Text

Description automatically generated

**Name: Muhammad Izham Bin Norhamadi**

**Matrix No: B032020039**

Lab 2

CMD Commands in security

Lab Steps

# Open CMD in Administrator mode

1. **Know the IP Address of any website**

- C:\WINDOWS\system32>ping [www.google.com](http://www.google.com)

* 1. Show and explain the results.

Text

Description automatically generated

* Information about the domain such as the ip address, packet loss rate and latency to the destination
  1. What is the purposes of “ping” command?
* Ping the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution

# Resolving DNS into IP

- C:\WINDOWS\system32>nslookup [www.google.com](http://www.google.com)

* 1. Show and explain the results.

Text

Description automatically generated

* Information shown is IPv4 address of the domain and IPv6 address
  1. How the results of "nslookup" can be used by network administrator?
* Nslookup can be used to get information from DNS server such as IP address and DNS record. It can also be used to troubleshoot DNS related problems.

# Displaying the route path between your computer to website

- C:\WINDOWS\system32>tracert www.google.com

* 1. Show and explain the results.

Text

Description automatically generated

* Testing route for packets to send to google.com
  1. How can “tracert” help network administrator during network analysis?
* tracert diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. Tracert can be used to find out where a packet stopped on the network and troubleshoot from there.

# ARP table

- C:\WINDOWS\system32>arp –a

* 1. Show and explain the results.

Graphical user interface

Description automatically generated with medium confidence

* List of the network interface, target system and physical (MAC) address of each system
  1. What is the purposes of ARP?
* Each time a computer's TCP/IP stack uses ARP to determine the Media Access Control (MAC) address for an IP address, it records the mapping in the ARP cache so that future ARP lookups go faster. ARP is useful when diagnosing duplicate IP assignment problems.

# Routing table, gateway, interface and metric

- C:\WINDOWS\system32>route print

* 1. Show and explain the results.

Graphical user interface, text

Description automatically generated

* Displaying Local Routing Table
  1. What is the use of “route” command?
* The local routing table allow the system to route to the appropriate interface to reach an address. The route command allows you to make manual entries into the network routing tables.

# See IP, gateway, DNS and other info

- C:\WINDOWS\system32>ipconfig/all

* 1. Show and explain the results.

Text

Description automatically generated

IP configuration for Windows devices and adapters

* 1. How can “ipconfig” used for troubleshooting network connectivity issues?
* Ipconfig displays all current TCP/IP network configuration values. This can be used to find network addresses from the system such as IPv4 address and IPv6

# See connection status

- C:\WINDOWS\system32>netstat –an

* 1. Show and explain the results.

A picture containing text

Description automatically generated

* Shows incoming and outgoing connections, as well as listening ports
  1. How can “netstart” help network administrator during network analysis?
* Network statistics (netstat) is a networking tool used for troubleshooting and configuration as well as monitoring tool for connections over the network

# System File Checker

- C:\WINDOWS\system32>sfc /scannow

* 1. Show and explain the results.

Text

Description automatically generated

Result of scanning system files

* 1. How can “sfc /scannow” help network administrator during network analysis?
* System File Checker tool (sfc) can scan and repair missing or corrupted system files that may cause network problems

# Wi-Fi password

* C:\WINDOWS\system32> netsh wlan show profile

Text

Description automatically generated

List of all wireless network profiles

* C:\WINDOWS\system32> netsh wlan show profile SSID key=clear (replace SSID with the name of the network)

Text

Description automatically generated

Detailed information on the specified wireless profile as well as clear password

* 1. Show and explain the results.
  2. What is the purposes of “netsh wlan show profile SSID key=clear” command?
* To retrieve password for the specified wifi

# Analysis Questions

1. You have been called in to troubleshoot client’s computer, which is unable to connect to the local area network. What command would you use to check the configuration? What information would you look for?

* Use ipconfig to check IPv4 address of the client’s computer to check if it’s properly assigned to the computer and unique to other IP address in the LAN

1. You have been called in to troubleshoot a client’s computer, which is able to connect to local area network but unable to connect to any other network. What command would you use to check the configuration? What information would you look for?

* Use ping command and check the connection with a common domain such as Google.com. If it was unable to connect then the internet provider is not properly configured to connect to the internet.

1. If you needed to obtain a user’s MAC address as well as the user’s network configuration information, what command and switch would you enter?

* Use ‘arp -a’ command to display list of network interface, ip address, and physical address of each system.

1. You have just pinged a remote computer. You would now like to retrieve the MAC address of the remote computer locally. How would you obtain the remote computer’s MAC address?

* Use ‘arp -a’ command

1. What information does ping return to the user?

* Information about the domain such as the ip address, packet loss rate and latency to the destination