Name: _____ **Student ID:**

You will need:
RedHat Linux 7.3 (VM)
WindowsXP Control (VM)
Windows XP (VM)
A computer with internet access

COS30015 IT Security

Lab 4 (week 4) Malware

In this lab you will infect a Windows virtual machine with spyware and other malware while observing their effects.

1. Download and Launch the COS30015 / **Redhat Linux with local network** VM image.
2. Download and Launch the COS30015 / **Windows XP with local network** VM.

Alternatively zipped copies are on Cloudstor here:
https://cloudstor.aarnet.edu.au/plus/s/RISyUom4r15oRa7

3. Click through any VMWare popups that may appear.

Part 1: Spyware

Vundo

4. In XP, start **Wireshark (desktop icon)**
   From the Wireshark menu…:
   select **Capture Options**
   Click "**Start**"

5. Open Explorer (NOT Internet Explorer!) *(or <Windows> + E)*
   `Start / Run…  Explorer.exe`
and go to the **C:\WINDOWS\System32** folder (in *Computer*). Sort the file listing by **date modified** such that the most recent file is at the top of the list. The most recent files should be ***wpa.dbl*** followed by some files starting with ***perf***….

Any newly created files will appear at the top of this list as they are added. You can press **F5** to refresh the list.

6. In XP Start the web browser and go to
http://192.168.100.104 or www.server.com

Do any files change in the System32 folder?

No change

7. In XP start the browser 

, go to http://192.168.100.104/nasty/ or www.server.com/nasty or click on the ***Free Software and Cracks*** link.

Click on ***passwords***
And **open** the file…

If you run the file as admin, you will be seriously infected. Fortunately this VM will revert to it's clean state if completely shutdown after the lab.

Name: _____ **Student ID:**_____

Launch 1001Passwords.exe.
Select Install,

Looks like some useful stuff…

Close the command window and have a look at System32 – refresh **(F5)…**

What files are new?

There are two newly added dlls with randomly generated names.
Sometimes there is a new .exe file (empty)

Observe the activity on ***Wireshark.***
It may take a few minutes before the Trojans wake up and start transmitting.
Scroll to the bottom of the packet list. You will see a series of unsuccessful name queries.
What do you see? Describe the colours and protocols.

There are packets marked in blue, black and yellow – Blue for DNS lookups, Yellow for NetBios Lookups and Black for ICMP replies (destination unreachable).

Observe the activity on Wireshark again. You may need to scroll to the right to see the Info about the packets at the bottom of the list.

Something is trying to get the IP addresses of three web sites.
You should see a Trojan try to contact ***SEARCHMEUP.BIZ***.

What other web sites are the Trojans trying to contact?

A variety of BIZ and HK domains
(changes from season to season, year to year depending on who has leased the malware distribution channel)

NOTE: The IP address of these sites is not known by the Trojan – it uses NetBIOS and ARP requests to find them.

How could we find out what the Trojans are trying to send to their masters?
(hint: DNS spoofing - man-in-the-middle attack)

Use a proxy server or something like Burp Suite to capture the packets and then connect to the malware. Display the traffic once the connection has been made.

Name: _____ **Student ID:**_____

8. Start ***MalwareBytes anti-malware***
   Start from the desktop icon, and then wait about a minute for the splash screen.
   Run a Quick scan.
   It should take about 2 minutes.

While that is happening, open Explorer.exe and go back to System32:

The top few files (.dlls) were put there by the malware.
Try deleting them. **What happens?**

Windows has locked one

The file that is loaded into memory is locked so that you can't delete it. After a re-boot the registry entries will be used to load both files into memory, as well as other Trojans which are stored in other places.

How many infections are found? What are they?

Trojan Vundo
May also detect: Generic Trojan, Mezzia trojan Vundo, Virtumonde, HiltQuilt

Try deleting it (***Remove*** in Malwarebytes)

What do you have to do?

Reboot

A file that is loaded into memory is locked so that you can't delete it. After a re-boot the registry entries will be used to load both files into memory, as well as other Trojans which are stored in other places.

