



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

### Experiment No.: 5

#### **Title: To understand basic diagnostic tools in Cyber Space**

<b>Aim and Objective of the Experiment:</b>
To understand basic diagnostic tools in Cyber Space

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

<b>Books/Journals/Websites referred:</b>
<b>Attack Statistics:</b> 1. <a href="https://www.digitalattackmap.com/">https://www.digitalattackmap.com/</a> 2. <a href="https://threatmap.checkpoint.com/">https://threatmap.checkpoint.com/</a> 3. <a href="#">MAP   Kaspersky Cyberthreat real-time map</a>

<b>Tools required:</b>

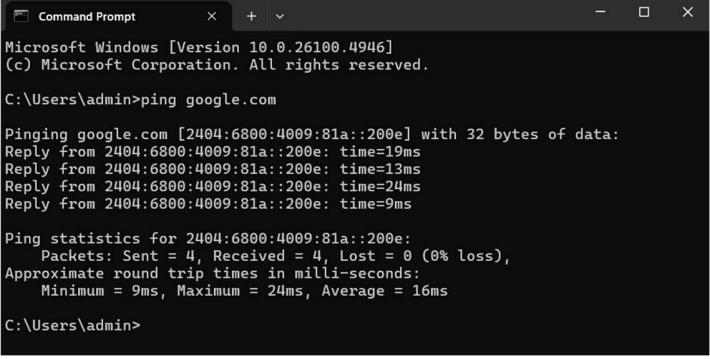
<b>Theory:</b>
Every Cyber expert needs a good set of tools in their toolbox to get a job done. These tools will serve to investigate and trouble shoot countless issues as they arise on network. Here are a few of the network commands every network tech should know.
<b>Attack Statistics:</b> 1. <a href="https://www.digitalattackmap.com/">https://www.digitalattackmap.com/</a> 2. <a href="https://threatmap.checkpoint.com/">https://threatmap.checkpoint.com/</a> 3. <a href="#">MAP   Kaspersky Cyberthreat real-time map</a>



**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	 <p>Shows packets sent, received, lost, and response time.</p>	Tests network connectivity.
hostname	<pre>C:\Users\admin&gt;hostname DESKTOP-TN0QS58  C:\Users\admin&gt;</pre> <p>Returns your computer's hostname (e.g., DESKTOP-123ABC).</p>	Identifies the machine name.



<b>ipconfig</b>	<pre>C:\Users\admin&gt;ipconfig  Windows IP Configuration  Wireless LAN adapter Local Area Connection* 1:   Media State . . . . . : Media disconnected   Connection-specific DNS Suffix . :  Wireless LAN adapter Local Area Connection* 2:   Media State . . . . . : Media disconnected   Connection-specific DNS Suffix . :  Wireless LAN adapter WiFi 2:   Connection-specific DNS Suffix . :   IPv6 Address . . . . . : 2402:e280:3d64:e9:d5dd:f519:860f:2f8 d  Temporary IPv6 Address. . . . . : 2402:e280:3d64:e9:813f:1143:95e:6319   Link-local IPv6 Address . . . . . : fe80::d4fd:599f:3e7b:290a%16   IPv4 Address . . . . . : 192.168.1.34   Subnet Mask . . . . . : 255.255.255.0   Default Gateway . . . . . : fe80::1%6                                 192.168.1.254  Ethernet adapter Bluetooth Network Connection:   Media State . . . . . : Media disconnected   Connection-specific DNS Suffix . :  C:\Users\admin&gt;</pre>	<p><b>Used for checking network configuration.</b></p> <p><b>Displays IP address, subnet mask, gateway, DNS.</b></p>
<b>nslookup</b>	<pre>C:\Users\admin&gt;nslookup google.com Server:  Unknown Address:  2402:e280:21fd:700::1  Non-authoritative answer: Name:      google.com Addresses: 2404:6800:4009:81a::200e           142.250.76.174  C:\Users\admin&gt;</pre>	<p><b>DNS lookup tool.</b></p> <p><b>Resolves domain to IP address (e.g., 142.250.183.14).</b></p>



<b>netstat -a</b>	<pre>C:\Users\admin&gt;netstat -a  Active Connections    Proto  Local Address          Foreign Address        State   TCP    0.0.0.0:135           DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:445           DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:3306          DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:5040          DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:5432          DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:33060         DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:49664         DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:49665         DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:49666         DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:49669         DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:49674         DESKTOP-TN0QS58:0   LISTENING   TCP    0.0.0.0:49686         DESKTOP-TN0QS58:0   LISTENING   TCP    127.0.0.1:27017       DESKTOP-TN0QS58:0   LISTENING   TCP    127.0.0.1:49680       kubernetes:49681    ESTABLISHED   TCP    127.0.0.1:49681       kubernetes:49680    ESTABLISHED   TCP    127.0.0.1:49682       kubernetes:49683    ESTABLISHED   TCP    127.0.0.1:49683       kubernetes:49682    ESTABLISHED   TCP    127.0.0.1:49684       kubernetes:49685    ESTABLISHED   TCP    127.0.0.1:49685       kubernetes:49684    ESTABLISHED   TCP    127.0.0.1:49691       kubernetes:49692    ESTABLISHED   TCP    127.0.0.1:49692       kubernetes:49691    ESTABLISHED   TCP    192.168.1.34:139      DESKTOP-TN0QS58:0   LISTENING   TCP    192.168.1.34:52739     52.187.79.109:https ESTABLISHED   TCP    192.168.1.34:61043     40.126.17.132:https ESTABLISHED   TCP    192.168.1.34:61044     52.104.141.25:https ESTABLISHED   TCP    192.168.1.34:61045     ldrv:https      ESTABLISHED  ^C C:\Users\admin&gt;</pre>	<p><b>Useful for identifying open/active ports.</b></p>
<b>speedtest</b>	<pre>C:\Users\admin&gt;cd Downloads\ookla-speedtest-1.2.0-win64 C:\Users\admin\Downloads\ookla-speedtest-1.2.0-win64&gt;speedtest.exe  Speedtest by Ookla    Server: Tata Play Fiber - Mumbai (id: 23647)   ISP: Tata Play Fiber Idle Latency: 24.00 ms (jitter: 24.72ms, low: 10.35ms, high: 49.76ms) Download: 22.80 Mbps [-] 0% - latency: 24.00 ms Download: 22.08 Mbps [ \ ] 3% - latency: 120.91 Download: 21.39 Mbps [ ] 4% - latency: 120.91 Download: 22.46 Mbps [=] 5% - latency: 120.91 Download: 23.51 Mbps [= \ ] 5% - latency: 120.91 Download: 24.71 Mbps [= \ ] 6% - latency: 120.91 Download: 24.69 Mbps [= \ ] 7% - latency: 131.92 Download: 25.00 Mbps [= / ] 8% - latency: 131.92 Download: 25.94 Mbps [= \ ] 8% - latency: 131.92 Download: 25.46 Mbps [= \ ] 9% - latency: 131.92 Download: 25.33 Mbps [== \ ] 10% - latency: 131.92 Download: 24.04 Mbps [== \ ] 11% - latency: 131.92 Download: 25.39 Mbps [== \ ] 11% - latency: 135.47 Download: 25.01 Mbps [== \ ] 12% - latency: 135.47 Download: 24.40 Mbps [== \ ] 13% - latency: 135.47 Download: 24.24 Mbps [== / ] 13% - latency: 135.47 Download: 24.11 Mbps [== \ ] 14% - latency: 200.65  Download: 29.46 Mbps [===== \ ] 96% - latency: 215.57 Download: 29.47 Mbps [===== \ ] 97% - latency: 215.57 Download: 29.49 Mbps [===== \ ] 98% - latency: 215.57 Download: 29.51 Mbps [===== \ ] 98% - latency: 215.57 Download: 29.52 Mbps [===== \ ] 99% - latency: 187.58 Download: 29.53 Mbps (data used: 49.6 MB)  Upload: 43.71 Mbps [===== \ ] 65% - latency: 249.49 Upload: 43.71 Mbps [===== / ] 69% - latency: 249.49 Upload: 43.73 Mbps [===== - ] 74% - latency: 249.49 Upload: 43.73 Mbps [===== \ ] 78% - latency: 249.49 Upload: 43.74 Mbps [===== \ ] 82% - latency: 249.49 Upload: 43.74 Mbps [===== / ] 87% - latency: 249.49 Upload: 43.72 Mbps [===== \ ] 91% - latency: 249.49 Upload: 43.70 Mbps [===== \ ] 95% - latency: 249.49 Upload: 43.72 Mbps (data used: 45.5 MB)    249.49 ms (jitter: 64.52ms, low: 15.76ms, high: 494.73ms)   Packet Loss: 0.0%   Result URL: https://www.speedtest.net/result/c/cc94bc29-d72d-4f44-94a3-4ea97404cda7 C:\Users\admin\Downloads\ookla-speedtest-1.2.0-win64&gt;</pre>	<p><b>(Required Speedtest CLI installed)</b> <b>Shows download &amp; upload speeds.</b></p> <p><b>Internet speed test.</b></p>



<b>tracert</b>	<pre>C:\Users\admin\Downloads&gt;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 [2404:6800:4009:8 1a::200e]  Trace complete.  C:\Users\admin\Downloads&gt;</pre>	<p><b>Helps diagnose routing issues.</b></p>
<b>arp -a</b>	<pre>C:\Users\admin\Downloads&gt;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&gt;</pre>	<p><b>Identifies local devices.</b></p>
<b>Whois (Website Statistics)</b>	<pre>C:\Users\admin\Downloads&gt;cd "C:\Users\admin\Downloads\WhoIs" C:\Users\admin\Downloads\WhoIs&gt;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#clientDelete Prohibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTrans ferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdate Prohibited Name Server: A.IANA-SERVERS.NET Name Server: B.IANA-SERVERS.NET DNSSEC: signedDelegation DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F1 20EE9F3A86764247C URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/ wicf/ &gt;&gt;&gt; Last update of whois database: 2025-08-20T06:28:44Z &lt;&lt;&lt;  For more information on Whois status codes, please visit https://icann.org/ epp</pre>	<p><b>We had to download and install the Sysinternals Whois utility, as it is not included by default in Windows.</b></p> <p><b>(Needs whois tool installed)</b></p> <p><b>Displays domain registration info.</b></p> <p><b>Useful for website details like it retrieves domain registration details like registrar, creation/expiry</b></p>



<p>NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.</p> <p>TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.</p> <p>The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.</p> <p>Connecting to whois.iana.org...</p> <pre>domain:      EXAMPLE.COM organisation: Internet Assigned Numbers Authority created:    1992-01-01 source:     IANA  Connecting to EXAMPLE.COM... A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond. C:\Users\admin\Downloads\WhoIs&gt;</pre>	<p><b>dates, name servers, and DNSSEC status.</b></p>
---	---

### 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:**