Course Name:	**Information and Cyber Security Laboratory**	**Semester:**	**VII**
Date of Performance:	**20 / 08 / 2025**	**Batch No.:**	**B – 1**
Faculty Name:	**Prof. Makrand Kulkarni**	**Roll No.:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**___ / 25**

Experiment No.: 5
Title: To understand basic diagnostic tools in Cyber Space

Aim and Objective of the Experiment:
To understand basic diagnostic tools in Cyber Space

COs to be achieved:
CO3: Comprehend concept of cyber-crime, threats, security, cyber offenses and methods used in cybercrime.

Books/Journals/Websites referred:
Attack Statistics: 1. https://www.digitalattackmap.com/ 2. https://threatmap.checkpoint.com/ 3. MAP | Kaspersky Cyberthreat real-time map

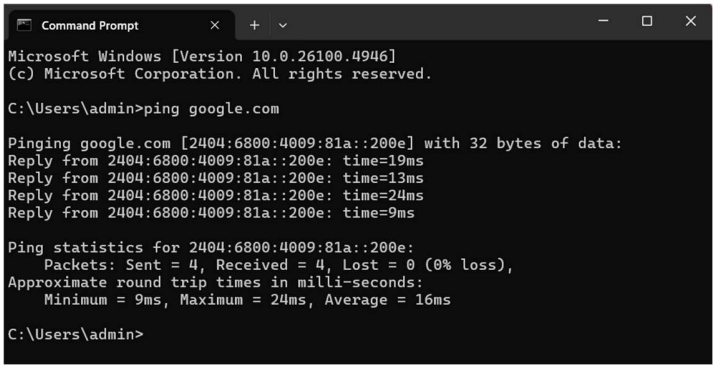
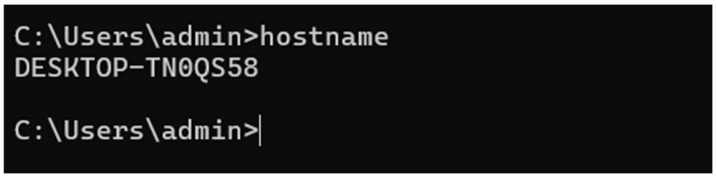
Tools required:

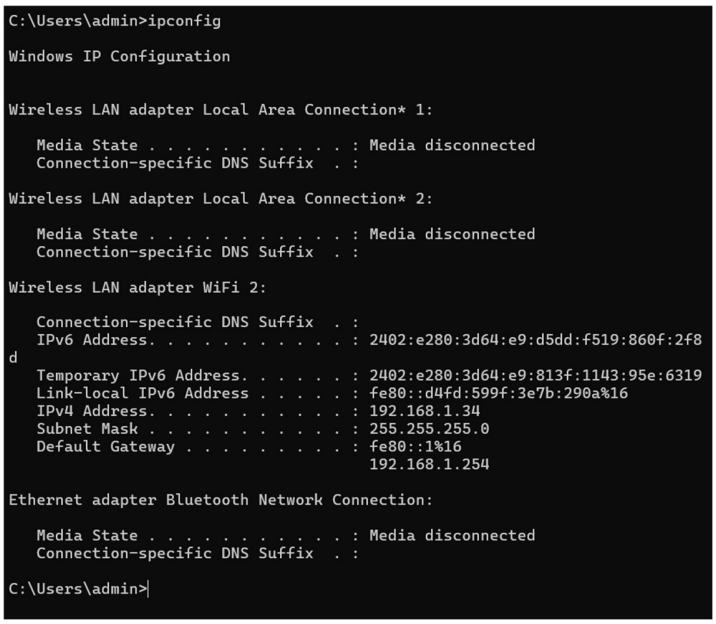
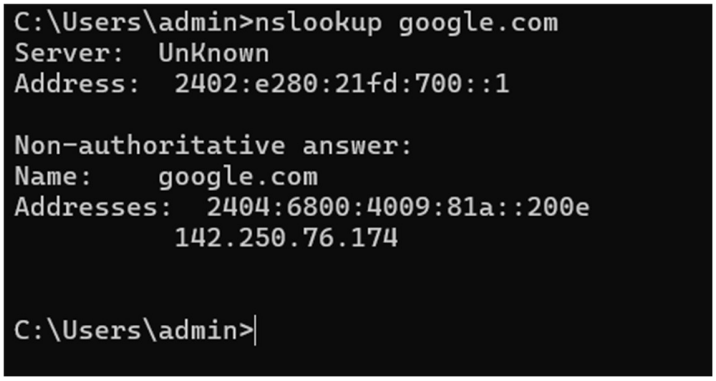
Theory:
Every Cyber expert needs a good set of tools in their toolbox to get a job done. These tools will serve to investigate and trouble shoot countless issues as they arise on network. Here are a few of the network commands every network tech should know. Attack Statistics: 1. https://www.digitalattackmap.com/ 2. https://threatmap.checkpoint.com/ 3. MAP | Kaspersky Cyberthreat real-time map TCP/IP: TCP/IP is Transmission Control Protocol / Internet Protocol, standard Internet communications protocols that allow digital computers to communicate over long distances.

