



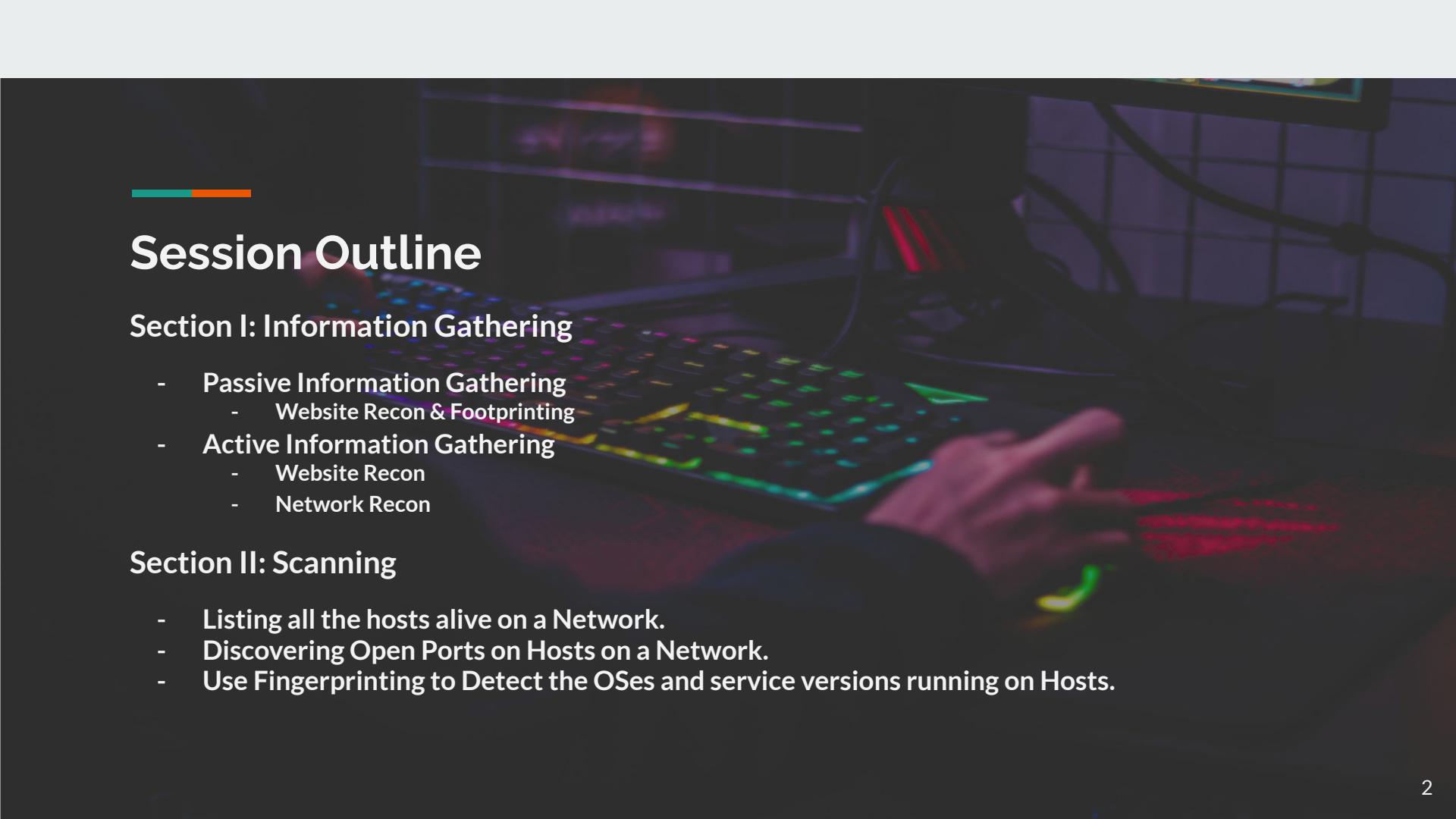
Recon Techniques: Gathering Information About the Target

A Guide to Passive and Active Recon against the target with An introduction to Enumerating information through services.

Speaker: Nimish Dudhe

Socials: [LinkedIn](#) [Medium](#)

Background Photo by [Axville](#) on [Unsplash](#)



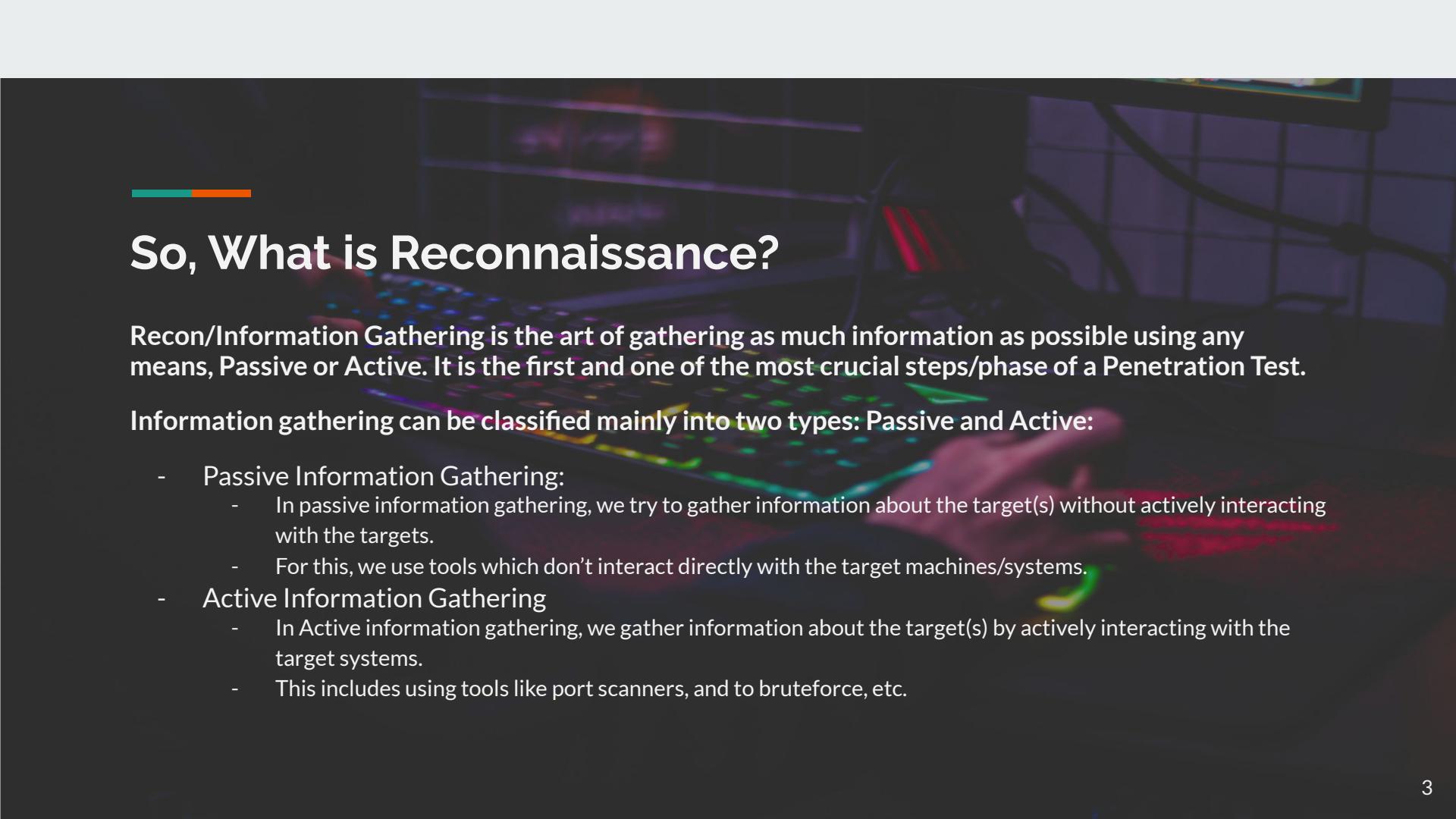
Session Outline

Section I: Information Gathering

- **Passive Information Gathering**
 - Website Recon & Footprinting
- **Active Information Gathering**
 - Website Recon
 - Network Recon

Section II: Scanning

- Listing all the hosts alive on a Network.
- Discovering Open Ports on Hosts on a Network.
- Use Fingerprinting to Detect the OSes and service versions running on Hosts.

