ETHICAL HACKING FOR BEGINNERS

INTRODUCTION

Topics

- What is hacking and ethical hacking?
- Hacker types
- Terminologies
- Networking commands

OVERVIEW OF HACKING

Hacking

- Exploiting system vulnerabilities and compromising security controls to gain unauthorized access
- new program or the making of changes to existing, usually complicated software

Hacker and Ethical Hacker

❖ Hacker

- Access computer system or network without authorization
- Breaks the law
- Own financial benefits

❖ Ethical Hacker

- Performs most of the same activities but with owner’s permission
- Employed by companies to perform Penetration Tests

necessity of ethical hackers?

Other types


Types of Hackers.
Whitehats
White Hats
Black Hats
Grey Hats
Srcript Kiddies
Spy Hackers
Suicide Hackers
Cyber Terrorist
State Sponsored Hacker

Real time famous hacking

- WannaCry ransomware attack
- Sony Pictures hack
- Zero day attack WhatsApp

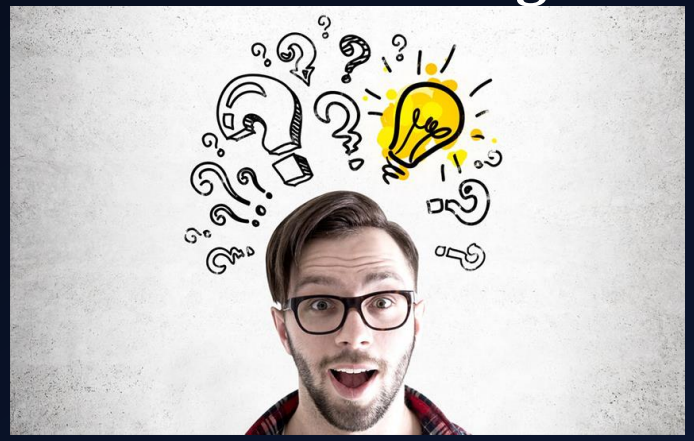
Basic terminologies

Word	Meaning
Vulnerability	Weakness Of The System
Exploit	Penetration Of Security Through Vulnerability
Payload	Part Of The Exploit Code That Automatically Malicious Activities Such As Destroying The System
Zero-day-attack	Attack That Exploits Application Vulnerabilities Before The Patch Is Released.
Bot	Controlled Remotely To Execute Automate Predefined Tasks

The Essential Skills To Becoming A Hacker

1. Basic Computer Skills
2. Networking Skills
3. Linux Skills
4. Wireshark
5. Virtualization(Linux,win,win10)
6. Security Concepts & Technologies, some electronics knowledge
7. Wireless Technologies
8. Scripting(python)

- 9. Database Skills(sql)
- 10. Web Applications
- 11. Advanced TCP/IP
- 12. Cryptography technique
- 13. Reverse Engineering
- 14. Think Creatively
- 15.Problem-Solving Skills



Basic Computer Networks and network commands

Network components

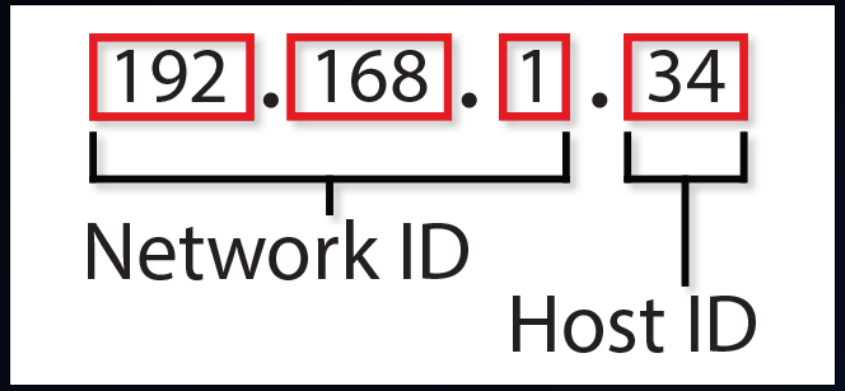
Modem

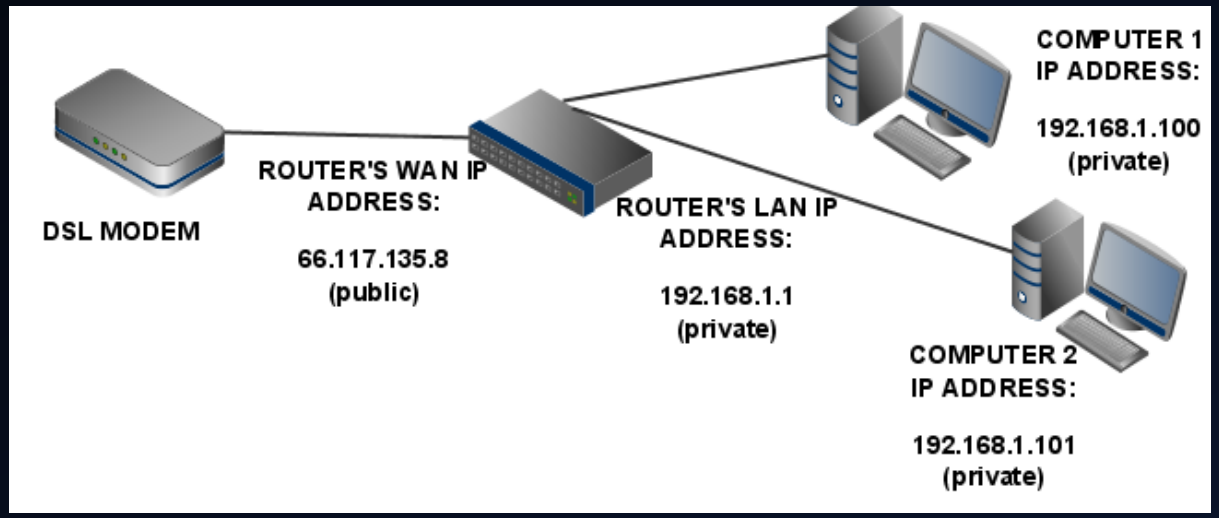
Router

Repeater

switch

IP_Address


192.168.1.34
Network ID
Host ID


DSL MODEM
ROUTER'S WAN IP ADDRESS:
66.117.135.8
(public)
ROUTER'S LAN IP ADDRESS:
192.168.1.1
(private)
COMPUTER 1 IP ADDRESS:
192.168.1.100
(private)
COMPUTER 2 IP ADDRESS:
192.168.1.101
(private)

IP_Address:

An IP Address Is A Numerical Label Assigned To Each Device Participating In A Computer Network That Uses The Internet Protocol For Communication.
Ipv4 – 74.125.236.48
Ipv6 - 2404:6800:4007:800::1012

Description	IPv4	IPv6
Address Length	32 bits	128 bits
Address representation	4 decimal numbers from 0-255 separated by periods	8 groups of 4 hexadecimal digits separated by colons
Address types	unicast, multicast, broadcast	unicast, multicast, anycast
Packet header	20 bytes long	40 bytes long, but simpler than the IPv4 packet header
Configuration	manual or through DHCP	auto-configuration of addresses is available
IPSec support	optional	Built-in

Protocol & Port

Definition for protocol:
Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used

Definition for port:
A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

Port #	Protocol
21	FTP Control
20	FTP Data
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS

Practical session

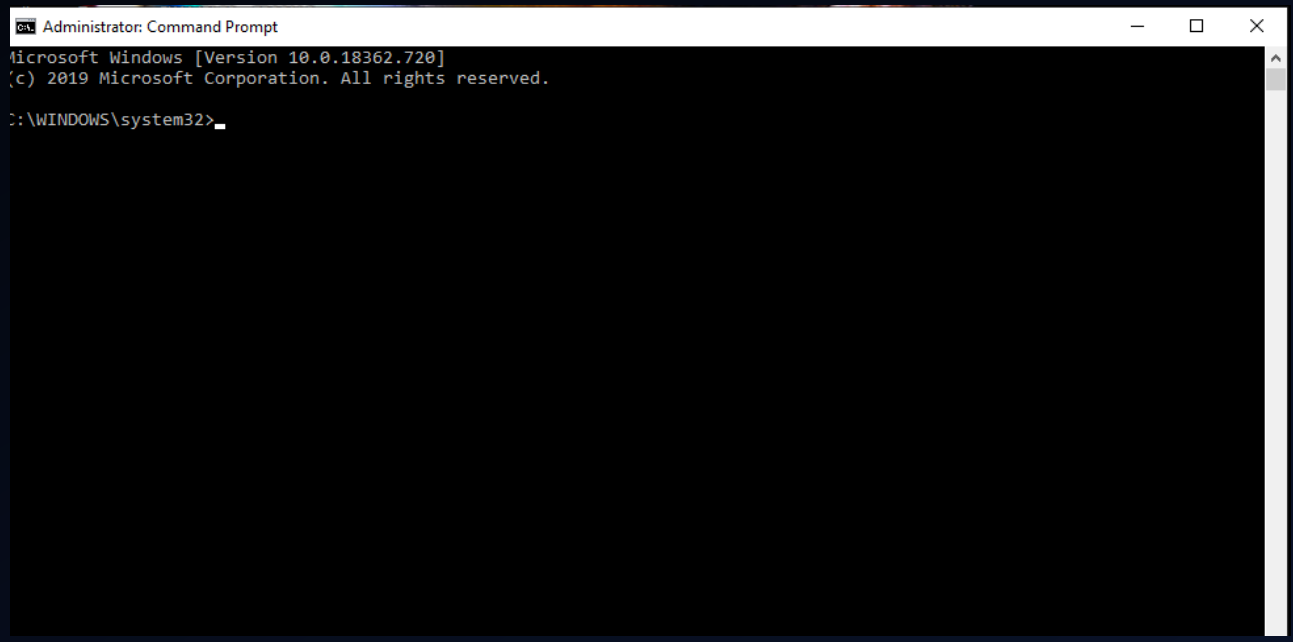
BASIC NETWORKING COMMANDS

NETWORK COMMANDS

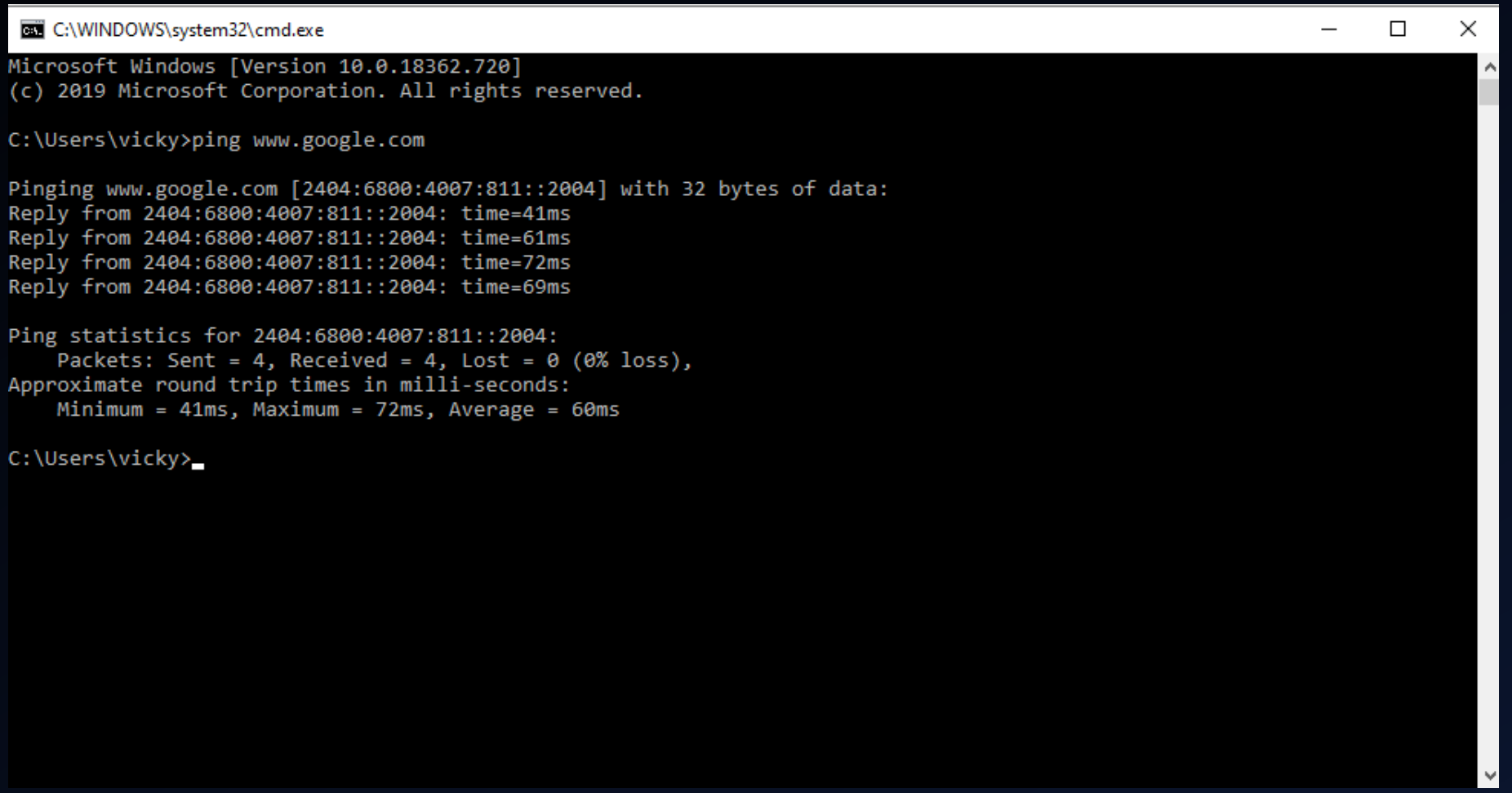
Discussing following commands

- ✓ Ping
- ✓ Ipconfig
- ✓ HOST Tracert & nslookup
