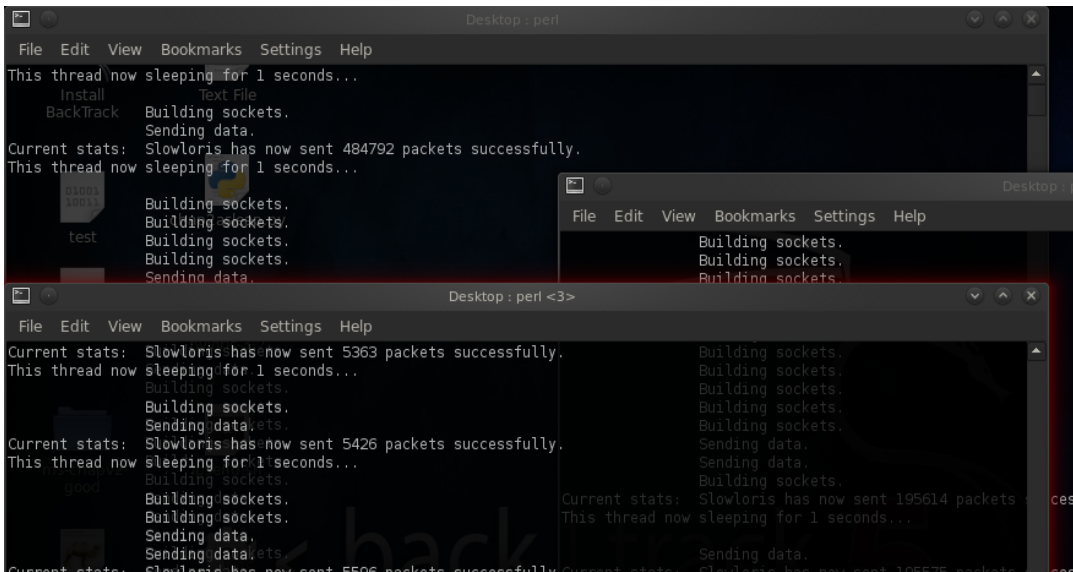


Figure 6.3 Enhancing Slowloris Dos attack on PPTP

6.1.1.2 Attacking PPTP VPN with Smurf6:

In this attack, the Hacker machine was Backtrack5 Linux. Starting the attack was carried out by open console terminal and the following command was written:

```
Smurf6 eth0 192.168.247.132
```

It can be seen that 192.168.247.132 is the IP address of Windows Server 2008 and *eth0* is the network interface of the Linux machine. Further details can be seen in Figure (6.4).

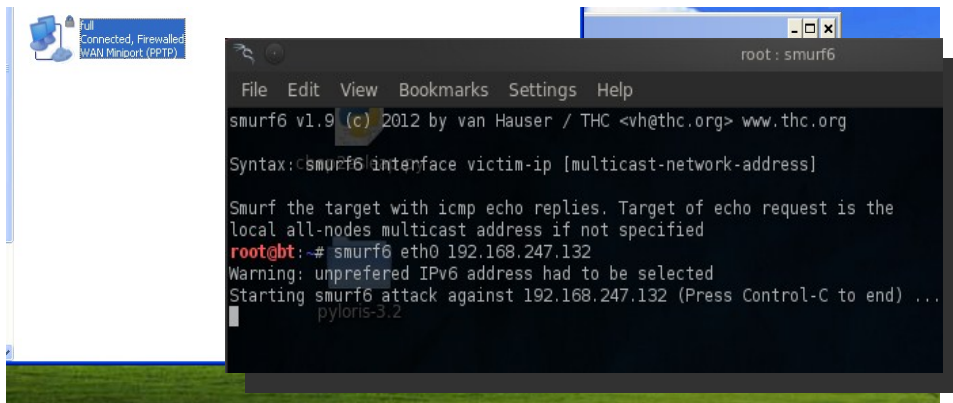


Figure 6.4 Smurf6 attack on PPTP

It can be seen that the client can still connect, but with a slow connection. The DOS attack has been improved by opening more terminals and applying Smurf6 to each one to simulate DOS Smurf6 and obtain better results, as shown in Figure (6.5).

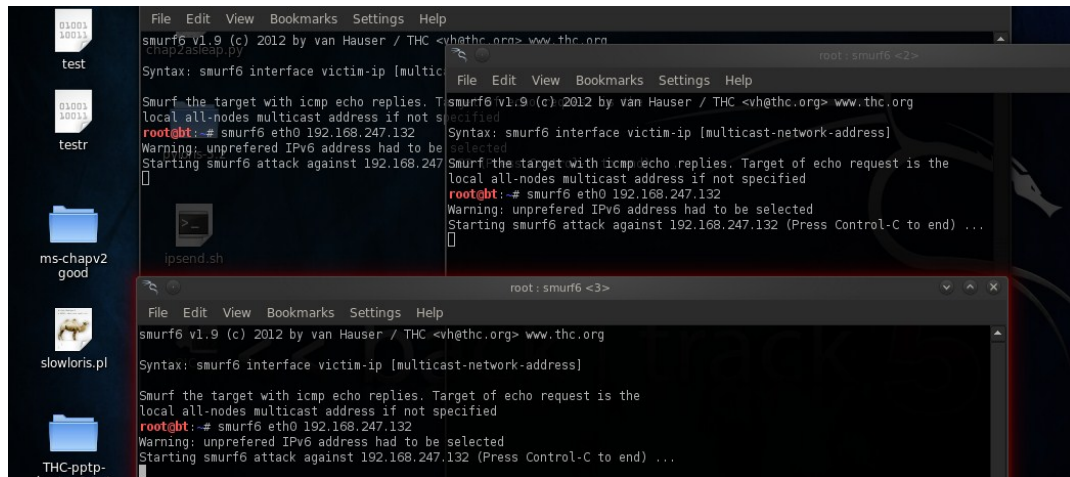


Figure 6.5 Enhanced Smurf6 Dos attack on PPTP

6.1.1.3 Attacking a PPTP VPN with LOIC:

In this attack, the hacker machine is Windows. Starting the attack was carried out by opening GUI tool and entering the target IP address and open service port with some configurable options, as shown in Figure (6.6).

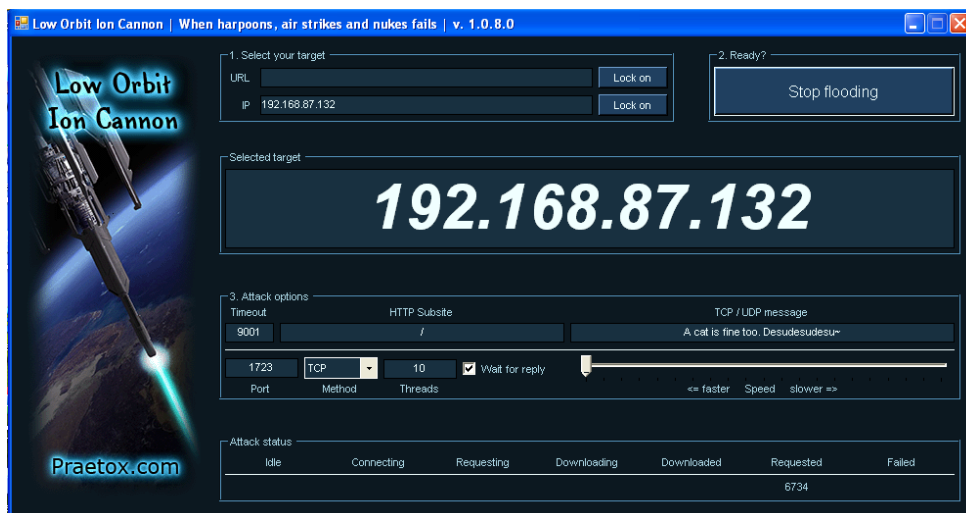


Figure 6.6 LOIC attack on PPTP

After applying this attack, the client is still connected to the VPN service, but the traffic has slowed and the time to connect has increased slightly. Figure (6.) shows some details:

```
C:\WINDOWS\system32\cmd.exe - ping 192.168.87.132 -t
Reply from 192.168.87.132: bytes=32 time=17ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time=8ms TTL=128
Reply from 192.168.87.132: bytes=32 time=43ms TTL=128
Request timed out.
Reply from 192.168.87.132: bytes=32 time=13ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time=15ms TTL=128
Request timed out.
Reply from 192.168.87.132: bytes=32 time=12ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
Reply from 192.168.87.132: bytes=32 time<1ms TTL=128
```

Figure 6.7 Effects of LOIC on VPN

6.1.2 Attacking SSL VPN

As mentioned previously in this thesis, we implemented an SSL VPN using Cisco ASA 5520 as an NAS (VPN gateway), and Windows XP client as a remote user, while the hacker machine here was Backtrack5 Linux or Windows XP.

6.1.2.1 Attacking an SSL VPN with Slowloris:

In this attack, the Hacker machine was Backtrack5 Linux. Starting the attack was carried out by opening a console terminal and writing the following command:

```
Perl ./slowloris.pl -dns 192.168.247.15 -port 443 -timeout 1 -num 1000 -cache
```

It can be seen that 192.168.247.15 is the IP address of the ASA and 443 is the open port for the SSL protocol. The timeout is the time between sending packets, while

num is the number of packets in each sending. More details can be seen in Figure (6.8).

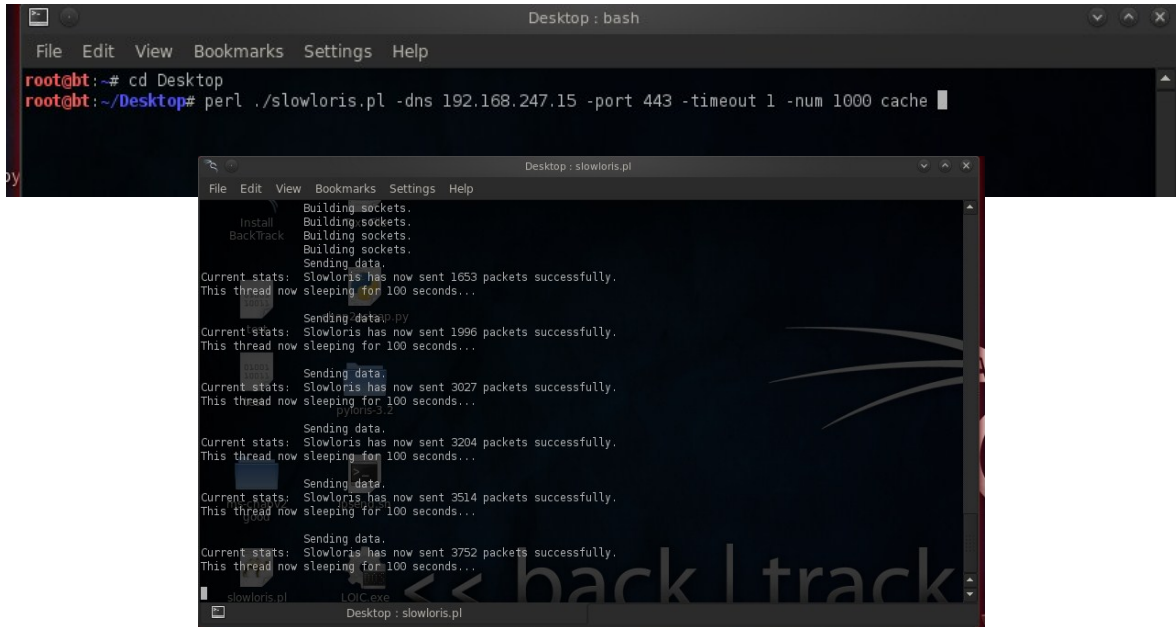


Figure 6.8 Slowloris attack on SSL

After a number of minutes, a client cannot connect to the server using an SSL connection or a slow connection, as shown in Figure (6.9).

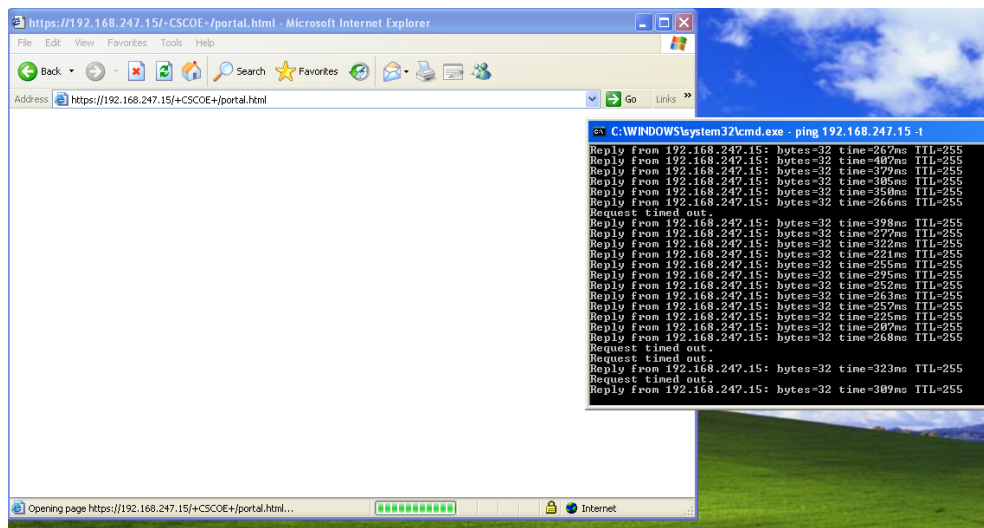


Figure 6.9 Effects of Slowloris on SSL VPN

It can be seen that the client connection had slowed and at times cannot connect. The DOS attack has been improved by opening more terminals and applying Slowloris in each to simulate DDOS Slowloris and obtain better results, as shown in Figure (6.10).

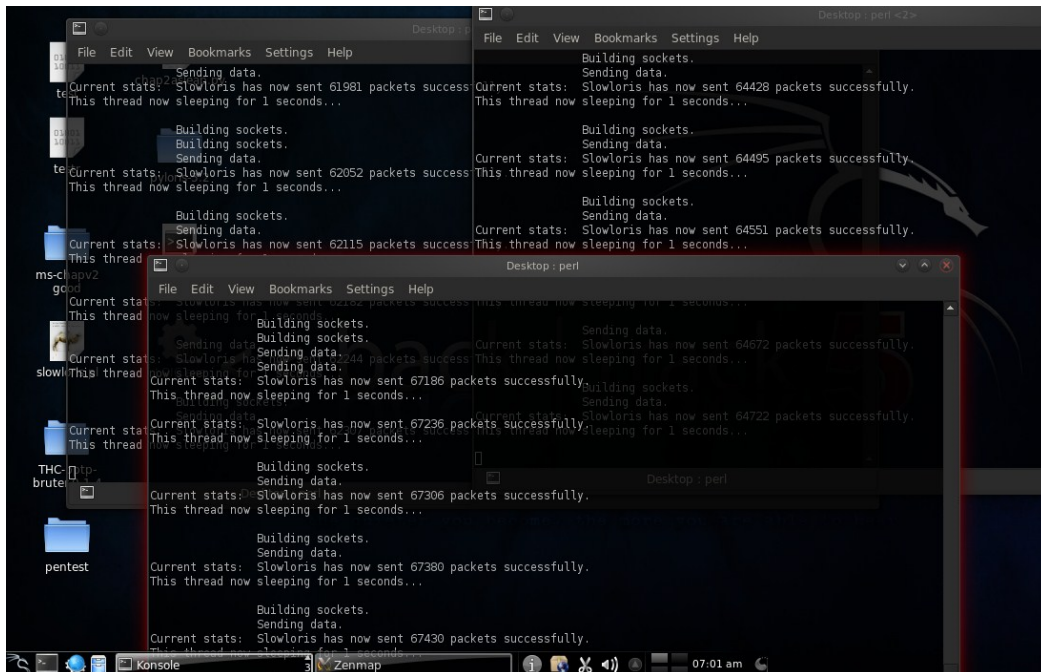


Figure 6.10 Enhanced Slowloris Dos attack on SSL

6.1.2.2 Attacking an SSL VPN with Smurf6:

In this attack, the Hacker machine was Backtrack5 Linux. Starting the attack was carried out by opening a console terminal and writing the following command:

```
Smurf6 eth0 192.168.247.15
```

It can be seen that 192.168.247.15 is the IP address of the ASA and *eth0* is the network interface of the Linux machine. Further details can be seen in Figure (6.11).

