# A Survey on Network Penetration Testing

G Jayasuryapal
Lovely Professional University
Phagwara, India
Suryapal.gandla@gmail.com

P. Meher Pranay
Lovely Professional University
Phagwara, India
Pranaypadamatinti@gmail.com

Harpreet Kaur
Lovely Professional University
Phagwara, India
harpreet.23521@lpu.co.in

Swati
Lovely Professional University
Phagwara, India
rampalswati@gmail.com

2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) | 978-1-6654-1450-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICIEM51511.2021.9445321

***Abstract* - Penetration on network is an important security measurements every company want to take into the consideration. Day-to-Day life as it is seen that cybercrimes are increasing due to lack of security practice. Penetration testing is an outstanding approach where pen tester evaluates the security of network and numerous applications by simulating attacks from attacker's view point .Additionally, penetration testing process follow certain rules and agreement that both the parties ( client and pen testing team). By this testing, the company's weakness will be detected like open servers and open ports etc. so we can take a countermeasure by doing penetration testing on the company. This paper contains some of the important terms and steps to do a strong penetration testing on organizations. Hence, this paper covered all the mechanisms including information gathering to the post exploitation.**

***Key words - Network Penetration Testing, Server Security, Vulnerability examination, External Enumeration***

## I. INTRODUCTION

Penetration testing[1] can be of different types like there is a network penetration testing, web penetration testing, IOT penetration testing, android penetration testing, iOS penetration testing. In this paper, general overview as to how to carry the process starting from information gathering to exploiting the target will be discussed.

The term network means inter link to each other and they can be able to communicate. The network penetration testing means a tester will allowed into the organization and he can be able to access for some of the services and will try to bypass some of the authentications. Furthermore, he tries to compromise the entire server or the organization data center if any vulnerability exists. So, how a researcher will do the organization's testing and what the terms he need to follow as well what tools and what types of tricks he will use we are going to discuss in this paper.

### *A. Fundamental of Network Penetration Test*

1. The Technology and the services [1][8] are increasing day-by-day as the company is ready to provide any type of service to his client as in some cases, they are ready to provide the organization internal access to the client so the company must want to maintain the privilege policy list to present the each client according to their service claiming.
2. Not only the internal and also for the external security purpose organization want to implement the firewall and DNS blacklisting intruders who try to play fraud with the request, will automatically get block by the firewall moreover preventing them to avail any type of service in the future and also the network penetration testing defines a company security strategy so the clients can trust the company so the company can increase the repudiation.

### *B. Advantage of Penetration Testing in Companies*

There are a lot of benefits of conducting penetration testing on the organizations.

- Server can be examined and if any vulnerability find on server like unused open ports or any service misconfiguration can be disclosed and the company will be in safe hands.
- If you are secure and offering a very good service to the clients, then the companies' repudiation will increase.
- So, a strategic penetration test will ensure users and prevent the organizational data from the intruder's.
- One can avoid the massive data breaches which can otherwise put them in a huge financial loss, therefore this can keep the business safe and secure.

- *Penetration Testing is are of two modes*

1. ***External Penetration Test** [1]* – The external term is used to define that the test is executed from outside of the organization. Therefore, as the organization will make a contract with the penetration tester that the total organization wants to be tested from outside and including all the services like website and social media accounts and GitHub everything which is linked to the company will be tested from external.
2. ***Internal Penetration Test*** – The internal penetration testing [1] can be done from inside of the organization.

   The tester is allowed into the company and he will have some service access then he will try to connect to the LAN network of that organization and tester will try to penetrate into the devices which is

978-1-6654-1450-0/21/$31.00 ©2021 IEEE

connected to the same LAN network. As a whole, in this type of attack, insider attack are simulated.

### C. *Penetration Testings are three types*

- Black Box
- White Box
- Gray Box

A. *Black Box:* In the black box testing the penetration tester is not provided with the specific information to penetrate into the networks. So, the tester needs to find out all the vulnerability by his own methodology and his own tools. Here the company is not going to provide any tools and the data which is to be tested.

B. *White Box:* In white box testing the penetration tester is provided the specific details and some special access to perform penetration testing. The company is co-operating with the tester by providing much details about the organization

C. *Gray Box:* The tester is provided with some little data or the idea about the network. In this type of testing, tester will be not provided the entire details but will be assisted with limited amount of data to carry the testing.

