Name: \_Aryev P. Bhardwejj\_

Import the VM provided in the file HackingLab.ova into your local Virtual Box lab (select the option “Include all network adapter MAC addresses” when importing). Make sure your own Kali Linux VM can communicate with all the other VM in the lab by means of the internal network (try nmap -sn 192.168.0.0/24, because inbound pings are filtered out by default in Windows). Then, answer the questions below, giving an explanation of how or why even if not explicitly asked.

Part A: Checking the environment

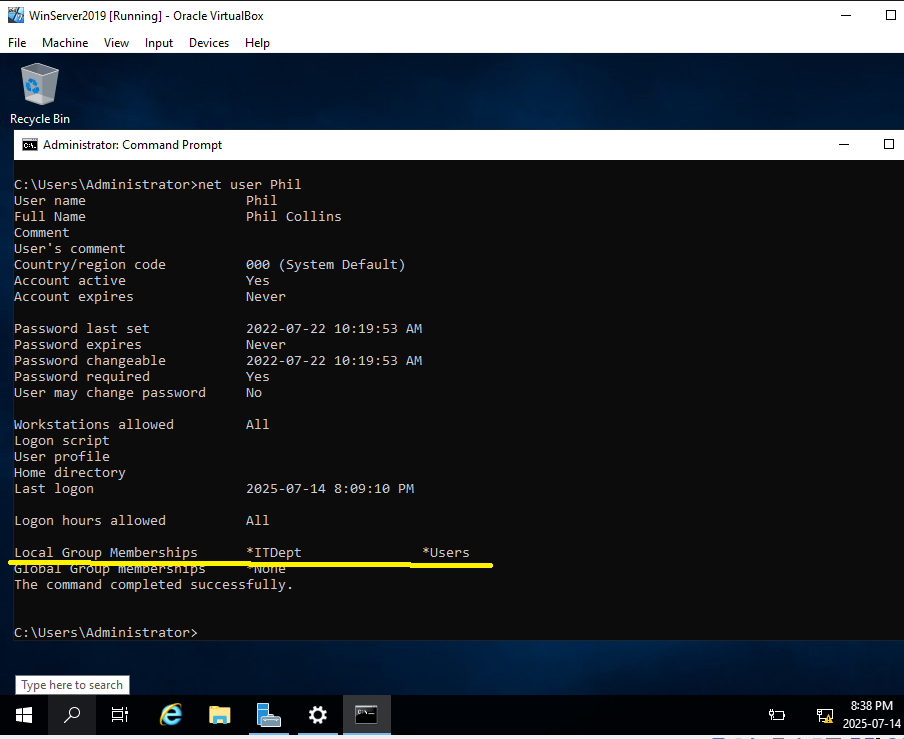
1. Perform a TCP SYN scan of just the Windows server. What services and ports did you discover?

Using **nmap -sS 192.168.0.31** command we performed a TCP SYN scan of the Windows server and discovered following open services and ports:

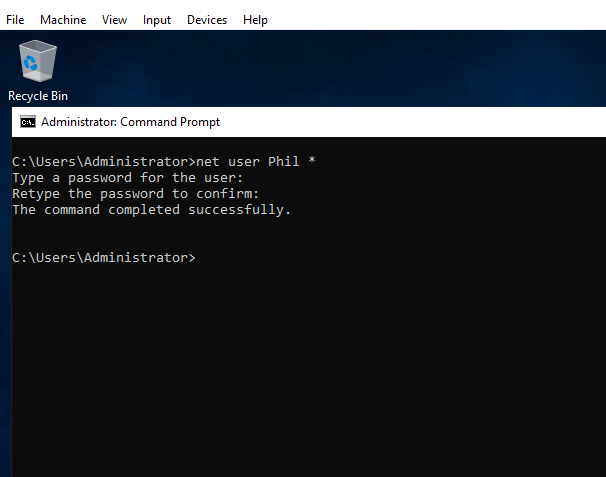
* **21/tcp:** ftp
* **80/tcp:** http
* **135/tcp:** msrpc
* **443/tcp:** https
* **445/tcp:** microsoft-ds



1. Open a session in the Windows server as Administrator and change Phil’s password for a random one of your choice. What group does this user belong to?