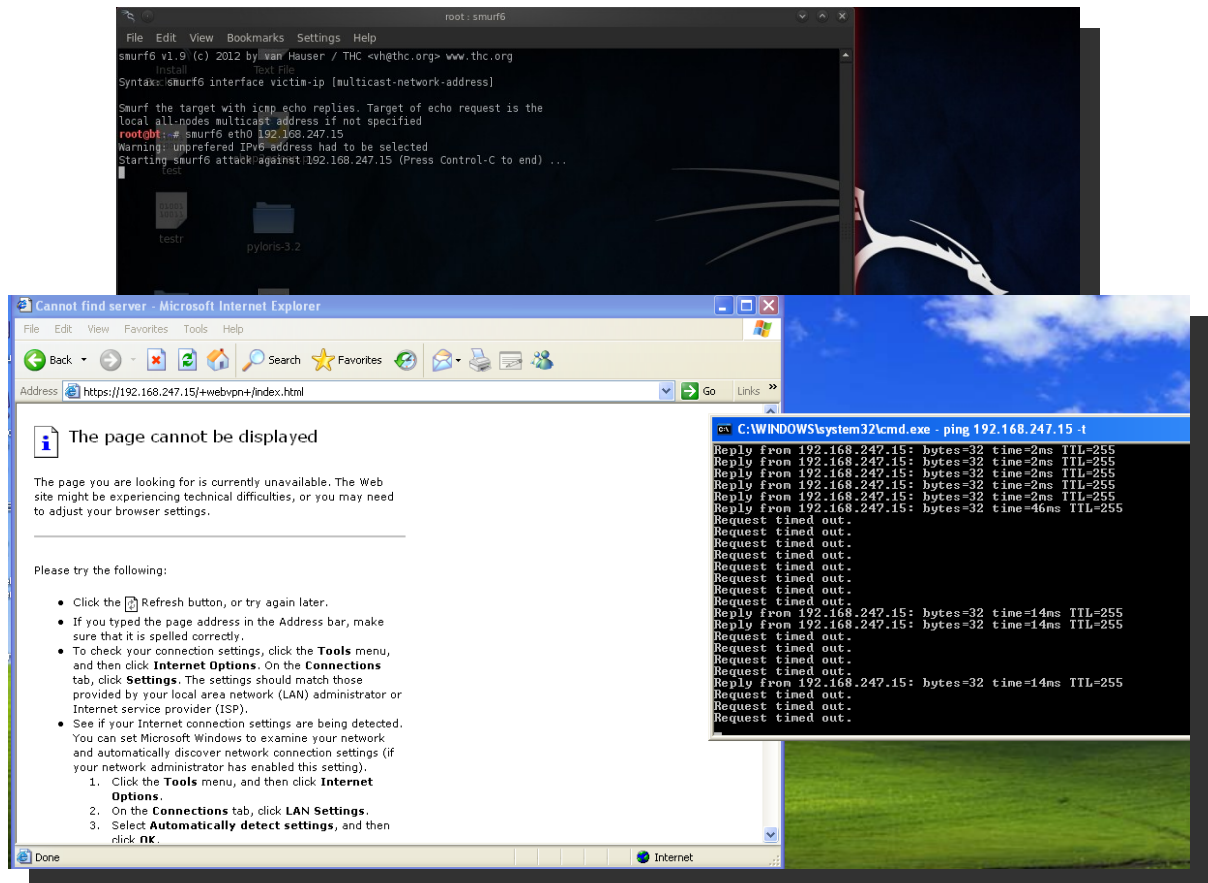


Figure 6.11 Smurf6 attack on SSL VPN

It can be seen that the client cannot connect using SSL.

The DOS attack has been improved by opening more terminals and applying Smurf6 to each to simulate DDOS Smurf6 and obtain better results, as shown in Figure (6.12).

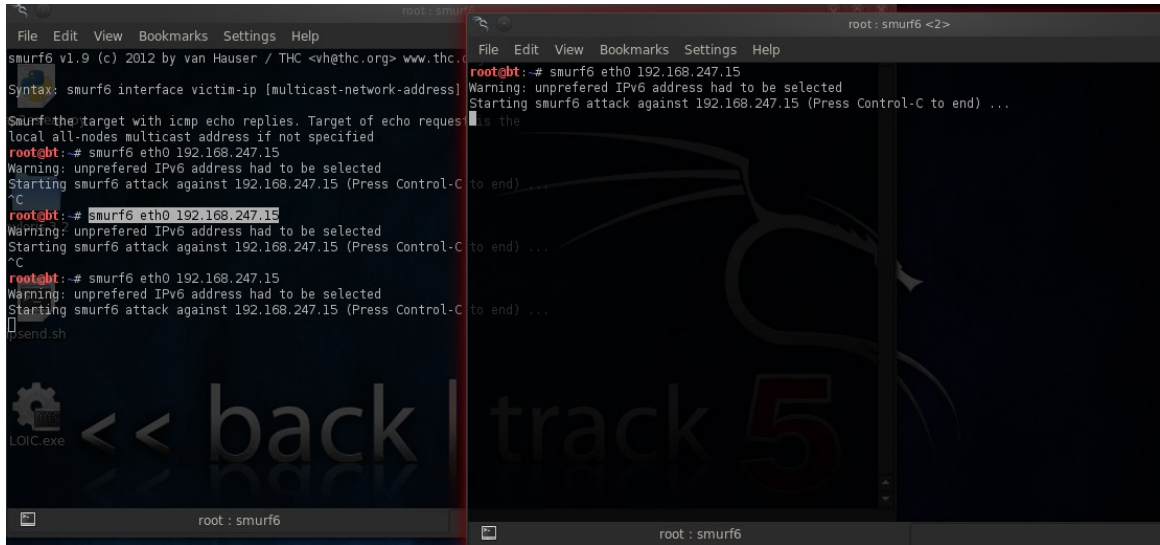


Figure 6.12 Enhanced Smurf6 DOS attack on SSL

6.1.2.3 Attacking SSL VPN with LOIC:

In this attack, the Hacker machine was Windows. Starting the attack was carried out by opening a GUI tool and entering the target IP address and open service port with some configurable options, as shown in Figure (6.13)

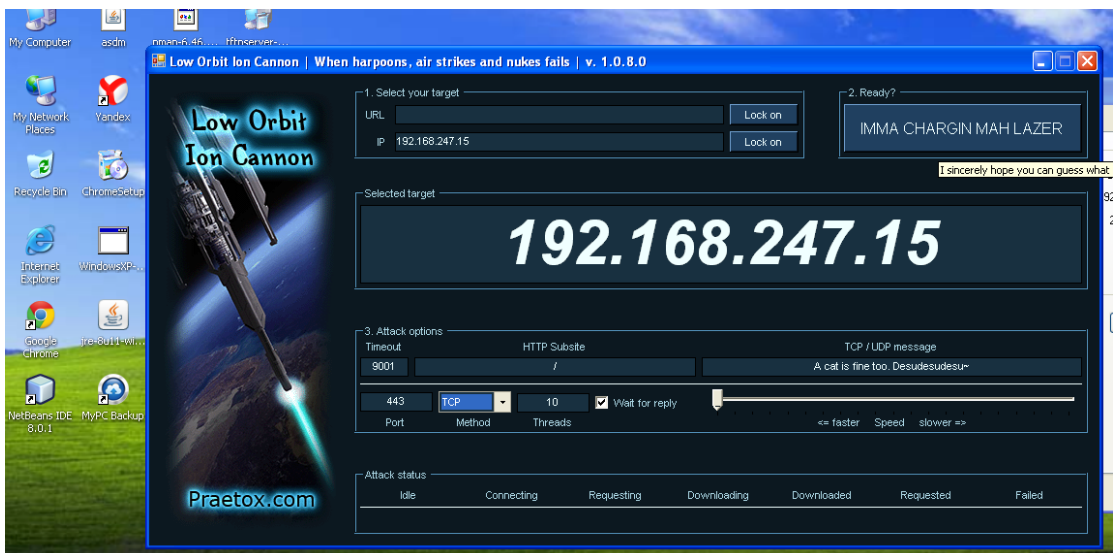


Figure 6.13 LOIC attack on SSL VPN

After applying this attack, the client still can connect to the VPN service, but the traffic slows and the time to connect increases slightly, as shown in Figure (6.14).

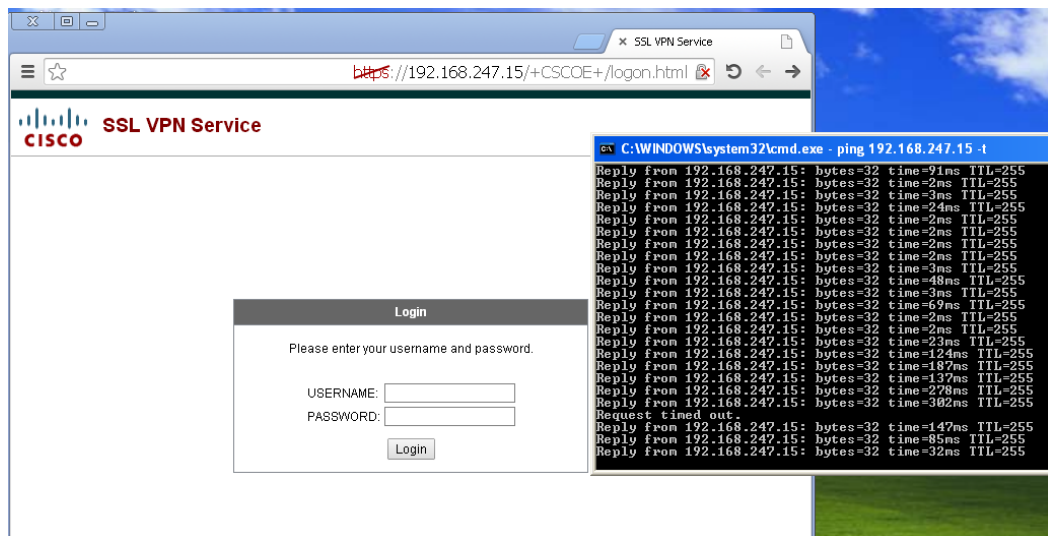


Figure 6.14 Effects of LOIC attack on SSL

It can be seen that client still can connect, but with a slow connection.

It can also be seen that this attack has been tested again to figure out the impact of the DOS attack on the tunnels, which leads to generating different types of SSL VPN using Cisco ASA. This type was (Any connect SSL), which uses a client application to generate a virtual tunnel that can be used for this test. Further details are found in Chapter 7.

6.2 Applying an MITM attack

6.2.1 Applying an MITM attack on PPTP VPN

In this section, the MITM (Man In The Middle) was applied using different tools, such as Ettercap, Cain and Abel and Subterfuge. The hacker machine here is Backtrack5 Linux or Windows XP.

6.2.1.1 MITM attacking a PPTP VPN using ETTERCAP.

In this attack, ARP poisoning has been carried out using the Ettercap tool as follows:

- First, we scan for hosts to detect the remote PPTP client and use it as the first target (victim) for an MITM attack.
- After determining the targets, we apply ARP poisoning to start sniffing the traffic by redirecting the packets to the attacker machine first.
- After the client (remote PPTP client) attempts to connect to the NAS (VPN gateway) (here we have Windows 2008 server), we acquire (sniff) the user name and the domain name in clear text, while the password we obtain is encrypted with MS-CHAPv2.

Figures (6.15) and (6.16) demonstrate the procedures of applying this attack using Ettercap.

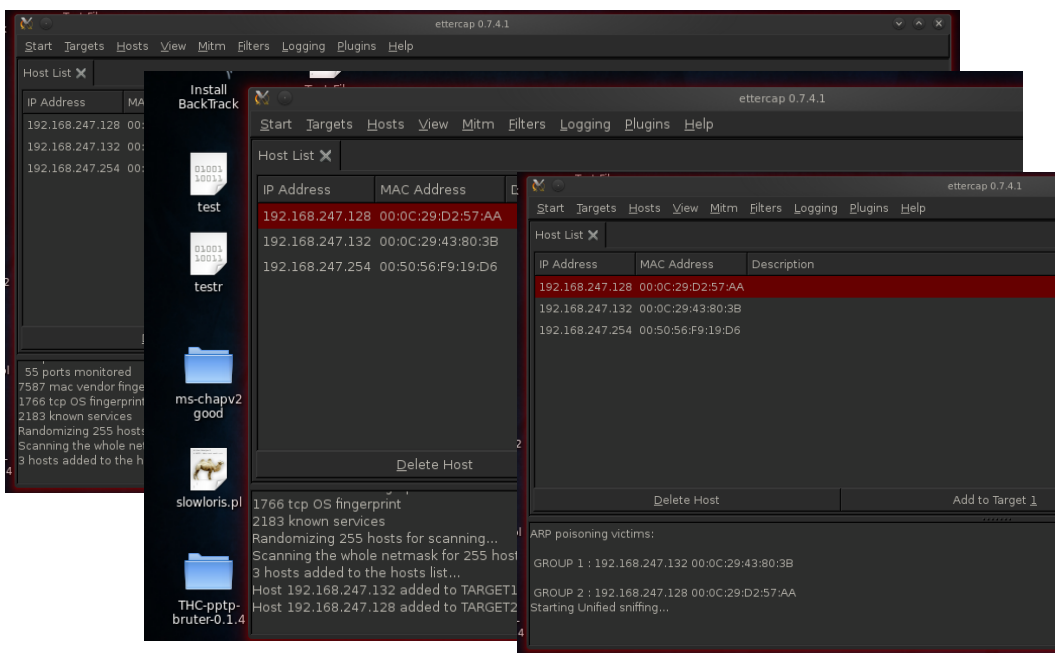


Figure 6.15 Applying MITM and waiting for the VPN to start

In addition, (PPTP-chapms), which attempts to make a tunnel, uses MS-chapv1 instead of MS-chapv2, which had been tried in this experiment. Figure (6.18) shows this clearly.

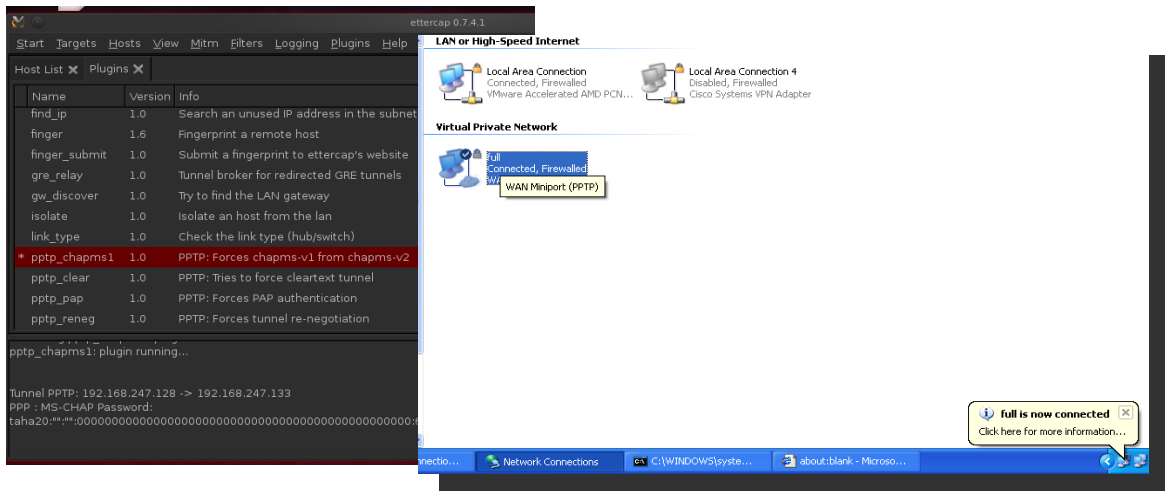


Figure 6.18 Applying PPTP-chapms1 plug-in

We can see clearly that this plugin worked properly and the connection has been accepted.

6.2.1.2 MITM attacking a PPTP VPN using Cain and Abel

In this attack, ARP poisoning has been carried out using the CAIN and ABEL tool and an MITM attack was applied as follows:

- First, we scan for hosts to detect the remote PPTP client and use it as the first target (victim) for the MITM attack.
- After determining the targets, we apply ARP poisoning to start sniffing the traffic by first redirecting the packets to the attacker machine.
- After the client (remote PPTP client) attempts to connect to the NAS or VPN gateway (here we have Windows 2008 Server), nothing results.

Figure (6.19) demonstrating the procedures for applying this attack using Cain and Abel.

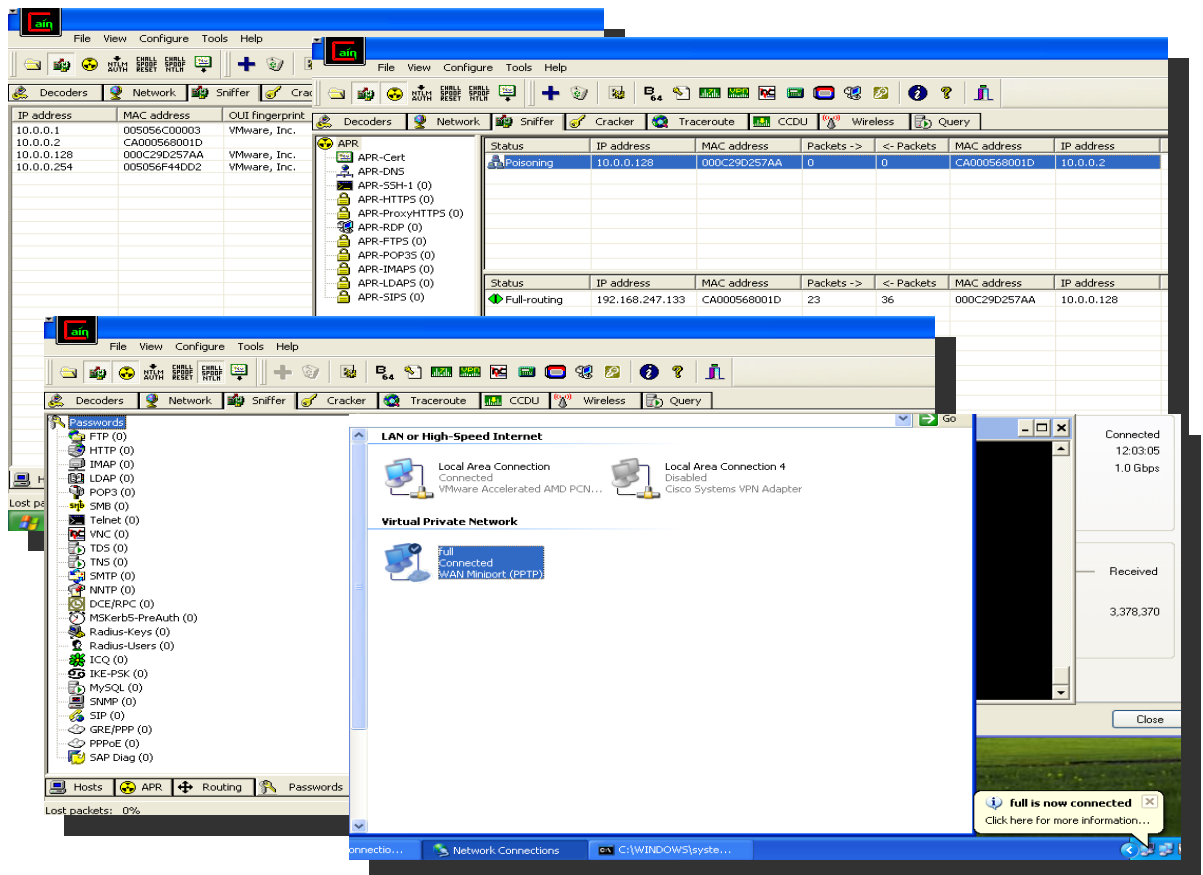


Figure 6.19 Applying MITM on PPTP using Cain and Abel

Unfortunately, when attempting to use more encryption using the Kerberos 5 protocol on Windows 2008 Server, the Cain and Abel tool sniffed the packets and it appeared to be easily cracked by a dictionary attack or brute force attack, but needed enough time, as seen in Figure (6.20).