When Malwarebytes has finished, Click on **Show Results**.
What are some of the names of some of the Trojans?

Trojan Vundo
May also detect: Generic Trojan, Mezzia trojan Vundo, Virtumonde, HiltQuilt

The malware may crash Malwarebytes… It's natural enemy

Click on the ***Additional Information*** tab for more information.

On the host PC, read here:

http://www.pc1news.com/news/0964/trojan-mezzia.html

Type *Vundo* into the search box. Vundo has many names and is constantly re-compiled and re-deployed.

How many versions are there? Earliest? Latest? What does it do?
Try Googling *Vundo history*.

Many.
Downloads other malware and pop-up ads, uses root-kit tricks to hide from the operating system.

9. On the lab PC, Look up **`CoolWebSearch`** on Google (host PC).

What is CoolWebSearch?

nasty spyware – a browser hijacker

The Trojans we saw today are mild and are easily removed. Some of the nastier ones require booting into safe mode and / or using another operating system to remove them.

Now that the VM has re-booted, note that there are still extra programs on the VM desktop. These will re-infect it if run.

We need to clean up VM, and the quickest way is to replace it.

Use the Start button to select ***Turn off*** (do not select ***restart***). This will ensure that VMPlayer closes and restores to VM to its previous (uninfected) state.
Start the XP VM up from Virtual Machine Launcher
You should get an uninfected fresh copy. If not, shut it down again and download a fresh copy from Virtual Machine Launcher.

Name: _____ **Student ID:**_____

Arucer

10. The VM image you're using can be infected with the Arucer Trojan. It opens a port (7777) and streams keystrokes out to its maker.

Let's get infected:

(Optionally) start Wireshark in the XP VM and start monitoring packets.
On the VM, open a terminal window (Start/Run/cmd)
Run `netstat -a`, and write down any LISTENING TCP ports

```
Proto  Local Address
 TCP    XPPro:epmap
 TCP    XPPro:microsoft-ds
 TCP    XPPro:1025
 TCP    XPPro:5000
 TCP    XPPro:netbios-ssn
```

In the browser, go to
http://www.server.com/bunny
Download and run the **`EnergisterDuoSetup.exe`** file
Click through all the prompts.

Let's detect it:
In the terminal window, run **`netstat -a`**
Is port 7777 listening?

```
...
TCP    XPPro:5000
TCP    XPPro:7777 yes- here it is!
TCP    XPPro:netbios-ssn
...
```

How do we know what it is? (a rhetorical question).
Does ***netstat*** have a command that reveals the binary?

Try ***netstat /?***

```
not in Windows.
```

Name: _____ **Student ID:**_____

Try *netstat –ao* and write down the PID number for port 7777

1652
(will be different for everybody)

3324 (for example)

On the desktop of the XP VM, locate "Process Explorer" (**procexp.exe**) and run it. Look up the PID you wrote down before.

Check the **`rundll32.exe`** process – Double click for **properties.** Select the TCP/IP tab.
There it is! port 7777

Check the other tabs to find where the **Arucer dll** is stored and where it is run. **What is the command line used to run it?**

rundll32 C:\WINDOWS\System32\Arucer.dll,Arucer

Try searching for the string "Arucer" in the registry.
In the command console, type **`regedit`**
Select the top of the tree, and **`Edit/Find`**... **`Arucer`**

You can probe Arucer by running ***arucerprobe.exe***. The binary is on Canvas with the source code.
Download it (Save Link As…), drag it onto the desktop of the VM and run it. You can monitor the interaction with Wireshark.

Part 2 . Remote Access

11. In the RedHat Linux VM, Log in as *root* (the password is *security*).

Find the executable called ***shell2***.

locate shell2

Where is shell2 located?

/home/student/

As a root user, you can go anywhere in the Linux file system, even into other user's home directories. However, we will log in as student.
log out:

exit

12. Log in to Linux as student

student (password)

Use ***ls –l*** to see what files are there and how big they are.

Look at the file: ***hello1.asm***
try
cat hello1.asm

What kind of code is this?

