AN OVERVIEW OF NETWORK PENETRATION TESTING

Chaitra N. Shivayogimath[1]

[1]*PG Student, Dept. of ECE, AMC Engineering College, Bangalore, Karnataka, India*

Abstract

Penetration testing is a well known method for actively evaluating and assessing the security of a network or an information system by simulating an attack from an attacker's perspective. A penetration tester must necessarily follow certain methodology so as to successfully identify the threats faced by an organization's network or information assets from a hacker and reduce an organization's IT security costs by providing a better return on security investments. This paper gives an overview of methodology of penetration testing and the tools used.

***Keywords** - Network Penetration Testing, Hacker, Vulnerability, Exploit, Security.*

--***--

1. INTRODUCTION

Penetration testing is a well known method for actively evaluating and assessing the security of a network or an information system by simulating an attack from an attacker's perspective. A penetration tester must necessarily follow certain methodology so as to successfully identify the threats faced by an organization's network or information assets from a hacker and reduce an organization's IT security costs by providing a better return on security investments. This paper gives an overview of methodology of penetration testing and the tools used.

This authorized attempt to evaluate the security of a network or an infrastructure by safely attempting to exploit the vulnerabilities helps in finding the loop holes in the network. These loopholes may allow an attacker to intrude and exploit the vulnerabilities.

Penetration tests can have serious consequences for the network on which they are run. If it is being badly conducted it can cause congestion and systems crashing. In the worst case scenario, it can result in the exactly the thing it is intended to prevent. This is the compromise of the systems by unauthorized intruders. It is therefore vital to have consent from the management of an organization before conducting a penetration test on its systems or network. [4]

1.1 Necessity of Network Penetration Test

1. The IT infrastructure is becoming more complex and wider. The internal networks have been given access over the internet to the legitimate users along with the user credentials and the privilege level, of course located outside the firewall. This increases the surface of attack. Such infrastructure needs to be assessed regularly for security threats.
2. Identification of what type of resources are exposed to the outer world, determining the security risk involved in it, detecting the possible types of attacks and preventing those attacks.

1.2 Benefits of Penetration Testing

1. Proactive identification of the criticality of the vulnerabilities and false positives given by the automated scanners. This helps in prioritizing the remedy action, whether the vulnerability is to be patched immediately or not based on the criticality.
2. Penetration testing helps complying the audit regulatory standards like PCI DSS, HIPAA and GLBA. This avoids the huge fines for non-compliance.
3. A security breach may cost heavily to an organization. There may be a network downtime leading to a heavy business loss. Penetration testing helps in avoiding these financial falls by identifying and addressing the risks. [4]

Depending on the needs, there are two types of penetration testing.

1. External Penetration Test – This test shows what a hacker can see into the network and exploits the vulnerabilities seen over the internet. Here the threat is from an external network from internet. This test is performed over the internet, bypassing the firewall.
2. Internal Penetration Test – This test shows risks from within the network. For example, what threat an internal disgruntled employee can pose to the network. This test is performed by connecting to the internal LAN.

Depending on the knowledge, there are three types of penetration testing, Black box, White box and Gray box. [6]

1. Black Box – This test is carried out with zero knowledge about the network. The tester is required to acquire knowledge using penetration testing tools or social engineering techniques. The publicly available information over internet may be used by the penetration tester.
2. White Box – This test is called complete knowledge testing. Testers are given full information about the target network. The information can be the host IP addresses, Domains owned by the com-

pany, Applications and their versions, Network diagrams, security defenses like IPS or IDS in the network.

3. Gray Box – The tester simulates an inside employee. The tester is given an account on the internal network and standard access to the network. This test assesses internal threats from employees within the company.

2. STEPS IN PENETRATION TESTING METHODOLOGY

2.1 Preparation for a Network Penetration Test

To carry out an exhaustive penetration testing and make it a success, there should be a proper goal defined for a penetration tester. A meeting between the penetration tester and the organization which requires a penetration test must be held. The meeting should clearly define the scope and the goal of the test. The network Diagram must be provided to the Pen tester* in case of a white box penetration testing to identify all the critical devices which require penetration testing to be done, this is not required in case of a black box test.

Another important agenda of the meeting should be the time window and the duration of the test. The organization must clearly define the time window which may be its non-business hours. This is to ensure that the Pen tester is not interrupted and also the business of the organization is unaffected. Due to the unusual traffic usage by the pen test may cause network congestion or may bring down the network by crashing the systems. For instance, a Denial –Of- Service test carried out on an online payment gateway may cause the disruption in the network and causing inconvenience to the customers thereby incurring loss to the organization.