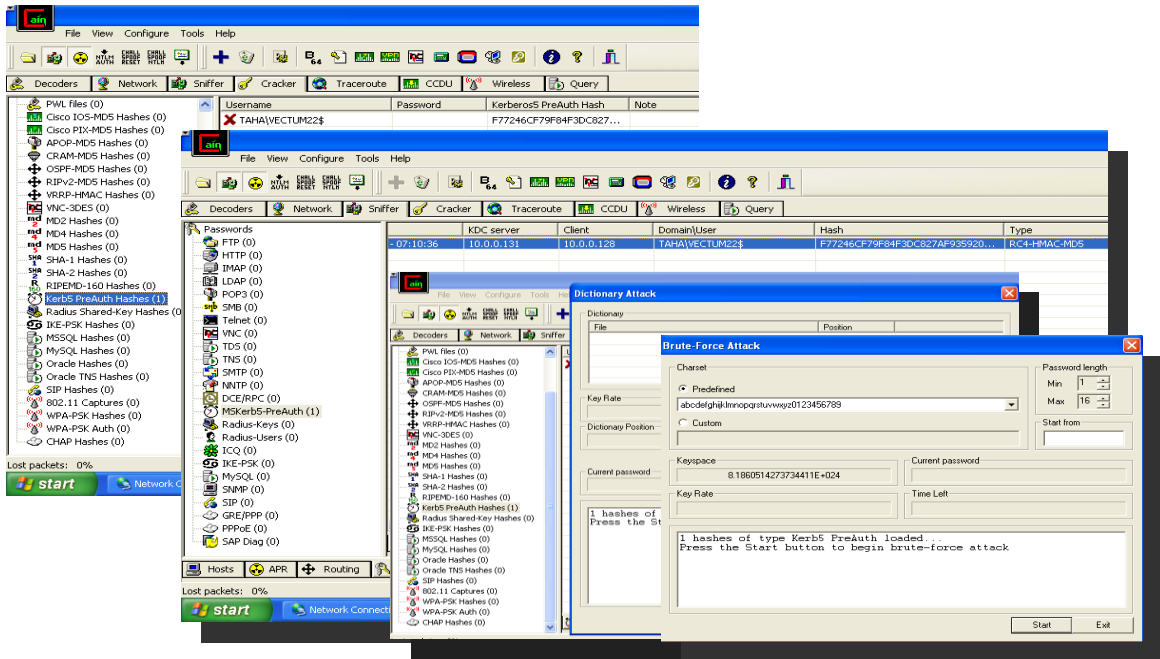


Figure 6.20 Sniffing Korberos5 packets

6.2.1.3 MITM attacking a PPTP VPN using Subterfuge

Because Subterfuge is an automated tool, a Man In The Middle attack does not need to be configured before the start. However, this option is also available if desired. Here we applied an MITM attack using the subterfuge framework after starting the subterfuge server by writing the command *Subterfuge*, as shown in figure (6.21).

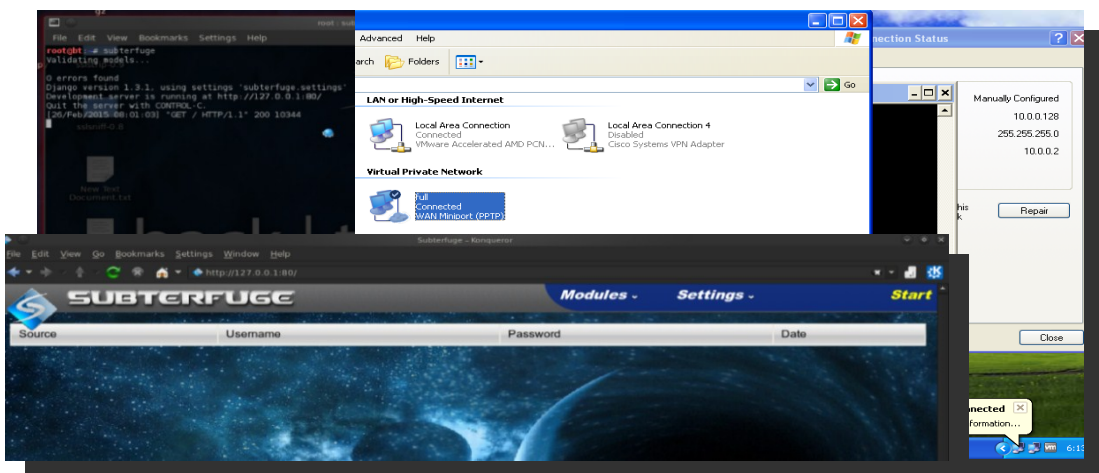


Figure 6.21 Applying MITM on PPTP with Subterfuge

As can be seen, no results were yielded using this tool against the PPTP protocol. There is another method that was not mentioned here to apply an MITM attack in a real and successive way. This is the creation of a fake VPN server on the attacker machine and by applying ARP poisoning, we can fool the victim machine to connect to the fake server, thereby sniffing and decrypting all packets. Moreover, additions can be made by using this information to connect to the real VPN server by generating two connections, one with the server and the other with the victim, which is the real concept of the Man In The Middle attack.

6.2.2 Applying an MITM attack on a SSL VPN

In this section MITM (Man In The Middle) had been applied using different tools such as Ettercap, Cain and Abel and Subterfuge, the hacker machine here was Backtrack5 Linux or windows XP.

6.2.2.1 MITM attacking SSL VPN using ETTERCAP

In this attack, ARP poisoning has been carried out using the Ettercap tool as follows:

- First, we scan for hosts to detect the remote SSL client and use it as the first target (victim) for an MITM attack.
- After determining the targets, we apply ARP poisoning to start sniffing the traffic by redirecting the packets to the attacker machine first.
- After the client (remote SSL client) attempts to connect to the VPN gateway (in this case Cisco ASA), we yield nothing, implying that this attack did not work here in these conditions. Figure (6.22) shows this experiment.

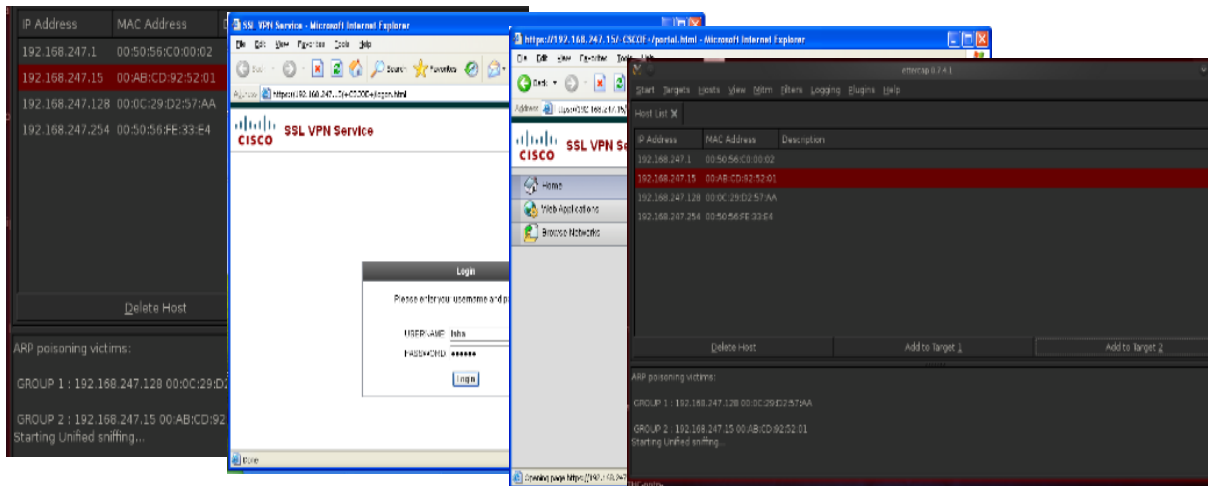


Figure 6.22 MITM attacking SSL using Ettercap

6.2.2.2 MITM attacking SSL VPN using Cain and Abel

In this attack, ARP poisoning has been carried out using the CAIN and ABEL tool and an MITM attack is applied as follows:

- First, we scan for hosts to detect the remote SSL client and use it as the first target (victim) for the MITM attack.
- After determining the targets, we apply ARP poisoning to start sniffing the traffic by first redirecting the packets to the attacker machine.
- After the client (remote SSL client) attempts to connect to the VPN gateway (here we have Cisco ASA), we acquire the clear text user name and password from the sniffed packets, as shown in Figure (6.23).

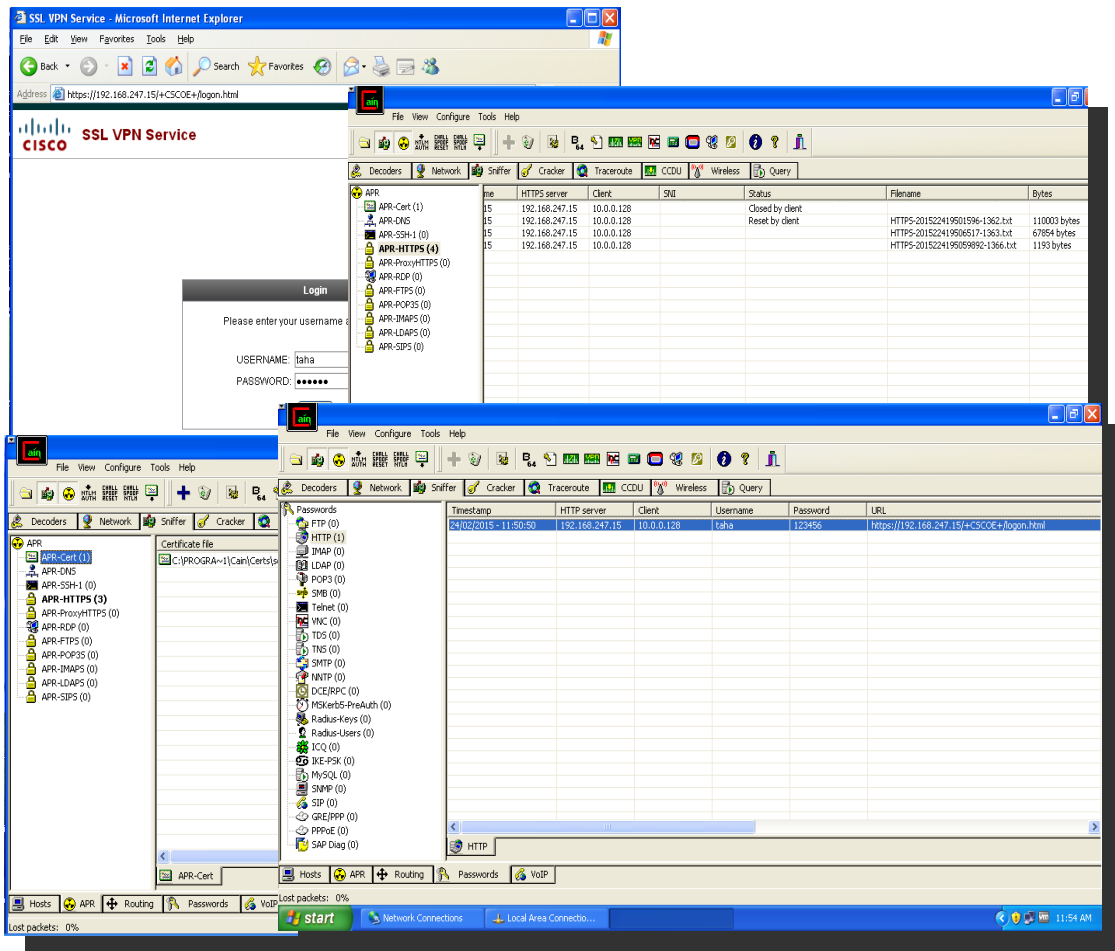


Figure 6.23 MITM attacking SSL VPN using Cain and Abel

6.2.2.3 MITM attacking an SSL VPN using Subterfuge

As mentioned in 6.2.1.3, it is not necessary to configure Subterfuge prior to starting. Nevertheless, that choice is also available if desired. Here, we applied an MITM attack using the subterfuge framework after starting the server of subterfuge by writing the command *Subterfuge*.

Figure (6.24) shows how to apply this and the results obtained after the connection was created.

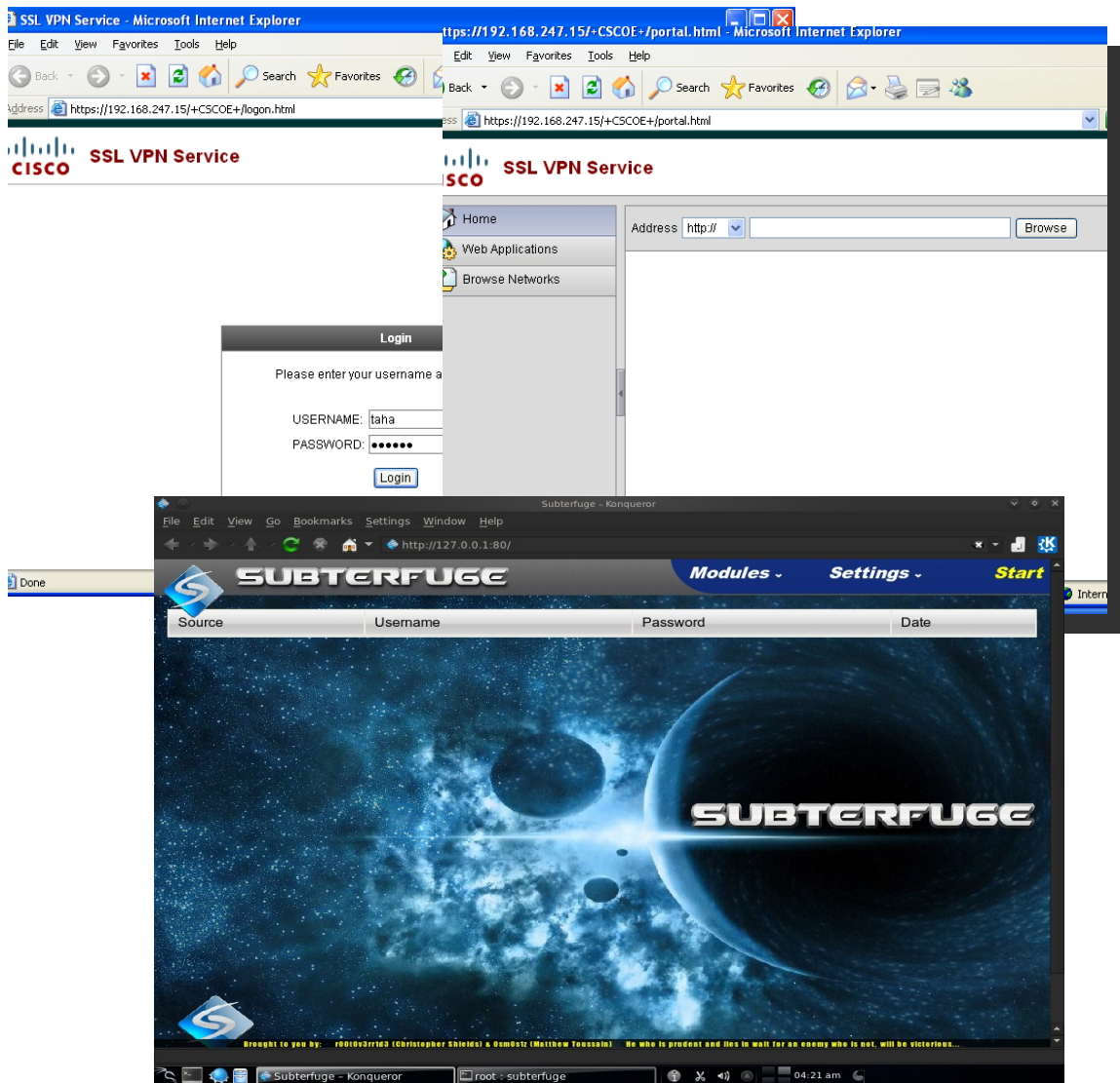


Figure 6.24 An MITM attacking PPTP VPN using Subterfuge

Note here that these results were obtained in a virtual environment under limited conditions. Moreover, it is important to care about whether there are more MITM mechanisms that were not mentioned here, including the application of ARP spoofing for both sides (victim and gateway) and enabling the IP forwarding.

6.3 Attacking the encryption

6.3.1 Attacking PPTP VPN Encryption

As referred to in Section 4.4, this type of attack of the tunnel by attempting to decrypt (crack) the encrypted passwords can be applied using different methods, such as brute forcing and dictionary attacks. The encrypted passwords are sent through a tunnel. In this chapter, two different methods are applied: the dictionary attack using the **Chap2asleap** script, and brute force attack using the **Chapcrack** script. The following sections explain this in more detail.