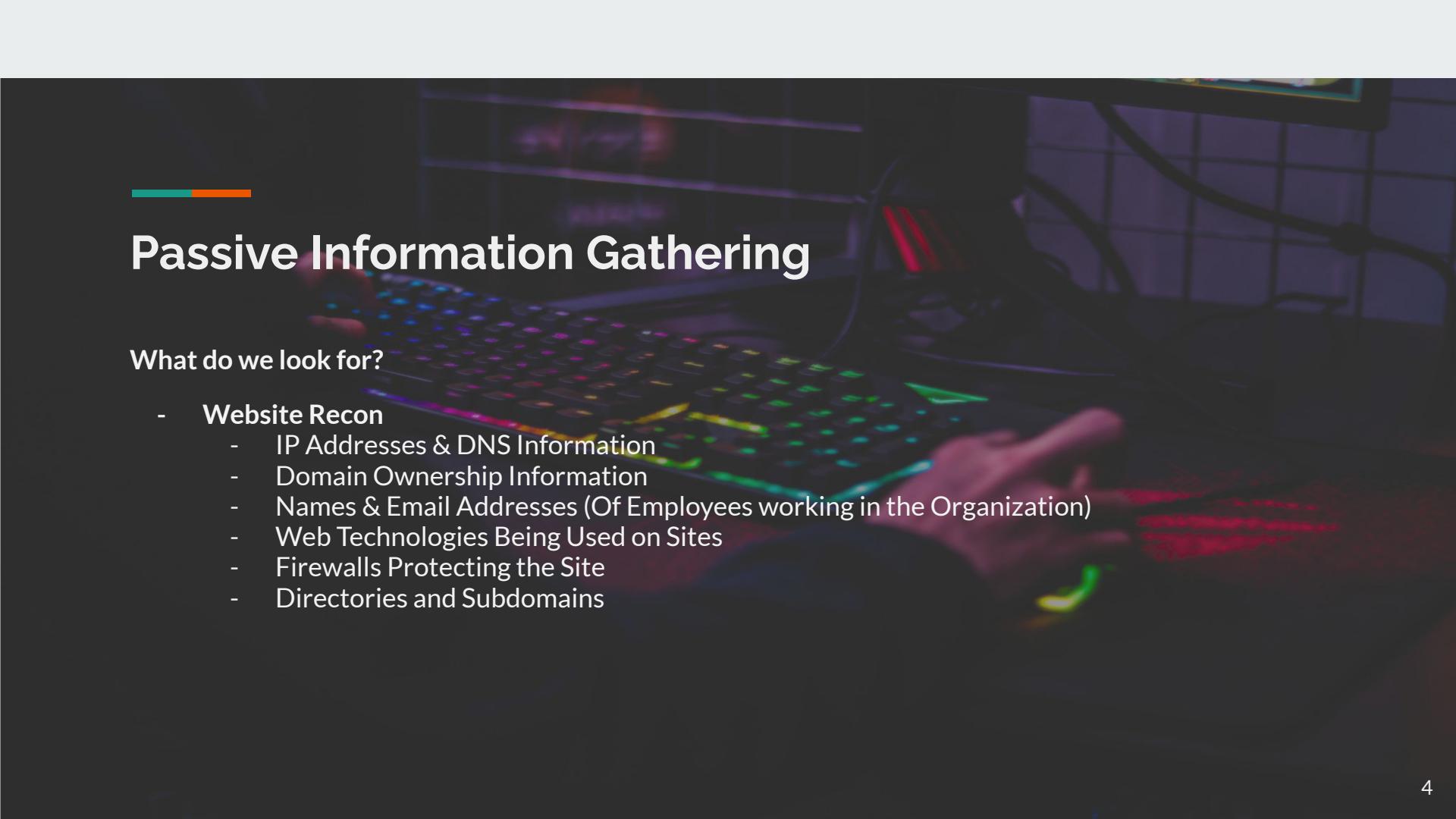


So, What is Reconnaissance?

Recon/Information Gathering is the art of gathering as much information as possible using any means, Passive or Active. It is the first and one of the most crucial steps/phase of a Penetration Test.

Information gathering can be **classified** mainly into two types: **Passive and Active**:

- **Passive Information Gathering:**
 - In passive information gathering, we try to gather information about the target(s) without actively interacting with the targets.
 - For this, we use tools which don't interact directly with the target machines/systems.
- **Active Information Gathering**
 - In Active information gathering, we gather information about the target(s) by actively interacting with the target systems.
 - This includes using tools like port scanners, and to bruteforce, etc.

A dark-themed slide featuring a blurred background image of a person's hands typing on a colorful, backlit keyboard. A computer monitor is visible in the background, displaying some graphical elements. Two horizontal bars, one teal and one orange, are positioned at the top left.

Passive Information Gathering

What do we look for?

- Website Recon
 - IP Addresses & DNS Information
 - Domain Ownership Information
 - Names & Email Addresses (Of Employees working in the Organization)
 - Web Technologies Being Used on Sites
 - Firewalls Protecting the Site
 - Directories and Subdomains

IP Addresses & DNS Information

- **host command**
 - **host** is a simple utility for performing DNS lookups.
 - It is normally used to convert names to IP addresses and vice versa.
 - When no arguments or options are given, host prints a short summary of its command-line arguments and options.
- **dig command**
 - Similar to host command, dig is a flexible tool for interrogating DNS name servers.
 - It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.
 - Other lookup tools tend to have less functionality than dig.

```
(secovfshanks@nootnoot)-[~]
$ host null.community
null.community has address 104.21.7.192
null.community has address 172.67.187.250
null.community has IPv6 address 2606:4700:3032::6815:7c0
null.community has IPv6 address 2606:4700:3036::ac43:bbfa
null.community mail is handled by 5 alt1.aspmx.l.google.com.
null.community mail is handled by 5 alt2.aspmx.l.google.com.
null.community mail is handled by 1 aspmx.l.google.com.
null.community mail is handled by 10 alt3.aspmx.l.google.com.
null.community mail is handled by 10 alt4.aspmx.l.google.com.
```

```
(secovfshanks@nootnoot)-[~]
$ dig null.community

; <>> DIG 9.19.17-1-Debian <>> null.community
; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33358
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
>null.community.           IN      A

;; ANSWER SECTION:
null.community.      300    IN      A      172.67.187.250
null.community.      300    IN      A      104.21.7.192

;; Query time: 3 msec
;; SERVER: 49.205.72.130#53(49.205.72.130) (UDP)
;; WHEN: Fri Nov 24 09:49:50 IST 2023
;; MSG SIZE  rcvd: 75
```

DNS Information (Records)

CLI Tools:

- host
- dnsrecon
- dig
- fierce

```
(secovfshanks㉿nootnoot)~]$ apropos dns | grep -i "lookup\|scan\|enum" | grep "(1)"  
delv (1)           - DNS lookup and validation utility  
dig (1)            - DNS lookup utility  
dnsenum (1)        - multithread script to enumerate information on a domain and to discover non-contiguous IP blocks  
dnsrecon (1)       - DNS Enumeration and Scanning Tool  
fierce (1)         - DNS scanner that helps locate non-contiguous IP space and hostnames against specified domains.  
host (1)           - DNS lookup utility  
mdig (1)           - DNS pipelined lookup utility  
  
(secovfshanks㉿nootnoot)~]$
```