## II. Penetration Testing Methodology

### A. *Preparation for a Network Penetration Test*

To perform a quality penetration testing [8][9] the tester or analyzer needs a good methodology . According to our survey, a tester have to divide his testing into the four steps

The four steps are information gathering, scanning, enumeration, post exploitation, reporting. First of all, the penetration tester needs to set the entire lab for testing the organization, as most of the testers use kali linux operating system to perform because this OS comes with pre-build tools. The tester will start according to the mode of test. First step in network penetration testing is, tester will connect to the LAN network and he will try to do ARP-ping scan because the ARP scan will bypass the access policy list which was set by the server security management and it will help to find the ip address of all the devices connected to the same LAN network.

After getting the IP address the tester will check where the IP address is a server or any other IOT devices is. After pen tester's confirmation, further he will try to do a network mapping scan. By scanning, all the open ports will be enumerated and the services and the services version can also be extracted by using this NMAP tool. After the NMAP, if any website host on the same server he will try to scan a website for any known vulnerabilities. Then, the tester will go with every way to find out any sensitive path to find out the vulnerability then tester will try to get reverse shell from the organization if any vulnerability exist. Then he will try to do post exploitation to get reverse shell from root. At last, tester will write a report which the report contains the entire testing procedure and tricks and tips, tools used by the tester and how he exploited the vulnerability and how he got access to the root shell. Everything will be mentioned in the report. This the common methodology every penetration tester will follow.

### B. *The following steps to conduct a quality Penetration Testing [8][9]*

1. *Reconnaissance or Information Gathering*

Recon means gathering the information. This is the vital phase in which we are going to perform some of the tricks that will help to collect the information of the organization.

The set of information can be anything as mentioned below the list to according to the information gathering the tester is going to perform the test on company.

A researcher always need to think like a black hacker to gather information about the company. Because every single information gathered will be used for the exploit.

- Internal network
- Sources address like ip
- Dns queries and zone transfers
- Fingerprinting
- Banner grabbing
- Social media accounts
- Applications active on network.
- About IDS, IPS using by the target.

To collect the better info about the target we go for the following-

a) Google database
b) Social media
c) Who is
d) Company website.

- *Google database and Social Media:* Here we know that most of the information can be gathered from the google hacking database here by using one of the technique like google dorks and we can expect the required result from the google database. If not, information can be gathered through social media accounts like where the company or an organization is supposed to be active most of the time.
- *Who is:* Whois [15][16] is a web based source provider about the website and the server where you can get the entire information about the registrar, domain provider and ASNI numbers

then we can also able to get admin information in some cases, then we can able to see the built date and expire date of the services.

2. *Scanning*
   Performing [4][5][6] Scanning is a process of gathering information without exploiting the system to find the hosts, ports and what services are running and can also find what versions they are running. They simply find all these information to exploit vulnerabilities.

- *Live IP Discovery:* Live IP Discovery in this phase we will find the exact IP address of the device in the local network. Here, the Tester will use some organized tools like NMAP, Hping3 Network discovery and some other tools similar to this For suppose if the tester use nmap he can also do ARPScan. Likewise, there is a specific feature for every Tool
- ICMP Ping Scan: This scan is [8] utilized to make ping. Let us assume, if an organization is utilizing some firewall so it will dismiss some requests for this situation we can't see the open ports so then this ping scan can be utilized to check the open ports it will bypass the firewall and make ping to the organization source address. But, in some cases the ICMP packet will be blocked, instead of this ICMP tester we send the ARP ping request so he can bypass all the firewall.

```
# nmap -Pn <ip > is used for ping scan
# ping <ip> is used to send icmp packet
# nmap -sn <ip> is used to sed the arp ping scan.
```

- Vulnerability Scanning: Vulnerability scanning [12][15] is a process of gathering information what data can we found without exploiting on the systems. We might can perform a port scan, which ports are open and what services are running and can also find the what versions there are running. All of these can be done on their systems without logging in and without performing any exploitation we can perform this scan both outside and inside the network and can gather information as much as possible from our systems.