6.3.1.1 Dictionary attacking PPTP to obtain the password

This attack is based on the encrypted challenges and responses that were sniffed with an MITM attack or even those which were sniffed using Wireshark. In this attack, the **Chap2asleap** script is used to change the form of the hash to a suitable form for the Asleap tool, which is used to apply a very fast dictionary attack. The command to run this tool in Linux Backtrack was as follows: `Python chap2asleap.py`. Then it asked about the user name, challenge and response. Finally, it changed the form of the hash. The new update of this tool automatically calls the tool **genkeys**. This tool has the job of generating comparison list files (`words.dat` and `words.idx`) from the passwords list file (`darkc0de.ls`) which will be used by the **Asleap** tool. Finally Asleap becomes ready to start the comparison. After some seconds, Asleap finds the password. Figure (6.25) shows the detailed operation.

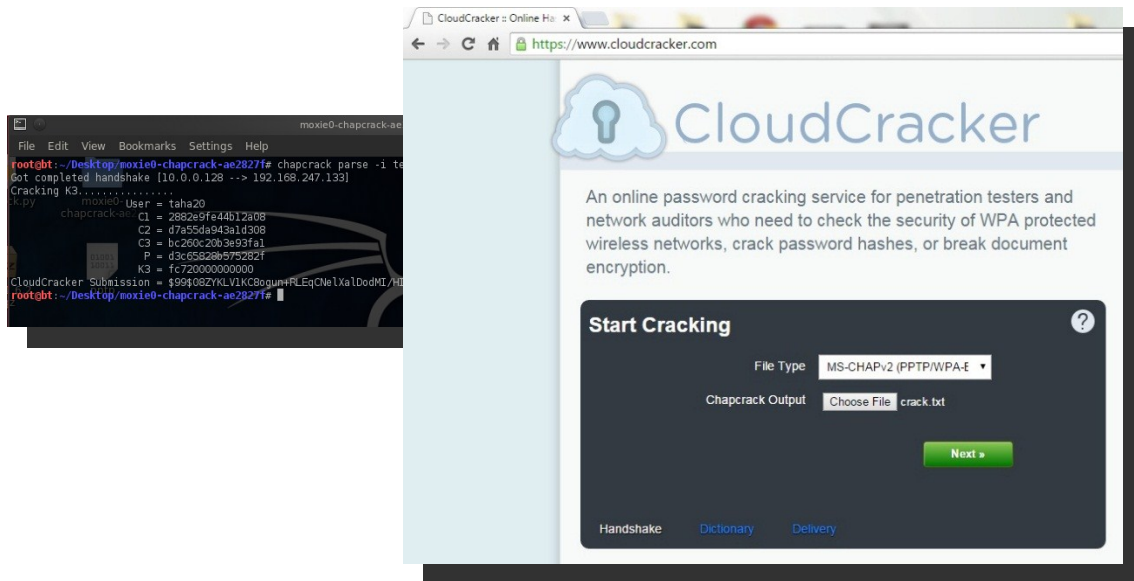


Figure 6.26 Brute Force attacking a PPTP VPN

6.3.2 Attacking SSL VPN Encryption

As in section 4.5, this attack is applied against HTTPS using the SSL Stripping technique. First of all, it needs to apply an MITM attack to eavesdrop on the traffic; then, by changing the protocol from HTTPS into HTTP, it easily eavesdrops on the passwords and usernames that are sent in clear text. It is important to note that the connection between the attacker and the server is still HTTPS; therefore, it cannot be recognized. In addition, another security attack, known as *heartbleed*, can be applied on some SSL systems where an attacker can reach recent information from the server memory which may contain very important information, such as user accounts and administrators. See 6.3.2.2.

6.3.2.1 Attacking an SSL VPN with SSLSTRIP

SSLSTRIP is a tool developed by Moxie Marlinspike and can be used to apply an SSLSTRIP attack by forcing the SSL tunnel to use HTTP instead of HTTPS. In this attack, this tool is used with an MITM attack which is applied using the Ettercap tool for ARP poisoning and unified sniffing. This attack encounters a problem when applied on a WAN. The attack procedures are as follows:

- ARP spoofing the two parties (client and gateway) by writing the commands in different console (terminal) windows:

```
Arpspoof -i eth0 -t 10.0.0.2 10.0.0.128
```

```
Arpspoof -i eth0 -t 10.0.0.128 10.0.0.2
```

Thus, ARP poisoning is applied and two sides are spoofed.

- Re-forwarding the packets sniffed back to the gateway by writing the command:

```
Echo 1 >/proc/sys/net/ipv4/ip_forward.
```

- Redirecting the packets to different ports that are used by SSLSTRIP, such as 10000 by writing the command:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000 , where 80 is the default port number .
```

- The SSLSTRIP script is running now by the command:

```
sslstrip -l 10000
```

Where 10000 is the port that sslstrip will listen to.

- Finally, the Ettercap tool is used for unified sniffing of the passwords, as shown in more detail in Figure (6.27).

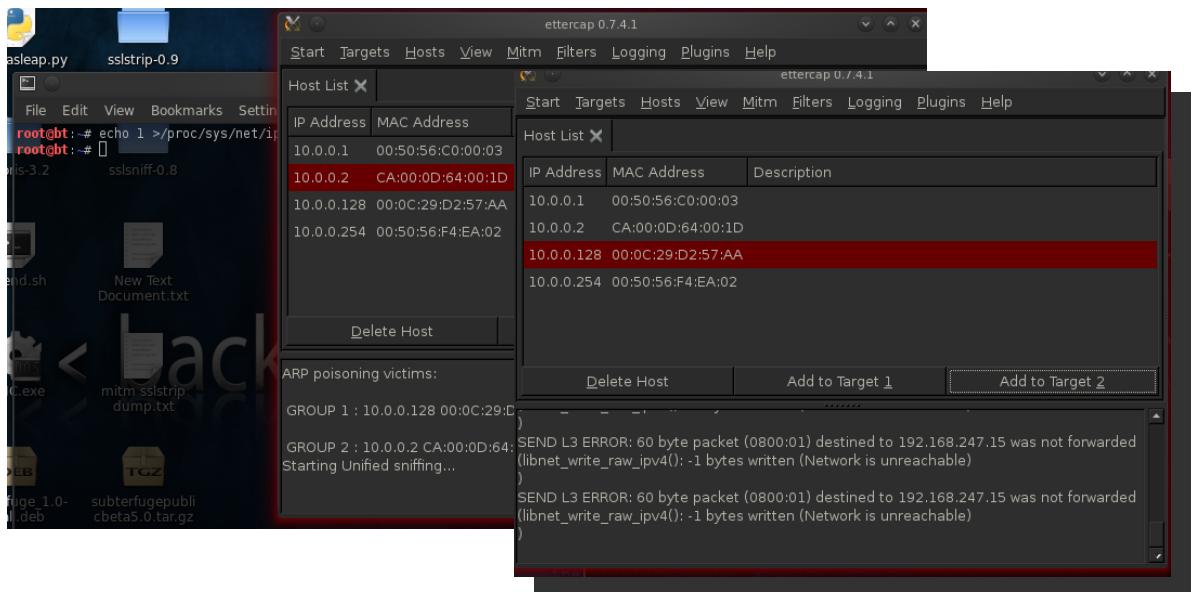


Figure 6.27 Attacking an SSL VPN with SSLSTRIP and Ettercap

The previous figure shows clearly that we receive an error regarding the layer. However, when the same attack is applied again but with a different tool (Cain and Abel), SSL stripping succeeded and passwords were sniffed after the MITM attack was applied, as shown in Figure (6.28).

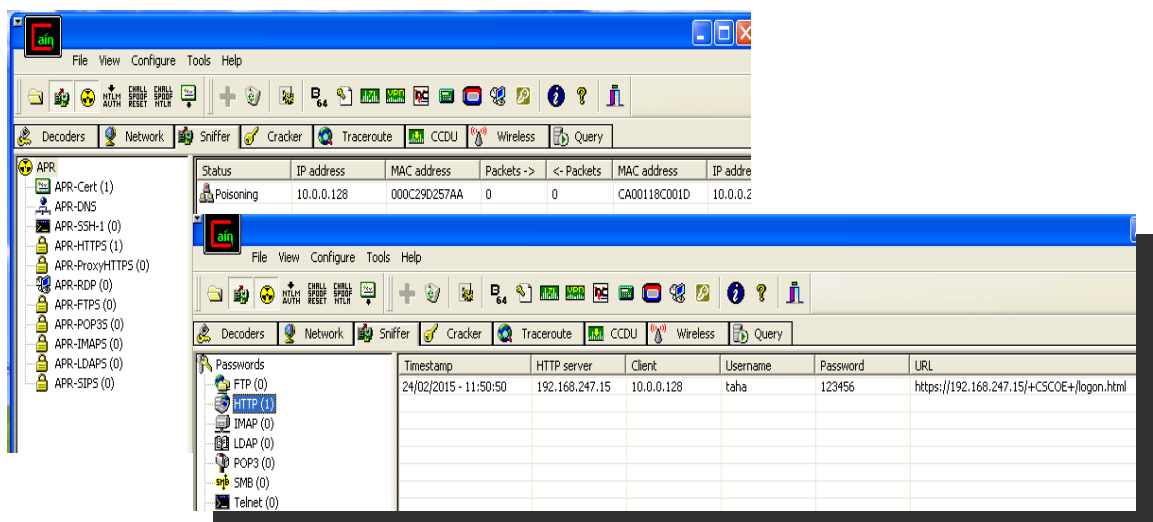


Figure 6.28 Attacking SSL VPN with Cain and Abel

6.3.2.2 Attacking an SSL VPN with the Heartbleed attack

Since the main aim of this thesis is not to break up the protocols but to analyze them from a security point of view, even a failed attack was mentioned to prove that the target protocol is still immune to this attack, or that the following attack proved that our Cisco ASA was not vulnerable to the Heartbleed attack, as shown in Figure (6.30).