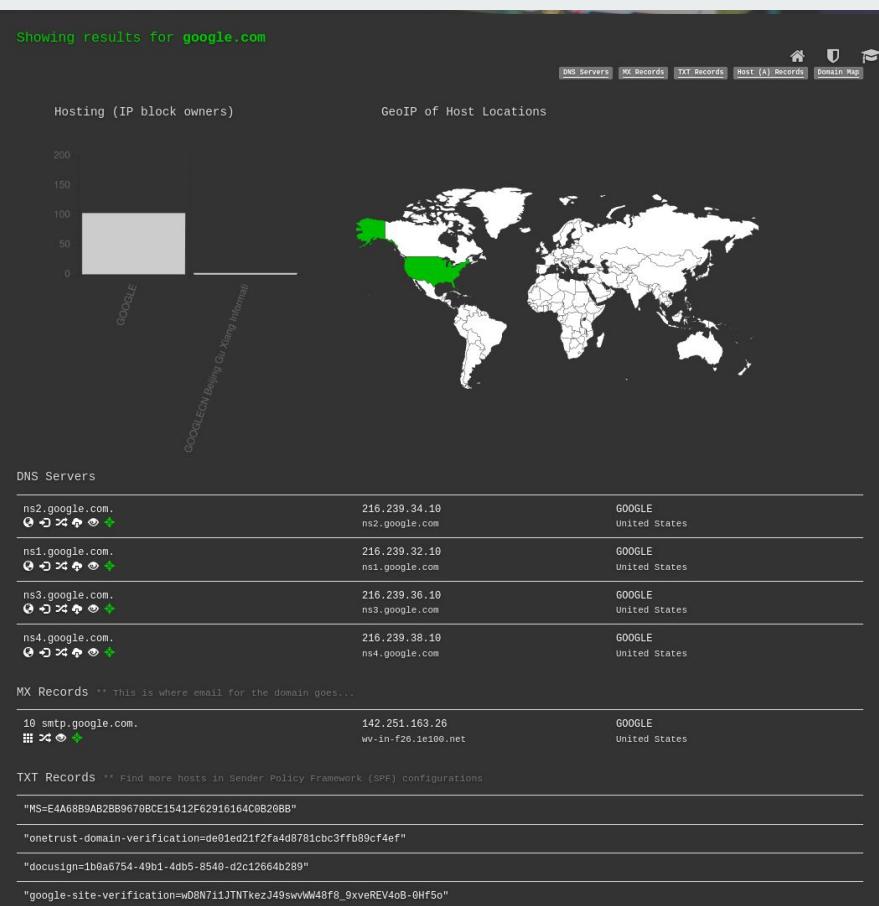
```
(secovfshanks㉿nootnoot)~]$ dnsrecon -d zonetransfer.me  
[*] std: Performing General Enumeration against: zonetransfer.me...  
[*] DNSSEC is not configured for zonetransfer.me  
[*] SOA nsztm1.digi.ninja 81.4.108.41  
[*] NS nsztm2.digi.ninja 34.225.33.2  
[*] Bind Version for 34.225.33.2 you"  
[*] NS nsztm1.digi.ninja 81.4.108.41  
[*] Bind Version for 81.4.108.41 secret"  
[*] MX ASPMX4.GOOGLEMAIL.COM 142.250.115.27  
[*] MX ASPMX2.GOOGLEMAIL.COM 173.194.202.27  
[*] MX ASPMX3.GOOGLEMAIL.COM 142.250.141.26  
[*] MX ALT1.ASPMX.L.GOOGLE.COM 173.194.202.26  
[*] MX ALT2.ASPMX.L.GOOGLE.COM 142.250.141.27  
[*] MX ASPMX.L.GOOGLE.COM 74.125.130.27  
[*] MX ASPMX5.GOOGLEMAIL.COM 64.233.171.27  
[*] MX ASPMX4.GOOGLEMAIL.COM 2607:f8b0:4023:1004::1b  
[*] MX ASPMX2.GOOGLEMAIL.COM 2607:f8b0:400e:c00::1a  
[*] MX ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4023:c0b::1a  
[*] MX ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:400e:c00::1a  
[*] MX ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4023:c0b::1a  
[*] MX ASPMX.L.GOOGLE.COM 2404:6800:4003:c06::1a  
[*] MX ASPMX5.GOOGLEMAIL.COM 2607:f8b0:4003:c15::1b  
  
(secovfshanks㉿nootnoot)~]$ fierce --domain zonetransfer.me --site-verification=typP28J7JAUHA9Fw2sHXMcCC0I6X8mmoVi04VlMewxA  
NS: nsztm1.digi.ninja nsztm2.digi.ninja.  
SOA: nsztm1.digi.ninja (81.4.108.41) www.zonetransfer.me 5.196.105.14 5060  
Zone: success Found  
{DNS name @>:  
    @ 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 '  
    @ 172800 900 1209600 3600\n'  
    @ 300 IN HINFO "Casio fx-700G" "Windows XP"\n'  
    @ 301 IN TXT '  
    "google-site-verification=typP28J7JAUHA9Fw2sHXMcCC0I6X8mmoVi04VlMewxA"\n'  
    @ 7200 IN MX 0 ASPMX.L.GOOGLE.COM.\n'  
    @ 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.\n'  
    @ 7200 IN MX 20 ALT2.ASPMX.L.GOOGLE.COM.\n'  
    @ 7200 IN MX 20 ASPMX2.GOOGLEMAIL.COM.\n'  
    @ 7200 IN MX 20 ASPMX3.GOOGLEMAIL.COM.\n'  
    @ 7200 IN MX 20 ASPMX4.GOOGLEMAIL.COM.\n'  
    @ 7200 IN MX 20 ASPMX5.GOOGLEMAIL.COM.\n'  
    @ 7200 IN A 5.196.105.14\n'  
    @ 7200 IN NS nsztm1.digi.ninja.\n'  
    @ 7200 IN NS nsztm2.digi.ninja.'  
<DNS name _acme-challenge>: '_acme-challenge' 301 IN TXT '  
    "60a05hbUJ9xSsvyy7pApQvwCUSSgGxvrbidjePEsZI"',  
<DNS name _sip._tcp>: '_sip._tcp' 14000 IN SRV 0 5060 www',  
<DNS name 14.105.196.5.IN-ADDR.ARPA>: '14.105.196.5.IN-ADDR.ARPA' 7200 IN PTR '  
    www',  
<DNS name asfdauthdns>: 'asfdauthdns' 7900 IN AFSDB 1 asfdbbox',  
<DNS name asfdbbox>: 'asfdbbox' 7200 IN A 127.0.0.1',  
<DNS name asfdbvolume>: 'asfdbvolume' 7800 IN AFSDB 1 asfdbbox',  
<DNS name canberra-office>: 'canberra-office' 7200 IN A 202.14.81.230',  
<DNS name cmdexec>: 'cmdexec' 300 IN TXT "; ls",  
<DNS name contact>: 'contact' 2592000 IN TXT "Remember to call or email Pippa '  
    on +44 123 4567890 or pippa@zonetransfer.me when making '  
    DNS changes".',  
<DNS name dc-office>: 'dc-office' 7200 IN A 143.228.181.132',  
<DNS name deadbeef>: 'deadbeef' 7201 IN AAAA dead:beaf::',  
<DNS name dr>: 'dr' 300 IN LOC 53 20 56.558 N 1 38 33.526 W 0.00m',  
<DNS name DZC>: 'DZC' 7200 IN TXT "AbcDfG6",  
<DNS name email>: 'email' 2222 IN NAPTR 1 1 "P" "E2U+email" '' .
```

DNS Information (Records)

Web Tools:

- dnsdumpster.com
 - who.is

DNS Records for google.com				
Hostname	Type	TTL	Priority	Content
google.com	SOA	41		ns1.google.com dns-admin@google.com 584847865 900 900 1800 60
google.com	NS	21600		ns4.google.com
google.com	NS	21600		ns1.google.com
google.com	NS	21600		ns2.google.com
google.com	NS	21600		ns3.google.com
google.com	A	117		142.251.163.138
google.com	A	117		142.251.163.101
google.com	A	117		142.251.163.139



Domain Ownership Info

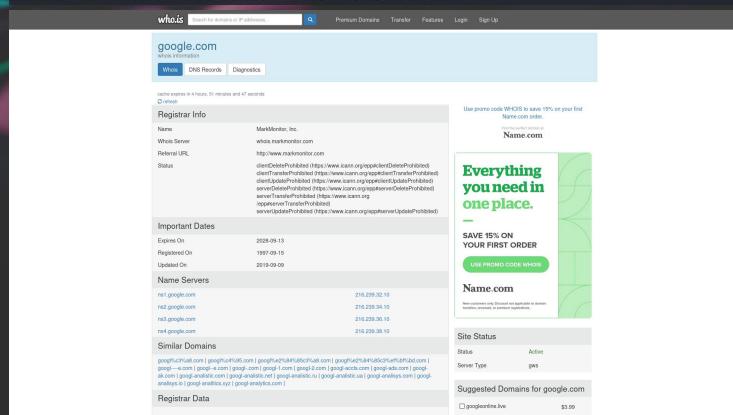
WHOIS is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees. These resources include domain names, IP address blocks and autonomous systems.

It has a public database that houses the information collected when someone registers a domain name or updates their DNS settings. ICANN, the International Corporation for Assigned Names and Numbers, regulates the WHOIS database.

Tools:

- whois Command Line Utility
 - who.is webpage

```
(secovfshanks@nootnoot)-[~]
└ whois google.com -H
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-11-24T04:27:38Z <<<
```



Gathering Email Addresses

- theHarvester
 - An Open source tool that utilizes Open Source Intelligence (OSINT)
 - The tool gathers names, emails, IPs, subdomains, and URLs by using multiple public resources such as yahoo, google, crt.sh, dnsdumpster, etc.
 - hunter.io
 - Hunter was created by Antoine Finkelstein and François Grante in 2015.
 - Freshly graduated, they saw the untapped potential of cold emails and wanted to address the challenges of prospecting and finding contact information.
 - To achieve great success rate while complying with privacy regulations, they decided to use emails found on the public web. Email Hunter was born.

```
$ [secofshanks$] rootoot] [-/Desktop/Tools/Recon/theHarvester]
$ ./theHarvester.py -d rgpt.ac.in -h yahoo,crftsh,duckduckgo
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
[*] Target: rgpt.ac.in
[*] Searching Yahoo...
[*] Searching CRFTSH...
[*] Searching DuckDuckGo...
[*] No IPs found.
[*] Emails found: 108
-----
20bs002@rgpt.ac.in
20ce002@rgpt.ac.in
```

Domain Search 

null.co.in null.co.in 25 results  Filters 

Type  Department  Show only results with 

25 results for your search  Export  Find by name 

Vibhor Mahajan vibhor@null.co.in  94% 3 sources 	 Information Security  Save as lead   Add to a campaign 
Raman Bedi raman@null.co.in  93% 2 sources 	 Save as lead   Add to a campaign 
Abhishek Datta abhishek@null.co.in  92% 1 source 	 Save as lead   Add to a campaign 

Network Forensics
   
Email pattern: `{first}@null.co.in`
Accept alt: YES 
Industry: Technology
Country: India

Technologies
   

Web Technologies Used on a Site

Technology Profilers

- Command Line Utilities
 - whatweb
- Web Browser Extensions
 - Wappalyzer
 - builtwith
- Websites
 - Netcraft's sitereport

The terminal window shows the following command and its output:

```
(secovfshanks@nootnoot)-[~]
$ whatweb https://nmap.org
https://nmap.org [200 OK] Apache[2.4.6], Country[RESERVED][ZZ], Google-Analytics[Universal][UA-11009417-1], HTML5, HTTPServer[CentOS][Apache/2.4.6 (CentOS)], IP[45.33.49.119], Script[application/ld+json], Strict-Transport-Security[max-age=3153600; preload], Title[Nmap: the Network Mapper - Free Security Scanner]

(secovfshanks@nootnoot)-[~]
$ whatweb https://www.google.com
https://www.google.com [200 OK] Cookies[1P_JAR,AEC,NID], Country[UNITED STATES][US], HTML5, HTTPServer[gws], Httponly[AEC,NID], IP[142.250.76.68], Script, Title[google], UncommonHeaders[content-security-policy-report-only,alt-svc], X-Frame-Option[s[SAMEORIGIN], X-XSS-Protection[0]]
```

The Wappalyzer extension interface displays the following technologies detected on the page:

Analytics	Web servers
Google Analytics G4	Google Web Server

JavaScript frameworks	Tag managers
GSAP 3.12.2	Google Tag Manager

Security	JavaScript libraries
HSTS	Lodash 4.17.21
reCAPTCHA	Closure Library

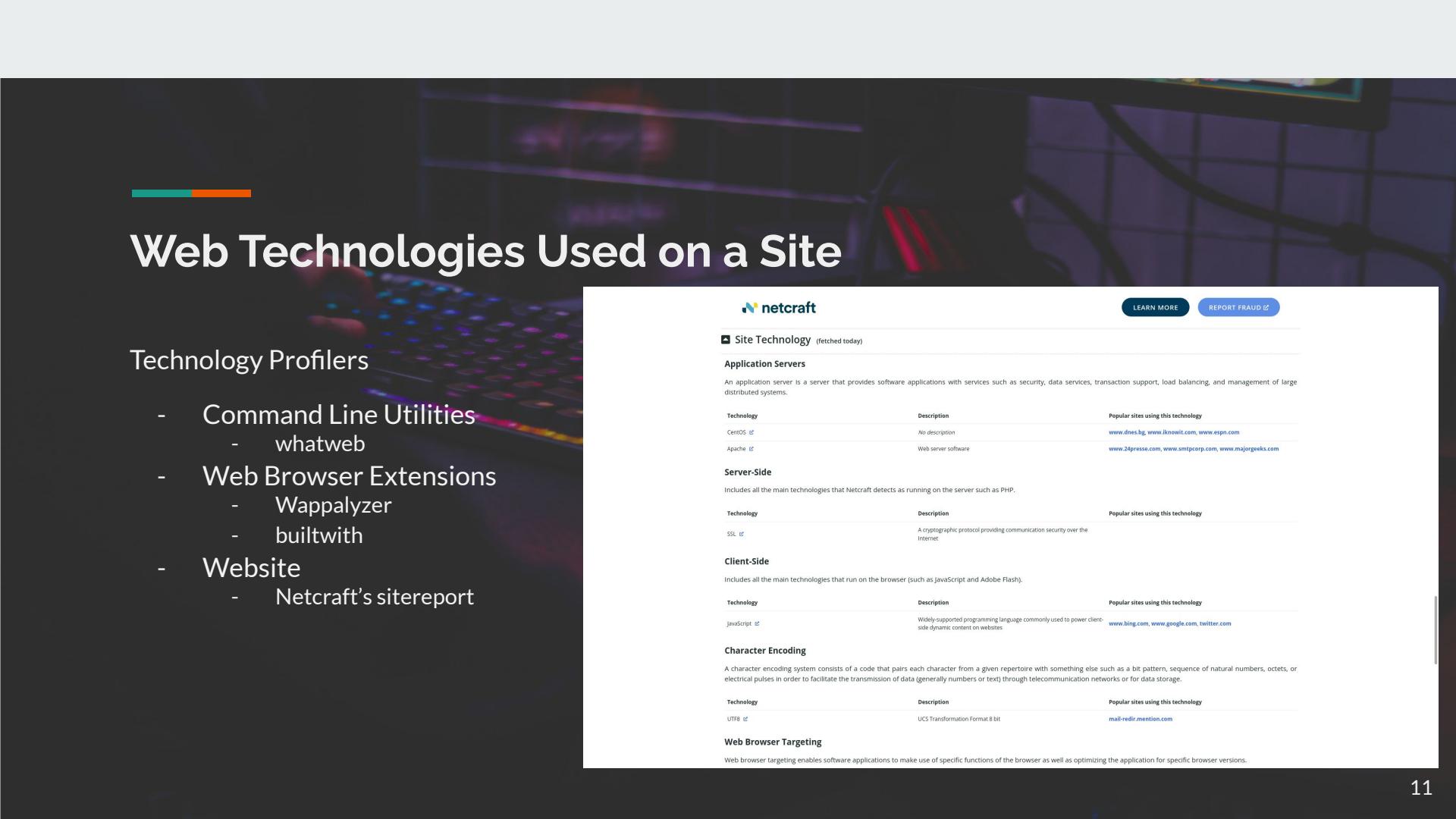
Font scripts	Performance
Google Font API	Priority Hints

On the right side, there are sections for Content Delivery Network, GStatic Google Static Content, JavaScript Libraries and Functions, Google API, and Web Servers.

Web Technologies Used on a Site

Technology Profilers

- Command Line Utilities
 - whatweb
- Web Browser Extensions
 - Wappalyzer
 - builtwith
- Website
 - Netcraft's sitereport



The screenshot shows a detailed analysis of a website's technology stack from Netcraft's sitereport. At the top, there's a navigation bar with 'LEARN MORE' and 'REPORT FRAUD' buttons. The main content area starts with a section titled 'Site Technology' (fetched today). It includes a table for 'Application Servers' showing CentOS and Apache, and another for 'Server-Side' technologies like PHP and MySQL. The 'Client-Side' section lists JavaScript and CSS. A 'Character Encoding' section discusses UTF-8. Finally, a 'Web Browser Targeting' section is present.

Technology	Description	Popular sites using this technology
CentOS	No description	www.dnes.bg , www.iknowit.com , www.espn.com
Apache	Web server software	www.24presse.com , www.smtpcorp.com , www.majorgeeks.com

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.bing.com , www.google.com , twitter.com

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	mail-redir.mention.com

Detecting Firewalls Used by the Site

wafw00f

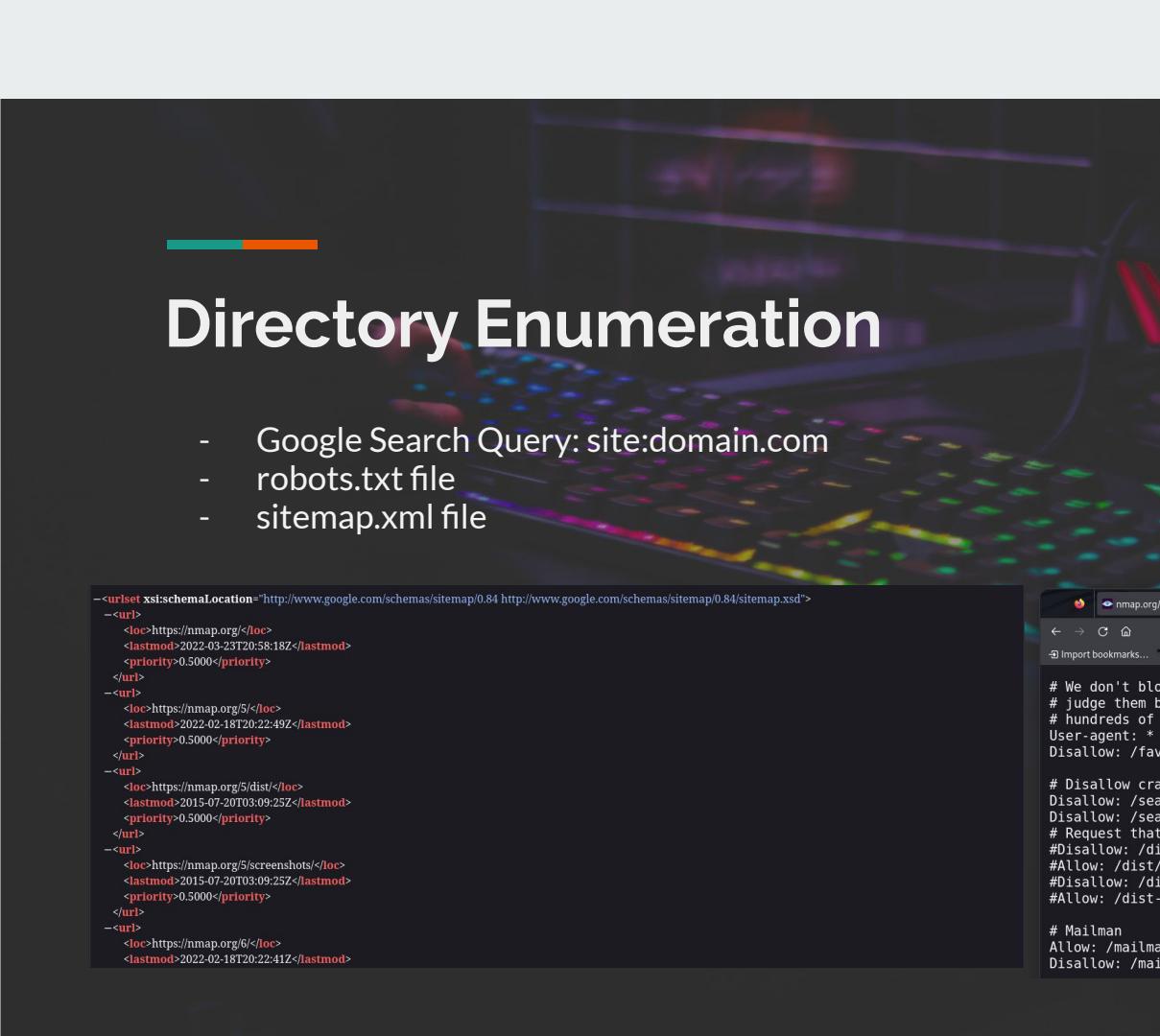
- Identify and fingerprint Web Application Firewall products.
- Sends a normal HTTP request and analyses the response; this identifies a number of WAF solutions.
- If that is not successful, it sends a number of (potentially malicious) HTTP requests and uses simple logic to deduce which WAF it is.
- If that is also not successful, it analyses the responses previously returned and uses another simple algorithm to guess if a WAF or security solution is active

```
(secovfshanks@nootnoot)-[~]$ wafw00f null.community
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://null.community
[+] The site https://null.community is behind Cloudflare (Cloudflare Inc.) WAF.
[-] Number of requests: 2
(secovfshanks@nootnoot)-[~]$
```

Directory Enumeration

- Google Search Query: site:domain.com
- robots.txt file
- sitemap.xml file

```
<urlset xsi:schemaLocation="http://www.google.com/schemas/sitemap/0.84 http://www.google.com/schemas/sitemap/0.84/sitemap.xsd">
  <><url>
    <loc>https://nmap.org/</loc>
    <lastmod>2022-03-23T20:58:18Z</lastmod>
    <priority>0.5000</priority>
  </url>
  <><url>
    <loc>https://nmap.org/5/</loc>
    <lastmod>2022-02-18T20:22:49Z</lastmod>
    <priority>0.5000</priority>
  </url>
  <><url>
    <loc>https://nmap.org/5/dist/</loc>
    <lastmod>2015-07-20T03:09:25Z</lastmod>
    <priority>0.5000</priority>
  </url>
  <><url>
    <loc>https://nmap.org/5/screenshots/</loc>
    <lastmod>2015-07-20T03:09:25Z</lastmod>
    <priority>0.5000</priority>
  </url>
  <><url>
    <loc>https://nmap.org/6/</loc>
    <lastmod>2022-02-18T20:22:41Z</lastmod>
```



Google search results for "site:nmap.org" showing various Nmap-related pages.

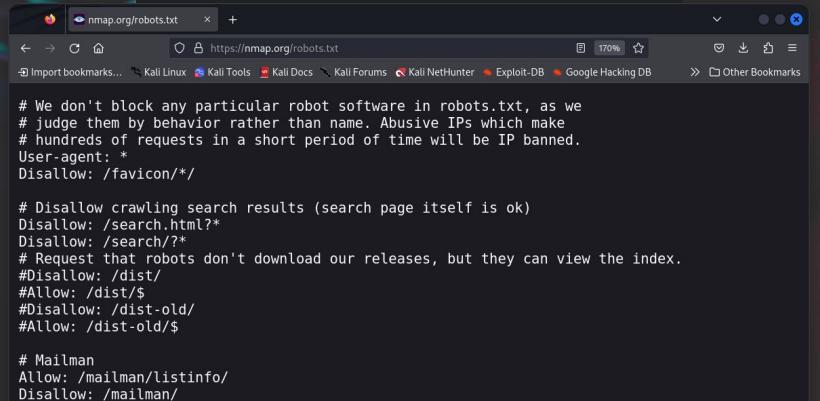
Try Google Search Console
www.google.com/webmasters/
Do you own nmap.org? Get indexing and ranking data from Google.

nmap.org
https://nmap.org/ :
Nmap: the Network Mapper - Free Security Scanner
Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it...

nmap.org
https://nmap.org/images/ :
Nmap.org/_images/
Name - Last modified - Size. [PARENTDIR] Parent Directory - [IMG] nmap_bnr_eyemap.png, 2023-03-20 11:29 ...

nmap.org
https://nmap.org/... :
Nmap 6 Release Notes
21 May 2012 — Nmap GUI and results viewer. It aims to provide advanced features for experienced Nmap users while also making Nmap easier for beginners to use.

nmap.org
https://nmap.org/... :
Nmap 5.00 Release Notes
16 Jul 2009 — Nmap ("Network Mapper") is a free and open source (license) utility for network exploration or security auditing. Many systems and network...



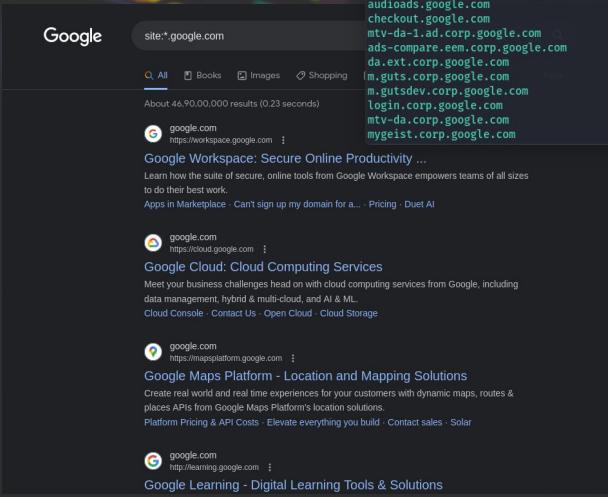
```
# We don't block any particular robot software in robots.txt, as we
# judge them by behavior rather than name. Abusive IPs which make
# hundreds of requests in a short period of time will be IP banned.
User-agent: *
Disallow: /favicon/*

# Disallow crawling search results (search page itself is ok)
Disallow: /search.html*
Disallow: /search/?*
# Request that robots don't download our releases, but they can view the index.
Disallow: /dist/
#Allow: /dist/$
#Disallow: /dist-old/
#Allow: /dist-old/$

# Mailman
Allow: /mailman/listinfo/
Disallow: /mailman/
```

Subdomain Enumeration

- Google Search Query: site:*.google.com
 - Sublist3r
 - theHarvester



```
[secovfshanks@nootnoot] - [~/Desktop/Tools/Recon/Sublist3r]  
$ ./sublist3r.py -d google.com
```

```
[+] Enumerating subdomains now for google.com
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in VirusTotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL Certificates..
[+] Searching now in PassiveDNS..
```

```
[+] Total Unique Subdomains Found  
www.google.com  
accounts.google.com  
freezone.accounts.google.com  
adwords.google.com  
qa.adz.google.com  
answers.google.com  
apps-secure-data-connector.google  
audioads.google.com  
checkout.google.com  
mtv-da-1.ad.corp.google.com  
ads-compare.eem.corp.google.com  
da.ext.corp.google.com  
m.guts.corp.google.com  
m.gutsdev.corp.google.com  
login.corp.google.com  
mtv.corp.google.com  
mtv-nist.corp.google.com
```

```
(secovfshanks@nootnoot)-[~/Desktop/Tools/Recon/theHarvester]$ ./theHarvester.py -d google.com -b yahoo
```

Read proxies.yaml from /etc/theHarvester/proxies.yaml

cmartorella@edge-secu

*] Target: google.

Active Information Gathering

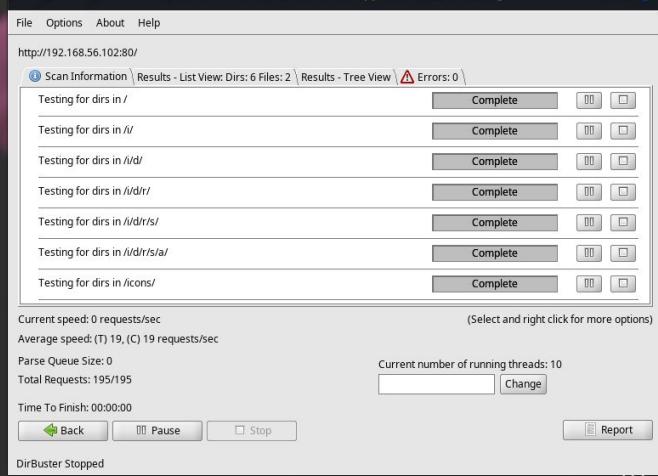
What do we look for?

- **Website Recon**
 - Listing Directories using Bruteforce
 - Listing Subdomains using Bruteforce
- **Network Recon**
 - Listing live Machines(Hosts) on the Network
 - Open Ports on live Hosts
 - Fingerprinting Targets and Services for Additional Information

Directory Listing

- gobuster
 - Is written in go.
 - Used to brute force URIs (Directories and Files), subdomains, etc.
- dirbuster
 - Developed at OWASP Lead by James Fisher.
 - A multithreaded Java application
 - Designed to brute force files and directories on web/application servers

```
(sec0vfshanks@nootnoot)-[~]
└─$ gobuster dir -u https://www.google.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          https://www.google.com
[+] Method:      GET
[+] Threads:     10
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/2006          (status: 301) [Size: 239] [→ https://trends.google.com/trends/yis/2006/]
/about          (status: 301) [Size: 218] [→ https://about.google/]
/contact        (Status: 301) [Size: 228] [→ https://www.google.com/contact/]
/images         (Status: 302) [Size: 225] [→ https://www.google.com/imghp]
/privacy        (Status: 302) [Size: 224] [→ https://privacy.google.com/]
/blog           (Status: 301) [Size: 221] [→ https://www.blog.google/]
/search          (Status: 302) [Size: 225] [→ https://www.google.com/webhp]
/home           (status: 301) [Size: 221] [→ https://home.google.com/]
/news            (status: 302) [Size: 0] [→ https://news.google.com/news]
/2005           (Status: 301) [Size: 239] [→ https://trends.google.com/trends/yis/2005/]
```



Subdomain Listing

- gobuster
 - Is written in go.
 - Used to brute force URIs (Directories and Files), subdomains, etc.
- dnsenum
 - Multithread script to enumerate information on a domain and to discover non-contiguous IP blocks.

```
[sec0fshanks@hostroot:~] $ gobuster dns -d google.com -w /usr/share/wordlists/amass/subdomains-top1ml-5000.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@Firefart)
=====
[+] Threads:          10
[+] Threads:          10
[+] Timeout:         10s
[+] Threads:          10
[+] Threads:          10
[+] Timeout:         10s
[+] Threads:          10
[+] Threads:          10
[+] Timeout:         10s
=====
Starting gobuster in DNS enumeration mode
=====
=====
Found: www.google.com
Found: mail.google.com
Found: smtp.google.com
Found: ns.google.com
Found: m.google.com
Found: ns1.google.com
Found: ns2.google.com
Found: blog.google.com
Found: ns3.google.com
Found: admin.google.com
Found: vpn.google.com
Found: mobile.google.com
Brute Forcing with /usr/share/dnsenum/dns.txt:
=====
about.google.com.          300   IN  CNAME  www3.l.google.com.
www3.l.google.com.        280   IN  A      142.250.77.174
accounts.google.com.       102   IN  A      142.250.77.109
admin.google.com.         116   IN  A      216.58.200.142
ads.google.com.           144   IN  A      142.250.196.14
america.google.com.       300   IN  CNAME  www3.l.google.com.
www3.l.google.com.        278   IN  A      142.250.77.174
ap.google.com.             300   IN  CNAME  www2.l.google.com.
www2.l.google.com.        55    IN  A      142.250.195.164
apps.google.com.          180   IN  CNAME  www3.l.google.com.
www3.l.google.com.        278   IN  A      142.250.77.174
archive.google.com.        300   IN  A      142.250.77.142
asia.google.com.          300   IN  A      142.250.193.164
blog.google.com.          300   IN  CNAME  www.blogger.com.
www.blogger.com.          126   IN  CNAME  blogger.l.google.com.
blogger.l.google.com.     111   IN  A      142.250.183.233
channel.google.com.        300   IN  A      142.250.205.238
d.google.com.              300   IN  CNAME  www3.l.google.com.
www3.l.google.com.        270   IN  A      142.250.77.174
directory.google.com.     300   IN  CNAME  www3.l.google.com.
www3.l.google.com.        269   IN  A      142.250.77.174
dns.google.com.            585   IN  A      8.8.4.4
dns.google.com.            585   IN  A      8.8.8.8
elections.google.com.     300   IN  A      142.250.195.174
environment.google.com.   300   IN  A      142.250.182.142
europe.google.com.        300   IN  A      142.250.67.68
finance.google.com.       197   IN  CNAME  www3.l.google.com.
www3.l.google.com.        264   IN  A      142.250.77.174
health.google.com.         300   IN  A      142.250.196.46
```

Section II: Scanning

List of Live Machines on a Network

- ARP (Address Resolution Protocol)
 - arp-scan (root privileges required)
- ICMP (Internet Control Message Protocol)
 - fping command
 - NMap Host Discovery
 - ICMP Echo Request Scan
 - Doesn't scan for open ports
- ZenMap Host Discovery
 - Same as NMap but in GUI >_<

```
[root@nootnoot] ~
# arp-scan -I vboxnet0 -g 192.168.56.0/24
Interface: vboxnet0, type: EN10MB, MAC: 0a:00:27:00:00:00, IPv4: 192.168.56.1
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.100 08:00:27:f5:1c:3a PCS Systemtechnik GmbH
192.168.56.101 08:00:27:d4:0f:a1 PCS Systemtechnik GmbH
192.168.56.102 08:00:27:5f:39:d2 PCS Systemtechnik GmbH
192.168.56.103 08:00:27:80:a9:44 PCS Systemtechnik GmbH
192.168.56.104 08:00:27:a9:29:2c PCS Systemtechnik GmbH

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.042 seconds (125.37 hosts/sec). 5 responded
```

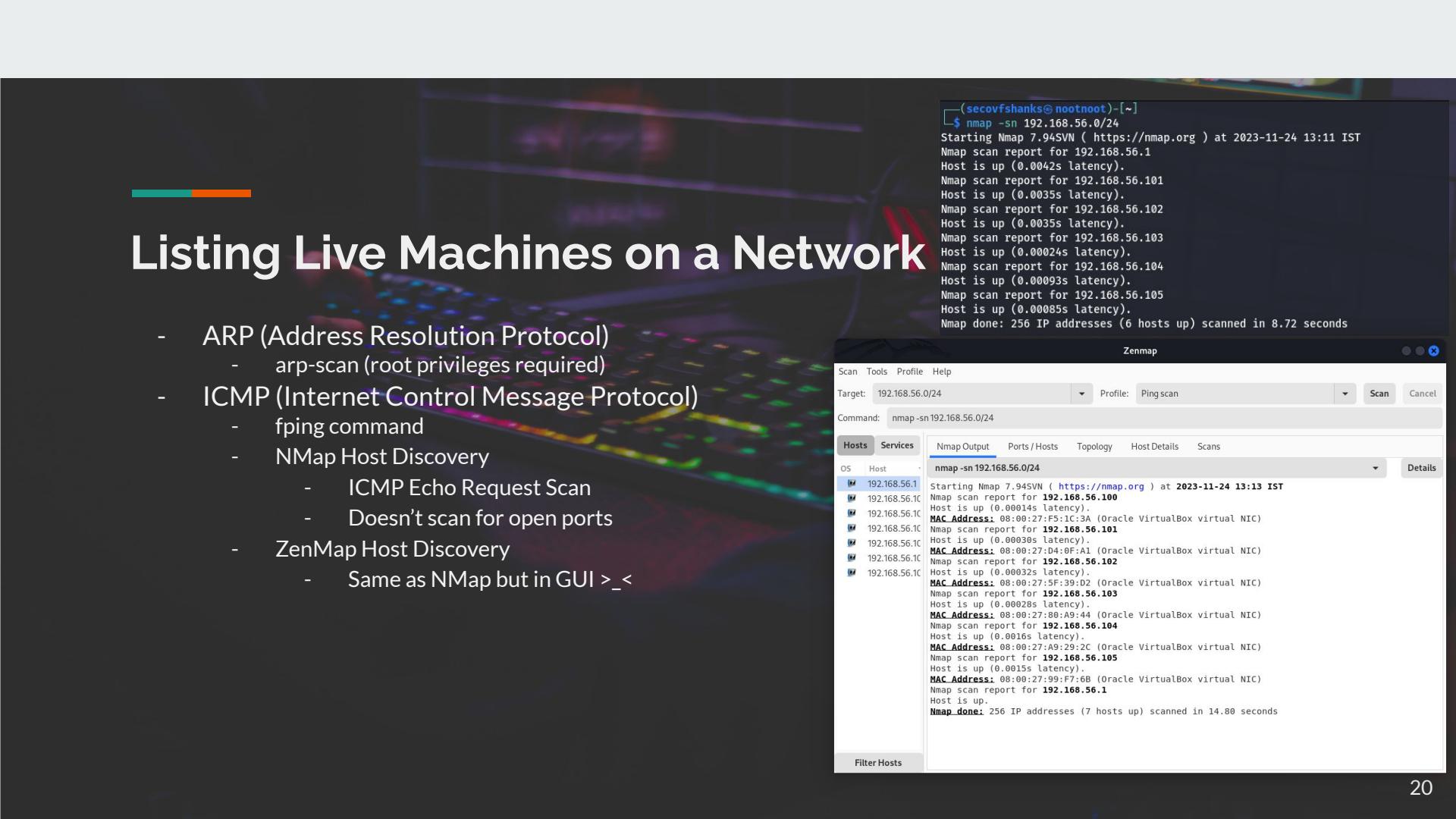
```
[root@nootnoot] ~
$
```

```
[secovfshanks@nootnoot] ~
$ fping -I vboxnet0 -g 192.168.56.0/24 2>/dev/null | grep -v unreachable
192.168.56.1 is alive
192.168.56.100 is alive
192.168.56.101 is alive
192.168.56.102 is alive
192.168.56.103 is alive
192.168.56.104 is alive
192.168.56.105 is alive
```

```
[secovfshanks@nootnoot] ~
$
```

List of Live Machines on a Network

- ARP (Address Resolution Protocol)
 - arp-scan (root privileges required)
- ICMP (Internet Control Message Protocol)
 - fping command
 - NMap Host Discovery
 - ICMP Echo Request Scan
 - Doesn't scan for open ports
- ZenMap Host Discovery
 - Same as NMap but in GUI >_<



secovfshanks@nootnoot:[~]\$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 13:11 IST
Nmap scan report for 192.168.56.1
Host is up (0.0042s latency).
Nmap scan report for 192.168.56.101
Host is up (0.0035s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0035s latency).
Nmap scan report for 192.168.56.103
Host is up (0.00024s latency).
Nmap scan report for 192.168.56.104
Host is up (0.00093s latency).
Nmap scan report for 192.168.56.105
Host is up (0.00085s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 8.72 seconds