Assembly language source code

Look at the file: *fixasm*
try
cat fixasm

What kind of code is this?

Bash (Linux command-line) script

Try to compile *hello1*. Try this:
nasm –f elf –o hello1.o hello1.asm

Link it:
ld –o hello1 hello1.o

Permit it to run:
chmod +x hello1

Run it:
./hello1

Can you explain what you just did?

compiled and linked a hello world application written in assembly language.

13. Have a look at *socket.asm*

Name: _____ **Student ID:**_____

more socket.asm

What does this program do? (read on to find out)

The
push long 0x68732f2f
push long 0x6e69622f
tells the operating system to create a shell (**/bin/sh**)

You can covert hex to ASCII at http://www.dolcevie.com/js/converter.html
- Use a browser on the host computer of course!
Type in 68732f2f6e69622f and convert.
Still doesn't make sense? Read it backwards!

The
push long 0xAAAA02AA
is the port number bound to a listening socket.

How many bytes are in *socket.s*?

96

ls -l socket.s

The code in ***socket.s*** could be inserted into the free space in a trusted (innocent) program, which the user would be tricked into installing / running.

Run socket:
./socket &

What does the & do?

launches the program in a new shell/thread

Alternatively, remote login to Linux using ssh (Putty) or Telnet and start **nohup socket** *before logging out.*

You can log out from Linux now. **socket** will keep running.
Now that socket is running, you can access the Linux shell remotely ***without logging in!***

14. In Windows XP (VM), start up Internet Explorer.
Surf to http://www.server.com/remote
Run the program ***Wintcpclient.exe***
You now have backdoor access to the RHLinux73!

If Wintcpclient stops as soon as it starts, go back to linux and login as student and type jobs a few times to unbind the port and kill the process.

Type in a few Linux commands to see where you are and what you can do.
Try
Ls
ps -al
touch zzz
rm zzz
cat /etc/passwd

14a. (alternative client) – you will have to repeat the **./socket &** command in Linux if you have already completed step 11.
Get a copy from the Cloudstor repo (URL at the top of this document).

~~You may need to set the IP address to something on the same subnet as RHLinux7.3. Try **ifconfig eth0 192.168.100.201** and then ping 192.168.100.104 to check connectivity.~~ Nup, should be set up

Open a Console (from the desktop)
type in nc 192.168.100.104 43690
You now have remote control of ***RedHat Linux*** !

15. If you have time, start up the Windows XP Control VM , surf (from the Windows XP VM) to www.control.com, and infect yourself with a RAT.
Open the appropriate RAT console (e.g. Gh0st.exe for gServer.exe), wait for the RAT to phone home, and then try out the remote controls.

Gh0stRAT: Start the client (Gh0st.exe) on XPControl, Download and run the server (gServer.exe).
In the XPControl VM the victim machine will soon appear in the Client console.

DarkComet: Start the Client (Client.exe) on XPControl. Create a server:
Edit Server / server module
Select Network Settings
Click the down arrow next to IP/DNS: Select Get LAN IP
Click Add this configuration
Select Install Message, add an icon and a message
Select Module Shield, click on Disable win firewall, disable windows UAC
Select Build Module, click Build Server
Select c:/Inetpub/wwwroot/gmail.exe
Backspace over the .exe, Save
Close window.
In Windows XP, download and run gmail.exe
In the XPControl VM the victim machine will soon appear in the Client console.

Back Orifice: Start the Client (BO2Kgui.exe) on XPControl. Download and run the server (dnsclient.exe).
In the XPControl VM, port scan the subnet for port 6666
Superscan: StartIP:192.168.100.0, End IP:192.168.100.255
start the scan. Note the IP which has port 6666 open.
Once the IP is discovered, add it into the Bo2Kgui console (File / New Server), Click to connect. The victim machine will soon appear in the Client console.

Sub7: Start the client (SubSeven.exe) on XPControl. Download and run the server (Server.exe). Click Connect on the client console.

16. Shut down all guest OSs, close VMWare, the browser, etc. and log out.

End of Lab