```
File Edit View Search Terminal Help
root@kali:~# python heartbleed.py 192.168.247.15
#####
Connecting to: 192.168.247.15:443 with TLSv1.1
Sending Client Hello...
Sending heartbeat request...
Unexpected EOF receiving record header - server closed connection
No heartbeat response received, server likely not vulnerable
#####
```

Figure 6.29 Attacking SSL VPN with the HeartBleed attack

CHAPTER 7

Results, Discussion and Comparisons

7.1 Overview

In this chapter, the results obtained in Chapter 6 are discussed with a simple comparison. Note that some tables and charts have been added for explanatory purposes only and have low accuracy. The following sections show this in further detail.

7.2 Attacking VPN protocols with a DOS Attack

The attacking procedures have been explained in Chapter 6, and here the results analysis and discussion are presented. The following charts explain the effect of DOS attacks on the connection time. Each row shows two sub-charts that show the situation before and after the attack. Finally, Tables (7.1) and (7.2) show the averages.

7.2.1 Attacking PPTP with a DOS

The following charts show a time graph that describes the effects of those attacks on a PPTP VPN and especially at connection time. Note that these graphs are for no means accurate.

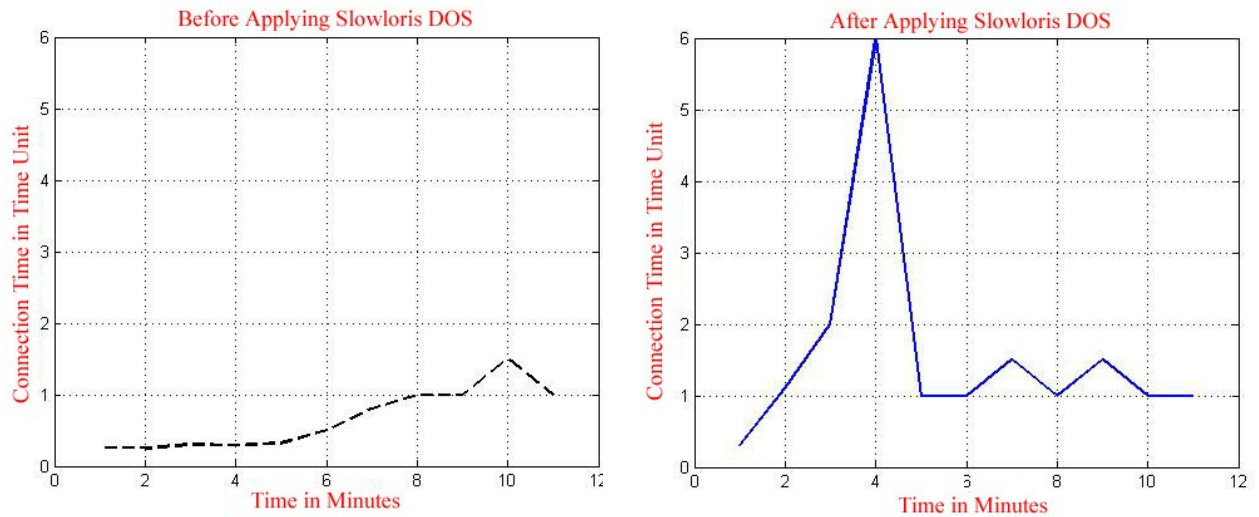


Figure 7.1 Effects of attacking PPTP with Slowloris on connection time

On the left side, one can see the chart pertaining to the connection time prior to the application of the Slowloris DOS attack. It is clear that the system was not very stable. If one looks at time axis, one notices a small increase at minute (10). By taking the average value of the chart, a more accurate result can be calculated. On the right side, the chart shows the effect of applying the Slowloris DOS attack to the PPTP VPN connection time. It can be seen at the start of the attack and especially at minute (4) that a sudden increase occurs due to the connection requests by Slowloris that were sent to the VPN gateway. Later, it returns to the values of the average, the value of the normal situation before applying the attack. A more accurate value can be found in Table (7.1).

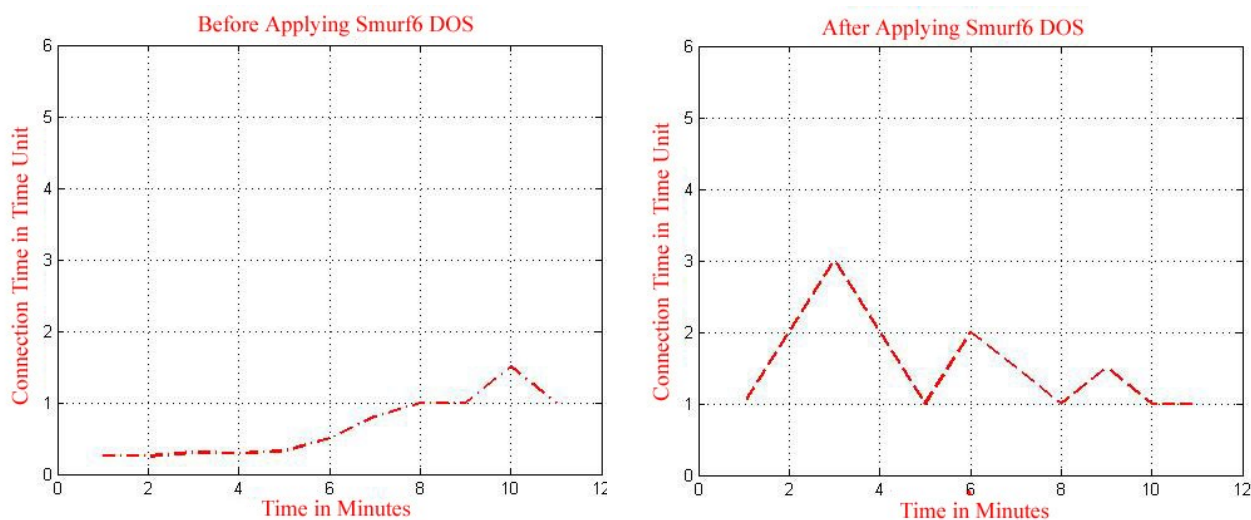


Figure 7.2 Effects of attacking PPTP with Smurf6 on connection time

On the left side, one can see the chart pertains to the connection time before applying the Smurf6 DOS attack. It is clear that the system was not very stable. If one looks at the time axis, one may see a small increase at minute (10). By taking the average value of the chart, a more accurate result can be calculated. On the right side, the chart shows the effect of applying the Smurf6 Dos attack on the PPTP VPN connection time. It can be seen that at the start of the attack and especially at minute (3), a sudden increase occurs, albeit less than what is seen in Slowloris. This is due to the flooding of requests by Smurf6 that were sent to the VPN gateway. Later, it incrementally returned to values near to the average of the normal situation prior to applying the attack. More accurate values can be found in Table (7.1).

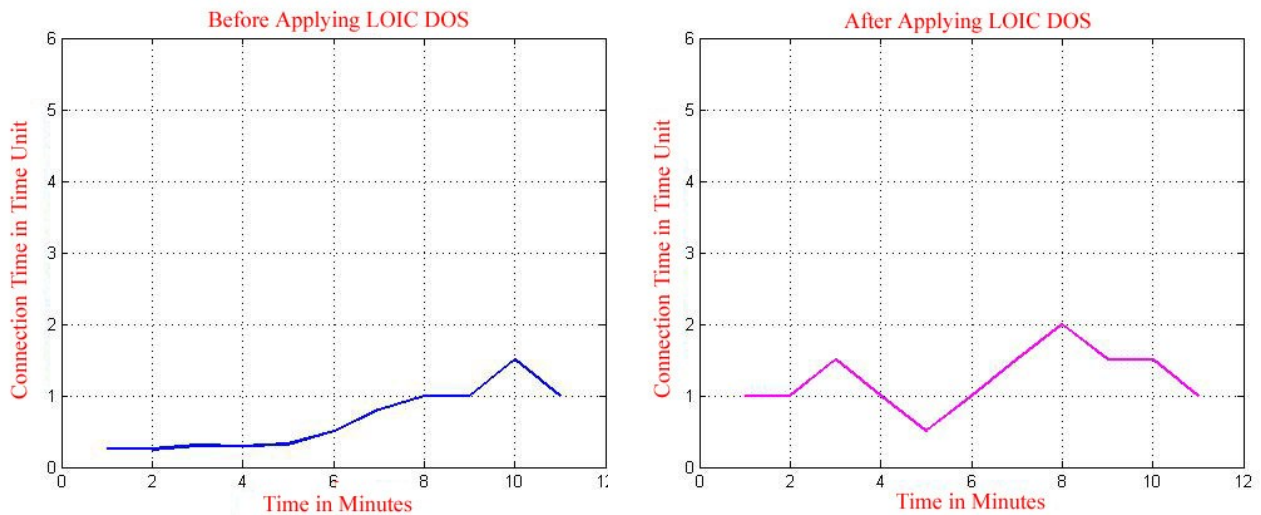


Figure 7.3 Effects of attacking PPTP with LOIC on connection time

On the left side, one can see the chart pertaining to the connection time prior to applying the LOIC DOS attack. It is clear that the system was not very stable. If one looks at the time axis, it can be observed that there was a small increase at minute (10). By taking the average value of the chart, a more accurate result can be calculated. On the right side, the chart shows the effect of applying the LOIC DOS attack to the PPTP VPN connection time. It appears that there was a small effect near to the normal average of the PPTP prior to application of the attack. More accurate values can be found in Table (7.1) showing the average effect of applying the DOS attack to the connection time, which makes the calculations more realistic and based on average values. Of note is the Average Difference calculated as follows:

$$\text{Average difference} = \text{average under attack} - \text{average before attack} \dots (1)$$

And the Average Impact has been calculated using the following formula:

$$\text{Average impact} = \frac{\text{average difference}}{\text{average before attack}} \times 100 \% \dots \dots \dots (2)$$

Attack Tool	Before attack			Under Attack			Average Difference	Average Impact
	Min	Max	AV	Min	Max	AV		
Slowloris	0.3	1.5	0.66	0.3	6	1.57	0.91	138%
Smurf6	1	1.5	1.27	1	3	1.55	0.28	22%
LIOC	0.3	1.5	1.09	0.5	2	1.227	0.137	12.6%

Table 7.1 The Average Impact of a DOS Attack on PPTP VPN Connection Time

Moreover, the effect of attacking a PPTP VPN with DOS on the data transmission rate for the VPN tunnel is shown in the following figures for the different DDOS tools. It is noticeable that the attack commences at second (200). Prior to that, the graphs show the normal behavior of the PPTP protocol when packets are exchanged between the client and the VPN gateway.

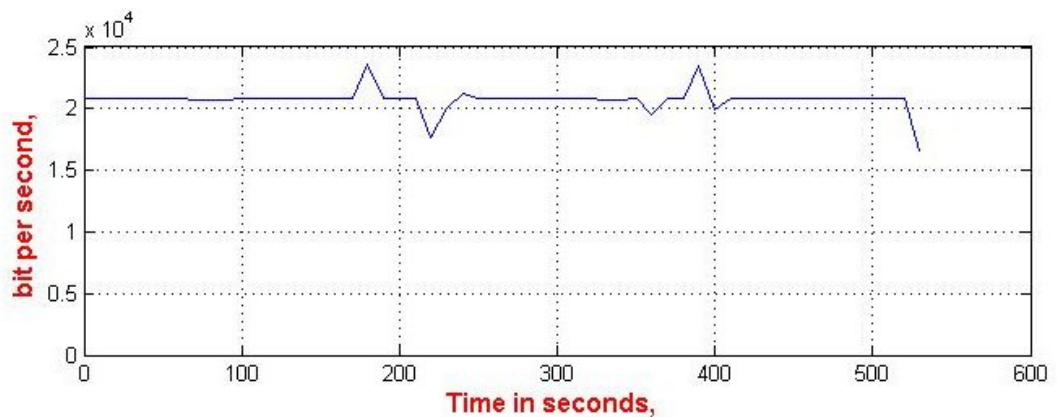


Figure 7.4 The effect of Slowloris on the PPTP transfer rate through the tunnel

The above figure illustrates the effect on the data transfer rate of attacking PPTP VPN with Slowloris. From time (0s) to (200s), the graph shows the normal situation before the attack. After time (200s), it shows the data transfer rate of the VPN under attack. A quick look at the graph gives the impression that it was a small effect and near to the average value.

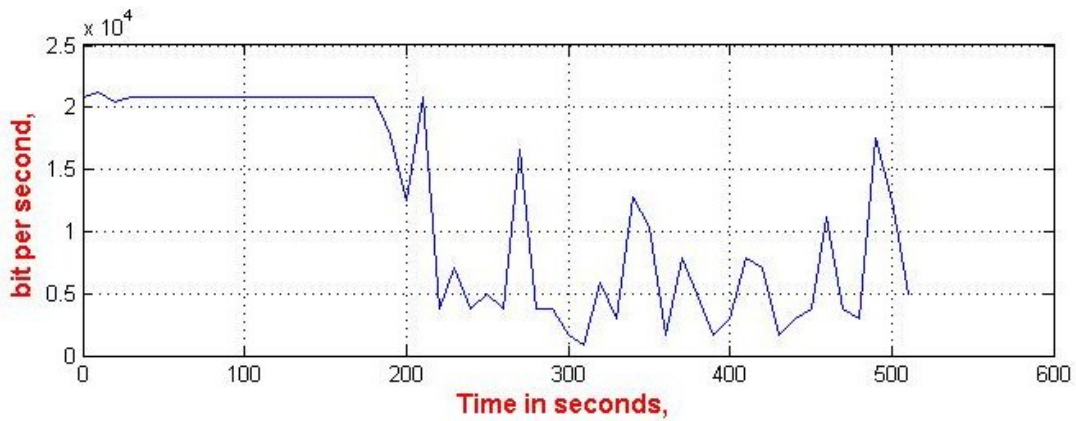


Figure 7.5 The effect of Smurf6 on PPTP transfer rate through tunnel

The previous figure illustrates the effect on the data transfer rate of attacking the PPTP VPN with Smurf6. From time (0s) to time (200s), the graph shows the normal situation before the attack. After time (200s), it shows the data transfer rate of the VPN under attack. A quick look at the graph gives the impression that there was a huge effect on this rate, which makes it unstable. Very distorted curves and Simi random values were found due to the huge flooding of the tunnel caused by the Smurf6 tool.

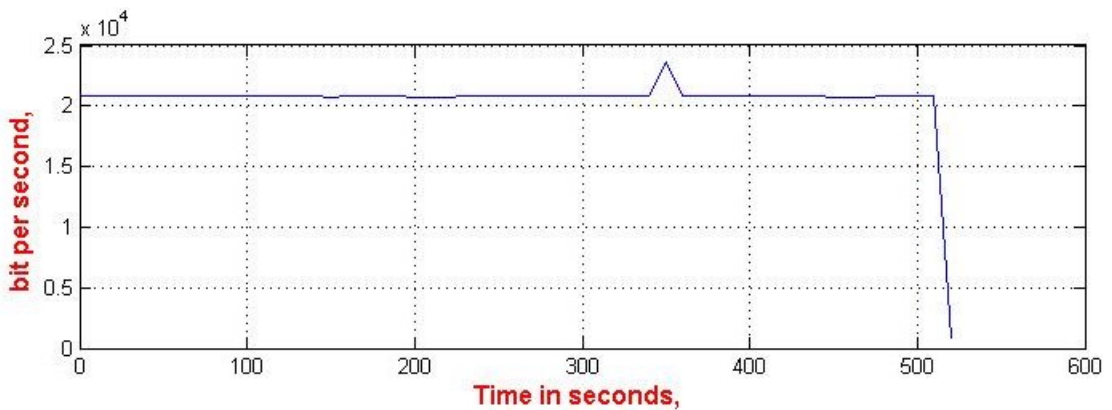


Figure 7.6 The effect of LOIC on PPTP transfer rate through the tunnel

The above figure illustrates the effect of attacking a PPTP VPN with LOIC on the data transfer rate. Starting from time (0s) and ending at (200s), the graph shows the normal situation before the attack. After (200s), it shows the data transfer rate of the

VPN under attack. A quick look at the graph gives the impression that it has a small effect which is near to the average value. Finally, the effect of attacking the PPTP VPN with DOS on the Round Trip Time for the VPN tunnel is shown in the following figures for the different DOS tools. It is important to note that the attack commences around second (200). Prior to that, the graph shows the normal behavior of the PPTP protocol when packets are exchanged between the client and the VPN gateway.

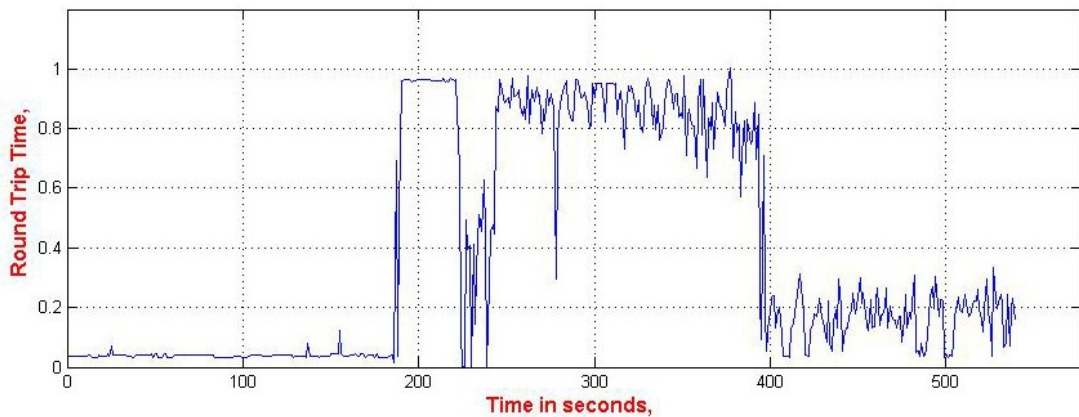


Figure 7.7 The effect of Slowloris on PPTP Round Trip Time

Figure (7.7) shows the effect of attacking a PPTP VPN with a Slowloris DOS on the Round Trip Time. A quick look shows that the average value of the RTT from the first second to second (200) at most is lower than the values under attack. The increase in the RTT is clear due to the attack.

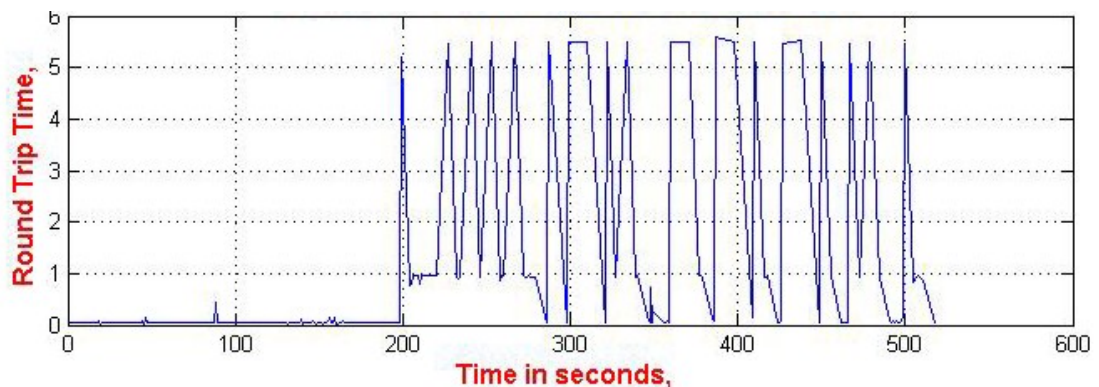


Figure 7.8 The effect of Smurf6 on PPTP Round Trip Time

The previous figure shows the effect of attacking a PPTP VPN with a Smurf6 DOS on the Round Trip Time. A quick look at the figure shows that the average value of the RTT from the first second until around second (200) is lower than the values under attack. The increase in the RTT is clear due to the extreme flood that is generated by the Smurf6 tool.

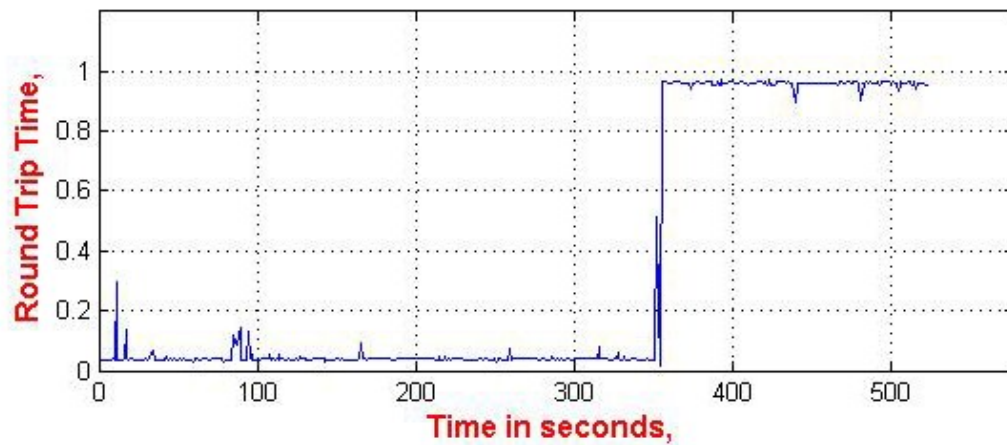


Figure 7.9 The effect of LOIC on PPTP Round Trip Time

The previous figure showed the effect of attacking the PPTP VPN with a LOIC DOS on the Round Trip Time. Fast looking shows that the average value of RTT from the first second until around the second (200) is lower than the values under attack. The increase in RTT is clear due to the LOIC Tool. Table (7.2) shows the average effect of applying a DOS attack on the Round Trip Time which makes the calculations more realistic and based on the average values. Attention should be given to the fact that the average difference has been calculated based on formula (1), and the average impact has been calculated using formula (2).

Attack Tool	Before attack			Under Attack			Average Difference	Average Impact
	Min	Max	AV	Min	Max	AV		
Slowloris	0.015	0.966	0.140	0.001	1.005	0.525	0.385	273.8%
Smurf6	0.030	5.187	0.117	0.034	5.577	1.607	1.489	1267%
LIOC	0.030	0.297	0.042	0.014	0.970	0.537	0.494	1161%

Table 7.2 The Average Impact of a DOS Attack on PPTP VPN RTT

7.2.2 Attacking SSL with DOS

The charts below show the time graph that describes the effects of different types of DOS attack on a SSL VPN and especially on connection time, CPU usage and resources. Note that these graphs are for illustration purposes only and therefore have low accuracy.

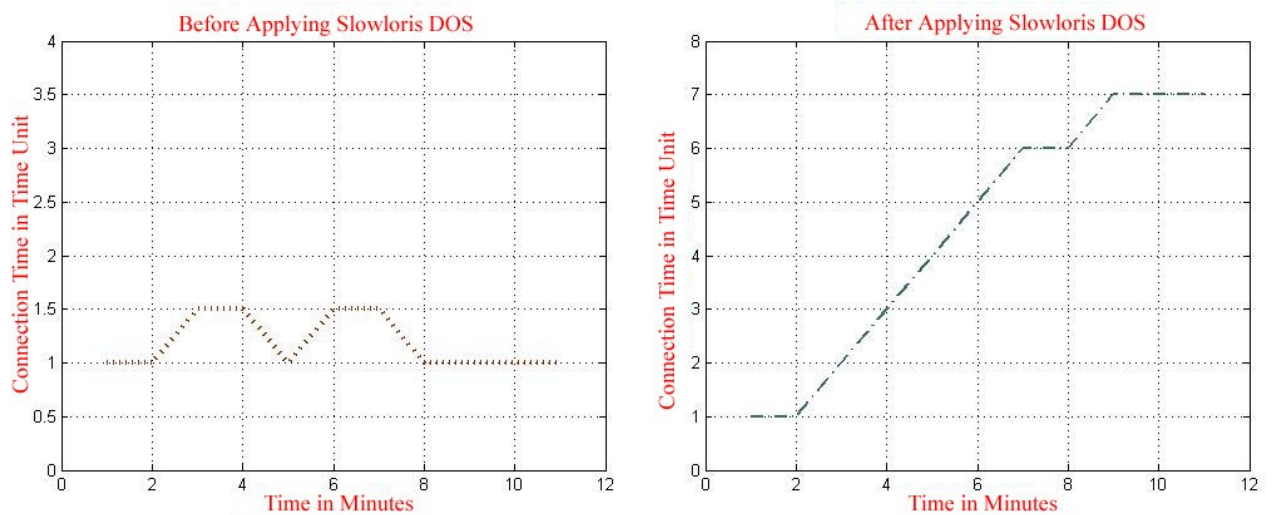


Figure 7.10 Effects of attacking SSL with Slowloris on connection time

On the left side, it can be seen from the chart pertaining to the connection time before applying a Slowloris DOS attack that it is clear that the system was not stable. A

small amount of distortion in the curves was found. . By taking the average value of the chart, a more accurate result can be calculated. On the right side, the chart shows the effect of applying a Slowloris DOS attack to the SSL VPN connection time. It can be seen that at the start of attack and especially at minute (2) that a semi-exponential increase occurs until minute (9). Later it maintains the same value. More accuracy can be found in Table (7.3).