User Phil belongs to the IT department as shown

Phil’s password was changed using cmd prompt as an Administrator using following command:



Part B: SMB enumeration

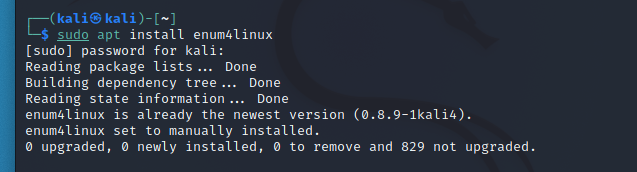
Reference tutorial for enum4linux: <https://www.hackercoolmagazine.com/smb-enumeration-with-kali-linux-enum4linuxacccheck-smbmap/>

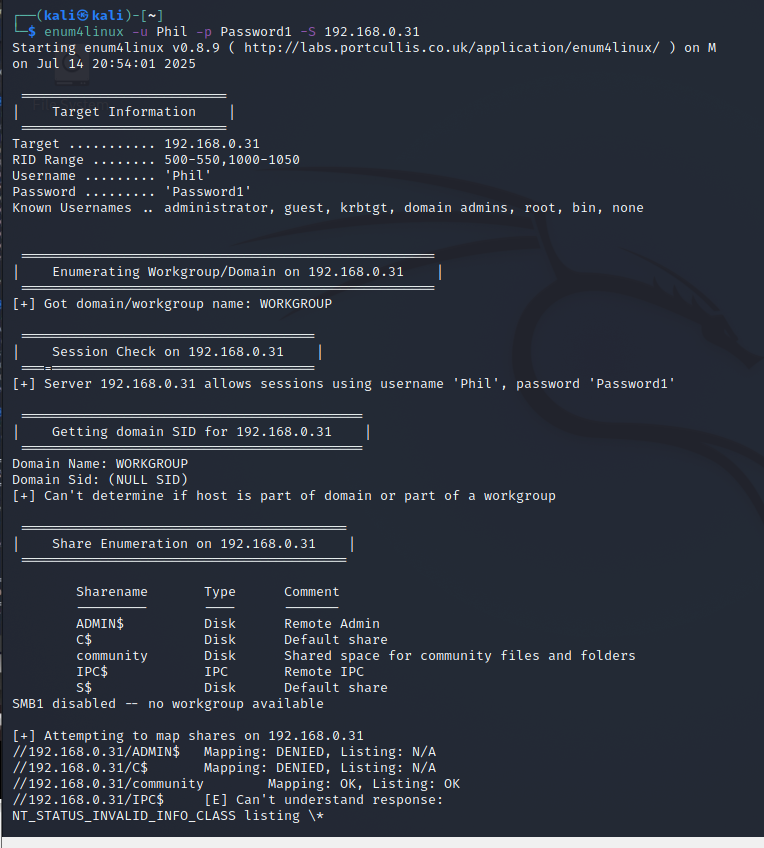
Getting started with Metasploit: https://ccom.uprrp.edu/~jortiz/cyber/labs/lab-metasploit.html

Reference for Metasploit: <https://www.offensive-security.com/metasploit-unleashed/scanner-smb-auxiliary-modules/>

1. Install the package enum4linux in your Kali VM. Then, enumerate the network shares of the Windows server using the credentials of Phil. What was the complete command?

On Kali, installed enum4linux package as shown

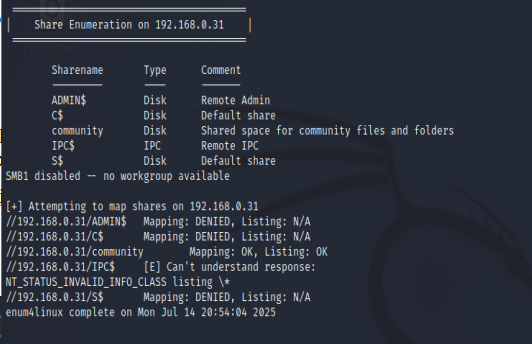


In order to enumerate the N/W shares of Windows server using Phil’s credentials, we used the following command: **enum4linux -u Phil -p Password1 -S 192.168.0.31**

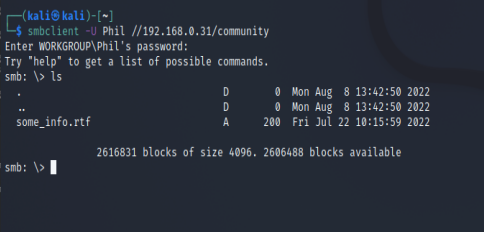
1. There is a share with the mapping not denied. Use it to execute the following command, which will open a SMB session. Capture a screenshot of the command “ls” run in the new SMB prompt.

