### COS30015 IT Security – Lab 2 August 2023 V2

### Introduction:

In this we are going to learn on:

1. How to connect to a server via Virtual Network on VirtualBox
2. Learn how to identify connections to Web Server
3. Learn introduction to Wireshark on Kali.

### Phase 1: Initial Preparations

In case you have not completed the CYSA2014 setup in VirtualBox, follow the steps below:

**Running CySCA2014InABox inside VirtualBox**

1. Execute your VirtualBox
2. In Windows File Explorer, navigate to the folder where you have unzipped the CySCA2014InABox.7z file earlier.
3. Double-click on CySCA2014InABox Virtual Machine Definition file (NOT the Virtual Machine Disk Format)

A screenshot of a computer

Description automatically generated

1. Your Image OS (UBUNTU 12.04.4) should be included now, then Click Start on VirtualBox
2. Login Username: **user** and password: **CYSCA2014user**
3. Once everything running well, you may close your virtual machine (Ubuntu OS), by choosing File – Close – Power off the machine. This is to continue any setup needed after this.

Ensure the following VM settings:

1. VirtualBox with CYSCA2014 VM with Network setting of Host-Only Adapter
2. VirtualBox with Kali Linux VM with Network setting of Host-Only Adapter
3. Ensure no error on Setting Panel (look at the bottom message of the panel). Example there is error on Display to be set to **VMSVGA**

**Phase 2: Execution of VMs**

Start both VMs and login using the following credential:

|  |  |
| --- | --- |
| Kali Linux: | Login: **kali**  Password: **kali** |
| CYSCA2014 VM | Login: **user**  Password: **CYSCA2014user** |

Identify their respective IP addresses using command **ifconfig**: (Fill-in below)

|  |  |
| --- | --- |
| Kali IP | 192.168.100.103 |
| CYSCA2014 IP | 192.168.56.101 |

Question:

|  |
| --- |
| What is the purpose loopback address in both VMs?  (You may search Google on this) |
| The IP address 127.0. 0.1 is called a loopback address. Packets sent to this address never reach the network but are looped through the network interface card only. This can be used for diagnostic purposes to verify that the internal path through the TCP/IP protocols is working. |

**Sample on Kali:**

A computer screen shot of a computer program

Description automatically generated

Now, ping from Kali to CYSCA using ping -c 3 <CYSCA IP Address>

Then ping from CYCSA to Kali using ping -c 3 <Kali IP Address>

This is to ensure that they are on the same internal local network of VirtualBox.

**Phase 3: Investigating CYSCA Server**

1. Enter command: ps – A | more

ps refer to process status, -A means all, vertical bar is a pipe, with more means, pause between terminal page when viewing.

Try also command: ps -e

1. Your terminal screen will pause between page showing list of running processes.
2. Press Enter one-by-one page, observe the list of the processes.
3. Look at any process name ending with **d** – these are daemons
4. Anything starts with k – these are hooks for the GUI, not important for us.
5. Using Google search for the following Linux processes and its purpose:

|  |  |
| --- | --- |
| **Process** | **Purpose** |
| udevd | udev is a generic device manager running as a daemon on a Linux system and listening (via a netlink socket) to uevents the kernel sends out if a new device is initialized or a device is removed from the system. Example: use plug in thumb drive |
| rsyslogd | **Rsyslog** is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. |
| acpid | ACPID is a completely flexible, totally extensible daemon for delivering ACPI events. It listens on a file (/proc/acpi/event) and when an event occurs, executes programs to handle the event. |
| sshd | The Secure Shell Daemon application (SSH daemon or sshd) is the daemon program for ssh. This program is an alternative to rlogin and rsh and provides encrypted communications between two untrusted hosts over an insecure network. The sshd is the daemon that listens for connections from clients on port 22. |
| atd |  |
| mysqld |  |

1. On your Windows host computer, using Google search for vulnerabilities related to:

|  |  |
| --- | --- |
| **Process** | **Vulnerabilities** |
| rsyslogd | Possible buffer overflow, remote code execution |
| sshd | The vulnerability, which is a signal handler race condition in OpenSSH's server (sshd), allows unauthenticated remote code execution (RCE) as root on glibc-based Linux systems; that presents a significant security risk. This race condition affects sshd in its default configuration |
| mysqld | 1. SQL Injection: · 2. Improper Input Validation: · 3. Concurrent Execution using Shared Resources |

1. We are now going to locate **access.log** of **CYSCA** server.

Purpose of **access.log** on server is:

|  |
| --- |
| Access log: An access log gathers data related to the files requested from the server. This log will reveal the number of users who accessed the server, how they were directed to the site, and their activity on the site. |

On CYSCA command enter:

find / -name access.log 2>/dev/null

What is the path return as the output?

|  |
| --- |
| Var/log/apache2/access.log |

1. We are going to view the access log contents. Two ways of doing this in command:

Enter command: more <the log path above>access.log

If you are using more on the terminal output, CTRL+C to stop the viewing.

Or viewing in Nano editor:

nano <the log path above>access.log

If you are using Nano, CTRL+V to move to next page and CTRL+X to exit the editor.

|  |
| --- |
| Describe what you see in the access.log  Web access log to the CYSCA Apache web server. Showing date/time and protocols among others. |

1. Now, we are going to view any errors on the server by viewing the error.log. Use the same command above, except you want to view **error.log**

Use Nano editor to view the error.log. Here is the sample error.log:

A screenshot of a computer

Description automatically generated

1. What do you think about error log on line 4?

|  |
| --- |
| Unable to identify image at the file location |

1. Exit Nano editor by CTRL+X. Don’t save or edit anything.

**Phase 4: Connecting Kali with CYSCA server.**

1. Show active network connection on Kali by entering on Kali Terminal, command of: netstat

Wait for a while for the output.

1. What is the purpose of netstat command above?

|  |
| --- |
| The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information. |

1. Now, we are going to filter the above output, only to show SSH connections. Use command: netstat -a|grep ssh

Any output on Kali? Go to CYSCA server, enter the same command. Any TCP connection occurs?

1. Let us connect to the CYSCA server using command:

ssh user@192.168.n.n

(Use the CYSCA IP that you have identified in Phase 2 above.)

If Kali has error regarding RSA key being offered by the server, enter this command:

ssh -oHostKeyAlgorithms=+ssh-dss user@<IP addr>

Don’t forget the CYSCA server password is: **CYSCA2014user**

1. You are now connected to CYSCA via SSH connection on Kali terminal. Open 2nd terminal on Kali and enter netstat command:

netstat -a|grep ssh

Wait for the output.

|  |
| --- |
| Provide screen capture of Kali output here: |

1. Go to CYSCA server and enter same command:

|  |
| --- |
| Provide screen capture of CYSCA output here: |

1. What is the SSH port number and what port number use to assists the connection?

|  |  |
| --- | --- |
| SSH port number: (Google it) | 22 |
| What port number assisting the Kali to CYSCA SSH connection? (Refer to the output number after the Kali IP address) | 60164 |

1. What happen if there is another computer connected to CYSCA server at this moment?

|  |  |
| --- | --- |
| Expected changes to the output of netstat command: | Yes |
| Any changes on port number assigned? | New random port number assign to client |

1. Now, we are going to observe TCP connection between Kali and CYSCA server. On Kali open Firefox browser. Then enter URL of CYSCA server IP address.

|  |
| --- |
| Describe what you see on the Firefox browser: |

1. Close Firefox once done.

**Phase 5: Investigating connections with Wireshark.**

Before we start, ensure CYSCA & Kali still running. Remember back the IP addresses for CYSCA and Kali in phase 1.

1. From Kali, SSH to CYSCA server if you are not done so. Remember command: ssh user@<CYSCA IP address> with password of **CYSCA2014user**
2. If you don’t have 2nd terminal open in Kali, open it now. So that on Kali you have terminal open that currently SSH with CYSCA and a terminal local to Kali. Observe the prompt.

Refer below:

A screenshot of a computer

Description automatically generated

1. Execute command: netstat -a|grep ssh on both Kali terminal and at CYSCA server. You should be able to see output of the SSH connection between both.
2. Now, open Wireshark on Kali by choosing Kali icon (Top Left), then in Search bar enter: **Wireshark**.
3. On Wireshark, select menu **Capture – Option – eth0**, Then enter **tcp** in the Capture filter for selected interfaces at the bottom. (Refre the figure below) Finally, click button **Start**.

A screenshot of a computer program

Description automatically generated

1. On Kali, re-open Firefox browser and browse over to CYSCA server by entering 192.168.n.n/index.php

You should see the **Welcome page of Fortress Certifications** a vulnerable website without security.

1. Now, view back the Wireshark screen. It should capture your TCP connection and HTTP GET statement of /index.php page.

|  |
| --- |
| Put screen capture of Wireshark captured results of connection between Firefox browser (on Kali) to CYSCA Fortress Website: |

1. Try to **Sign in** and enter Email: user@yahoo.com

and password: secretpassword.

Click Login and don’t save the login on Firefox

1. You are going to have invalid username and password. But… Go to Wireshark again. And find the attempt to login result.

**Hint**: Find/Scroll until you can see HTTP POST /login.php

1. Can you see the Email and Password is sent to CYSCA server via HTTP POST. Both are not encrypted.

|  |
| --- |
| Put screen capture of the Email and Password exposed during the HTTP POST statement here: |

Now, you why HTTP alone is not secured compared to HTTPS.

1. On Kali Terminal, enter command: netstat -ap (this is to see all protocols). Scroll the results slowly until you can see Firefox connection and Wireshark on the same terminal screen.

|  |
| --- |
| Provide screen capture of the connections here: |

1. Now, go to CYSCA, enter command: netstat -ap|more
2. Press enter slowly to view page by page on the results.

|  |
| --- |
| Provide screen capture of the result where you can see the connection between Kali IP and CYSCA IP here: |

1. What can you say about the connection?

|  |
| --- |
| Answer: |

1. We are about to complete. Go to Kali, on SSH terminal connecting to CYSCA enter: **exit** and close the terminal.
2. On Wireshark, click the **red Stop** button (Near the Shark fin). Then Quit Wireshark. For the message regarding save result, in our class we always use “Continue Without Saving”.
3. Close any Kali terminal and Firefox browser. Then Shutdown Kali.
4. On CYSCA serve a proper shutdown is by entering command: sudo poweroff. And give the password.