Pen tester should make sure that any information or data obtained during the test should be either destroyed or kept confidential. This is a very important precaution to be taken. The organization can sue the pen testers otherwise.

2.2 The Important Steps followed in an Exhaustive Penetration Testing

2.2.1 Reconnaissance or Information Gathering

This is a very important step a Pen tester must follow. After the pre planning and the goal definition, the pen tester must gather as much information as possible about the target network. Important to note, this is the case when it is a black box testing and when the organization has not provided any information to the tester.

A Pen tester must gather information from an attacker's perspective. Anything that is useful to attackers is necessary to be collected:

- Network Diagrams
- IP Addresses
- Domain names
- Device type
- Applications and their versions.
- Security defenses such as IDS, IPS.

To gather this information we look into:

a. Google & Social or professional networking websites
b. Monster.com
c. IP Registries
d. DNS Registrars
e. The Company's website.

2.2.1.1 Google & Social or Professional Networking Websites:

Search with the keyword along with the company name. The relevant information from the search results can be selected. For instance, search with the keyword 'ASA firewall' with the company name 'Demo Bank'. A LinkedIn profile of an employee working at Demo Bank can be obtained as the search result. By this we can get to know that Demo bank's network comprises of ASA Firewall. Resumes of the employees give out lot of information.

2.2.1.2 Monster.com:

Lot of information can be obtained from the Job Sites. Search with the company name and the list of search results appear, which gives information regarding the network devices or the applications using which the company's network infrastructure is built.

2.2.1.3 IP Registries:

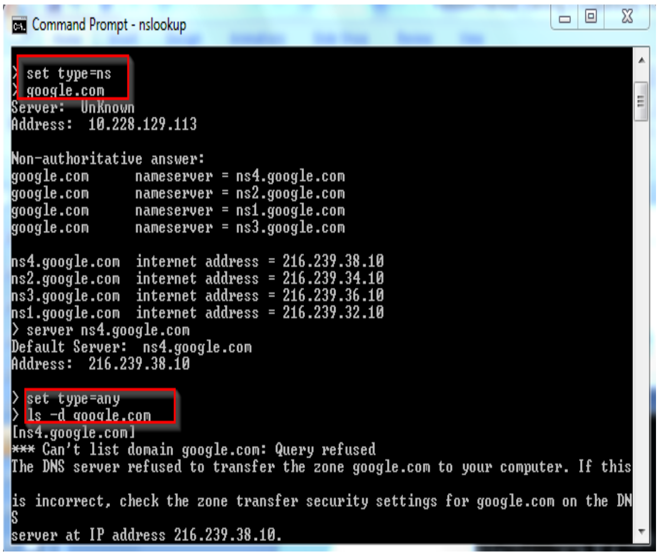
When the IP Addresses are not provided by the organization, the Pen tester has to find out the block of IP addresses belonging to the organization. IP Address registries help us in finding them.

- ARIN – American Registry for Internet Numbers. US Region.
- RIPE - Réseaux IP Européens. Is a collaborative forum open to all parties interested in wide area IP networks in Europe.
- APNIC – Asia Pacific Network Information Centre. Asia Pacific region.

For instance, to find the block of IP addresses belonging to Google. Enter the key word Google in http://whois.arin.net/ui. [1][5]

2.2.1.4 DNS Registrars:

Use the Whois.net or any other whois databases to find all the sub domains. Nslookup is another windows tool to find the IP addresses associated with the given domain name, to find the name server and for zone transfers. An example is as shown in the screenshot below.



```
> set type=ns
> google.com
Server:  UnKnown
Address:  10.228.129.113

Non-authoritative answer:
google.com      nameserver = ns4.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns3.google.com

ns4.google.com  internet address = 216.239.38.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns1.google.com  internet address = 216.239.32.10
> server ns4.google.com
Default Server:  ns4.google.com
Address:  216.239.38.10

> set type=any
> ls -d google.com
[ns4.google.com]
*** Can't list domain google.com: Query refused
The DNS server refused to transfer the zone google.com to your computer. If this

is incorrect, check the zone transfer security settings for google.com on the DN
S
server at IP address 216.239.38.10.
```

Fig 1- NSLookup

The table below summarizes the tools required for this phase.

Table 1: Reconnaisance

Techniques	Open Source search	Name, admin, IPaddresses, name servers	DNS Zone transfer
Tools	Google search engine	Whois ARIN APNIC	Nslookup ls –d Dig deeper Sam spade

2.2.2 Scanning [1]:

Scanning is a method for bulk target assessment. To discover the live IP addresses in the network, to discover the open ports on the machines, to fingerprint the services and to detect the vulnerabilities which is done by the vulnerability scanners.

