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.

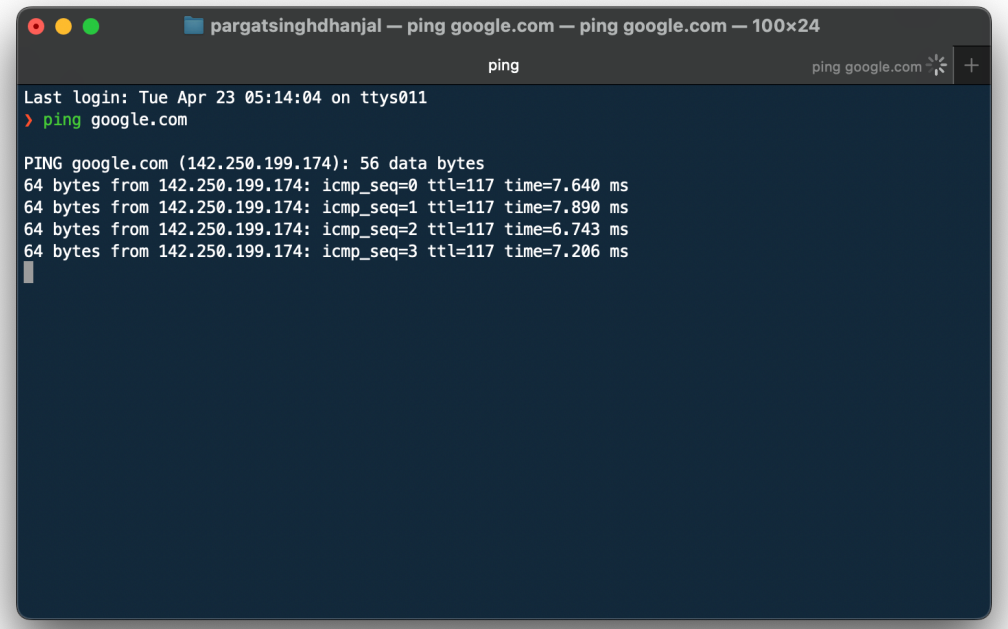
Theory:

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.

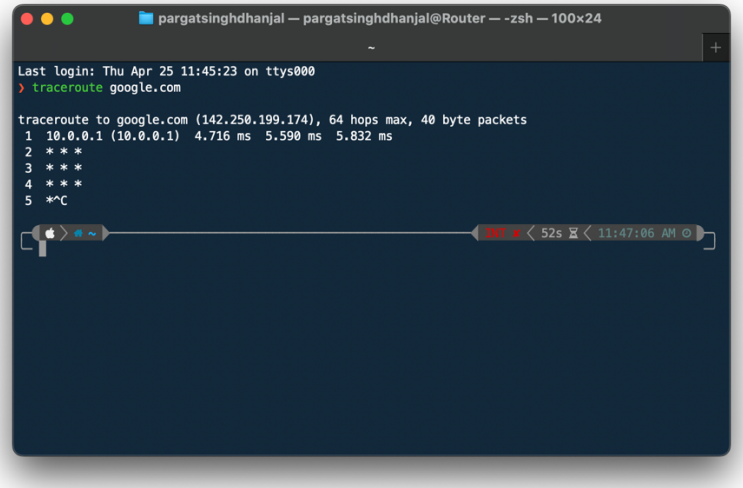
Implementation details:

Basic Networking Command Line Tool:

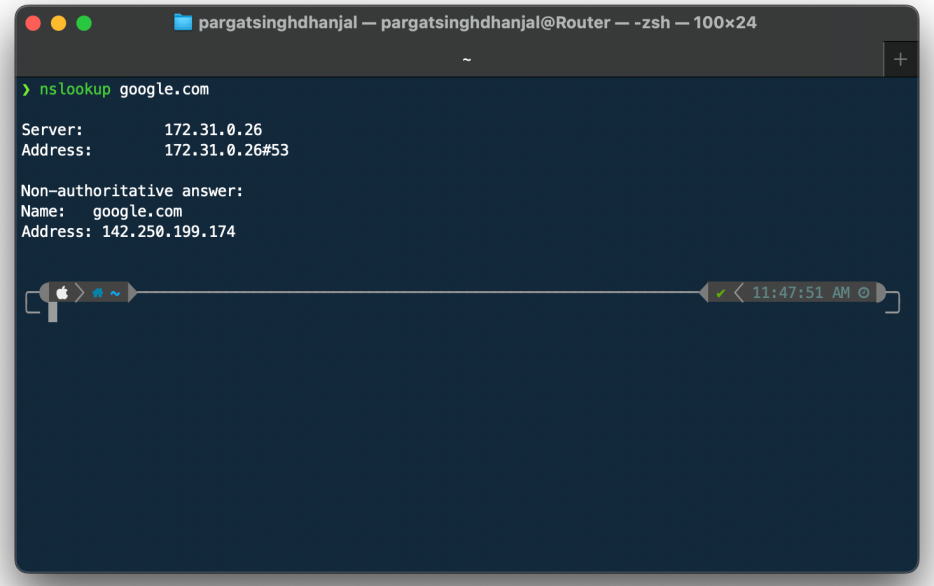
ping: The **ping** command is used to test the reachability of a host on an IP network. It sends ICMP Echo Request messages to the target host and waits for ICMP Echo Reply messages. This tool is commonly used to check if a host is reachable and to measure round-trip time for packets