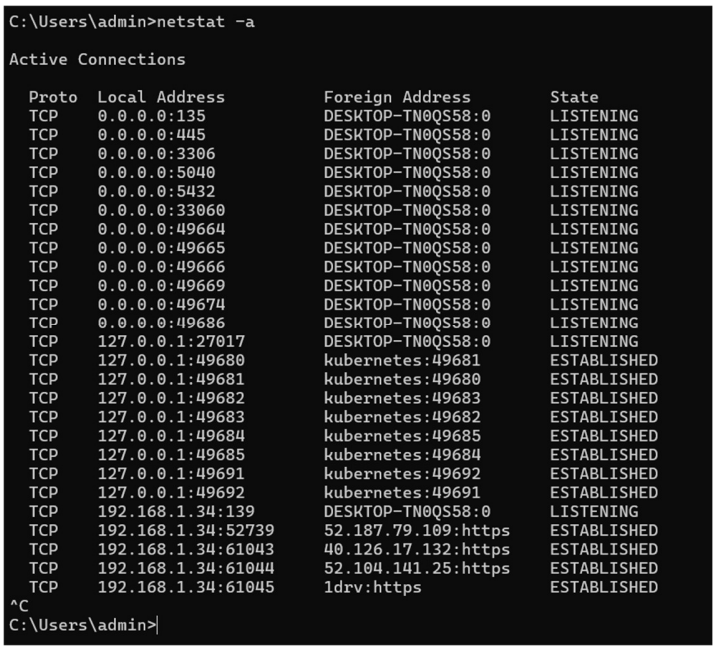
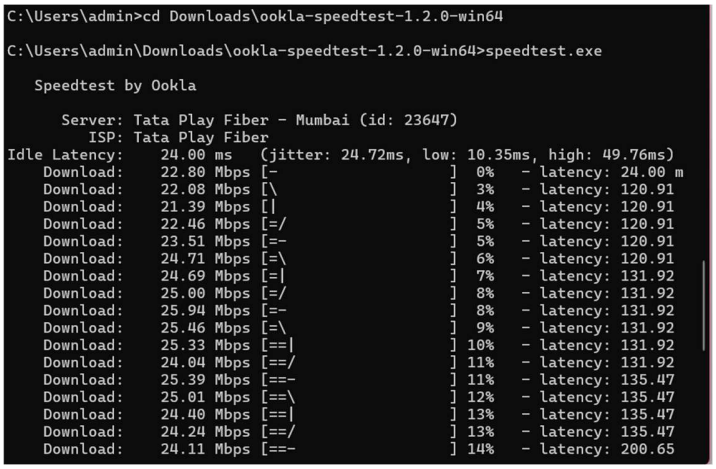
Implementation details:

1. Find out attacks statistics depends on the type of attacks
2. Top targeted Country/Top targeted Industries/Top Malware types
3. Cyber Attack statistics on India for last week
4. Add screenshots wherever applied.

Output / Screenshots:

Name Of the Command	Output	Remarks
ping	 **Shows packets sent, received, lost, and response time.**	**Tests network connectivity.**
hostname	 **Returns your computer's hostname (e.g., DESKTOP-123ABC).**	**Identifies the machine name.**

ipconfig	 **Displays IP address, subnet mask, gateway, DNS.**	**Used for checking network configuration.**
nslookup	 **Resolves domain to IP address (e.g., 142.250.183.14).**	**DNS lookup tool.**

netstat -a	 **Lists active connections, ports in use.**	**Useful for identifying open/active ports.**
speedtest		**(Required Speedtest CLI installed) Shows download & upload speeds.** **Internet speed test.**

tracert	`C:\Users\admin\Downloads>tracert google.com`
	
	`Tracing route to google.com [2404:6800:4009:81a::200e]`
	`over a maximum of 30 hops:`
	