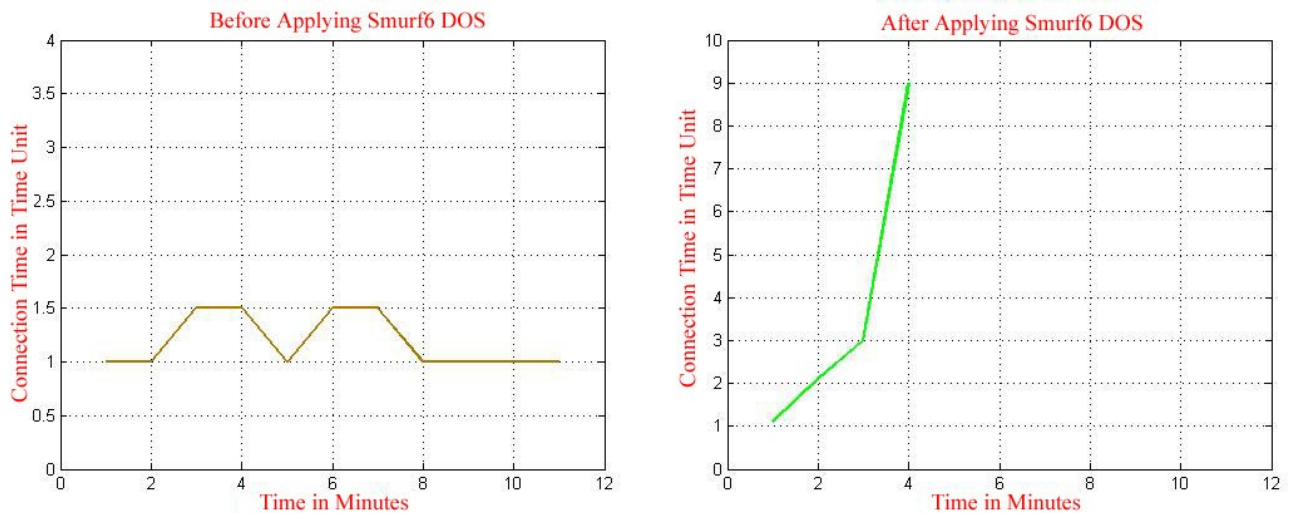


Figure 7.11 Effects of attacking SSL with Smurf6 on connection time

Similarly to the previous figure, on the left side, one can see the chart pertaining to the connection time before applying the Smurf6 DOS attack. It is clear that the system was not stable as a small amount of disorder in the values was observed. On the right side, the chart shows the effect of applying the Smurf6 Dos attack to the SSL VPN connection time. It can be seen at the start of attack, and especially at minute (2), that a huge increase was found until minute (4). This was a new behavior. The rapid increase here is due to the large value, which is due to the effect of the Smurf6 tool on the network. More accuracy can be found in Table (7.3).

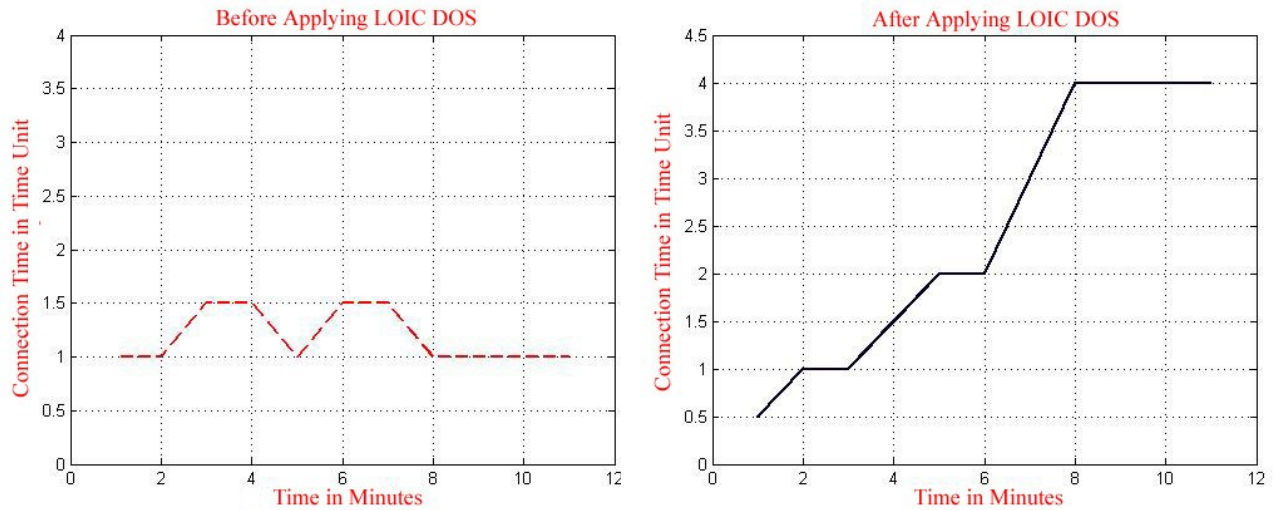


Figure 7.12 Effects of attacking SSL with LOIC on connection time

On the right side, the chart shows the effect of applying an LOIC DOS attack to the SSL VPN connection time. It can be seen at the start of the attack, and especially at minute (2), that a ladder increase occurs until minute (8). Table (7.3) shows the average effect of applying a DOS attack on the connection time, which makes the calculations more realistic and based on the average values. Attention should be given to the fact that the average difference is calculated based on formula (1), and the average impact is calculated using formula (2).

Attack Tool	Before attack			Under Attack			Average Difference	Average Impact
	Min	Max	AV	Min	Max	AV		
Slowloris	1	1.5	1.23	1	7	4.5	3.27	265.9%
Smurf6	1	1.5	1.23	1	9	7.1	5.87	477%
LIOC	1	1.5	1.23	0.5	4	2.1	0.87	72%

Table 7.3 The Average Impact of DOS Attack on an SSL VPN

Moreover, the effect of attacking the SSL VPN with DOS on the data transmission rate for the VPN tunnel is shown in the following figures for the different DOS tools. Of note is the attack which starts at second 200. Prior to that, the graphs show the normal behavior for the SSL protocol when packets are exchanged between the client and the VPN gateway.

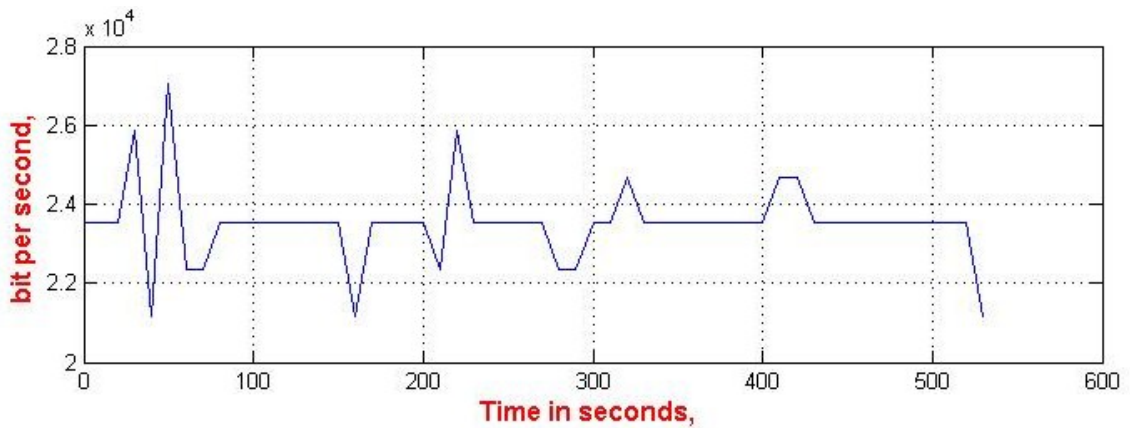


Figure 7.13 The effect of Slowloris on SSL transfer rate through the tunnel

The previous figure illustrates the effect of attacking an SSL VPN with Slowloris on the data transfer rate. From time (0s) to (200s), the graph shows the normal situation before the attack; after time (200s), it shows the data transfer rate of the VPN under attack. A quick look at the graph gives the impression that there was a small effect on this rate, which makes it a little troubled due to the effect of the Slowloris tool.

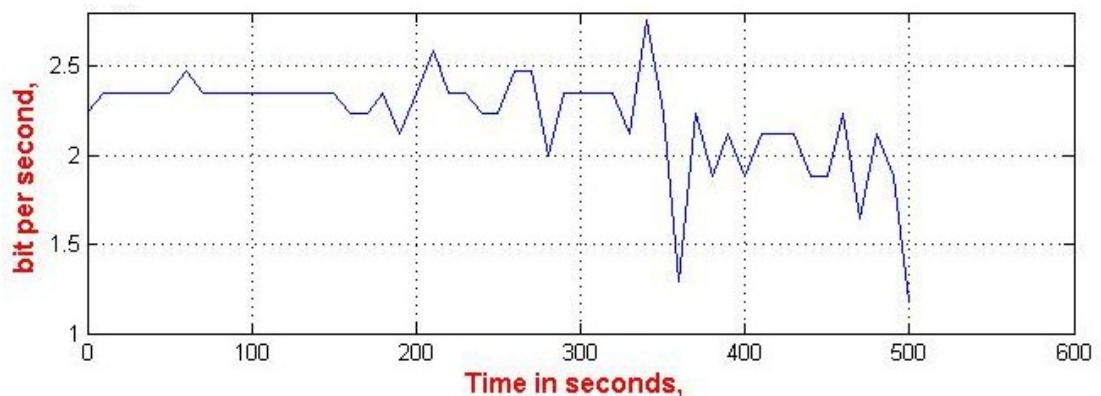


Figure 7.14 The effect of Smurf6 on the SSL transfer rate through tunnel

The previous figure illustrates the effect of attacking an SSL VPN with Smurf6 on the data transfer rate. From time (0s) to time (200s), the graph shows the normal situation prior to the attack. After time (200s), it shows the data transfer rate of the SSL VPN under attack. A quick look at the graph gives the impression that there was a clear effect on this rate and this caused it a small amount of disorder in the values due to the effect of the Smurf6 tool.

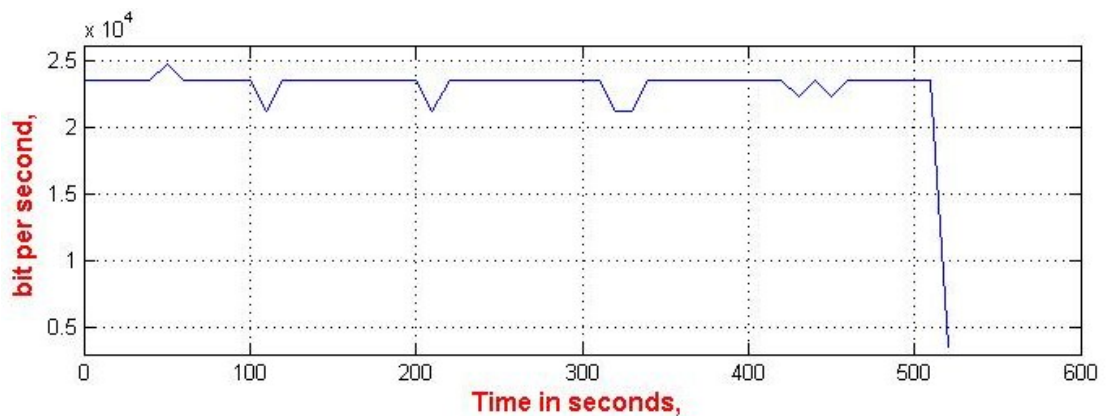


Figure 7.15 The effect of LOIC on SSL transfer rate through the tunnel

The previous figure illustrates the effect of attacking an SSL VPN with LOIC on the data transfer rate. From time (0s) to time (200s), the graph shows the normal situation prior to the attack. After time (200s), it shows the data transfer rate of the SSL VPN under attack. A quick look at the graph gives the impression that there was a small effect on this rate and this caused a small amount of disorder in values due to the effect of the LOIC tool.

Finally, the effect of attacking an SSL VPN with a DOS on the Round Trip Time for the VPN tunnel is shown in the following figures for the different DOS tools. Attention should be given to the fact that the attack started approximately at time 200s. Prior to that, the graph shows the normal behavior for the SSL protocol when packets are exchanged between the client and the VPN gateway.

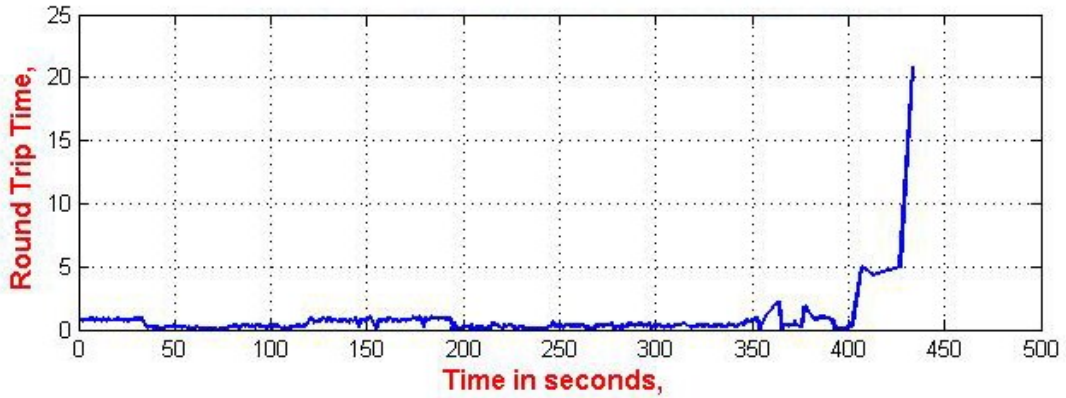


Figure 7.16 The effect of Slowloris on the SSL Round Trip Time

Figure (7.16) shows the effect of attacking an SSL VPN with a Slowloris DOS on the Round Trip Time. A quick look shows that the average value of the RTT from the first second until second (200) at most is lower than the values under the attack. The increase in the RTT is clear due to the attack.

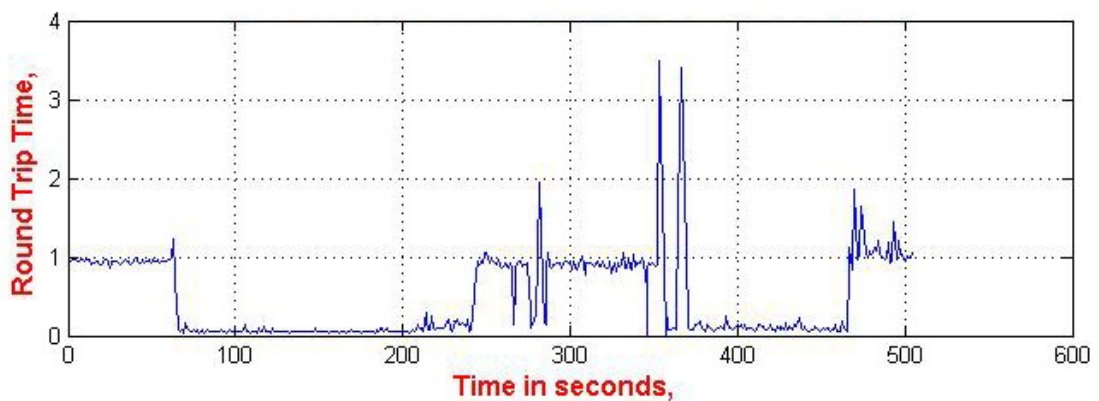


Figure 7.17 The effect of Smurf6 on SSL Round Trip Time

The previous figure shows the effect of attacking an SSL VPN with a Smurf DOS on the Round Trip Time. A quick look shows that the average value of the RTT from the first second until second (200) at most is lower than the values under attack. The increase in the RTT is clearly due to the attack. Table (7.4) shows further details.

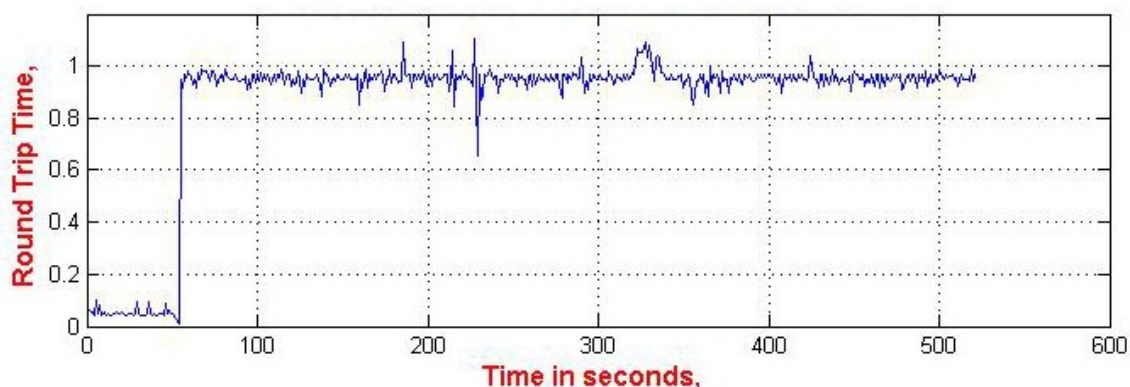


Figure 7.18 The effect of LOIC on the SSL Round Trip Time

This figure shows the effect of attacking an SSL VPN with an LOIC DOS on the Round Trip Time. A quick look shows that the average value of the RTT from the first second until second (200) at most is lower than the values under attack. The increase in the RTT is clearly due to the attack.

Table (7.4) shows the average effect of applying a DOS attack on the Round Trip Time, which makes the calculations more realistic and based on the average values. Attention should be given to the fact that the average difference is calculated based on formula (1), and the average impact is calculated using formula (2).

Attack Tool	Before attack			Under Attack			Average Difference	Average Impact
	Min	Max	AV	Min	Max	AV		
Slowloris	0.045	1.017	0.490	0.004	20.88	0.538	0.047	9.7%
Smurf6	0.041	1.221	0.330	0.003	3.480	0.565	0.235	71.2%
LIOC	0.008	1.093	0.720	0.657	1.105	0.955	0.234	32.6%

Table 7.4: The Average Impact of a DOS Attack on the SSL VPN RTT

7.3 Attacking VPN protocols with MITM Attack

The attack procedures are explained in Chapter 6 and here the results analysis and discussion are presented. The following tables show the results of attacking VPN protocols (PPTP and SSL) with an MITM attack using different tools. Each table shows the results of one tool. The same procedure was carried out on the two protocols.

7.3.1 Attacking PPTP with an MITM

Tables (7.5), (7.6) and (7.7) statistically demonstrate the successful processes and the fail processes clearly after attacking SSL VPN with different tools (Ettercap, Cain and Abel, Subterfuge). Note that the letters in the following tables have the following meanings:

S: Success, F: Fail, E: Encrypted (the passwords sniffed were encrypted), C: Clear Text (not encrypted).

Ettercap vs. PPTP				
Network	ARP Poisoning	Sniffing	Data Sniffed	Attack Result
LAN	S	S	E	S

Table 7.5 Attacking PPTP with an MITM using Ettercap

Cain and Abel VS. PPTP				
Network	ARP Poisoning	Sniffing	Data Sniffed	Attack Result
LAN	S	S	E	S
WAN	S	S	E	S

Table 7.6 Attacking PPTP with an MITM using Cain and Abel

Subterfuge VS. PPTP				
Network	ARP Poisoning	Sniffing	Data Sniffed	Attack Result
LAN	F	-----	-----	F
WAN	F	-----	-----	F

Table 7.7 Attacking PPTP with an MITM using Subterfuge

7.3.2 Attacking SSL with an MITM

Tables (7.8), (7.9) and (7.10) statistically demonstrate the successful process and fail process clearly after attacking SSL VPN with different tools (Ettercap, Cain and Abel, Subterfuge). Note that the letters in the following tables have the following meanings:

S: Success, F: Fail, E: Encrypted (the passwords sniffed were encrypted), C: Clear Text (not encrypted).

Ettercap VS. SSL				
Network	ARP Poisoning	Sniffing	Data Sniffed	Attack Result
LAN	S	---	---	F

Table 7.8 Attacking SSL with an MITM using Ettercap

Cain and Abel VS. SSL				
Network	ARP Poisoning	Sniffing	Data Sniffed	Attack Result
LAN	S	S	C	S
WAN	S	S	C	S

Table 7.9 Attacking SSL with MITM using Cain and Abel

Subterfuge VS. SSL				
Network	ARP Poisoning	Sniffing	Data Sniffed	Attack Result
LAN	F	---	---	F
WAN	F	---	---	F

Table 7.10 Attacking SSL with an MITM using Subterfuge

7.4 Attacking VPN protocols encryption

This attack methodology has different kinds of attack because of the different nature of encryption and different authentication algorithms in each protocol. For example, PPTP uses MS-CHAPv2 for authentication and 3DES for encryption, while SSL has different algorithms for these procedures.

7.4.1 Attacking PPTP VPN Encryption

As mentioned in Section 6.3.1, two types of attack have been applied to the PPTP VPN to break the MS-CHAPv2 encryption either by using the Dictionary attack (with the Chap2asleap script and the Asleap tool) or by using a Brute Force attack (with Chapcrack and cloudcracker.com). The following table describes the result of these attacks in detail.

Attacking PPTP MS-CHAPv2				
Attack Type	Success Rate	Time Needed	Maximum Time	Attack Result
Dictionary	50 – 80 %	10 Sec	Minutes	Success
Brute Force	100 %	15 Hour	24 Hour	Success

Table 7.11 Attacking PPTP VPN Encryption

It is clear that our two attacks are successfully done. For the Dictionary attack, it is necessary to note that the success rate is based on a number of factors, such as the complexity of the password hash, the Dictionary list and attacker computer speed. Nevertheless, these are still very fast relative to the Brute Force attack, where all possible probabilities must be attempted. Finally, this experiment proved that the MS-CHAPv2 for the PPTP VPN can be easily and successfully defeated with the appropriate tools.

7.4.2 Attacking SSL VPN Encryption

