Assignment 04

Aim: Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup,

nikto, dmitry to gather information about networks and domain registrars. Theory: WHOIS: 1. Domain Information: WHOIS provides details about domain names, including registration and expiration dates, domain owner's contact information, and name servers. 2. Domain Ownership: It helps identify the owner or organization associated with a domain, aiding in investigations and establishing online presence. 3. Registrar Details: WHOIS reveals the domain registrar responsible for managing the domain, assisting in addressing technical issues or contacting the registrar. 4. DNS Information: WHOIS displays DNS-related details, such as name server information and IP addresses, crucial for network configuration. 5. Abuse Reporting: It offers a way to report abuse, like spam or trademark infringements, by contacting the domain owner or registrar. dig (Domain Information Groper): 1. DNS Queries: dig queries DNS servers to retrieve various DNS-related information, including

- A, AAAA, MX, and CNAME records.
- 2. DNS Resolution: It assists in resolving domain names to IP addresses, crucial for network communication.
- 3. Name Server Lookup: dig identifies authoritative name servers for a domain, ensuring proper DNS routing.

- 4. TTL (Time to Live): dig displays TTL values for DNS records, indicating how long the record should be cached before being refreshed.
- 5. Reverse DNS Lookup: It performs reverse DNS lookups, mapping IP addresses to domain names, aiding in identifying services associated with an IP.

traceroute:

- 1. Network Path Analysis: traceroute traces the path that packets take from source to destination, identifying intermediate routers and their response times.
- 2. Hop Identification: It helps pinpoint network bottlenecks, delays, or connectivity issues by showing delays at each hop.
- 3. Route Divergence: traceroute can reveal if packets are taking unexpected routes, indicating potential network misconfigurations or malicious activity.
- 4. MTU Discovery: It assists in Maximum Transmission Unit (MTU) discovery, optimizing data transmission by avoiding fragmentation.
- 5. Geo-Location: traceroute can provide approximate geographical locations of routers, aiding in network monitoring and troubleshooting.

nslookup:

- 1. DNS Record Lookup: nslookup retrieves DNS records, including A, MX, PTR, and NS records, helping understand domain configurations.
- 2. Domain IP Resolution: It resolves domain names to IP addresses, aiding in troubleshooting and network analysis.

- 3. Name Server Information: nslookup provides details about authoritative name servers for a domain, ensuring proper DNS resolution.
- 4. Reverse DNS Lookup: Similar to dig, nslookup performs reverse DNS lookups to map IP addresses to domain names.
- 5. Query Type Customization: It allows querying specific DNS record types, tailoring the information retrieved for different purposes.

nikto:

- 1. Web Server Vulnerability Scanner: nikto scans web servers for known vulnerabilities, misconfigurations, and security issues.
- 2. Directory and File Enumeration: It identifies hidden directories, files, or CGI scripts on a web server, aiding in potential attack vectors.
- 3. HTTP Methods Analysis: nikto examines supported HTTP methods, revealing potential weaknesses or security gaps.
- 4. Outdated Software Detection: It flags outdated software versions on web servers that could be exploited by attackers.

5. nikto checks for SSL/TLS vulnerabilities and configuration weaknesses, enhancing the security of data transmission.

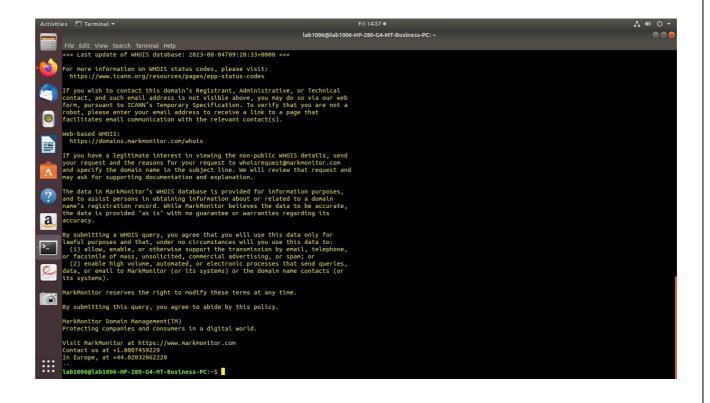
dmitry:

- 1. Information Gathering: dmitry gathers information about target domains, IP addresses, email addresses, and network services.
- 2. WHOIS Lookup: It performs WHOIS queries to retrieve domain registration and ownership details.

- 3. Subdomain Enumeration: dmitry identifies subdomains associated with a target domain, aiding in understanding the target's online presence.
- 4. Network Port Scanning: It scans open ports on a target system, revealing potential entry points for unauthorized access.
- 5. Banner Grabbing: dmitry captures banners and other information from network services, assisting in service identification and version detection.

```
Main Status: electroterorhibited https://cann.org/eppserver/ransfer/rohibited bomain Status: server/ransfer/rohibited https://cann.org/eppserver/ransfer/rohibited bomain Status: server/ransfer/rohibited https://cann.org/eppserver/ransfer/rohibited bomain Status: server/ransfer/rohibited https://cann.org/eppserver/ransfer/rohibited bomain Status: server/ransfer/rohibited https://clann.org/eppserver/ransfer/rohibited bomain Status: server/ransfer/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/solicion/soli
```

```
Authented except as reasonably necessary to register demain names or modify existing registrations; the data in Verising flobal Registry Services' (Verising) whost database is provided by Verising flobal Registry Services (Verising) whost database is provided by Verising flobal Registry Services (Verising) whost database is provided by Verising for a flow of the f
```



```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig geeksforgeeks.org

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> geeksforgeeks.org

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18253

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
 ; EDNS: version: 0, flags:; udp: 65494
 ;; QUESTION SECTION:
 ;geeksforgeeks.org. IN A

;; ANSWER SECTION:
 geeksforgeeks.org. 30 IN A 34.218.62.116

;; Query time: 29 msec
 ;; SERVER: 127.0.0.53#53(127.0.0.53)
 ;; WHEN: Fri Aug 04 14:58:30 IST 2023
 ;; MSG SIZE rcvd: 62
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig geeksforgeeks.org

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> geeksforgeeks.org

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18253
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;geeksforgeeks.org. IN A

;; ANSWER SECTION:
geeksforgeeks.org. 30 IN A 34.218.62.116

;; Query time: 29 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Aug 04 14:58:30 IST 2023
;; MSG SIZE rcvd: 62
```

```
Lab1006@Lab1006-HP-280-G4-MT-Business-PC:~$ nslookup google.com
Server: 127.0.0.53
Address: 127.0.0.53#53

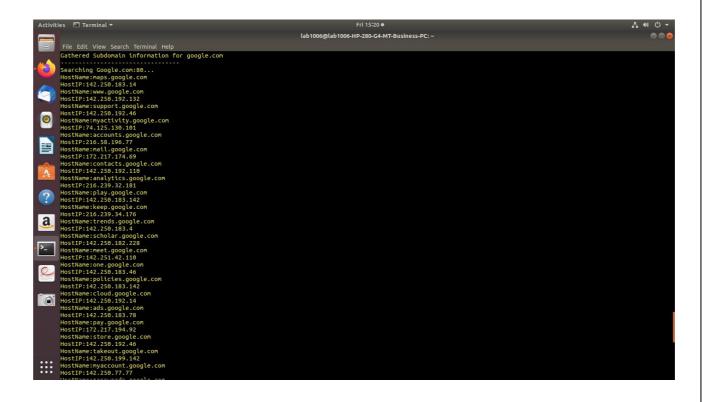
Non-authoritative answer:
Name: google.com
Address: 142.251.42.14
Name: google.com
Address: 2404:6800:4009:82f::200e
```

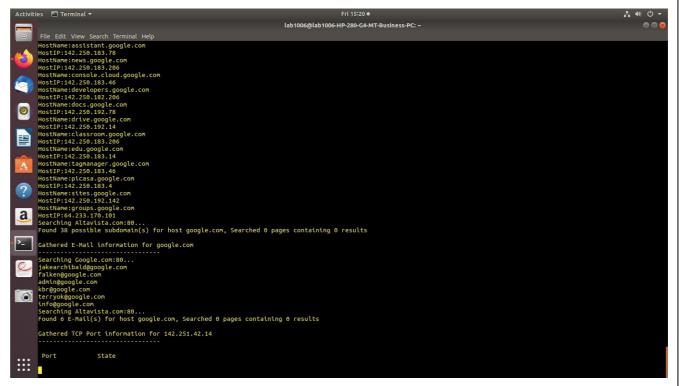
```
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h 128.199.222.244
- Nikto v2.1.5

^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h 128.199.222.244
- Nikto v2.1.5
+ No web server found on 128.199.222.244:80
+ 0 host(s) tested
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
remarks: http://www.lama.org/assignments/lpv4-recovered-address-space remarks: http://www.lama.org/assignments/lpv4-recovered-address-space remarks: http://www.lama.org/assignments/lpv4-recovered-address-space remarks: http://www.afrintc.net/ whois.afrintc.net remarks: http://www.afrintc.net/ whois.afrintc.net remarks: ARIN (Morthern America) remarks: http://www.afrintc.net/ whois.afrinted remarks: http://www.afrintc.net/ whois.afrinted remarks: http://www.afrintc.net/ whois.afrin.net remarks: http://www.lamic.net/ whois.afrin.net/ remarks: http://www.lamic.net/ whois.afrin.net/ whois.afrin.net/ remarks: http://www.lamic.net/ remarks: http://www.lamic.
```

```
Domain Name: COOCLE.COW
Registry Domain 10: 238514 DOMAIN CON-VRSN
Registry Mondin 10: 238514 DOMAIN CON-VRSN
Registry MODIS Server: whois.markmonitor.com
Registra Mil. Namy Modis 10: 200
Registra Mil. Namy Modis 10: 200
Creation Date: 1997-09-1516-1907-02
Registra: Rarkmonitor Inc.
Registra: Rarkmonitor Inc.
Registra: Rarkmonitor Inc.
Registra: Rarkmonitor Inc.
Registra: Date: 2028-09-1416-1902-02
Registra: Palku Di: 202
Registra: Date: Date: 2028-09-1416-1902-002
Registra: Date: Date:
```





```
Labion Selabion 6-HP-280-G4-MT-Business-PC:-$ nikto -h google.com
Nikto v2.1.5

Target IP: 142.251.42.14

Target Hostname: google.com
Target Port: 80

Start Time: 2023-08-04 15:22:53 (GMT5.5)

Server: gws
Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
Uncommon header 'x-xss-protection' found, with contents: 0
Uncommon header 'x-xss-protection' found, with contents: 0
Uncommon header 'x-xss-protection' found, with contents: 0
Nonot page | redirects to: http://www.google.com/
Not page | redirects to: http://www.google.com/
Uncommon header 'referrer-policy' found, with contents: no-referrer
NO GCI Directories found (use 'c all' to force check all possible dirs)
Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load balancer or proxy is in place
Uncommon header 'x-content-type-options' found, with contents: cross-origin
Cookie NE Created without the httponly flag
Cookie NE Created without the ht
```

Conclusion: Network reconnaissance tools such as WHOIS, dig, traceroute, nslookup, nikto, and dmitry provide vital insights into network structures, domain configurations, and security vulnerabilities. By utilizing these tools effectively, professionals can enhance cybersecurity efforts, troubleshoot network issues, and make informed decisions to safeguard digital assets and ensure smooth network operations. These tools remain essential in the ever-evolving landscape of technology, enabling proactive security measures and efficient network management.