



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Lab 3: Information is Wealth – Collect your wealth

Part 2

Cisco | **Networking Academy**[®]
| **Mind Wide Open**[™]

Task 2: Assign and investigate!!!**Work with your Team and collaborate with other teams**

Team Name		
	Member Name	Role
1		Manager
2		Analyst – T3
3		Analyst – T2
4		Analyst – T1
5		Analyst – T1

Define roles and responsibilities of each member (manager) and agree on it (members)

1. Manager:

(Record your responsibility as per the Roles)

(Record your responsibility as per the task given)

2. Analyst T3

(Record your responsibility as per the Roles)

(Record your responsibility as per the task given)

3. Analyst T2

(Record your responsibility as per the Roles)

(Record your responsibility as per the task given)

4. Analyst T1

(Record your responsibility as per the Roles)

(Record your responsibility as per the task given)

5. Analyst T1

(Record your responsibility as per the Roles)

(Record your responsibility as per the task given)

Conduct a search using your virtual machine to find out recent malware.

1. List out the malwares you find during your search. (The more in the list will give your more options to work)



2. Choose any two examples of malware by discussing with your Team and with other teams in the class, (This is a very important part of today's lab. Note that the two examples your team selects should be unique from other team. If any team has similar choices, both the team loses points)

- 1.
- 2.



Note that the two malware you choose should be a different malware type, and be prepared to discuss details on what each does, how it each is transmitted and the impact each cause.

3. Record all the discussion within the team here.



Examples of malware types include:

Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit and Vulnerability.

Search for malware by visiting the following websites (not limited to) using the following search terms:

McAfee Threat Center Threat Landscape Dashboard

Malwarebytes Labs Threat Center (Top 10 Malware)

Securityweek.com > virus-threats > virus-malware

Technewsworld.com > security > malware

4. From the two you selected and discussed, select one and write a short summary that explains what the malware does, how it is transmitted, and the impact it causes.



Task 3: Observe**Description ¹**

Social engineering is an attack with the goal of getting a victim to enter personal or sensitive information, this type of attack can be performed by an attacker utilizing a keylogger, phishing email, or an in-person method. This lab requires the research of social engineering and the identification of ways to recognize and prevent it.

5. List out different methods used in social engineering to gain access to information.

6. Compare these methods with your (as a team) day to day activities and list out the common activity/ actions which makes your vulnerable. (For example: I use or be generic, People use hotspots/ public Wi-Fi to access their mobile phones)

7. Share your thoughts, why Social Engineering is a real threat?

8. Share your thoughts, AS A Team, how can a person defend oneself from Social Engineering Attacks?

Task 4: Collect

Identify the processes running on a computer, the protocol they are using, and their local and remote port addresses.

Download and install the TCPView software.

Use a browser and observe the TCPView window.

Description ¹

For a hacker to establish a connection to a remote computer, a port must be listening on that device. This may be due to infection by malware, or a vulnerability in a legitimate piece of software. A utility, such as TCPView, can be used to detect open ports, monitor them in real-time, and close active ports and processes using them.

Instructions

Download and install the TCPView software.

Search internet for TCPView Software. List out the websites which offers a download.

Which website/ link do you think is safe to download the software? Why?

TCPView v3.05

07/25/2011 • 2 minutes to read • ●●

By Mark Russinovich

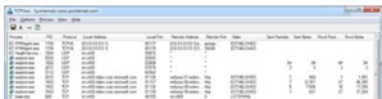
Published: July 25, 2011

 [Download TCPView \(285 KB\)](#)

[Run now from Sysinternals Live.](#)

Introduction

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.



- TCPView - Sysinternals: www.sysinternals.com

[illegible]

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Save Undo Redo

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
lsass.exe	476	TCP	pi	58702	pi	0	LISTENING				
lsass.exe	476	TCPV6	pi	58702	pi	0	LISTENING				
services.exe	468	TCP	pi	49155	pi	0	LISTENING				
services.exe	468	TCPV6	pi	49155	pi	0	LISTENING				
svchost.exe	716	TCP	pi	epmap	pi	0	LISTENING				
svchost.exe	768	TCP	pi	49153	pi	0	LISTENING				
svchost.exe	924	TCP	pi	49154	pi	0	LISTENING				
svchost.exe	1408	UDP	pi.cisco.com	ssdp	*	*		36	17,142	462	91,080
svchost.exe	1408	UDP	pi	ssdp	*	*					
svchost.exe	312	UDP	pi	ws-discovery	*	*					
svchost.exe	1408	UDP	pi	ws-discovery	*	*					
svchost.exe	1408	UDP	pi	ws-discovery	*	*					
svchost.exe	312	UDP	pi	ws-discovery	*	*					
svchost.exe	972	UDP	pi	llmnr	*	*					
svchost.exe	972	UDP	pi	54649	*	*					
svchost.exe	1408	UDP	pi	61427	*	*					
svchost.exe	312	UDP	pi	61464	*	*					
svchost.exe	1408	UDP	pi.cisco.com	63677	*	*					
svchost.exe	1408	UDP	pi	63678	*	*					
svchost.exe	716	TCPV6	pi	epmap	pi	0	LISTENING				
svchost.exe	2300	TCPV6	pi	3587	pi	0	LISTENING				
svchost.exe	768	TCPV6	pi	49153	pi	0	LISTENING				
svchost.exe	924	TCPV6	pi	49154	pi	0	LISTENING				
svchost.exe	1408	UDPV6	[0.0.0.0:0.0.0.1]	1900	*	*					
svchost.exe	1408	UDPDG	pi.cisco.com	1900	*	*					

Endpoints: 55 Established: 1 Listening: 24 Time Wait: 0 Close Wait: 0

Set your TCPView to "Always on Top". Use a browser and observe the TCPView window.

Note: Use the Help section of the program to help you answer the following questions.

Open any browser and browse any website. Eg: google.com, cisco.com etc

What happens in the TCPView window?

You could see a lot of colors highlighting in the tool. What is represented by the colors?

Close a process (my choice would be the web browser) and see what happens?

Note:

To close a process directly, right-click the process and choose End Process. Using this method can cause a program or the operating system to become unstable. Only end processes that you know are safe to end.

This method can be used to stop malware from communicating.