# Lab-4-2: Network Security – Vulnerability Identification

This lab covers the topic of vulnerability identification in regarding to network security. We are covering basic vulnerability identification tactics including identification of services. The aim of today’s lab is to document all vulnerabilities on our target system (Metasploitable2).

**Exercise-4-2-1: Operating System Detection**

Last week we used nmap to perform a quick scan of Metasploitable2. We discovered some open ports and the associated running services but we have yet to determine the operating system version on the target. This is essential information to collect and will aid in performing vulnerability identification.

Firstly, let use nmap and attempt to discover the operating system version. Execute the following command on your Kali Linux system (make sure Metasploitable2 is also running):

nmap –O 192.168.19.128

The –O option in the command, enables operating system detection

**Q1.** According to nmap, what operating system is Metasploitable2 running on?

Linux 2.6.X

Now, let us check the actual operating system version on Metasploitable2. We can use this output to check how well our operating system detection methods worked. **Make sure you are in the Metasploitable2 virtual machine**, and execute the following command:

uname –a

To get even more information about the Metasploitable2 operating system, try the following command as well:

cat /etc/lsb-release

**Q2.** Based on the information obtained from the above commands, what operating system is Metasplotable2 running on? Try to include the Linux kernel version and Linux distribution information.

Ubuntu 8.04

Linux 2.6.24-16-server

So far, we have performed active operating system detection. It would be prudent to attempt a passive detection technique as well. We will attempt this using the p0f tool. Try the following executing the following command on your Kali Linux machine:

p0f –i eth0

In the above example:

* p0f is the name of the application
* -i is the command line option to include a networking interface
* eth0 is the networking interface to use (ETHernet)

Unfortunately, in our network there is not much network traffic (as it is a closed, isolated virtual machine network). So we will have to generate some network traffic using the netcat tool. If you remember, we used this tool last class to perform banner grabbing. Open a new terminal window in Kali Linux, and execute the following command:

nc 192.168.19.128 80

Use the IP addresses to distinguish the flow of traffic (sender and receiver) from the p0f tool so you can answer the following question.

**Q4.** What does the p0f tool report as the Metasploitable2 operating system?

2.6.X

**Q5.** Based on the results from the previous exercises, and the theory provided in the class, provide a brief summary of at least one advantage and one disadvantage of each operating system detection method.

P0f nothing happens until traffic is generated – passive

Active tools are more accurate, etc the finger print methods for nmap

**Exercise-4-2-2: Vulnerability Identification**

Finding vulnerabilities is a major aspect of information gathering and contributes to the success of performing a useful and exhaustive security audit. We are going to use nmap and some useful scanning features to find out more about our target system (Metasploitable2).

Start by using nmap to scan the target machine (Metasploitable2) and perform automated identification of all services. Use the following command:

nmap -sV 192.168.19.128

In the above example:

* nmap is the name of the application
* -sV is a scanning method called “service version”
* 192.168.19.128 is the target IP address of Metasploitable2

**Q6.** Document all output of service running on the Metasploitable2 system.

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 rexecd

513/tcp open login?

514/tcp open shell Netkit rshd

1099/tcp open rmiregistry GNU Classpath grmiregistry

1524/tcp open shell 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 Unreal ircd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 00:0C:29:FA:DD:2A (VMware)

Service Info: Hosts: metasploitable.localdomain, localhost, 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 107.60 seconds

Now try increasing the range of ports we will scan. Check the lecture slides for information about how to accomplish this.

**Q7.** List any additional services and/or open ports that you discovered by extending the range of ports.

Netdiscover

Netcat

Nmap –p 0-65535 192.168.19.128

Now, we have a list of the following information:

1. Open ports
2. Services running
3. Software versions

Let’s try running some nmap scripts to help automate discovery of some vulnerabilities in the software (e.g., old unpatched versions) and misconfiguration (e.g., a service without a password). Execute the following command to invoke the nmap authorisation script to automate the checking of common vulnerabilities.

nmap --script auth 192.168.19.128

In the above example:

* nmap is the name of the application
* --script is an option to request that a script should be run
* auth is the name of the script to run
* 192.168.19.128 is the target IP address of Metasploitable2

Review the output thoroughly. If you are stuck or confused about the output, try researching or work together with a partner.

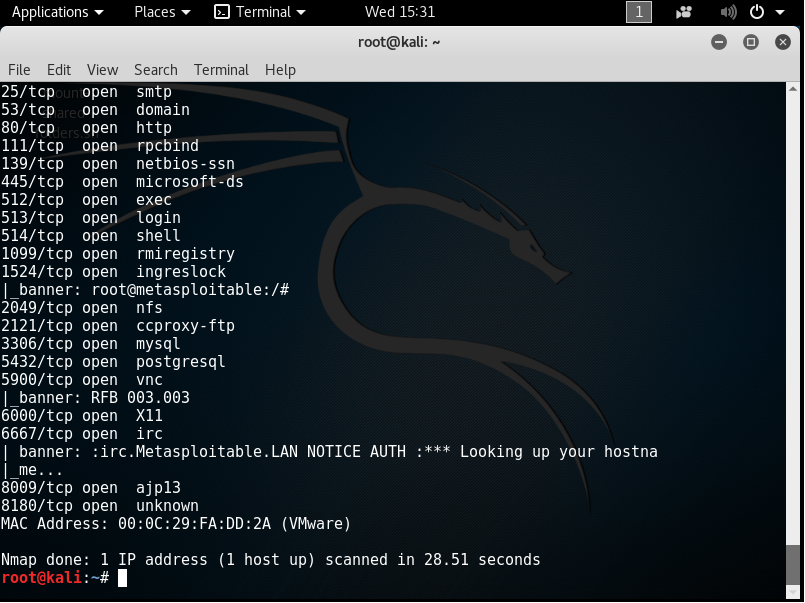
**Q8.** Based on the results of the auth script, can you identify any usernames and passwords? Document any you may find.

Username: tomcat

Password was empty or was called tomcat again

**Q9.** Attempt to gain access to a service provided by the Metasploitable2 system. If successful, include a brief description of your method and a screenshot.

Accessed the banner service by executing the following command: nmap –script banner 192.168.19.128



**BONUS Q10.** Try out some more nmap scripts (see: <https://nmap.org/nsedoc/index.html>). There are many tutorials on the Internet available. Select a script and test it against Metasploitable2. Document any interesting or useful information you can obtain that may aid our security audit.