smbclient -U Phil //192.168.0.31/SHARE\_NAME

Share Community is where mapping is not (as shown below)

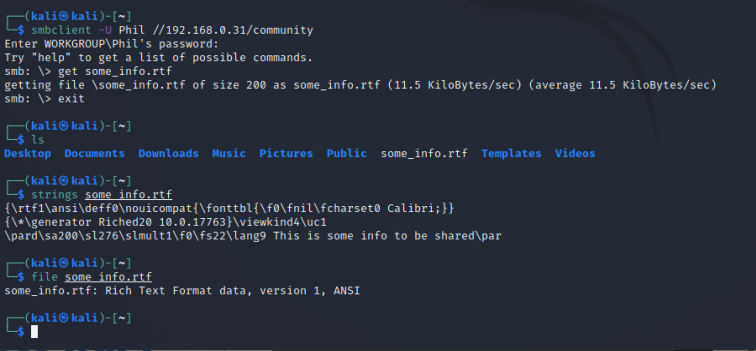


as seen below running ls command shows some\_info.rtf is available

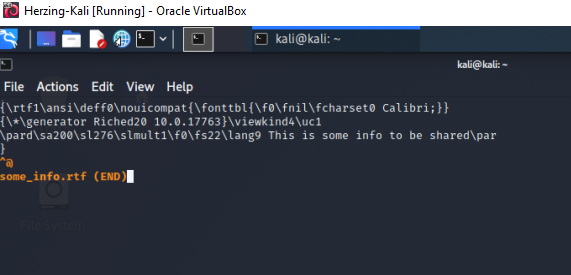


1. Get the only file in the share with the command “get”, then exit. From the Linux shell, use the commands “file” and “strings” to show information about the file and its content.

The following screen shot shows ‘get’ command execution, then ‘file’ and ‘strings’ commands execution.



Using less some\_info.rtf command shows the contents of the file as shown below:

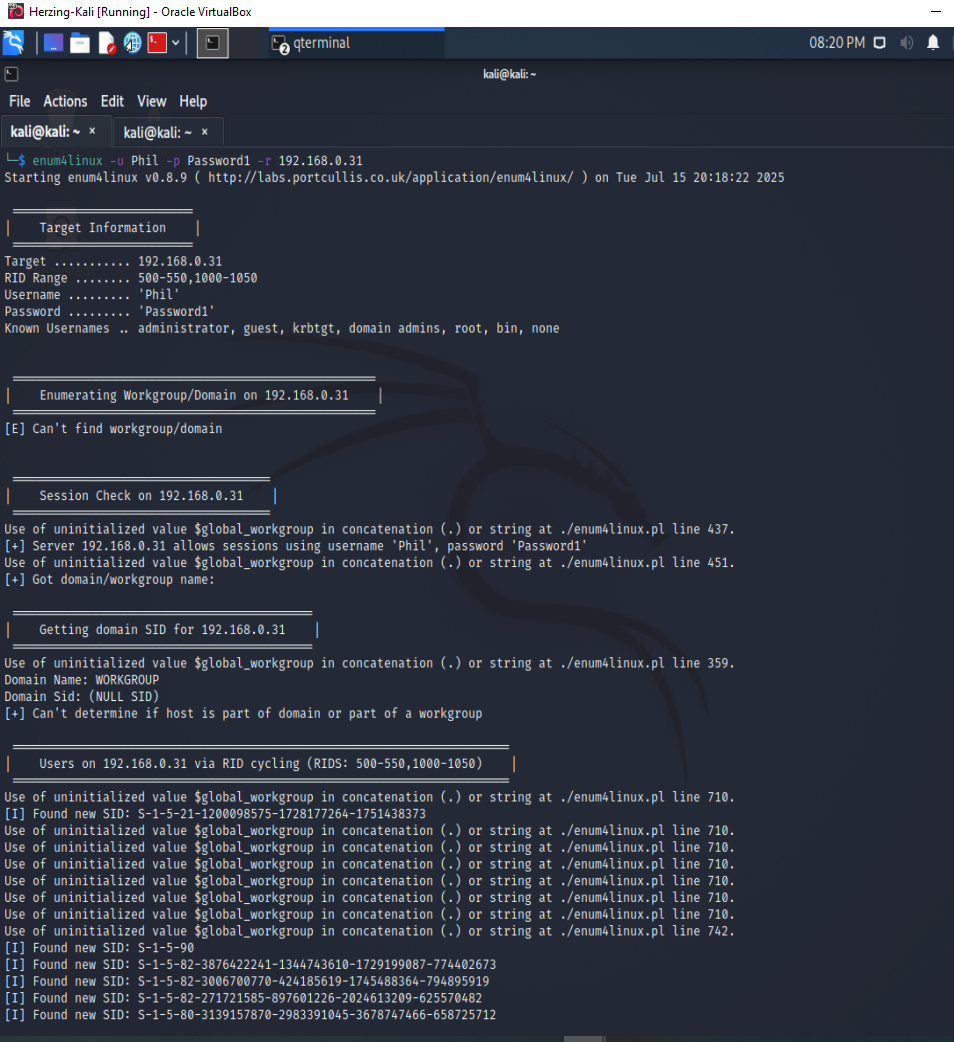


1. Enumerate the users and groups using the credentials of Phil. What command did you use? What is the SID of the ITDept group? Tip: get help with --help about two different options to enumerate users.

The command used to enumerate users and groups with the credentials of "Phil" is:

enum4linux -u Phil -p Password1 -r 192.168.0.31

In the screenshot below, we see four users which have been enumerated.

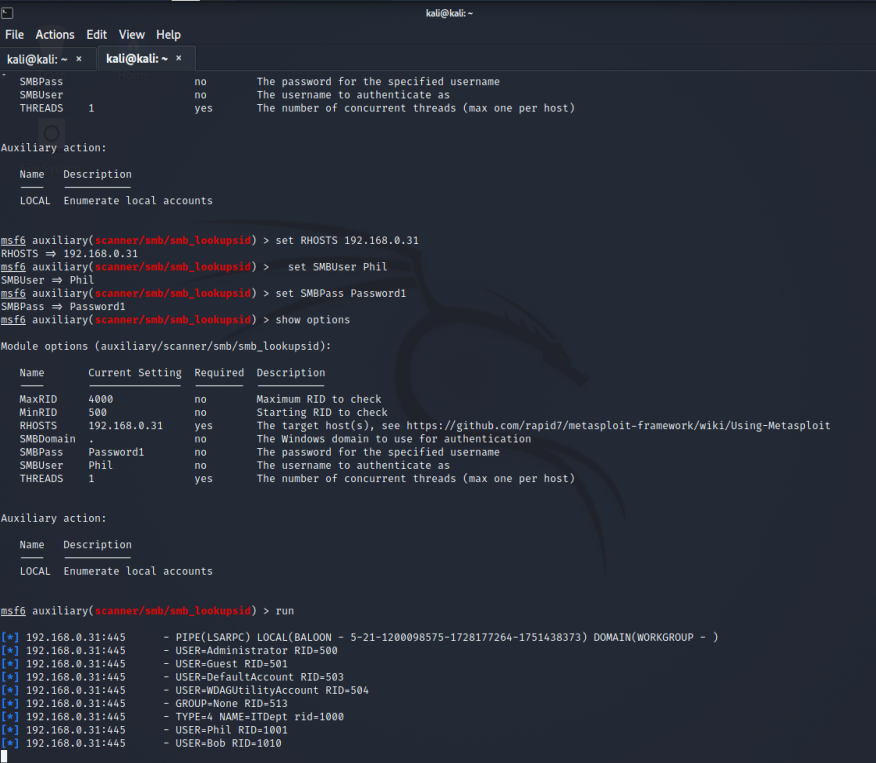


1. To try a different method, execute “msfdb init && msfconsole” to initialize and start the Metasploit Framework, which is an interactive tool accepting commands on the new prompt. To set the module you need to enumerate patches in Windows, execute the command “use auxiliary/scanner/smb/smb\_lookupsid”, then “show options”. Capture a screenshot.

Here’s the screen shot as instructed.



1. Set the required variables with “set VARIABLE VALUE” for a enumeration using Phil’s credentials (check the reference tutorial). Then, execute “run”.



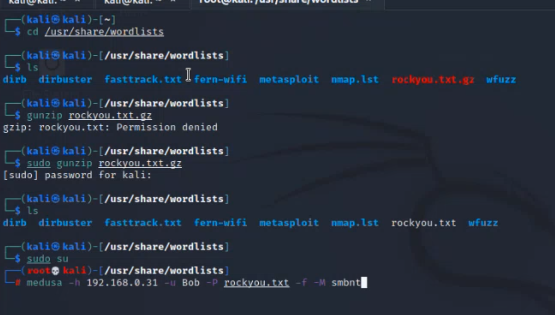
Part C: Dictionary attack

Reference tutorial: <https://en.kali.tools/?p=200>

1. Using the tool medusa, obtain the password of the user Bob. You will need the password dictionary file rockyou.txt located in /usr/share/wordlists, and the parameter -f to stop after the password is found. What is the command you used?