  Scanners are very powerful in which they use various techniques to identify vulnerabilities like servers, and what applications are running.

  They simply gather information but they don’t try to exploit vulnerabilities and they simply try out the vulnerabilities if it works or not.

  In some cases we can also use Nmap as a vulnerability scanner

  Vulnerability scanners will have own database. Which will find out the weaknesses of asset

  Nessus is a one of the vulnerability scanner which is maintained and provided by the tenable company.

As per the information[4][5] about new vulnerabilities is found in infosec community the Tenable's investigation staff plans programs ("modules") that enable Nessus to provide their quality. The modules contain information, the estimation to test for the presence of the security issue. We can pick detached module update likewise, the below we mention are some free and open source tools

- ZAP
- SQLMAP
- WPSCAN
- WEBSEARCH

The following are Commercial scanners available on internet

- Acunetix
- Net sparker
- Burp Scanner
- NTOSpider

## III. ENUMERATION

Enumeration [4][5][9] is the main part of the entire testing part because if the tester got the IP address and some information about the company which the tester done in the scanning part. The tester will enumerate about the result which he will come to a point whether the information gathered is correct or not if it is then how the information will be used to exploit the target company.

The tester will try to enumerate all the result about the company website and some default usernames or passwords which the company use GitHub page for their product services or any important and the type of network and types of devices used etc.so here the mention phases can be done in this enumeration part.

1. NetBIOS list
2. LDAP list
3. NTP
4. Windows list
5. UNIX/Linux list

- *NetBIOS:* NetBIOS means network basic input output. It will provide the services on the session layer of OSI-reference model. This will provide a service of communication which the local area network connected systems.

  It runs on the port 139 in windows. To provide the communication through server message block.

- *NetBIOS Tools:* The following are the famous NetBIOS tools.
  - ***Nbtstat*****:** Nbstat is a utility that shows show experiences and current TCP/IP links utilizing NBT (NetBIOS over TCP/IP), which investigates NetBIOS name goal issues. Routinely, name goal is performed when NetBIOS over TCP/IP is working precisely
  - ***Super scan*****:** It is a tool utilized by framework organizations and script kiddies to evaluate a PC's security. Framework organizations can utilize it to test for conceivable unapproved open ports on their PC organizations, while crackers use it to check for problematic ports to acquire illicit admittance to a framework.
  - *NetBIOS* ***security controls***
    1. SMB server access need to be limit and it should discard the SMB login to the outers.
    2. Disable the smbmap enumeration here we need to restrict the access to the SMB share directory.

  - *LDAP*: LDAP [10][12] means Light-Weight Directory Access Protocol. It is an Internet convention for getting to distributed catalog administrations like Active Directory or OpenLDAP. It helps read-just exercise that doesn't adjust LDAP record data for example – browsing, search, etc.
  - *LDAP enumeration tools:*
    1. ***Softerra Administrator***: Softerra is an LDAP Browser which is a lightweight version of Softerra LDAP Administrator. It helps read-just exercises that don't adjust LDAP record data, for example, browsing, search, etc.
    2. ***JXplorer*****:** JXplorer is a cross-stage LDAP program and proofreader. It is a principles consistent universally useful LDAP customer that can be utilized to look, peruse and alter any standard LDAP registry, or any catalog administration with an LDAP or DSML interface. It is profoundly adaptable and can be broadened and modified in various manners.
    3. ***LDAP Admin Tool***: LDAP Admin is a free Windows LDAP customer and organization device for LDAP catalog the board. This application allows you to search, alter, make and erase protests on the LDAP server.

- *LDAP security controls*
  1. SSL will be used to encode LDAP correspondences.
  2. Kerberos have to use here to limit the access to known customers.
  3. Account lockout functionality will be implemented so no chance to do brute force.

- *NTP*

  NTP [10] means network time protocol. And it is the protocol that uses the internet to sync computer time to some external reference.

  So by using the NTP tester can gather the information of connected hosts to the NTP server and the tester can able to enumerate the services and versions of their services running on the NTP.

  NTP will rely on the specialist of server design, specialist queries the NTP server. It deals only with the User Datagram Protocol (UDP) and the notable port of 123.