- ✓ Netstat
- ✓ Arp -a

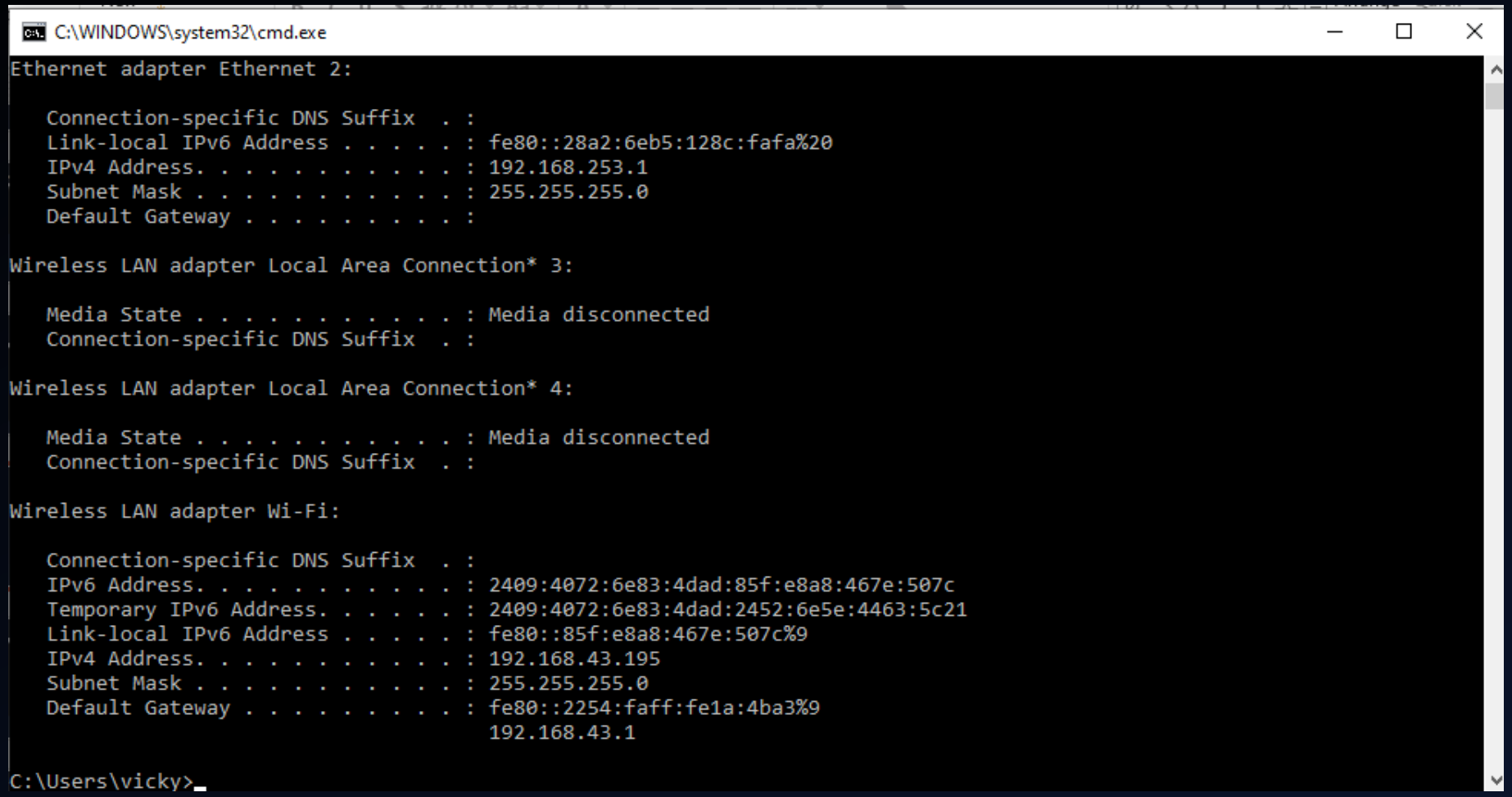
- Windows command shell



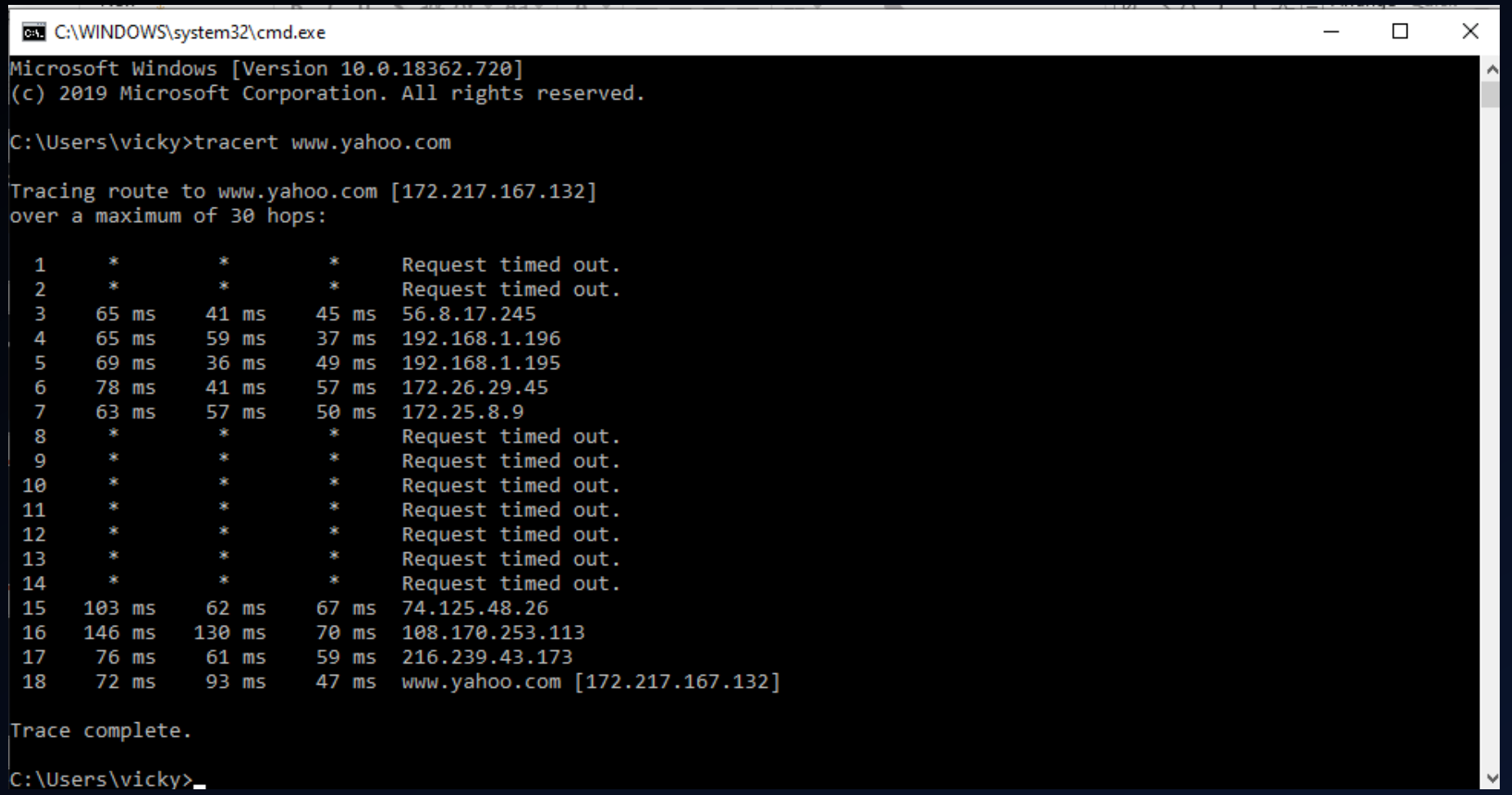
Ping


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\vicky>ping www.google.com
Pinging www.google.com [2404:6800:4007:811::2004] with 32 bytes of data:
Reply from 2404:6800:4007:811::2004: time=41ms
Reply from 2404:6800:4007:811::2004: time=61ms
Reply from 2404:6800:4007:811::2004: time=72ms
Reply from 2404:6800:4007:811::2004: time=69ms
Ping statistics for 2404:6800:4007:811::2004:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 41ms, Maximum = 72ms, Average = 60ms
C:\Users\vicky>