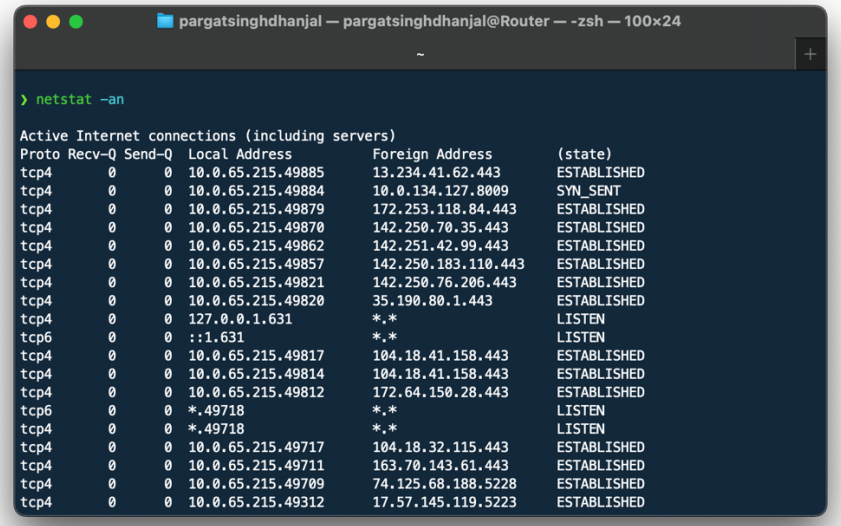
traceroute/tracert: The **traceroute** command on Unix-like systems and **tracert** on Windows is used to trace the path that packets take from the local host to a destination host. It shows the IP addresses of routers along the path and the time it takes for packets to travel to each router.
Example:



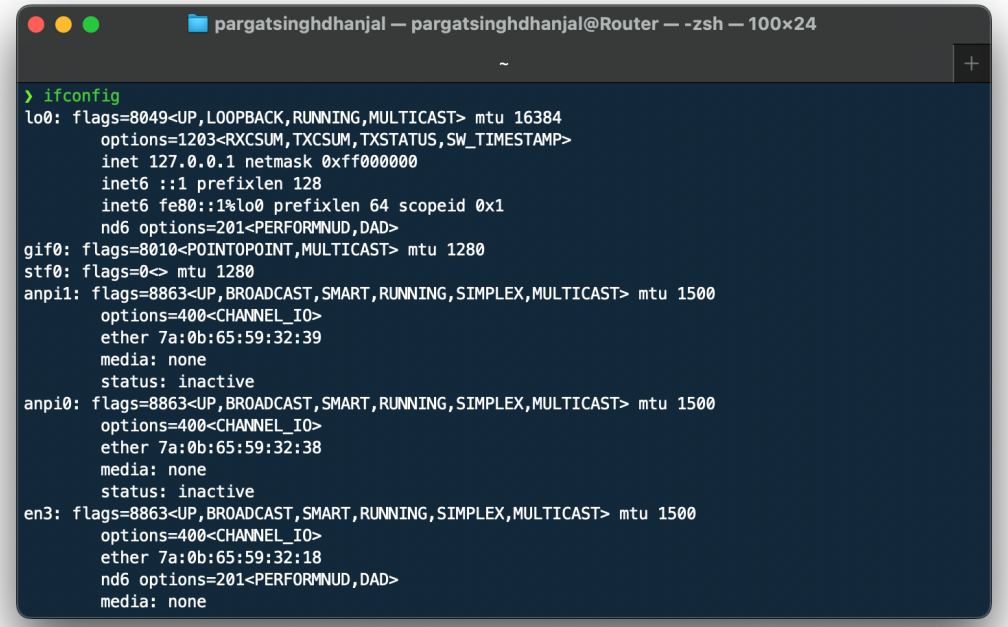
nslookup: The **nslookup** command is a network administration tool for querying Domain Name System (DNS) servers to obtain domain name or IP address mapping, or other DNS records. It can be used to troubleshoot DNS-related issues.
Example:



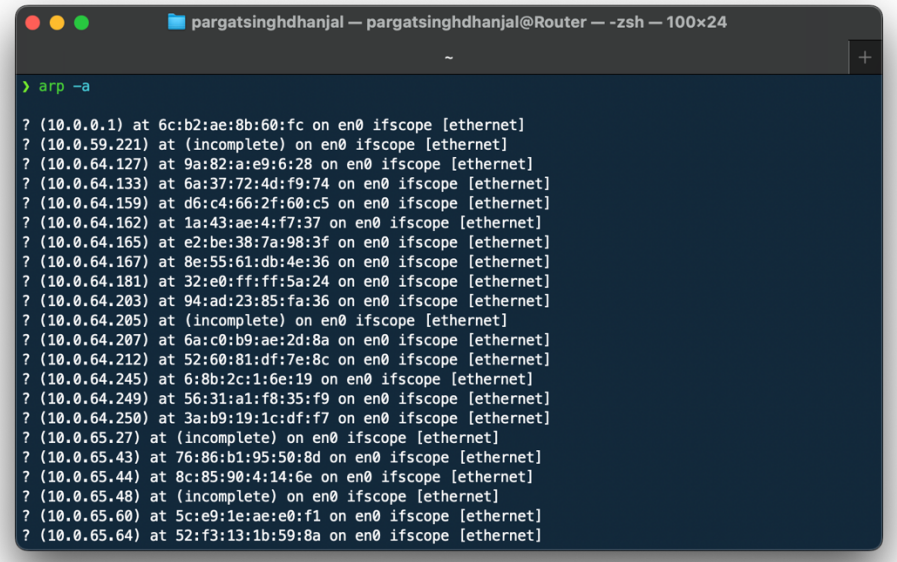
netstat: The **netstat** command displays active network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
Example:



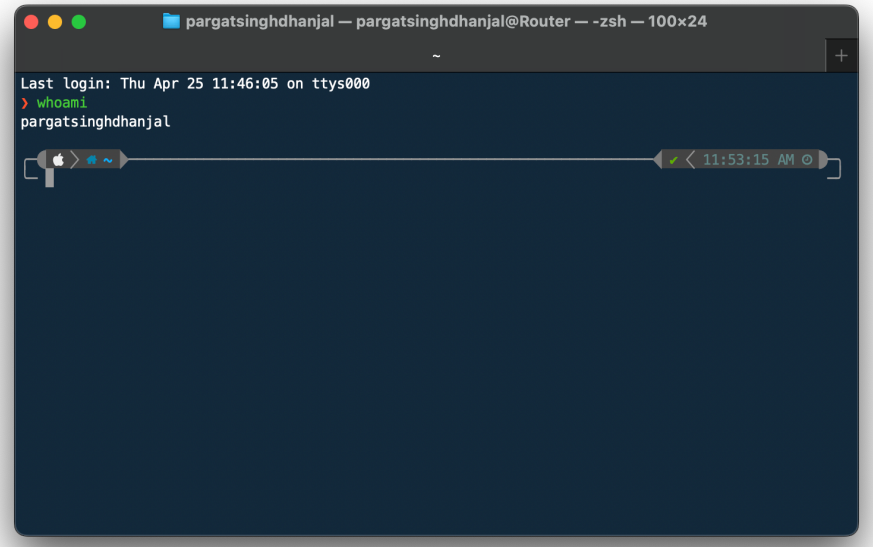
ipconfig/ifconfig: **ipconfig** on Windows and **ifconfig** on Unix-like systems are used to view and configure network interface parameters, such as IP address, subnet mask, and default gateway. It also displays other network-related information.
Example (Windows):



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:

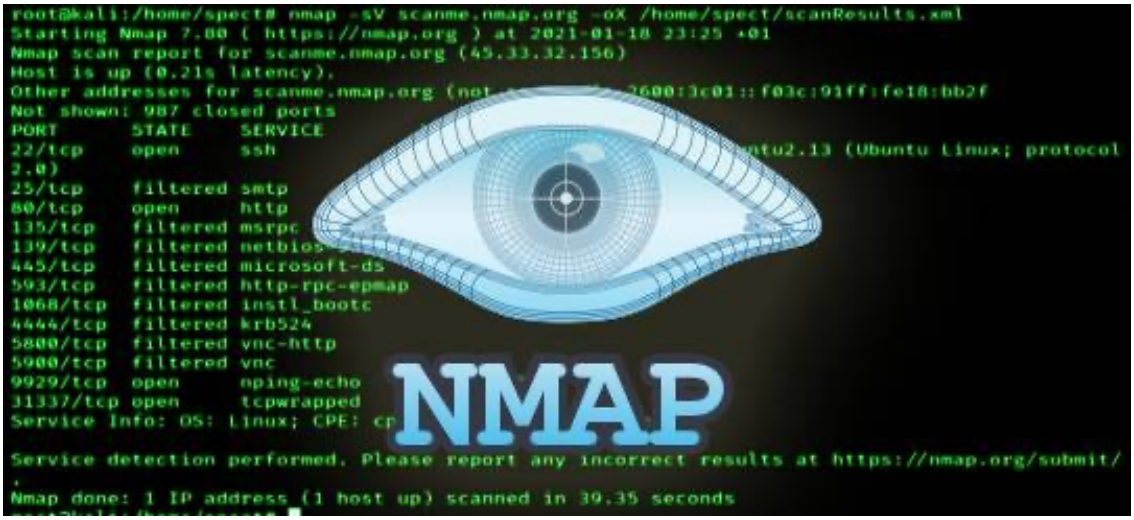


whoami: The whoami command displays your login name. Unlike using the command who and specifying am i, the whoami command also works when you have root authority since it does not examine the /etc/utmp file.



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



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

OpenVAS

Open Vulnerability Assessment Scanner

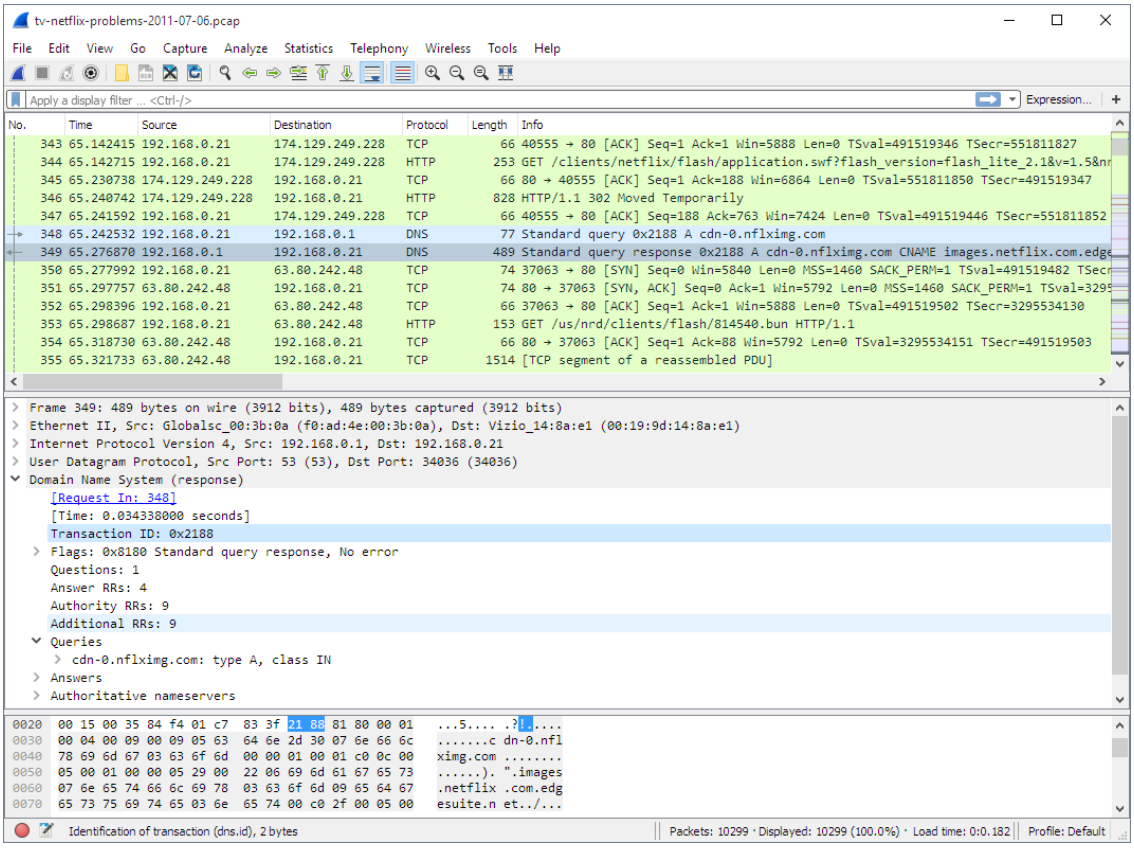
3. **Metasploit Framework**:
   - **Description**: Metasploit is a widely-used penetration testing framework that enables security researchers to test and exploit vulnerabilities in systems. It offers a vast collection of exploits, payloads, and auxiliary modules.
   - **Features**: Exploit development, payload generation, post-exploitation modules, etc.
   - **Website**: Metasploit

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

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

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

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



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

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.4.44#dev}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral 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')
```

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

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

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.