The SSL VPN passwords were attacked with different methods from those which were used to attack the PPTP VPN because of the difference in the components of the protocols and encryption algorithms (see 6.3.2). Two attacks were applied against the SSL VPN to steal the secret passwords or secret information either by forcing the HTTP connection and losing the encryption (such as in the SSL strip attack) or by attacking the server cookies (such as in the Heartbleed attack). The following table describes the results obtained after applying those attacks.

Attacking SSL VPN				
Attack type	Success Rate	Sniffing	Data Sniffed	Attack Result
SSL strip	60-90%	Success	Clear Text	Success
Heart bleed	50 %	Fail	---	Fail

Table 7.12 Attacking SSL VPN Encryption

7.5 VPN Protocols Comparison (PPTP vs. SSL)

To make the comparison fairer, the two protocols were compared with the equivalent attacks that can be applied to both. Then, the average of the vulnerability to the other attacks was taken as some of them can be applied to PPTP only and others to SSL only. Finally, a simple analysis was carried out based on the results of the comparison. Appendix A shows a comparison table for the PPTP and SSL VPN after applying a DOS and an MITM attack, which were applied to both protocols, while Table (7.13) shows the average vulnerability to different attacks on PPTP and SSL VPNs.

Attack type	PPTP	Attack Type	SSL
Dictionary Attack	Vulnerable	SSL Strip Attack	Vulnerable
Brute Force Attack	Vulnerable	Heart Bleeding Attack	Not Vulnerable
DOS Attack	Vulnerable	DOS Attack	Vulnerable
MITM Attack	Vulnerable	MITM Attack	Less than 50%

Table 7.13 Average Vulnerability for Different Attacks on PPTP and SSL

It is clear that SSL has more resistance against these attacks under specific conditions on average. It is important to mention here that the average vulnerability against a DOS and an MITM attack in the previous table is based on the following simple statistics:

- For a DOS attack: If we go back to the results from Tables (7.1) and (7.2) and based on average of results, we produce the following table:

Protocol Type	Success	Fail
PPTP	2	1
SSL	2	1

Table 7.14 Average of DOS Attack Results for PPTP and SSL

- For an MITM attack: If we return to the results from Tables (7.5-7.10) and based on averages of results, we produce the following table:

Protocol Type	Success	Fail
PPTP	3	2
SSL	2	3

Table 7.15 Average of the MITM Attack Results for PPTP and SSL

More details can be calculated from the charts in Figures (7.19-7.21) which show the effects of a DOS attack using different tools on the two VPN networks:

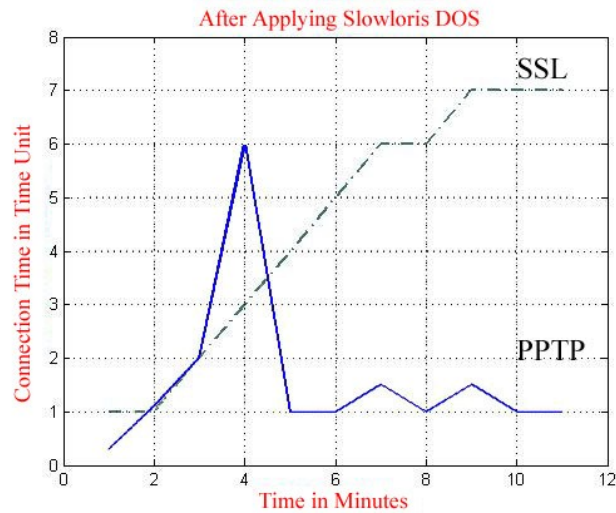


Figure 7.19 Effects of the DOS using Slowloris on SSL and PPTP

The previous figure shows the difference in impact of the Slowloris DOS on the connection time between PPTP and SSL. At minute (2), the SSL graph shows a ramp increase until minute (4), where it attempts to maintain its value at minute (4), and then decreases the same way to near the average value, due probably to the Windows 2008 Server having started using virtual memory to recover the lack of memory due to the Slowloris attack. A quick look at this figure enables us to see the difference in impact clearly, most notably that SSL was more affected than PPTP.

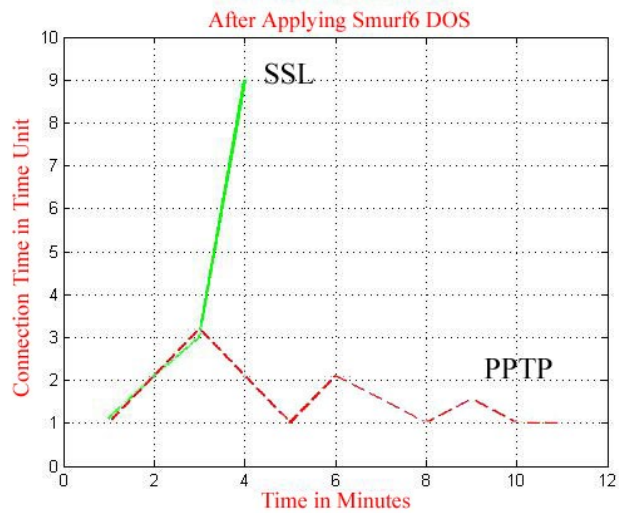


Figure 7.20 Effects of the DOS using Smurf6 on SSL and PPTP

Figure (7.20) repeats the same scenario but with some differences. For example, PPTP here reached its peak value at minute (3) and it was (3 time units). Later, step by step it decreased to be near to the average value. On other hand, SSL has a rapid increase between (minute 2 and minute 4), where it reached its peak value; then later the connection stops.

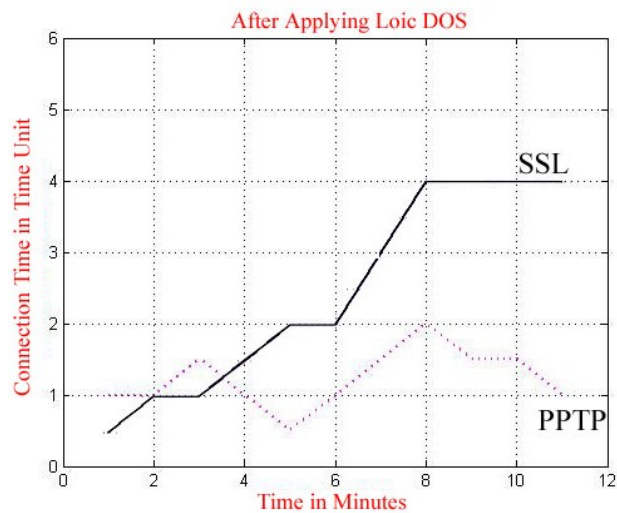


Figure 7.21 Effects of a DOS using LOIC on SSL and PPTP

Again an LOIC DOS shows low impact on both SSL and PPTP with a clear difference that can be easily calculated from the previous chart SSL is still more affected than PPTP.

Moreover, the following figures show simple comparisons between the two protocols in terms of the impact of DOS attacks on the transfer rate of data through tunnels.

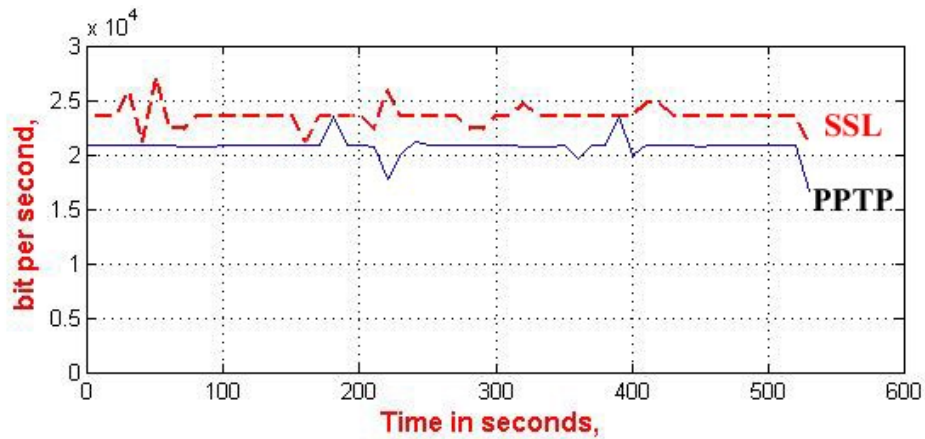


Figure 7.22 Effects of Slowloris on the transfer rate in SSL and PPTP

As can be clearly seen in this figure, the PPTP has a lower transfer rate on average than SSL, whose transfer rate measured approximately (17 Kbps), while SSL measured at a rate of approximately (25 Kbps) in this graph. In addition, the PPTP was more affected by the Slowloris DOS in terms of transfer rate.

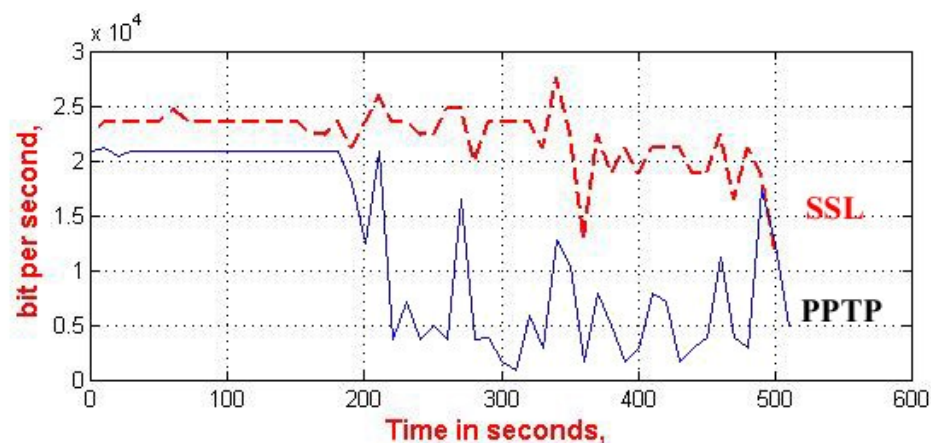


Figure 7.23 Effects of Smurf6 on transfer rate in SSL and PPTP

Similarly, both SSL and PPTP were affected by Smurf6, as can be clearly seen in Figure (7.23). However, generally PPTP was more affected here than SSL in terms of transfer rate.

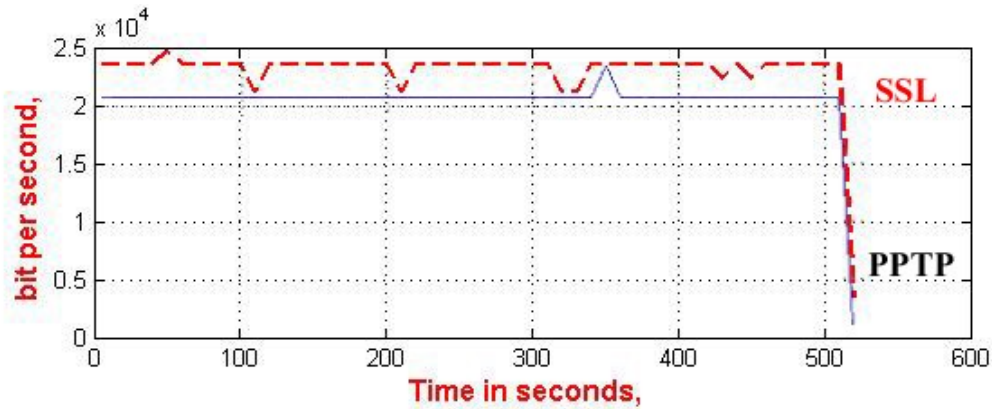


Figure 7.24 Effects of LOIC on the transfer rate of SSL and PPTP

The effect of the LOIC attack here is small and on average, SSL here is slightly more affected on average. After (200s), the effect of the LOIC is found. Finally, the following figures show a simple comparison based on the effect of the DOS attack on the Round Trip Time:

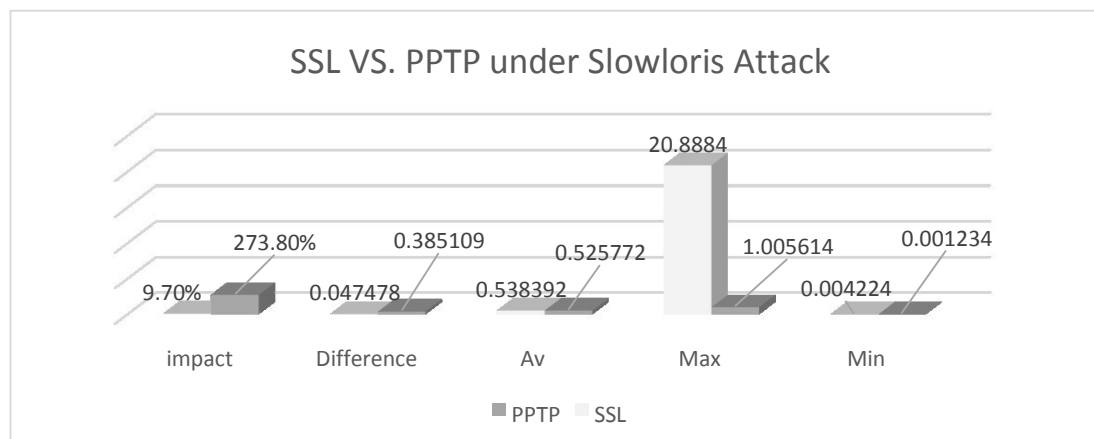


Figure 7.25 SSL vs. PPTP based on the effect of Slowloris on RTT

As can be clearly seen in this figure, PPTP has a higher RTT on average than SSL. Its maximum value was approximately (20), while SSL has a value of approximately

(1) in this graph; thus, PPTP was more affected by Slowloris DOS in terms of Round Trip Time.

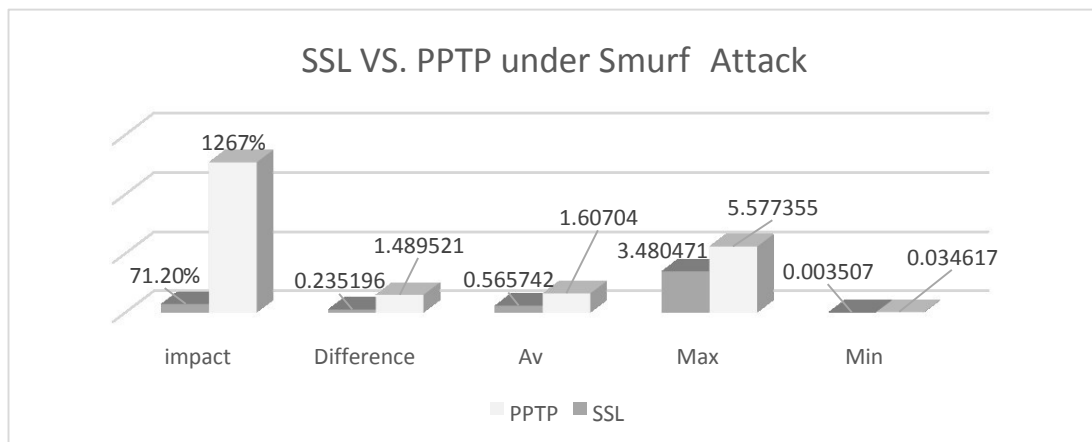


Figure 7.26 SSL vs. PPTP based on the effect of Smurf6 on RTT

It is clearly seen in this figure that PPTP has a higher RTT on average than SSL, whose maximum value measured at approximately (5.5), while SSL yielded a value of approximately (3.4) in this graph; thus, PPTP was more affected by Slowloris DOS in terms of Round Trip Time.

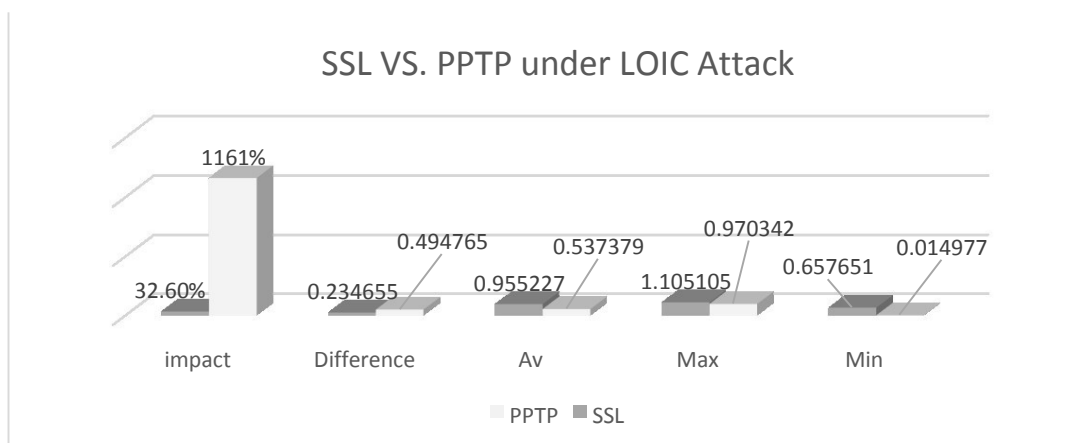


Figure 7.27 SSL vs. PPTP based on the effect of the LOIC on RTT

In this figure, PPTP has a higher RTT on average than SSL, whose maximum value was approximately (0.9), while SSL yielded a value of approximately (1.1) in this graph. Thus, PPTP was more affected on average, by LOIC DOS in terms of Round Trip Time.

CHAPTER 8

Conclusions, Recommendations and Future Works

8.1 Conclusions

The VPN has become one of the most attractive technologies of networking and communications, and it was developed to cover the different needs of secure communication.

A VPN is a group of computers owned by a single foundation which can be classified into two kinds: Site-to-Site and Remote Access. Remote Access is more vulnerable to attacks. Different types of VPN protocols are available. IPsec, PPTP, L2TP and SSL are some of the more famous VPN protocols, and some protocols encrypt data (payloads) in packets only, while others encrypt both the header and payload to provide more security for information. Different types of attacks can be applied against VPNs, which vary between slowing down the network, sniffing secret information and even service denial. DOS, MITM and Cryptanalysis are some of the more famous attacks against networks, especially VPNs. For this work, two types of VPN, namely SSL and PPTP were established and virtually emulated using GNS3 and VMware tools as a virtual environment. Different types of attack had been applied on these networks and were used for vulnerability test purposes.

From the results of these attacks on SSL and PPTP, some important results appeared:

- Attacking PPTP with a DOS using Slowloris, Smurf6 and LOIC showed higher impacts during the first 5 minutes while it was establishing connections to the server. Later it dropped. Figures 7.1-7.3 show a greater number of connections at a time and gave more impact, while attacking SSL with DOS using the same tools showed different behavior. The impact continued increasing with time, (Figures 7.4-7.6).

- PPTP less effected than SSL in terms of connection time, while SSL was more robust in terms of RTT and transfer rate.
- Attacking PPTP and SSL with an MITM attack using Ettercap, Cain and Abel, and subterfuge showed that PPTP has more resistance to an MITM attack than SSL under the same conditions on average (Tables 7.3-7.8).
- PPTP MS-CHAPv2 can be Dictionary attacked with a 50-to-80-percent success rate depending on password lists and attacker machine resources.
- PPTP MS-CHAPv2 can be attacked using Brute Force attack techniques with a 100-percent success rate taking a maximum of 24 hours depending on the complexity of the password; thus, PPTP is fully vulnerable to this attack.
- Attacking SSL with SSL strip showed that it is vulnerable to this attack nearly 80 percent of the time, thus it was generally vulnerable.
- SSL was not vulnerable to a Heart Bleeding attack, as shown in 6.3.2.2.
- Both SSL and PPTP are vulnerable to an MITM attack when the Cain and Abel tool was used, but data sniffed from PPTP was still encrypted while SSL data was sniffed in clear text; thus, PPTP is still more secure than SSL against an MITM attack.
- Based on the average number of attacks that are applied to both SSL and PPTP protocols, PPTP was more vulnerable to attack than this version of SSL.
- More password complexity provides more security. As shown in this work, decrypting encrypted passwords is based on the complexity of passwords and other factors (capability of attacker machine and password lists if dictionary attacked); thus, using passwords with letters (in upper and lower case), numbers and special characters (such as @ # \$ & . etc.) The high number of characters increases robustness against some attacks, especially the Brute Force attack.

- Increasing the encryption bits causes an increase in robustness, but in balance with performance, more encryption and complexity leads to lower speed and performance.