2.2.2.1 Live IP Discovery:

There are various tools for scanning a network like Nmap, Hping2, and Netcat. Nmap is most popular and favorite tool of Pen testers. Nmap is available for both Linux and Windows. Download the command-line utility for Nmap from [8] and run the required commands for Live IP discovery from the command prompt.

The four basic approaches for live IP discovery are:

- Ping each IP for a response (ICMP)
- Send SYN packets to popular ports
- Send SYN packets to all 64K ports
- Send SYN packets to a few specific ports

ICMP Ping Scan:

This involves sending ICMP Echo request to each IP address. If an ICMP Echo response is obtained, then the IP is live. This scan is performed by the usage of the nmap command:

Nmap –sP <IP_RANGE>

Here –sP is the nmap switch for ping scan.

But, most of the firewalls block ICMP packets. This scan fails if the above said condition prevails.

Popular Ports SYN Scan:

This scan sends SYN packets to only 1024 popular ports. SYN packets will not be blocked by a firewall unlike ICMP ping packets, so this scan is reliable than Ping scan. Usually there will be at least one popular port listening for services on a host. Hence this scan helps in identifying a live host accurately than Ping scan. This scan is performed by the usage of the nmap command:

Nmap –sS –P0 <IP_RANGE>

Here –sS switch performs the task of sending SYN packets to the target host.

The -P0 tells nmap to treat IP as live even without an ICMP response.

All Ports SYN Scan:

Similar to Popular ports SYN scan, the SYN packets are probed but, for all the 64000 ports. This scan takes longer time than the popular ports scan. Optimizing of the scan should be done by including the maximum round trip time switch. This reduces the time taken to wait for the response for the SYN packet. This scan results in higher accuracy. Certain hosts with obscure ports missed in the popular ports scan will be identified in this scan. This scan is performed by the usage of the nmap command along with optimization:

Nmap –sS –p1-65535 –P0 –max-rtt-timeout <time> <IP_RANGE>

Specific Ports SYN Scan:

SYN packets are probed to specific ports required to scan. While scanning the web application servers we know that port 80 & 443 are commonly used ports to listen services on a web application server. This scan is performed by the usage of the nmap command along with optimization:

Nmap –sS –p80,443 –P0 <IP_RANGE>

Out of the above mentioned scans, all ports SYN scan along with timing optimization is preferred and efficient.

UDP scan may be also performed to make sure that all live hosts are discovered which are listening only over UDP ports. But this takes really longer time and hence not preferred often.

Nmap deduces if a port is open or closed by studying the response to different types of packets. For TCP ports a SYN packet is sent and for UDP a zero byte packet is sent. The table below shows the response from different states of ports. [5]

Table 2: Ports status

	TCP	UDP
Open	SYN-ACK	Silence
Closed	RST or none	ICMP port unreachable

OS and Service Fingerprinting:

OS detection is to be done to know the OS running on the target host, by which known vulnerabilities can be exploited. This is done using the Nmap command:

```
Nmap –O <IP_RANGE>
```

15-16 special packets are sent and the responses are compared against the nmap's database. The nmap database has over 1500 operating systems.

The packets sent by nmap for OS Finger printing are:

- 13 TCP packets – 10 for open ports and 3 for closed ports.
- 1 UDP packet for a closed port.
- 2 ICMP Packets.

Frequently OS fingerprinting fails due to the firewall that drops the packets. Windows fingerprinting is too global and not accurate.

Service fingerprinting is performed to determine the protocol running on the port, the brand of the server and the version of the server.

Nmap performs this by using the switch –sV

```
Nmap –sV –P0 <IP_RANGE>
```

Combining all these scan types and switches in nmap, the best command to finger print service and OS :

```
Nmap –sS –sV –O –P0 –p1-65535 –max-rtt-timeout<time>
<IP_RANGE>
```

2.2.2.2 Vulnerability Scanning:

Once the list of Live IP Addresses is obtained, vulnerability scanning should be scheduled. There are various vulnerability scanners available free and commercially. Nessus is one of the best open source tools for testing potential vulnerabilities. Qualys guard is a commercial vulnerability scanner. [1]

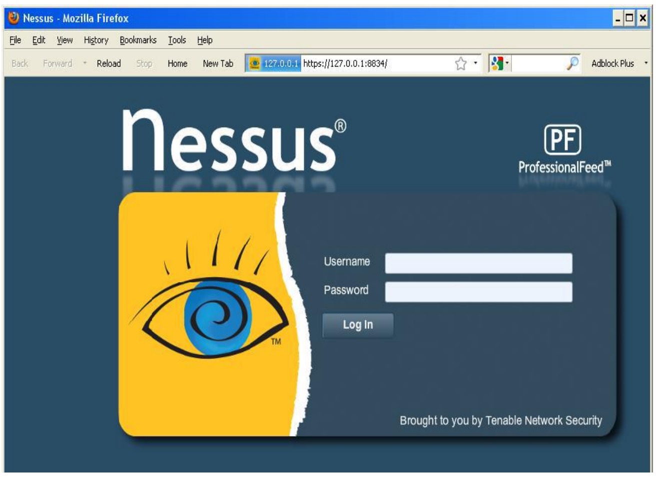
The vulnerability scanners have their own database which is updated periodically with new vulnerabilities found. Download Nessus from [9].

The Nessus project was originally started by Mr. Renaud Darison [5].

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. An activation code is necessary for online plugin update. We can choose offline plugin update as well, which does not require the purchase of an activation code.

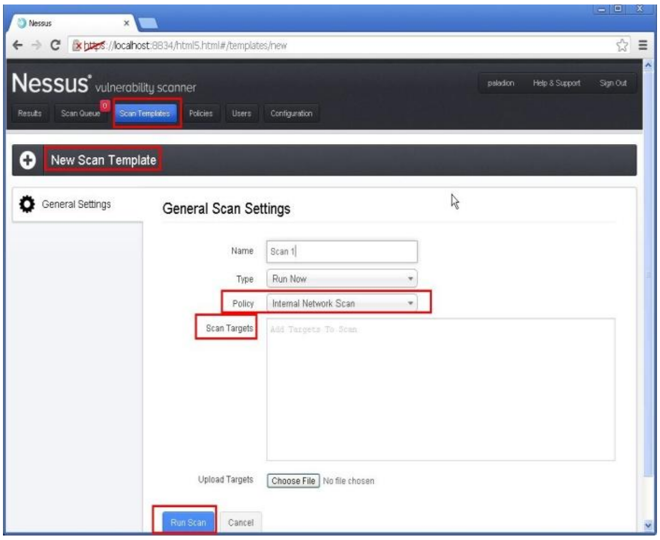
These plugins are written in a special scripting language called "NASL" which is supported by the Nessus engine [7]. NASL stands for Nessus Attack Scripting Language. Basically, plugins are security checks written in NASL. It is a very 'easy to write' scripting language.

The screenshots below show the procedure for nessus scan.



Nessus - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Back Forward Reload Stop Home New Tab
https://127.0.0.1:8834/
Adblock Plus
Nessus®
PF ProfessionalFeed™
Username
Password
Log In
Brought to you by Tenable Network Security

Fig 2. Nessus Login screen



Nessus
https://localhost:8834/html5.html#/templates/new
Nessus vulnerability scanner
paladion Help & Support Sign Out
Results Scan Queue 0 Scan Templates Policies Users Configuration
New Scan Template
General Settings
Choose File
Run Scan Cancel

General Scan Settings

Name: Scan 1

Type: Run Now

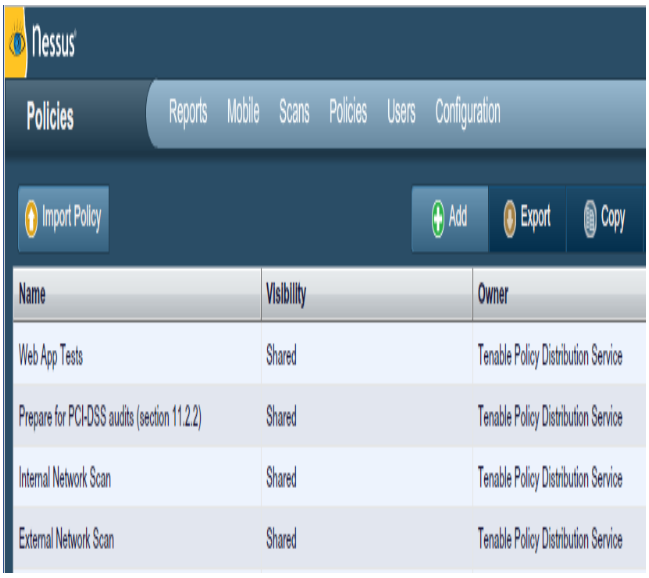
Policy: Internal Network Scan

Scan Targets: Add Targets To Scan

Upload Targets: No file chosen

Fig 3. Scheduling a scan

Appropriate policy is to be selected based on the type of scan (Internal or external). The report generated can be downloaded to the local system from which the scan is preformed.



Name	Visibility	Owner
Web App Tests	Shared	Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2)	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
External Network Scan	Shared	Tenable Policy Distribution Service

Fig 4. Nessus Scan Policy

Apart from the vulnerability scanners, Nmap has the vulnerability scan switch. The following command is to be executed to run the nmap vulnerability scan:

```
nmap -sS -sV -P0 -O -p1-65535 -A -v --max-rate 500 --reason -iL <inputfile.txt> >> <outputfile.txt>
```

The –A switch performs an aggressive vulnerability scan on the target hosts.

The table below summarizes the tools required for this phase. [5]

Table 3: Scanning

Techniques	Ping sweep	TCP/UDP port scan	OS Detection	Vulnerability Scan
Tools	Nmap Fping icmpenum	Nmap Superscan fscan	Nmap Queso	Nessus Qualys Nikto Nmap

2.2.3 Enumeration

In this step the Pen tester actively tries to obtain user names, network share information and application version information of running services. This step is most intrusive scanning since the Pen tester tries to enumerate the valid user accounts and shares information. The table below lists the enumeration tools and techniques. [5]

Table 4: Enumeration

Techniques	List User Accounts	List File shares	Identify applications
Tools	Null sessions DumpACL Sid2usre on-SiteAdmin	Show amount NAT	Banner grabbing by telnet, netcat or rpcinfo

The reported vulnerabilities have to be tested manually and confirmed since the vulnerabilities reported by the scanners may be false positives at times.

There are various tools for testing the vulnerabilities associated with each port. This leads to an extensive penetration testing.

The risk ratings for the findings are assigned as per the owasp risk rating methodology which is given in [10].

3. CONCLUSIONS

A network can never be completely secure. A Pen tester should have the knowledge of how a hacker will work to penetrate the network by finding new loop holes and vulnerabilities. There are zero-day attacks which come up every day. The network should be fully patched with the latest OS and the patches for the software installed. Penetration test should be regularly performed. Every quarterly is a recommended duration of time for an ideal pen test. [3]

Amidst various constraints such as lack of time and improper definition of scope of the project, penetration tester has to carry out the test to the best of the efficiency by making use of the tools well. It is better to have small automation scripts for time consuming tasks.

4. FUTURE SCOPE

Hackers are finding more and different ways everyday to penetrate through the network. There are Zero-day attacks which need lot of time and new tools to be discovered to safe guard the network. There is a requirement to develop new penetration testing tools, than relying on the existing old ones. New methodologies and processes are to be discovered and implemented to make the penetration testing more exhaustive.

REFERENCES

[1]. Timothy P. Layton, Sr. “Penetration Studies – A Technical Overview”. URL: http://www.sans.org/reading-room/whitepapers/testing/penetration-studies-technical-overview-267

[2]. SANS Institute InfoSec Reading Room ” Penetration Testing: The Third Party Hacker ” URL: http://www.sans.org/reading-room/whitepapers/testing/penetration-testing-third-party-hacker-264

[3]. Dave Burrows GIAC Security Essentials Certification (GSEC) Version 1.3 “Penetration 101 – Introduction to becoming a Penetration Tester”
URL: http://www.sans.org/reading-room/whitepapers/testing/penetration-101-introduction-penetration-tester-266
[4]. Chan Tuck Wai “Conducting a Penetration Test on an Organization”
[5]. C. Edward Chow “Penetrate Testing”. http://www.coursehero.com/file/2835086/penetrateTest/
[6]. Anand Sudula, SSA Global Technologies “ Penetration Testing”.
http://www.docstoc.com/docs/36432625/Penetration-Testing-Penetration-Testing-Anand-Sudula-CISA-CISSP-SSA-Global-Technologies
[7]. Hemil Shah “Writing NASL Scripts” URL: http://www.infosecwriters.com/text_resources/pdf/NASL_HShah.pdf
[8]. Nmap download URL: http://www.nmap.org
[9]. Nessus download URL: http://www.tenable.com/products/nessus
[10]. Owasp URL: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

BIOGRAPHIE

Chaitra N. Shivayogimath completed her Bachelor of Engineering from BMS Institute of Technology, Karnataka India in 2011.She is Pursuing Master in Technology at AMC Engineering College, Bangalore, India.She has been certified CE|HV7, by the EC-Council. Her areas of interest are Network Penetration testing, Vulnarability Assessment, Wireless Networks, Computer Networks.