

Faculty of Business, IT, and Management
HACK2200 Hacking and Exploits
Lab 2: Scanning and Enumeration

Instructions

- This assignment should be completed individually.
- This assignment is designed for the purpose of education and training, but not for any illegal activities including hacking. Beware to only use these exploits on hosts that you have permission to hack.
- When a question asks for screenshots, your screenshots **must**:
 - Include the full window (the application window, or the terminal window, etc...),
 - have the PROMPT setup as per the instructions, including the date and time in the same format provided in the instructions. Screenshots without the prompt setup will receive zero credit,
 - be clearly readable,
 - include all the information required by the question, and
 - not include extra commands, failed attempts and/or error messages.
- Failure to follow submission instructions will result in marks deduction. There will be mark deductions for including more than what is required in the instructions. Do not replace any screenshot that is not marked for replacement. These screenshots are to guide you only.
- The below instructions are guidelines, you are expected to troubleshoot any errors you run into.
- There will be mark deductions for including more than what is required in the instructions.
- Read and complete the lab instructions below and finish all the tasks. Replace screenshots that are labeled as sample-replace only, and answer the questions where highlighted.
- Once completed, submit the Answer File only to the assignment dropbox.

Introduction

Scanning is one of the most important phases of intelligence gathering for an attacker. In the process of scanning, the attacker tries to gather information about the specific IP addresses that can be accessed over the Internet, the target's operating systems and system architecture, and the services running on each computer [1].

One of the tools used to conduct network scanning is Nmap ("Network Mapper") available at <https://nmap.org/>. It is a free and open-source ([license](#)) utility for network discovery and security auditing. Nmap uses raw IP packets to determine:

- what hosts are available on the network,

- what services (application name and version) those hosts are offering,
- what operating systems (and OS versions) they are running, and
- what type of packet filters/firewalls are in use.

It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems.

After scanning, we want to enumerate the network. Enumeration is usually the first step taken by a hacker to compromise a system. During enumeration, the attacker's objective is to identify valid user accounts or groups that will provide anonymity once the system has been compromised. Enumeration involves making active connections to the target system or subjecting it to direct queries.

In this lab we will explore:

Part 1 – Network Scanning

Part 2 – Enumeration

Lab Setup

We will use the machines you prepared during the first week:

- 1- Kali Linux (KaliVM)
- 2- Metasploitable 3 Ubuntu (MS3UBUNTU)
- 3- Metasploitable 3 Windows Server 2008 (MS3WS2008)

Part 1 – Network Scanning

Step 1: Start the lab virtual machines

1. Start your Kali virtual machine (KaliVM), your Metasploitable3 Windows Server 2008 machine (MS3WS2008), and Metasploitable3 Ubuntu (MS3UBUNTU) machine.
2. Login to each machine, and take a note of each machine's IP address. Write the IP addresses in your answer file.