- Establishing a VPN without firewalls makes it less immune to attacks (especially DOS attacks).
- The use of digital certificates increases the security of a VPN network and makes it more resistant to some attacks (especially an MITM attack and SSL Strip).

8.2 Recommendations

Based on this work and its results, some recommendations and alerts can be concluded to keep a VPN more secure or even help to increase security resistance against common attacks that may be encountered on the Internet:

- The use of firewalls to become more resistant against some DOS attacks, especially those that use smart filters with DMZ.
- Control the connection time for each connection thread to a server to avoid an application layer DOS attack.
- Use complex passwords with higher encryption bit numbers and different characters to increase immunity against encryption attacking.
- Use digital certificates to decrease the effect of an MITM attack on the network.
- Control the SSL server so it does not accept being forced to work with older version protocols or insecure connections to avoid the danger of an SSL Strip attack.
- Keep remote computers updated with new antivirus and antispyware tools and avoid any connection with public networks as much as possible in addition to avoiding the attack of viruses or Trojans that can sniff connection information of a VPN which is saved on that machine.

8.3 Future Works

According to the results of this thesis, two main common problems are still found in networks and in VPNs especially. The first is the ARP poisoning and DNS spoofing. This problem needs more study to find suitable solutions that disallow attackers from sending messages to broadcast addresses by telling that this machine is the gateway or others.

The second important issue is finding solutions that enable other parties to communicate with SSL servers without the need to force them to work with older versions or in an unsecure state.

REFERENCES

1. **Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee and Alexander Schmid, (1999),** “*A Comprehensive Guide to Virtual Private Networks*”, International Technical Support Organization, IBM.
2. **Charlie Scott, Paul Wolfe, and Mike Erwin (1999),** “*Virtual Private Networks*”. O'Reilly Media, Inc.
3. **Net Gear Inc., (2005),** “*Virtual Private Network Basics*”, Chapter 2.
4. **Mijlud M. Alsbabayee, (2005),** “*Theoretical and Practical Virtual Private Networks*”.
5. **Roy Hills, (2005),** “*Common VPN Security Flows*”, NTA Monitoring Ltd.
6. **Rainer Enders and Clint Stewart., (2011),** “*Debunking the Myths of SSL VPN Security*”, NCP.
7. **Koen Van Besien, (2006),** “*Implementation of VPN Network (Master Thesis)*”, NCP.
8. **Martin Hack and EVP, (2011)** “*Remote Access Challenges, Top 7 Remote Access Myths*”, NCP Engineering, NCP Secure Communications.
9. **Special Administrative Region, (2008),** “*VPN Security*”, **Hong Kong government.**

10. **Steve Pitts, (2004)**, “*VPN Aggressive Mode PSK Brute Force Attack*”, SANS Institute.
11. **Kevin Benton and Ty Bross, (2012)**, “Timing Analysis of SSL/TLS Man In The Middle Attack”,
12. **Gopy Nath Nayak and Shafalika Ghosh Samaddar, (2010)**, “*Different Flavors of Man in the Middle Attack, Consequence and Feasible Solutions*”, Motial Nehru National Institute of Technology, Allahabad, India.
13. **Syngress.com, (2005)**, “*Advance VPN Concepts and Tunnel Monitoring*”, Chapter 5.
14. **Equinox AG and Equinox USA, (2005)**, “*VPN Configuration Guide*”.
15. **Chris Wilson, (2005)**, “*GNS3 Simulation Guide*”, Packt Publishing.
16. **Duane Norton, (2004)**, “*An Ettercap Primer*”, SANS Institute.
17. **Alexandre Borges, (2014)**, “*How To Perform Heart Bleed Attack*”,
18. **Microsoft, (2014)**, “*Point To Point Tunneling Protocol (PPTP) Profile*”, Microsoft.
19. **James S. Tiller, (2001)**, “*Security of Virtual Private Networks*”.
20. **(2001)**, “*ICMP Attack Illustrated*”, SANS Institute.
21. **Hawke Robinson, (2002)**, “*Microsoft PPTP VPN Vulnerabilities Exploits in Action*”, SANS Institute.

22. **Mirkuvie and Peter Reiher, (2004)**, “*A Taxonomy of DDOS Defense Mechanisms*”.
23. **Ralph J. Notraro, (2011)**, “*IPsec and PPTP VPN Exploit*”, Minnesota State University.
24. **Bharin Bharat Bhansali, (2001)**, “*Man in the Middle –A Brief*”, SANS Institute.
25. **Seung Yeob Nam, Dongwon Kim and Jeongeun Kim, (2010)**, “*Preventing ARP Poisoning Based Man In The Middle Attacks*”.
26. **ADC Monthly Attack Analysis, (2012)**, “*Denial of Service Attack, a Comprehensive Guide to Trend, Technique and Technology*”, EMPERVA.
27. **John E. Canavan, (2005)**, “*Fundamentals of Network Security* ”,.
28. **Nebrija University, (2007)**, “*Cain and Abel v 2.5 Password Cracking via ARP Poisoning Attack*”, Madrid.
29. **Bruce Schneier and Mudge, (2005)**, “*Cryptanalysis of Microsoft Point to Point Tunneling Protocol (PPTP)*”.
30. **Peter Burkholder, (2002)**, “*SSL Man in the Middle Attacks*”, SANS Institute.
31. **Eman Salem ALashwali, (2013)**, “*Cryptographic Vulnerabilities in Real Life Web Server*”, King Abdul-Aziz University, KSA.
32. **Amir Herzberg and Haya Shulman, (2009)**, “*Stealth MITM DOS Attacks on Secure Channels*”.

33. **Rolf Oppliger, Ruedi Rytz and Thomas Holderegger, (2009)**, “*Internet Banking: Clint Side Attacks and Protection Mechanisms*”.
34. **Lan Green, (2005)**, “*DNS Spoofing By Man In The Middle*”, SANS Institute.
35. **Christopher M Shields and Matthew M. Toussain, (2005)**, “*Subterfuge the MITM Framework*”.
36. **CISCO , (2005)**, “*IP Tunneling and VPNs*”,
37. **Byeong-Ho Kang and Maricel O. Balitanas, (2009)**, “*Vulnerabilities of VPN using IPsec and Defensive Measures*”, University of Tasmania, Australia, Hannam University.
38. **Neon Surge, (2005)**, “*Understanding PPTP and VPN's*”, Rhino9 Publications.
39. “*Setting up a Virtual Private Network (VPN)*”, UABS University, Ukraine. Available from: <http://study2.uabs.edu.ua/files/domb95735r.pdf>. [23 July 2015].
40. **Darshina Patel**, “*Study as if You Have not Reached Your Goal*”, (July 6, 2010). Available from: <http://kellystarpurl.blogspot.com.tr/2010/07/internet-refers-to-world-wide.html>. [23 July 2015].
41. “*Remote Access VPN*”, Computer and Network Security, (January 27, 2012). Available from: <http://rtfq.net/security/firewall-pages/quick-and-dirty-vpn/remote-access-vpn>. [23 July 2015].
42. **Evgeniia Gromyko**, “*Investigation of Digital Certificates Verification of Reliability and Resistance to External Attacks*”, Bachelor’s Thesis in Information Technology, May 2014.

43. **Oberdiessbach**, "*MD5 - Message Digest (Fingerprint, Checksum)*", Akadia Global Competence in Today's Information Technology, Available from: <http://www.akadia.com/services/md5.html>. [23 July 2015].
44. **Thayathorn Phokaphet**, "*Information Security*", Security Blogspot, (19 march 2015). Available from: <http://it02-security.blogspot.com.tr>. [23 July 2015].
45. "*What is a Digital Certificate, and Why Do You Need One?*", Comodo Group, Inc. (2015). Available from: <https://www.comodo.com/resources/small-business/digital-certificates4.php>. [23 July 2015].
46. **Hakan Uzun**, "*VPN (Virtual Private Network) What is it?*", (July 22, 2015). Available from: <http://www.hakanuzuner.com/index.php/vpn-virtual-private-network-nedir.html> . [23 July 2015].
47. Andrew Mason, "*IPSec Overview Part Two: Modes and Transforms*", Cisco Press, (Feb22,2002). Available from: <http://www.ciscopress.com/articles/article.asp?p=25477>. [August 2, 2015].
48. "*IPsec & IKE*", VPN R76 Administration Guide, (27 August 2014). Available from: https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13847.htm. [23 July 2015].
49. "*What is VPN?*", Microsoft (2015). Available from: [https://technet.microsoft.com/nl-nl/library/cc739294\(v=ws.10\).aspx](https://technet.microsoft.com/nl-nl/library/cc739294(v=ws.10).aspx). [23 July 2015].

50. **Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki,** "*Distributed Denial of Service Attacks*", National Technical University of Athens, The Internet Protocol Journal - Volume 7, Number 4. Available from: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html. [23 July 2015].
51. **Santosh Sumar,** "*What is Man In The Middle or MITM Attack*", Spirit of the Grey Hat Blogspot. Available from: <http://spiritofthegreyhat.blogspot.com.tr/2014/05/what-is-man-in-middle-or-mitm-attack.html>. [23 July 2015].
52. **King Kan,** "*The Detection and Prevention, Web Application Attacks the New Format by Enforcing Hypertext Transfer Protocols*", (25 February 2007). Available from : <http://amkingkan.blogspot.com.tr/2014/02/blog-post.html>. [23 July 2015].

APPENDIX A

Attack Type	Attack Tool	PPTP					SSL			
		Connection Success		Connection Time	Speed		Connection Success		Connection Time	Speed
DOS	Slowloris	X		X	-		X		X	X
	Smurf6	X		X	-		X		X	X
	LOIC	-		-	-		-		-	X
MITM	Attack Tool	NET	ARP Poisoning	Sniffing	Data Sniffed	Attack Success	ARP Poisoning	Sniffing	Data Sniffed	Attack Success
	Ettercap	L	S	S	E	S	S	F	F	S
		W	S	F	F	F	F	F	F	F
	Cain and Abel	L	S	S	E	S	S	S	C	S
		W	S	S	E	S	S	S	C	S
	Subterfuge	L	F	F	F	F	F	F	F	F
		W	F	F	F	F	F	F	F	F

Total results comparison table for SSL and PPTP under MITM and DOS attacks , L : LAN , S : Success , E : Encrypted W : WAN , F : Fail , C : Clear Text , X : Affected

APPENDIX B

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: ALJADIR Taha

Date and Place of Birth: September, 1982

Email: tahatx@yahoo.com

EDUCATION

Degree	Institution	Year of Graduation
B.Sc.	Technical University , Mosul	2004
High School	Al-Zuhur High school	2000

WORK EXPERIENCE

Year	Place	Enrollment
2011	Computer Engineer	Specialist
2009	Alhadbaa University	Lecturer
2005	Global Art for TV Production	Graphic Designer

LANGUAGES

Arabic, English, Beginner Turkish

HOBBIES

Succor, Travel, Books, Swimming, Fitness