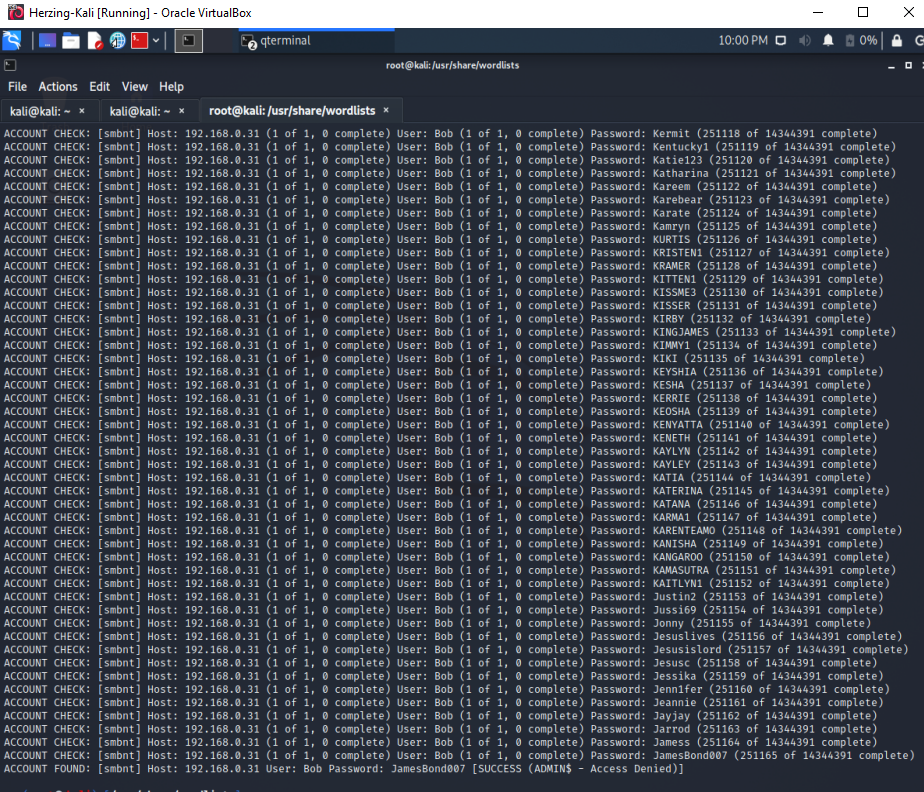
The following command was used:

**medusa -h 192.168.0.31 -u Bob -P rockyou.txt -f -M smbnt**



1. What is Bob’s password? Capture a screenshot of the last lines.

Bob’s password: JamesBond007



Part D: Research

1. What Metasploit Framework module would be useful to perform a TCP port scan?

The Metasploit Framework module that would be useful to perform a TCP port scan is located under the auxiliary scanner modules, specifically: auxiliary/scanner/portscan/tcp

1. And to search for endpoints with RDP open?

To search for endpoints with RDP open using Metasploit Framework, you would use an auxiliary scanner module specifically designed for RDP. The relevant module path is:

auxiliary/scanner/rdp/rdp\_scanner

1. What the module auxiliary/scanner/ssl/openssl\_heartbleed would be used for? What is the CVE of the vulnerability it exploits?

The Metasploit Framework module auxiliary/scanner/ssl/openssl\_heartbleed is used to detect and assess the presence of the Heartbleed vulnerability in OpenSSL implementations on a target system. This critical vulnerability allows an attacker to read memory from the server, potentially exposing sensitive data.

The **CVE** (Common Vulnerabilities and Exposures) for Heartbleed: The Heartbleed vulnerability is officially identified by **CVE-2014-0160**.

1. What medusa modules could you use against a mail server?

When looking for medusa modules to use against a mail server, you would typically consider the common protocols used by mail servers -

Imap (for Internet Message Access Protocol)

pop3 (for Post Office Protocol version 3)

smtp (for Simple Mail Transfer Protocol)

1. What medusa modules allow to set the user-agent?

The Medusa modules that allow you to set the User-Agent are the HTTP-based modules, such as http, http-get, http-post, and those designed for web forms like webform.mod. The User-Agent is an HTTP header, making it relevant when brute-forcing web authentication services.