	`1 21 ms 38 ms 4 ms 2402:e280:3d64:e9::1`
	`2 7 ms 40 ms 29 ms 2402:e280:4100::2`
	`3 40 ms 16 ms 30 ms 2001:4860:1:1::e9e`
	`4 42 ms 55 ms 11 ms 2404:6800:8281:40::1`
	`5 48 ms 34 ms 18 ms 2001:4860:0:1::7b7c`
	`6 33 ms 15 ms 10 ms 2001:4860:0:1::87b2`
	`7 13 ms 33 ms 14 ms 2001:4860:0:1::8769`
	`8 17 ms 7 ms * 2001:4860:0:1::4c6f`
	`9 18 ms 21 ms 29 ms bom12s09-in-x0e.1e100.net [2404:6800:4009:81a::200e]`
	
	`Trace complete.`
	
	`C:\Users\admin\Downloads>`
	
	Shows hop-by-hop route packets take.
		Helps diagnose routing issues.

arp -a	`C:\Users\admin\Downloads>arp -a`
	
	`Interface: 192.168.1.34 --- 0x10`
	`Internet Address Physical Address Type`
	`192.168.1.52 dc-45-46-a3-86-26 dynamic`
	`192.168.1.90 5c-b4-7e-6b-45-f9 dynamic`
	`192.168.1.254 78-17-35-b3-55-60 dynamic`
	`192.168.1.255 ff-ff-ff-ff-ff-ff static`
	`224.0.0.22 01-00-5e-00-00-16 static`
	`224.0.0.251 01-00-5e-00-00-fb static`
	`224.0.0.252 01-00-5e-00-00-fc static`
	`239.255.255.250 01-00-5e-7f-ff-fa static`
	`255.255.255.255 ff-ff-ff-ff-ff-ff static`
	
	`C:\Users\admin\Downloads>`
	
	Lists ARP table (IP to MAC mapping).
		Identifies local devices.

Whois (Website Statistics)	`C:\Users\admin\Downloads>cd "C:\Users\admin\Downloads\WhoIs"`
	
	`C:\Users\admin\Downloads\WhoIs>whois.exe example.com`
	
	`Whois v1.21 - Domain information lookup`
	`Copyright (C) 2005-2019 Mark Russinovich`
	`Sysinternals - www.sysinternals.com`
	
	`Connecting to COM.whois-servers.net...`
	
	`WHOIS Server: whois.iana.org`
	`Registrar URL: http://res-dom.iana.org`
	`Updated Date: 2025-08-14T07:01:39Z`
	`Creation Date: 1995-08-14T04:00:00Z`
	`Registry Expiry Date: 2026-08-13T04:00:00Z`
	`Registrar: RESERVED-Internet Assigned Numbers Authority`
	`Registrar IANA ID: 376`
	`Registrar Abuse Contact Email:`
	`Registrar Abuse Contact Phone:`
	`Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited`
	`Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited`
	`Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited`
	`Name Server: A.IANA-SERVERS.NET`
	`Name Server: B.IANA-SERVERS.NET`
	`DNSSEC: signedDelegation`
	`DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C`
	`URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/`
	`>>> Last update of whois database: 2025-08-20T06:28:44Z <<<`
	
	`For more information on Whois status codes, please visit https://icann.org/epp`
		We had to download and install the Sysinternals Whois utility, as it is not included by default in Windows.
		
		(Needs whois tool installed) Displays domain registration info.
		Useful for website details like it retrieves domain registration details like registrar, creation/expiry

dates, name servers, and DNSSEC status.

Post Lab Subjective/Objective type Questions:

1. **Name two common types of cyber-attacks and their reported frequency.**
   - Ransomware
     Accounts for about 35% of all cyberattacks and has surged by approximately 84% year-over-year.
   - Phishing
     Has experienced an explosive rise—phishing attacks increased by 1,265%, driven largely by generative AI tactics.

   These statistics reflect broad trends across industries globally.

2. **Which country and industry were most targeted by cyber-attacks recently?**
   - Country: The United States has become the global epicenter for ransomware,

accounting for 50% of all such attacks worldwide.

- Industry: Within the U.S., the manufacturing sector has been the most heavily targeted by ransomware (1,063 attacks), followed by the technology (922 attacks) and healthcare (672 attacks) industries.

3. **How many cyber-attacks were reported in India last week?**
   According to a recent report, the Indian healthcare sector alone faced 8,614 cyberattacks in a single week—more than four times the global average. (Tripwire)

Conclusion:

The experiment demonstrated how basic networking commands (ping, nslookup, tracert, etc.) help in analyzing connectivity, configurations, and domain information. Additional tools like Speedtest and Whois had to be downloaded, showing the importance of external utilities for extended network diagnostics.

Signature of faculty in-charge with Date: