



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1 Roll No.: 16010121045

Experiment No. 1

Title: (i) Study of Basic networking command-line tools
(ii) Study of 10 Vulnerability assessment and Penetration testing tools.

Objective:

1. Study of Basic networking command-line tools.
2. Study of 10 Vulnerability assessment and Penetration testing tools.

CO	Outcome
CO1	Understand penetration testing with scope of its ethical implications, documentation and reporting

Books/ Journals/ Websites referred:

https://www.cyberarrow.io/blog/2021/01/19/top-15-pentest-tools-for-ethical-hacking-used-by-pros/?campaignid=19769035107&adgroupid=&adid=&gclid=Cj0KCQjw8e-gBhD0ARIsAJiDsaVfTgRZDlmGhaEH7QxOKXL9ztrmxuSM9OjsnnhtTfjoNDjczq_J84QaApb1EALw_wcB

Pre Lab/ Prior Concepts:

Students should have prior knowledge of Networking Basics, Linux Fundamentals, Web Technologies, Network Packet Analysis, Linux Command-Line Skills, Web Application Basics, Understanding of HTTP and HTTPS, Virtualization, Basic Security Concepts.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Theory:

Security tools serve different purposes but are often used together in security assessments to ensure a thorough examination of both web application and network security. In the dynamic landscape of cybersecurity, comprehending and mastering security tools is paramount for professionals engaged in ethical hacking, penetration testing, and network analysis. Three key tools—Kali Linux, Burp Suite, and Wireshark—stand out as indispensable assets in the cybersecurity arsenal.

Implementation details:

Basic Networking Command Line Tool:

ping: The **ping** command is used to test the reachability of a host on an IP network. It sends ICMP Echo Request messages to the target host and waits for ICMP Echo Reply messages. This tool is commonly used to check if a host is reachable and to measure round-trip time for packets

```
pargatsinghdhanjal — ping google.com — ping google.com — 100x24
ping
ping google.com

Last login: Tue Apr 23 05:14:04 on ttys011
> ping google.com

PING google.com (142.250.199.174): 56 data bytes
64 bytes from 142.250.199.174: icmp_seq=0 ttl=117 time=7.640 ms
64 bytes from 142.250.199.174: icmp_seq=1 ttl=117 time=7.890 ms
64 bytes from 142.250.199.174: icmp_seq=2 ttl=117 time=6.743 ms
64 bytes from 142.250.199.174: icmp_seq=3 ttl=117 time=7.206 ms
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

traceroute/tracert: The **traceroute** command on Unix-like systems and **tracert** on Windows is used to trace the path that packets take from the local host to a destination host. It shows the IP addresses of routers along the path and the time it takes for packets to travel to each router.

Example:

```
pargatsinghdhanjal — pargatsinghdhanjal@Router — -zsh — 100x24
Last login: Thu Apr 25 11:45:23 on ttys000
> traceroute google.com

traceroute to google.com (142.250.199.174), 64 hops max, 40 byte packets
 1  10.0.0.1 (10.0.0.1)  4.716 ms  5.590 ms  5.832 ms
 2  * * *
 3  * * *
 4  * * *
 5  *^C
```

nslookup: The **nslookup** command is a network administration tool for querying Domain Name System (DNS) servers to obtain domain name or IP address mapping, or other DNS records. It can be used to troubleshoot DNS-related issues.

Example:

```
pargatsinghdhanjal — pargatsinghdhanjal@Router — -zsh — 100x24
> nslookup google.com

Server:      172.31.0.26
Address:     172.31.0.26#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.199.174
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

netstat: The **netstat** command displays active network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Example:

```
pargatsinghdhanjal — pargatsinghdhanjal@Router — -zsh — 100x24

> netstat -an

Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 10.0.65.215.49885       13.234.41.62.443       ESTABLISHED
tcp4    0      0 10.0.65.215.49884       10.0.134.127.8009      SYN_SENT
tcp4    0      0 10.0.65.215.49879       172.253.118.84.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49870       142.250.70.35.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49862       142.251.42.99.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49857       142.250.183.110.443    ESTABLISHED
tcp4    0      0 10.0.65.215.49821       142.250.76.206.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49820       35.190.80.1.443        ESTABLISHED
tcp4    0      0 127.0.0.1.631           *.*                     LISTEN
tcp6    0      0 ::1.631                 *.*                     LISTEN
tcp4    0      0 10.0.65.215.49817       104.18.41.158.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49814       104.18.41.158.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49812       172.64.150.28.443     ESTABLISHED
tcp6    0      0 *.49718                 *.*                     LISTEN
tcp4    0      0 *.49718                 *.*                     LISTEN
tcp4    0      0 10.0.65.215.49717       104.18.32.115.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49711       163.70.143.61.443     ESTABLISHED
tcp4    0      0 10.0.65.215.49709       74.125.68.188.5228    ESTABLISHED
tcp4    0      0 10.0.65.215.49312       17.57.145.119.5223    ESTABLISHED
```

ipconfig/ifconfig: **ipconfig** on Windows and **ifconfig** on Unix-like systems are used to view and configure network interface parameters, such as IP address, subnet mask, and default gateway. It also displays other network-related information.

Example (Windows):

```
pargatsinghdhanjal — pargatsinghdhanjal@Router — -zsh — 100x24

> ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM, TXCSUM, TXSTATUS, SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anp11: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 7a:0b:65:59:32:39
    media: none
    status: inactive
anp10: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 7a:0b:65:59:32:38
    media: none
    status: inactive
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 7a:0b:65:59:32:18
    nd6 options=201<PERFORMNUD,DAD>
    media: none
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

arp: The **arp** command displays and modifies the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses on a local network.

Example:

```
> arp -a

? (10.0.0.1) at 6c:b2:ae:8b:60:fc on en0 ifscope [ethernet]
? (10.0.59.221) at (incomplete) on en0 ifscope [ethernet]
? (10.0.64.127) at 9a:82:a:e9:6:28 on en0 ifscope [ethernet]
? (10.0.64.133) at 6a:37:72:4d:f9:74 on en0 ifscope [ethernet]
? (10.0.64.159) at d6:c4:66:2f:60:c5 on en0 ifscope [ethernet]
? (10.0.64.162) at 1a:43:ae:4:f7:37 on en0 ifscope [ethernet]
? (10.0.64.165) at e2:be:38:7a:98:3f on en0 ifscope [ethernet]
? (10.0.64.167) at 8e:55:61:db:4e:36 on en0 ifscope [ethernet]
? (10.0.64.181) at 32:e0:ff:ff:5a:24 on en0 ifscope [ethernet]
? (10.0.64.203) at 94:ad:23:85:fa:36 on en0 ifscope [ethernet]
? (10.0.64.205) at (incomplete) on en0 ifscope [ethernet]
? (10.0.64.207) at 6a:c0:b9:ae:2d:8a on en0 ifscope [ethernet]
? (10.0.64.212) at 52:60:81:df:7e:8c on en0 ifscope [ethernet]
? (10.0.64.245) at 6:8b:2c:1:6e:19 on en0 ifscope [ethernet]
? (10.0.64.249) at 56:31:a1:f8:35:f9 on en0 ifscope [ethernet]
? (10.0.64.250) at 3a:b9:19:1c:df:f7 on en0 ifscope [ethernet]
? (10.0.65.27) at (incomplete) on en0 ifscope [ethernet]
? (10.0.65.43) at 76:86:b1:95:50:8d on en0 ifscope [ethernet]
? (10.0.65.44) at 8c:85:90:4:14:6e on en0 ifscope [ethernet]
? (10.0.65.48) at (incomplete) on en0 ifscope [ethernet]
? (10.0.65.60) at 5c:e9:1e:ae:e0:f1 on en0 ifscope [ethernet]
? (10.0.65.64) at 52:f3:13:1b:59:8a on en0 ifscope [ethernet]
```

whoami: The **whoami** command displays your login name. Unlike using the command **who** and specifying **am i**, the **whoami** command also works when you have root authority since it does not examine the **/etc/utmp** file.

```
Last login: Thu Apr 25 11:46:05 on ttys000
> whoami
pargatsinghdhanjal
```

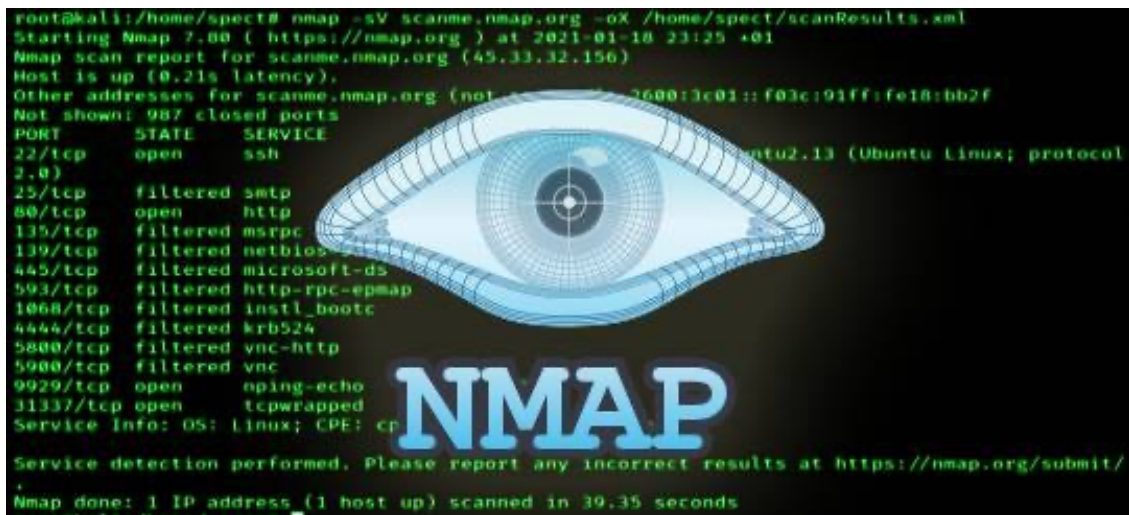



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Vulnerability Assessment and Penetration Testing Tools:

1. Nmap (Network Mapper):

- **Description:** Nmap is a powerful open-source network scanning tool used for discovering hosts and services on a computer network. It's widely used for network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- **Features:** Port scanning, service version detection, OS detection, scriptable interaction with the target, etc.
- **Website:** [Nmap](https://nmap.org)



2. OpenVAS (Open Vulnerability Assessment System):

- **Description:** OpenVAS is a full-featured vulnerability scanner that detects security issues in servers, network devices, and applications. It provides comprehensive vulnerability scanning and management capabilities.
- **Features:** Remote and local security checks, compliance audits, centralized vulnerability management, etc.
- **Website:** [OpenVAS](https://www.openvas.org)



OpenVAS

Open Vulnerability Assessment Scanner



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

3. Metasploit Framework:

- **Description:** Metasploit is a widely-used penetration testing framework that enables security researchers to test and exploit vulnerabilities in systems. It offers a vast collection of exploits, payloads, and auxiliary modules.
- **Features:** Exploit development, payload generation, post-exploitation modules, etc.
- **Website:** [Metasploit](https://www.metasploit.com/)



Metasploit

4. Burp Suite:

- **Description:** Burp Suite is a popular web vulnerability scanner used for testing web applications for security vulnerabilities. It includes various tools for web application security testing, including scanning, crawling, and fuzzing.
- **Features:** Web vulnerability scanning, proxying, crawling, fuzzing, etc.
- **Website:** [Burp Suite](https://portswigger.net/burp)





Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

5. OWASP ZAP (Zed Attack Proxy):

- **Description:** OWASP ZAP is a free and open-source web application security scanner used for finding security vulnerabilities in web applications during the development and testing phases.
- **Features:** Automated scanner, intercepting proxy, passive scanning, scripting, etc.
- **Website:** [OWASP ZAP](https://owasp.org/zap/)



OWASP
Zed Attack Proxy

6. Nessus:

- **Description:** Nessus is a comprehensive vulnerability scanner that identifies security vulnerabilities, misconfigurations, and compliance issues in networks, systems, and applications.
- **Features:** Vulnerability scanning, configuration auditing, compliance checking, etc.
- **Website:** [Nessus](https://www.tenable.com/products/nessus)



Nessus[®]
vulnerability scanner

7. Wireshark:

- **Description:** Wireshark is a widely-used network protocol analyzer that captures and interactively browses the traffic running on a computer network. It's useful for analyzing network protocols, troubleshooting network issues, and inspecting packet captures.
- **Features:** Packet capturing, protocol analysis, live capture and offline analysis, etc.
- **Website:** [Wireshark](https://www.wireshark.org/)



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of packets. Packet 348 is a DNS Standard query for 'cdn-0.nflximg.com'. Packet 349 is the corresponding DNS Standard query response. The bottom pane shows the details of packet 349, including the transaction ID, flags, questions, answer RRs, and authoritative nameservers.

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

8. Sqlmap:

- **Description:** Sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications.
- **Features:** SQL injection detection, database fingerprinting, data retrieval, etc.
- **Website:** [Sqlmap](http://sqlmap.org)

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

9. Acunetix:

- **Description:** Acunetix is a web vulnerability scanner used for detecting and managing security vulnerabilities in web applications. It provides a comprehensive set of tools for identifying vulnerabilities like SQL injection, cross-site scripting (XSS), and more.
- **Features:** Web vulnerability scanning, scanning for OWASP Top 10 vulnerabilities, etc.
- **Website:** [Acunetix](https://www.acunetix.com)



Acunetix

10. Aircrack-ng:

- **Description:** Aircrack-ng is a network software suite consisting of a packet sniffer, detector, WEP and WPA/WPA2-PSK cracker, and analysis tool for wireless LANs. It's primarily used for assessing the security of Wi-Fi networks.
- **Features:** Packet capturing, WEP and WPA/WPA2-PSK cracking, replay attacks, etc.
- **Website:** [Aircrack-ng](https://www.aircrack-ng.org)



Conclusion:

In summary, understanding basic networking command-line tools is essential for diagnosing network issues, while familiarity with vulnerability assessment and penetration testing tools is crucial for fortifying cybersecurity defenses.