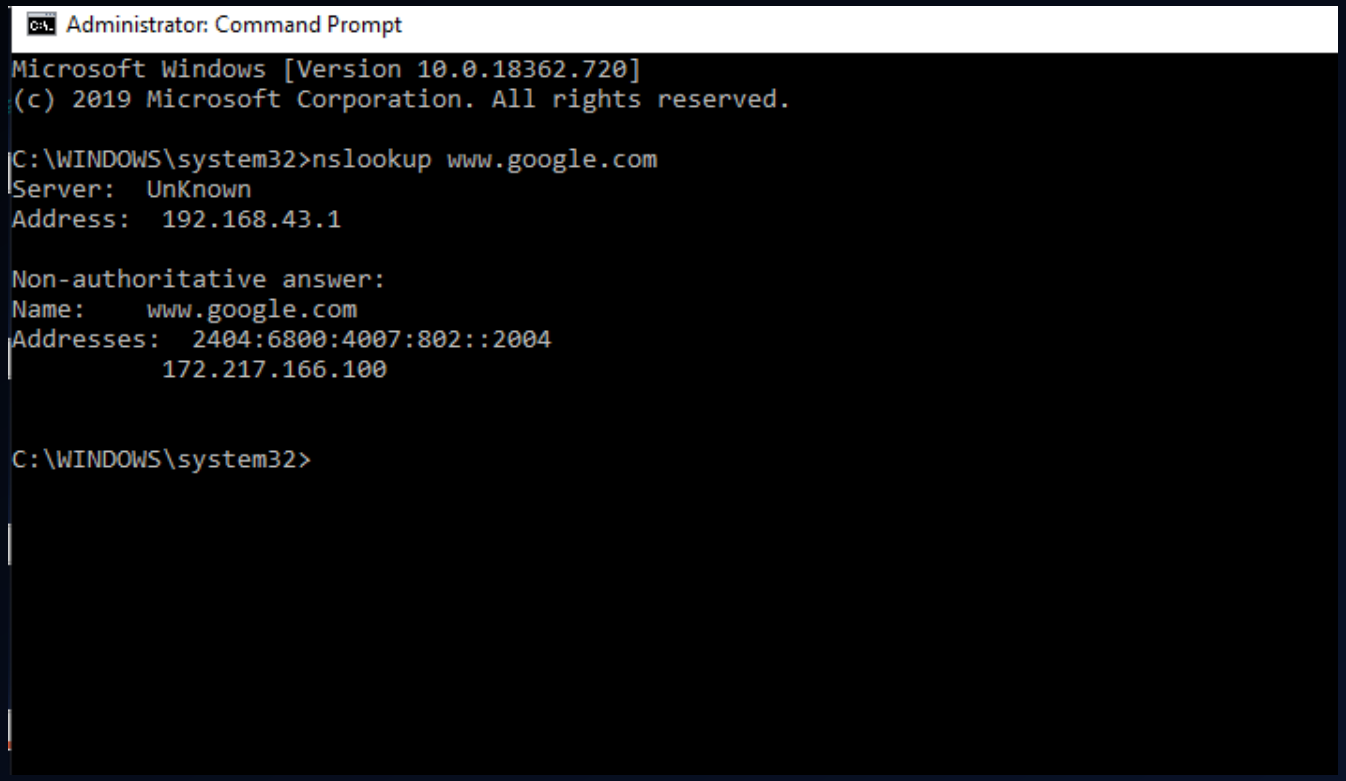
Ipconfig


C:\WINDOWS\system32\cmd.exe
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::28a2:6eb5:128c:fafa%20
IPv4 Address. . . . . : 192.168.253.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 4:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2409:4072:6e83:4dad:85f:e8a8:467e:507c
Temporary IPv6 Address. . . . . : 2409:4072:6e83:4dad:2452:6e5e:4463:5c21
Link-local IPv6 Address . . . . . : fe80::85f:e8a8:467e:507c%9
IPv4 Address. . . . . : 192.168.43.195
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::2254:faff:fe1a:4ba3%9
192.168.43.1
C:\Users\vicky>

Tracert


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\vicky>tracert www.yahoo.com
Tracing route to www.yahoo.com [172.217.167.132]
over a maximum of 30 hops:
1 * * * Request timed out.
2 * * * Request timed out.
3 65 ms 41 ms 45 ms 56.8.17.245
4 65 ms 59 ms 37 ms 192.168.1.196
5 69 ms 36 ms 49 ms 192.168.1.195
6 78 ms 41 ms 57 ms 172.26.29.45
7 63 ms 57 ms 50 ms 172.25.8.9
8 * * * Request timed out.
9 * * * Request timed out.
10 * * * Request timed out.
11 * * * Request timed out.
12 * * * Request timed out.
13 * * * Request timed out.
14 * * * Request timed out.
15 103 ms 62 ms 67 ms 74.125.48.26
16 146 ms 130 ms 70 ms 108.170.253.113
17 76 ms 61 ms 59 ms 216.239.43.173
18 72 ms 93 ms 47 ms www.yahoo.com [172.217.167.132]
Trace complete.
C:\Users\vicky>

nslookup


Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>nslookup www.google.com
Server: UnKnown
Address: 192.168.43.1
Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4007:802::2004
          172.217.166.100
C:\WINDOWS\system32>