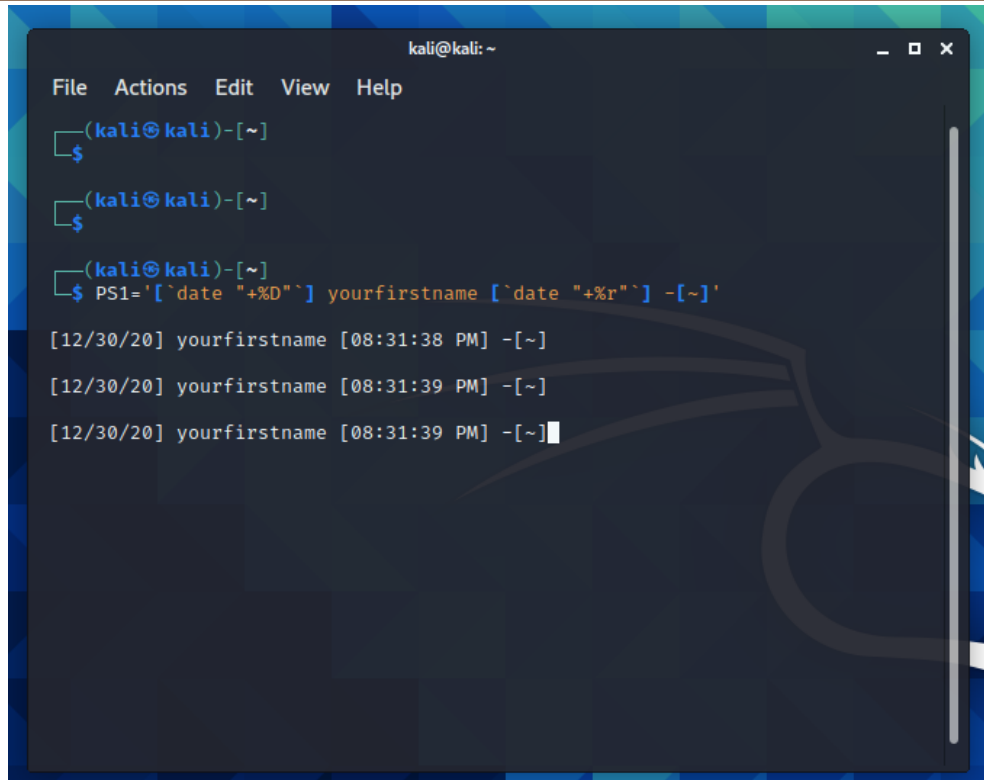
Question 1 – What is the IP address of your KaliVM, MS3WS2008, and MS3UBUNTU?
Write your answers in the answer file.

3. On your KaliVM, change the terminal prompt to be your first name.

You can do that using the following command:

```
(kali@kali)-[~] PS1='[`date "+%D"`] yourfirstname [`date "+%r"`] -[~]'
```

Your terminal should look similar to the screen below:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$ PS1='[`date "+%D"`] yourfirstname [`date "+%r"`] -[~]'  
[12/30/20] yourfirstname [08:31:38 PM] -[~]  
[12/30/20] yourfirstname [08:31:39 PM] -[~]  
[12/30/20] yourfirstname [08:31:39 PM] -[~]
```

All commands in the following tasks are to be run on your KaliVM, targeting your MS3WS2008 and MS3UBUNTU VMs.

Step 2: Scanning MS3WS2008 using nmap

We will use nmap to scan our target machines and find the services running on them:

1. On your KaliVM, scan the MS3WS2008 machine, using the IP address you obtained in the previous step:

```
KaliVM# sudo nmap -sS -sV -O [target IP address]
```

Take a screenshot to replace the one below, and place it under Screenshot#1 in the answer file.

```

kali@kali: ~
File Actions Edit View Help

[12/30/20] romari [09:10:25 PM] -[~]

[12/30/20] romari [09:10:25 PM] -[~]sudo nmap -sS -sV -O 192.168.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 21:10 EST
Nmap scan report for 192.168.2.4
Host is up (0.00034s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
22/tcp    open  ssh          OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http         Microsoft IIS httpd 7.5
4848/tcp  open  ssl/apache-httpd
8022/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http         Sun GlassFish Open Source Edition 4.0
8383/tcp  open  ssl/http     Apache httpd
9200/tcp  open  wap-wsp?
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  java-rmi     Java RMI
49159/tcp open  tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
_
SF-Port9200-TCP:V=7.91%I=7%D=12/30%Time=5FED3326P=x86_64-pc-linux-gnu%r(G
SF:etRequest,18D,"HTTP/1.0\x20200\x200K\r\nContent-Type:\x20application/j
SF:son\x20charset=UTF-8\r\nContent-Length:\x2010\r\n\r\n(\r\n)\x20\x20"

```

We can see that there is a number of open ports and services on the target machine such as ftpd on port 21. These services may contain vulnerabilities that can be exploited. Based on the results of your scan, answer the following questions:

Question 2 - What is the OS reported by nmap of the target machine?

Question 3 - List 5 of the running services with their version and the ports they are running on.

Step 3: Scanning MS3UBUNTU using nmap

Repeat Step 2 while targeting MS3UBUNTU machine.

Take a screenshot to replace the one below, and place it under Screenshot#2 in the answer file.

```

kali@kali: ~
File Actions Edit View Help

[12/30/20] romari [09:44:04 PM] ~
[12/30/20] romari [09:44:05 PM] ~
[12/30/20] romari [09:44:06 PM] ~[~]sudo nmap -sS -sV -O 192.168.2.5
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 21:44 EST
Nmap scan report for 192.168.2.5
Host is up (0.00065s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp    open  ipp      CUPS 1.7
3000/tcp   closed ppp
3306/tcp   open  mysql    MySQL (unauthorized)
8080/tcp   open  http     Jetty 8.1.7.v20120910
8181/tcp   closed intermapper
MAC address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds

[12/30/20] romari [09:44:27 PM] ~

```

Based on the results of your scan, answer the following questions:

Question 4 - What is the OS reported by nmap of the target machine?

Question 5 - List 5 of the running services with their version and the ports they are running on.

End of Part 1 – Scanning Networks

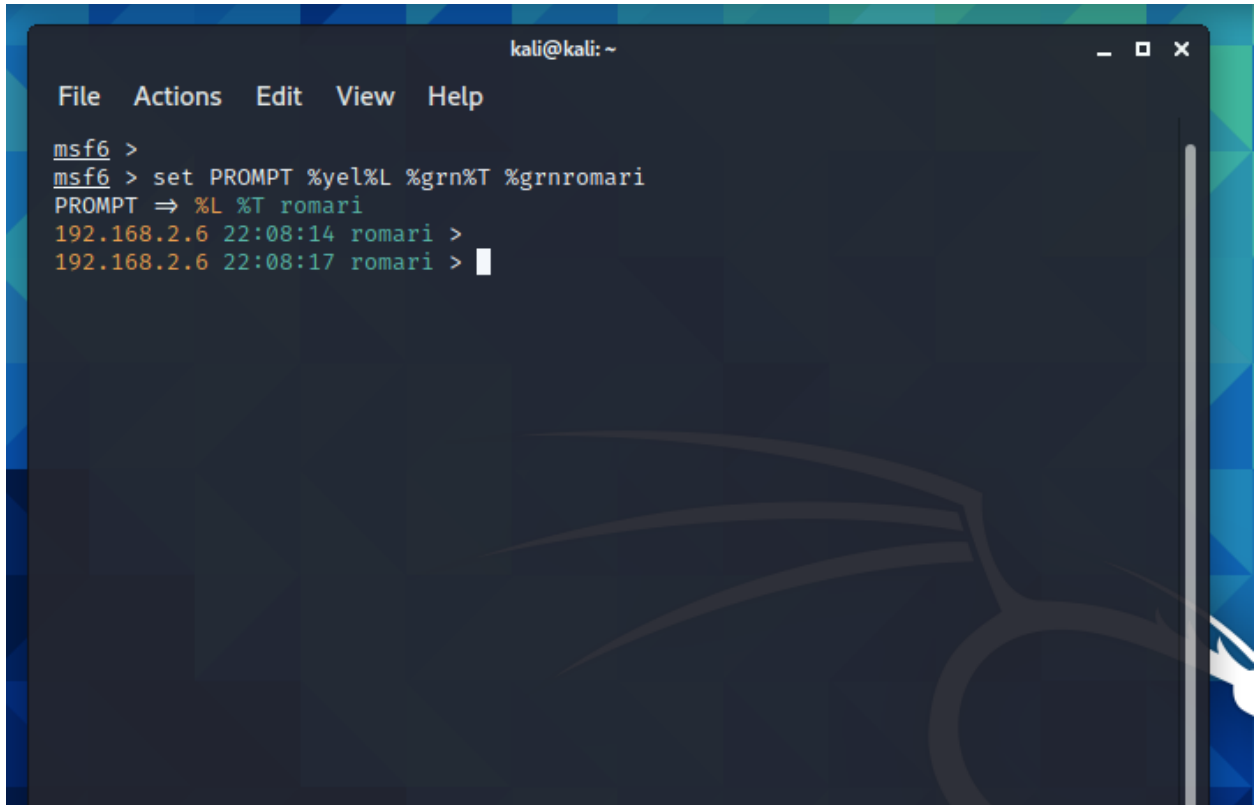
Part 2 - Enumeration

Step 1: Enumerating users with snmp_enumusers

In this task, we will use the msfconsole on your KaliVM to run snmp_enumusers script .

- 1- Start an msf console, and change the console prompt:

```
KaliVM# msfconsole  
Msf6> set PROMPT %yel%L %grn%T %grnyourfirstname
```



- 2- To use the snmp_enumusers script, run the following commands using **MS3WS2008** as your target machine:

```
msfconsole# use auxiliary/scanner/snmp/snmp_enumusers  
msfconsole# show options  
msfconsole# set RHOSTS [target IP address]  
msfconsole# run
```

Take a screenshot to replace the one below, and place it under Screenshot#3 in the answer file.


```

kali@kali: ~
File Actions Edit View Help
192.168.2.6 23:23:15 romari >
192.168.2.6 23:23:15 romari >
192.168.2.6 23:24:13 romari >
192.168.2.6 23:24:13 romari > use auxiliary/scanner/snmp/snmp_enumusers
192.168.2.6 23:25:22 romari auxiliary(scanner/snmp/snmp_enumusers) >
192.168.2.6 23:25:23 romari auxiliary(scanner/snmp/snmp_enumusers) > show options

Module options (auxiliary/scanner/snmp/snmp_enumusers):

  Name      Current Setting  Required  Description
  ---      -
  COMMUNITY public          yes       SNMP Community string
  RETRIES   1              yes       SNMP Retries
  RHOSTS    192.168.2.4    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     161            yes       The target port (UDP)
  THREADS   1              yes       The number of concurrent threads (max one per host)
  TIMEOUT   1              yes       SNMP Timeout
  VERSION   1              yes       SNMP Version <1/2c>

192.168.2.6 23:25:26 romari auxiliary(scanner/snmp/snmp_enumusers) >
192.168.2.6 23:25:27 romari auxiliary(scanner/snmp/snmp_enumusers) > set RHOSTS 192.168.2.4
RHOSTS => 192.168.2.4
192.168.2.6 23:25:35 romari auxiliary(scanner/snmp/snmp_enumusers) >
192.168.2.6 23:25:36 romari auxiliary(scanner/snmp/snmp_enumusers) > run

[+] 192.168.2.4:161 Found 20 users: Administrator, Guest, anakin_skywalker, artoo_detoo, ben_kenobi, boba_fett, c_three_pio, ch
ewbacca, dakin_vader, greedo, han_solo, jabba_hutt, jarjar_binks, kylo_ren, lando_calrissian, leia_organa, luke_skywalker, sshd
, sshd_server, vagrant
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
192.168.2.6 23:25:43 romari auxiliary(scanner/snmp/snmp_enumusers) >

```

Question 6 - List 3 user accounts that were found by the snmp_enumusers script

Exit msfconsole.

Step 2: Repeat Step 1 while targeting MS3UBUNTU machine, but use enum4linux command instead running the following command in the kali linux terminal:

```
KaliVM# enum4linux
```

Take a screenshot to replace the one below, and place it under Screenshot#4 in the answer file.

```

kali@kali: ~
File Actions Edit View Help

[12/30/20] romar [11:49:46 PM] -[~]
[12/30/20] romar [11:49:46 PM] -[~]
[12/30/20] romar [11:49:47 PM] -[~]enum4linux 192.168.2.5
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 30 23:49:59 2020

+-----+-----+
| Target Information |
+-----+-----+
Target ..... 192.168.2.5
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

+-----+-----+
| Enumerate Workgroup/Domain on 192.168.2.5 |
+-----+-----+
[E] Can't find workgroup/domain

+-----+-----+
| Nbtstat Information for 192.168.2.5 |
+-----+-----+
Looking up status of 192.168.2.5
No reply from 192.168.2.5

```

Question 7 - List 3 user accounts that were found by the enum4linux script

End of Part 2 - Enumeration