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 preprated 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 Mestapolitable3 Windows Server 2008 machine (MS3WS2008), and Metaspolitable3 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.

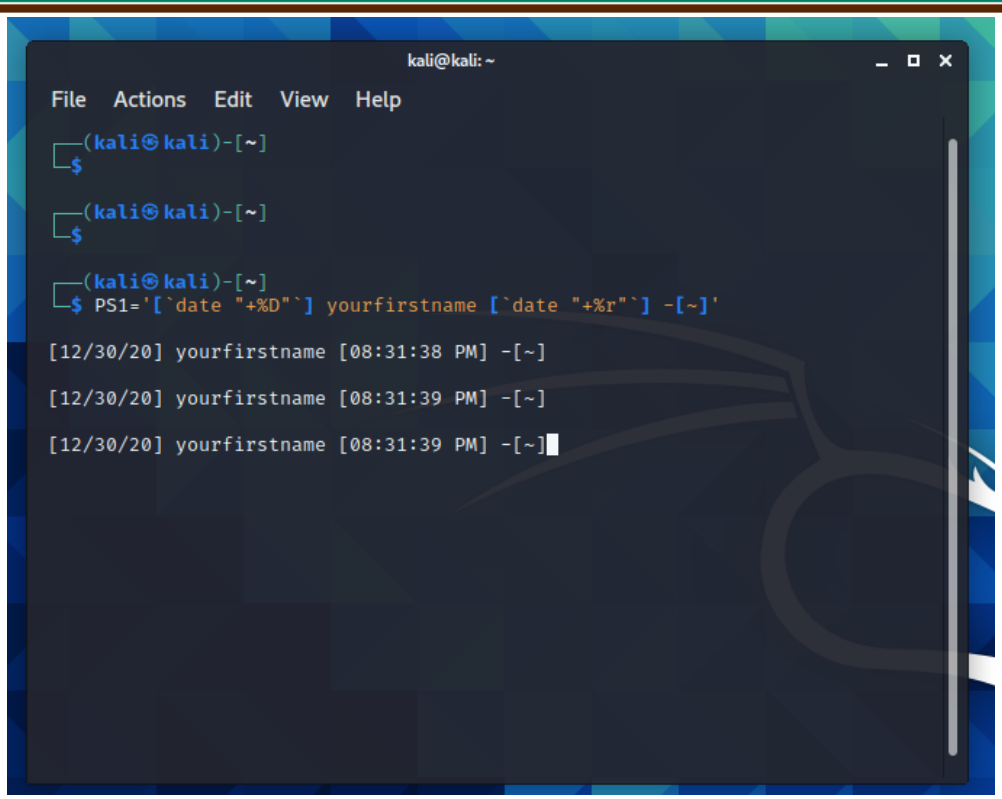
   Question 1 – What is the IP address of your KaliVM, MS3WS2008, and MS3UBUNTU? Write your answers in the answer file.

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:



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

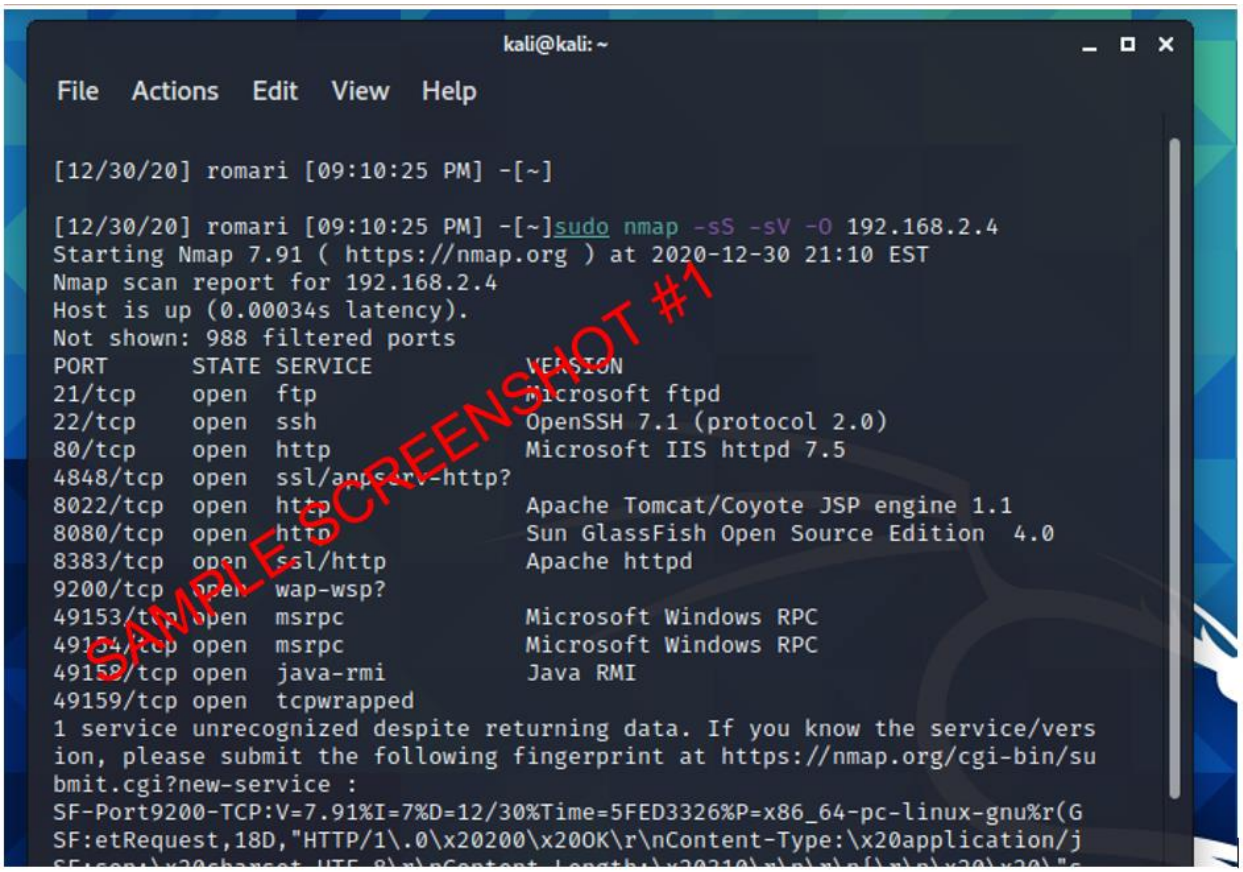
Step 2: Scanning MS3WS2008 using nmap

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.



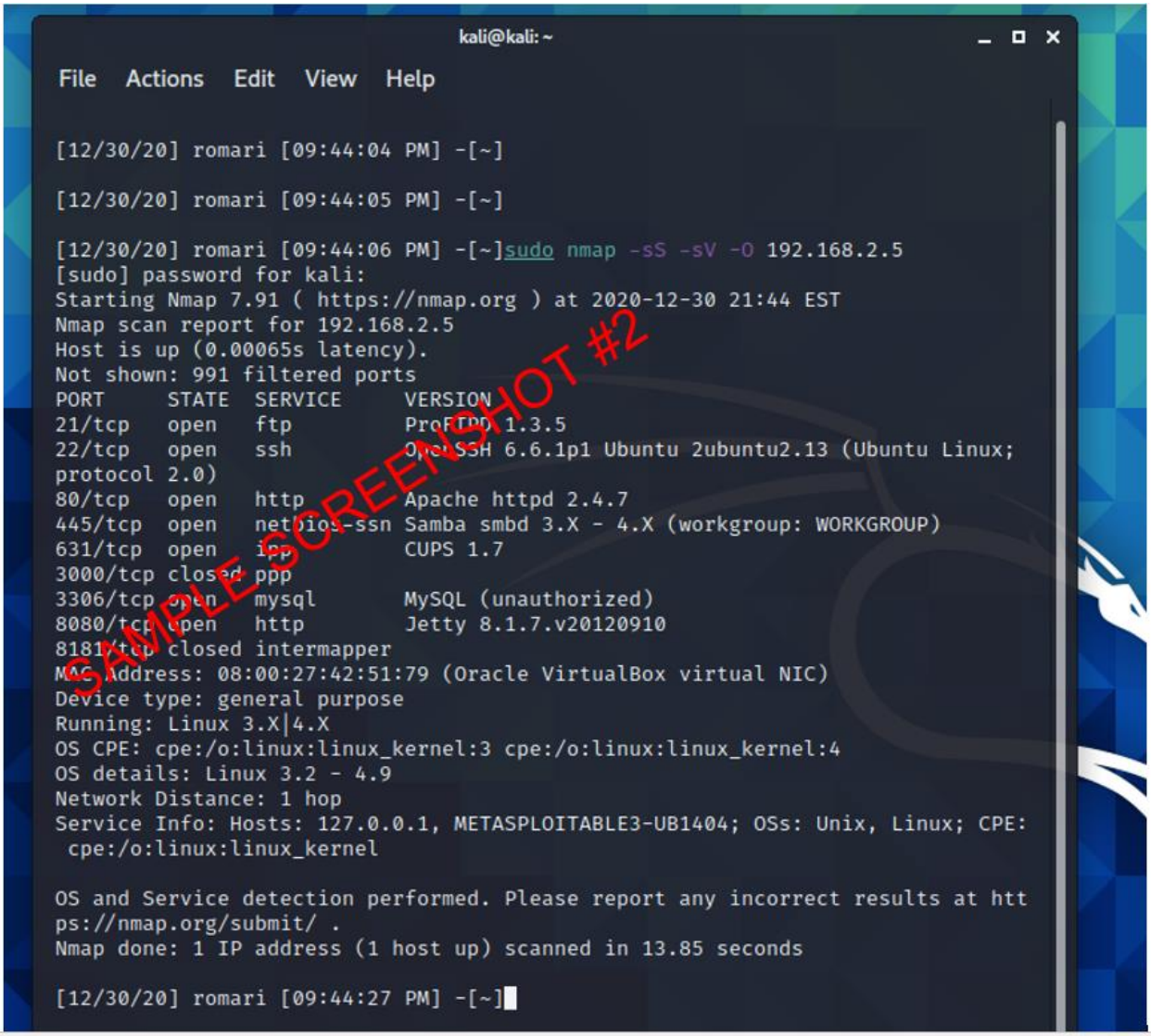
We can see that there is a number of open ports and services on the target machine such as ftpd on port 21. These services may contain vulnerabilities that can be exploited.
Based on the results of your scan, answer the following questions:

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.



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

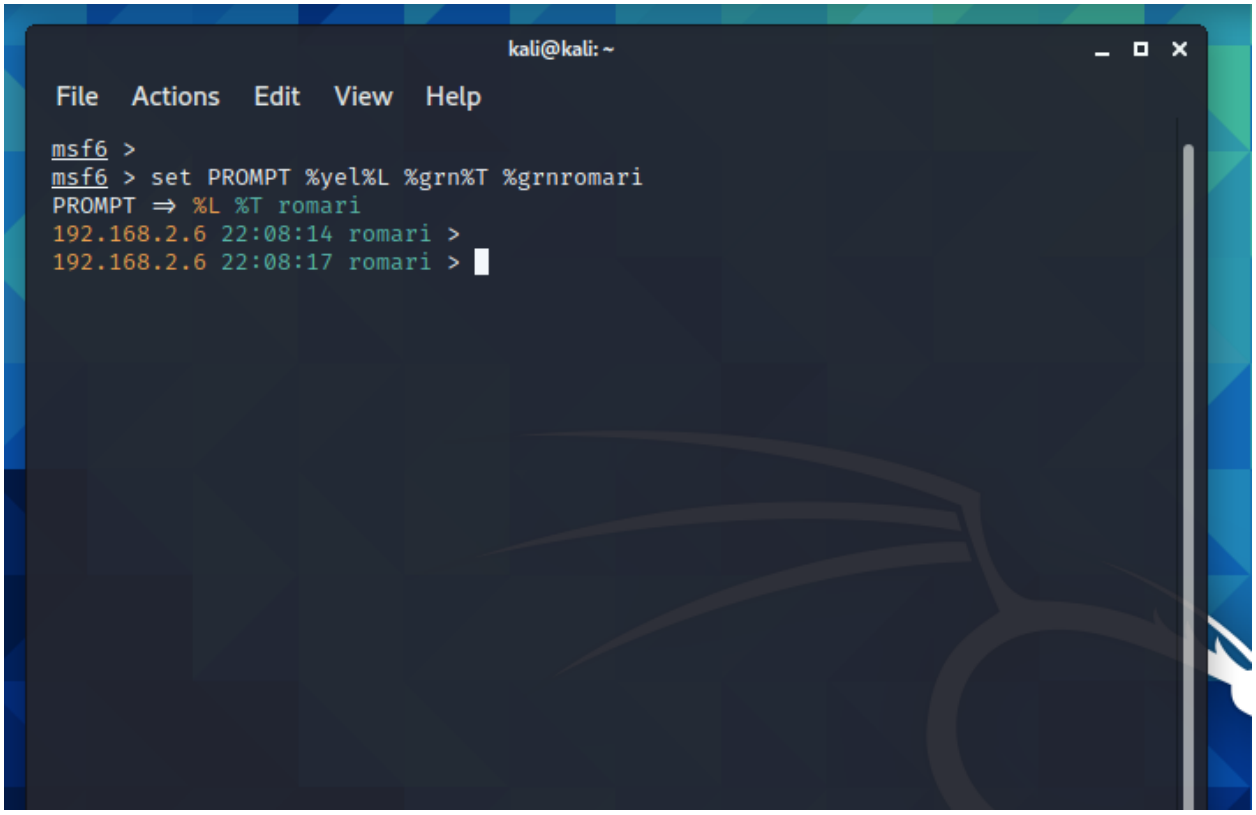
Part 2 - Enumeration

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:

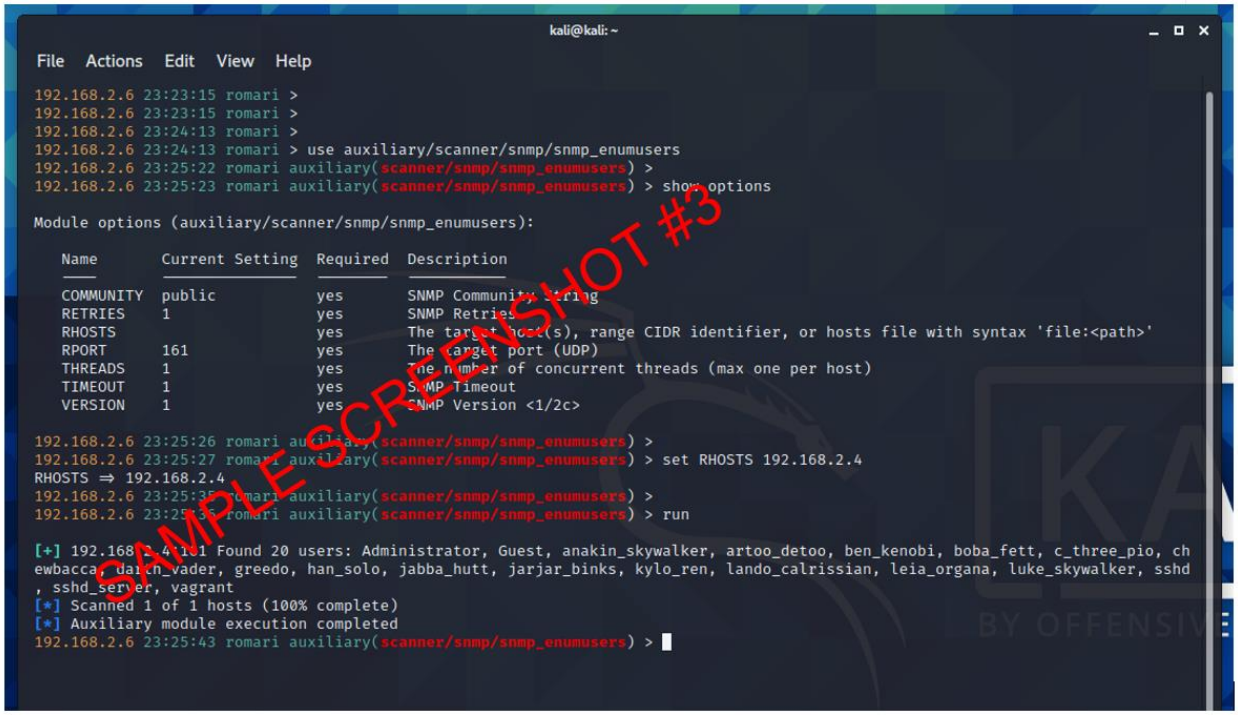
```
KaliVM# msfconsole
Msf6> set PROMPT %yel%L %grn%T %grnyourfirstname
```