  NTP will check the inside time of 10 millisecond over the public networks

- *NTP enumeration*
  1. An attacker can distinguish the accompanying information by querying a NTP server.
  2. Total number of users connected to the NTP can be able to enumerate by using this NTP service.
  3. Total fingerprinting can be done like what devices are using inside the company and what type of OS is using by them.

  - **NTP trace**: Queries to decide from where the NTP server refreshes its time and follows the chain of NTP servers from a source.
  - **NTP dc**: Inquiry the NTP daemon about its present status and to demand changes in the state.
  - **NTP:** Screens NTP daemon NTPD activities and decides execution.

- *NTP security controls*
  1. Enable the login for event logs checking
  2. Total filter the traffic using system monitor tools or IDS AND IPS.
  3. If NTP is not used then close the service if in case the tester confines the service is in use by the company then make sure whether the NTP second is implemented.

- *Windows Enumeration*

  Windows enumeration [18][20] can be specified with various devices from System internals. Much more system internal devices can be able to download. The accompanying rundown is the rundown of some related packages.

1. **PSExec:** Execute measures on far off machines.
2. **PSFile:** Presentation's rundown of records opened distantly.
3. **PSInfo**: Showcases establishment, introduce date, bit construct, actual memory, processors type and number, etc.
4. **PSKill:** Slaughter measures on nearby or far off machines
5. **PsGetSid:** Make an interpretation of SID to show name and the other way around.

- *Windows Security Controls*
    1. If a windows server is not using some of the ports or services then make sure that close the unused ports and stop the services running on that ports.
    2. Make sure whether the windows firewall is in protective mode and DNS blacklisting need to be implemented.

- *UNIX or Linux*

    This OS [18] can be counted with various command-line utilities given by the OS. Coming up next is the some of utilities

    1. Finger: Identify clients on distant machines
    2. **Enum4Linux**: This tool can be used to enumerate all the services and all the types of functionalities belongs to the OS.
    3. **Show mount**: Identify list of shared directories.
    4. **RPCInfo:** Identify far off system calls.

- *Linux Enum Tools*

    *LINUX Security Controls*

    1. Make sure [18] that the unused ports should need to be close and need to use strong password instead of default userid and password.
    2. Ensure that the ARP table and implement the IDS OR IPS to wrap up the IP fragment to the attack vector will decrease.

After this, the part of the tester will have an entire mind map to hack into the servers then after getting into the servers the tester will use to do post-exploitation. So, the post-exploitation is called privilege escalation.

## IV. Post Exploitation

So in this[13] entire phases only can be seen the tricks and some important term to do post-exploitation Not every command or type of exploitation will work on every computer so we have to use and analyze multiple types of steps or tricks to get access as root.

First, we will see how to check all the operating system details so if any misconfiguration it may use tester to get root access.

- *To know the distribution type? And what version?*
    - cat /etc/*-release #it will show you the OS release date
    - cat /etc/lsb-release   #Debain based
    - cat /etc/issue # it will show the version of distro
    - cat /etc/redhat-release #Redhat based.

- *What's the kernel version? Is it 64-bit?*
    - uname –a
    - uname –mrs
    - cat /proc/version
    - dmesg | grep Linux
    - rpm -q kernel

Hence, in [19] this manner the tester will try to gather some information about the operating system then if any old version is running in the kernel then tester will try to exploit.

For example, if the tester found that the target machine is running Linux 3.5 version so the tester will search known exploit in the google hacking database and one tool is used

In the Linux and the tool name is SEARCHSPOLOIT with this tool the tester will check known exploit for specific version.

The following command can be used to search by using Searchsploit

```
# searchsploit <service version>
```

If attacker want to download the script from searchsploit the -m keyword is used as the command shows

```
# searchsploit -m <service version>
```

Then tester we try to exploit with specific script to get root access.

The next type of exploit is SUID AND GUID

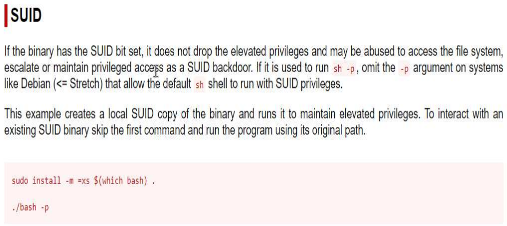
To exploit this type of mechanism in the operating system the tester will enter the following command as shown

# find / -perm -u=s -type f 2>/dev/null (this command to check the SUID files or process running on the present user)

Thus, by this command the all process running in the present user as root will be displayed.

For example if the service like /usr/bin/bash is running as SUID in the present user the we need to go the GFTOBINS website then search for bash and filter for SUID then some of the commands will we displayed to get reverse shell from the root as using SUID we can exploit and we can able to gain reverse shell from root.

This screen shot will show how the results will be displayed after filtering for SUID for bash in GFTObins website page.



**SUID**

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .

./bash -p
```

Figure 1.

Hence, it is possible to exploit SUID and GID

Next if this tricks are not exploited then we can able to use some scripts like Linux exploit suggester, linpeas, Linux Enum. So by this we can easily bypass the security and get reverse shell from root.

## V. Drawbacks In Network Penetration Testing

As in the network penetration testing the tester will only test the internal networks or servers. So here for the external testing again the organization want to be hire the testing team like red team which do external and black box testing. This reason might impact on the internal penetration testers.

## VI. Conclusion

In conclusion, we can understand the power of penetration testing as through this paper it has been seen the steps and phases, types of penetration testing and then modes of penetration testing. By this, we can get that if a penetration tester have a great methodology then tester can perform the strong and quality network testing. The companies can afford penetration testing for sure to maintain the confidentiality integrity and availability because if the company is maintain the good security then every client is ready to share there data and at the same time company can built its repudiation.

In the midst of different requirements like absence of time and improper meaning of extent of the venture, entrance analyzer needs to complete the test to the most amazing aspect the productivity by utilizing the apparatuses well. It is smarter to have little robotization contents for tedious assignments.

## VII. Scope In Network Penetration Testing

Scope In the network penetration testing is vast as we talk about the developing the world is running equal with the modern technology so the every device or new technology needs the security so providing a continues or doing a vulnerability assessment will not keep your data security so here the penetration testing will offer you with a great and quality type of service providing that it will test every device or asset form starting to end point. So, network penetration testing is highly recommended to keep IT company's data safe and secure.

## References

[1] Nmap cheat sheet see-security hacking defined experts by Nativ.y,2015.

[2] Redondo, Jose Manuel (2019) Towards improving productivity in NMAP Security Audits, Journal of web engineering.

[3] Lyon Gordon NMAP-the Network Mapper-free security lancer,2017.

[4] Probabilistic engineering analysis using the NESSUS software by Thacker B.H, Riha D.S. Structural safety, 2006

[5] Exploration of computer network by vulnerability scanner NESSUS by Balatska V.,2020.

[6] Vulnerabilities mapping based on OWASP-SANS: A survey for static application security testing (SAST) by Li.j ,2020.

[7] A guide for running an effective penetration testing program by Creasey j. crest ,2017.

[8] Ethical hacking and penetration guide by Baloch R,2017.

[9] A guide to penetration testing by Tang A., Network security,2014.

[10] OSSTMM: The open-source security testing methodology manual: v3, Herzog p. Isecom ,2016.

[11] Using open-source software for web application security testing, Simic D., JITA - Journal of Information Technology and Applications (Banja Luka) – APEIRON, 2017.

[12] Automating post-exploitation with deep reinforcement learning, Maeda R., Mimura M., computers and security, 2021.

[13] Content management systems hacking probabilities for admin access with google dorking and database code injection for web content security, Phule A.K., Kamble M., 2nd International Conference on Data, Engineering and Applications IDEA ,2020.

[14] WHOIS, Troia V., Hunting Cyber Criminals,2020.

[15] The impact of GDPR on WHOIS: Implications for businesses facing cybercrime, Ferrante A.J., cyber security: A Peer-Reviewed Journal ,2018.

[16] Linux Server Security - Hack and Defend, Binnie C., John Wikey & Sons, Inc,2016.

[17] Hack Proofing Your Web Applications: The Only Way to Stop a Hacker Is to Think Like One, Syngress media I.S.,2001.

[18] Linux From Scratch, Beekmans G. Linux,2010.

[29] Security Enumeration for cyber- physical systems, Schelte D., Pernul G., Lecture Notes in computer Science,2020.