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.



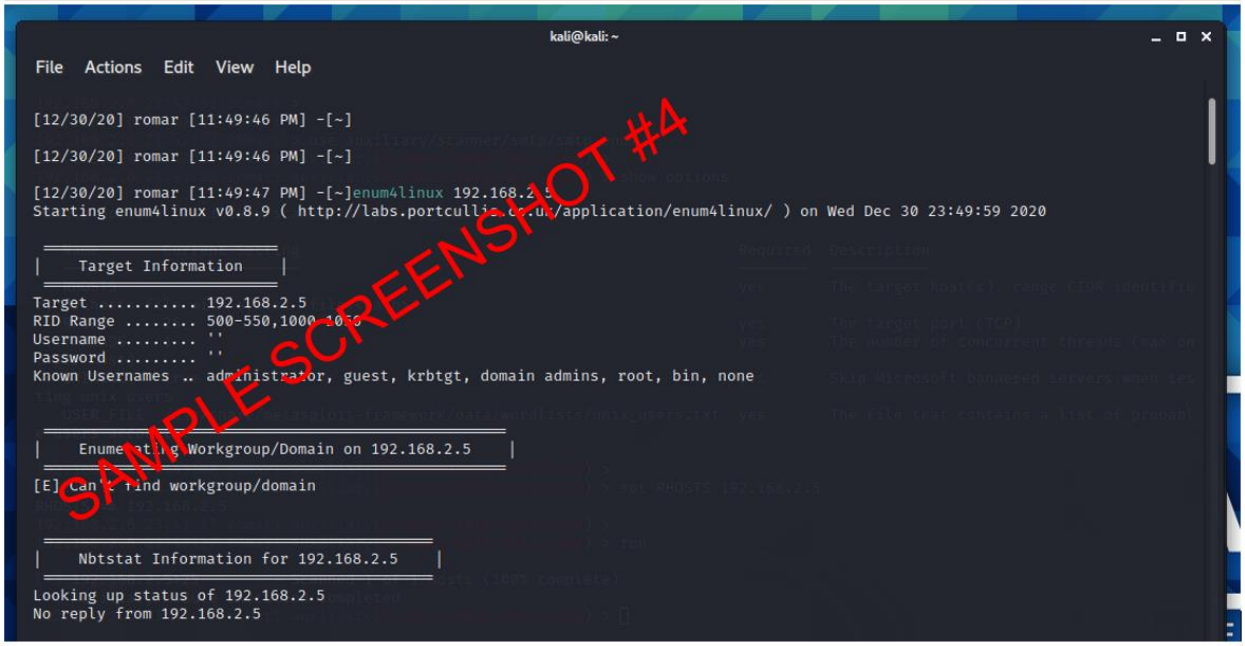
Question 6 - List 3 user accounts that were found by the snmp_enumusers script

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.



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

End of Part 2 - Enumeration