Zenmap

Scan Tools Profile Help

Target: 192.168.56.0/24 Profile: Ping scan

Command: nmap -sn 192.168.56.0/24

Hosts Services

OS Host

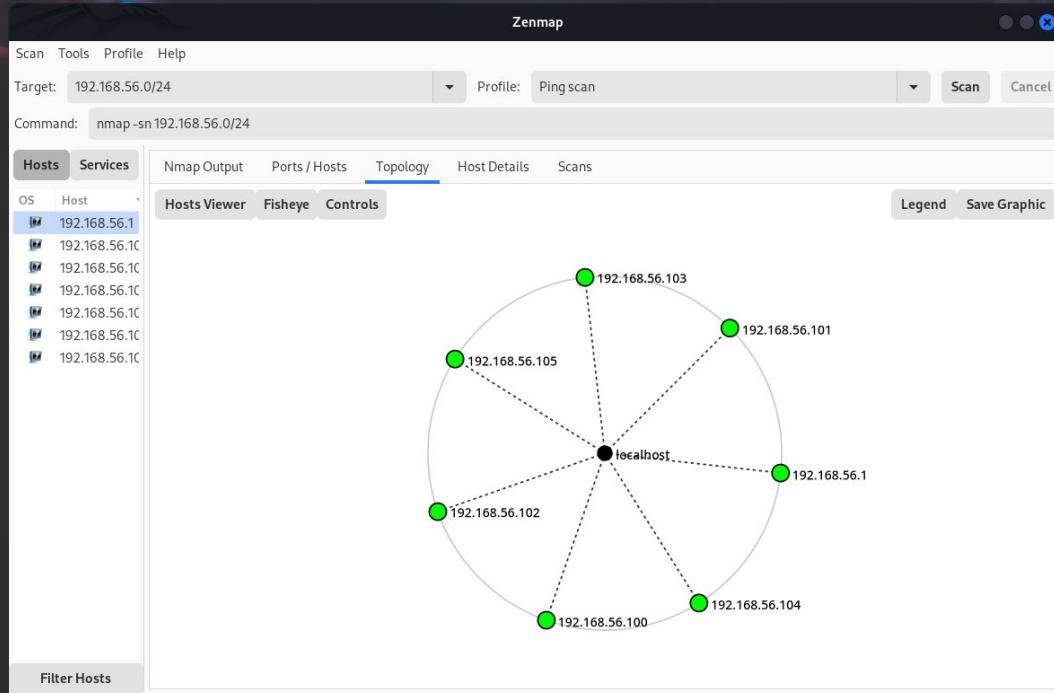
192.168.56.1	192.168.56.100
192.168.56.101	192.168.56.101
192.168.56.102	192.168.56.102
192.168.56.103	192.168.56.103
192.168.56.104	192.168.56.104
192.168.56.105	192.168.56.105

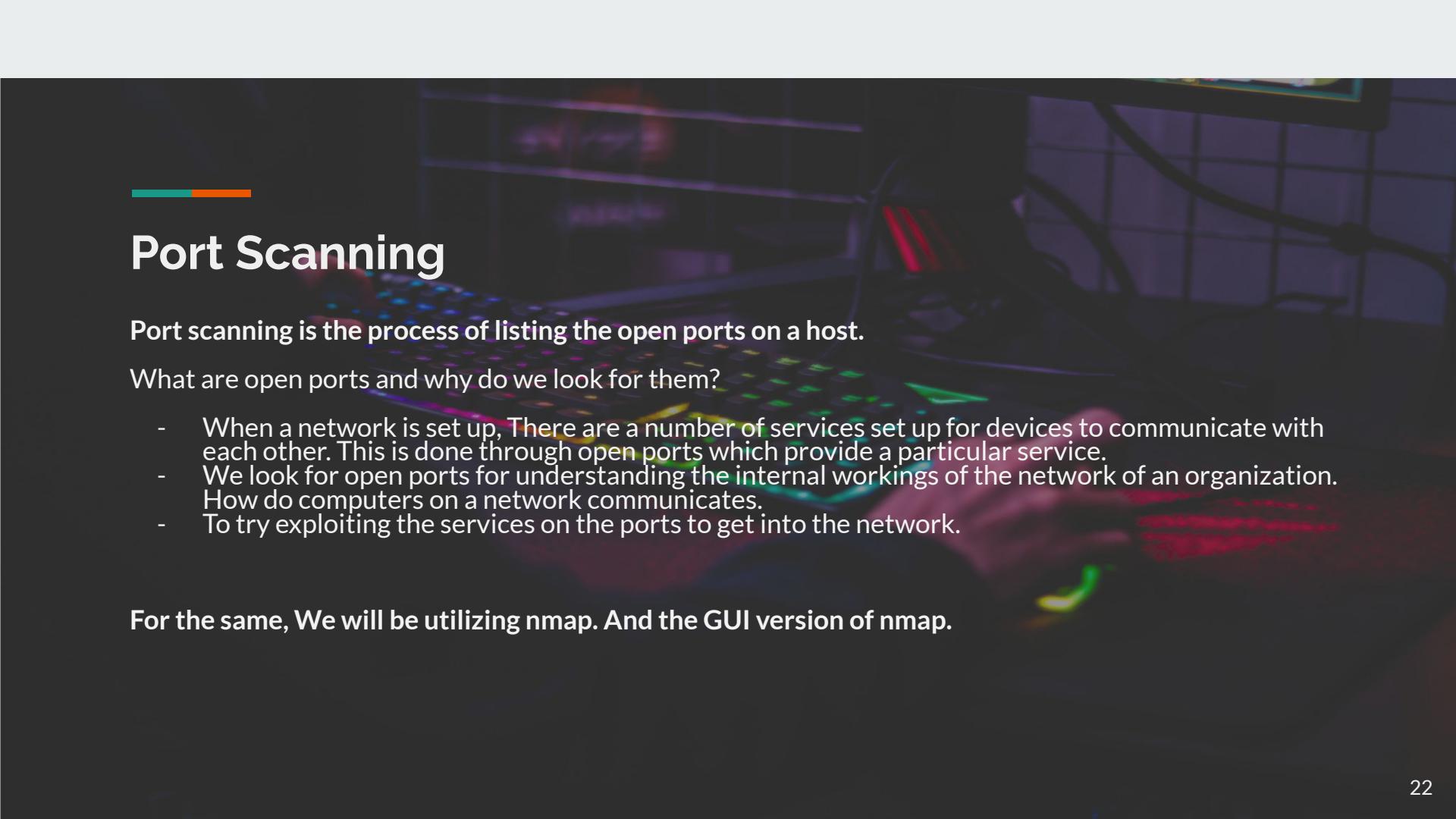
Nmap Output Ports/Hosts Topology Host Details Scans

nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 13:13 IST
Nmap scan report for 192.168.56.100
Host is up (0.00014s latency).
MAC Address: 08:00:27:F5:1C:3A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.00038s latency).
MAC Address: 08:00:27:D4:0F:A1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).
MAC Address: 08:00:27:5F:39:D2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00028s latency).
MAC Address: 08:00:27:89:A9:44 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.0016s latency).
MAC Address: 08:00:27:A9:29:20 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105
Host is up (0.0015s latency).
MAC Address: 08:00:27:99:F7:6B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.1
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 14.80 seconds

Filter Hosts

Zenmap Scan Network Topology





Port Scanning

Port scanning is the process of listing the open ports on a host.

What are open ports and why do we look for them?

- When a network is set up, There are a number of services set up for devices to communicate with each other. This is done through open ports which provide a particular service.
- We look for open ports for understanding the internal workings of the network of an organization. How do computers on a network communicates.
- To try exploiting the services on the ports to get into the network.

For the same, We will be utilizing nmap. And the GUI version of nmap.

NMap: Scanning TCP Ports on a Single Host

Default Scan:

- Scans the 1000 most common TCP Ports of a Host
- Command: **nmap ip**

All Port Scan:

- Scans All The 65535 TCP Ports of a Host
- Command: **nmap -p- ip**

```
(secovfshanks㉿nootnoot)-[~]
└ $ nmap 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-24 13:52 IST
Nmap scan report for 192.168.56.103
Host is up (0.00038s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.04 seconds
```

```
(secovfshanks㉿nootnoot)-[~]
└ $ nmap -p- 192.168.56.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-24 13:57 IST
Nmap scan report for 192.168.56.104
Host is up (0.00038s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1028/tcp  open  unknown
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 22.94 seconds
```

NMap: Scanning UDP Ports on a Single Host

UDP Scan:

- Scans the 1000 most common UDP Ports of a Host
- Command: `sudo nmap -sU ip`

UDP All Port Scan:

- Scans All The 65535 UDP Ports of a Host
- Command: `sudo nmap -p- -sU ip`

```
(secovfshanks㉿nootnoot)-[~]
$ sudo nmap -sU 192.168.56.104
[sudo] password for secovfshanks:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-24 14:01 IST
Nmap scan report for 192.168.56.104
Host is up (0.00016s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp   open|filtered  ntp
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
500/udp   open|filtered isakmp
1027/udp  open|filtered unknown
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
MAC Address: 08:00:27:A9:29:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
```

```
(secovfshanks㉿nootnoot)-[~]
$ sudo nmap -p- -sU 192.168.56.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-24 14:02 IST
Nmap scan report for 192.168.56.104
Host is up (0.000081s latency).
Not shown: 65526 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp   open|filtered  ntp
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
500/udp   open|filtered isakmp
1027/udp  open|filtered unknown
1900/udp  open|filtered upnp
3527/udp  open|filtered beserver-msg-q
4500/udp  open|filtered nat-t-ike
MAC Address: 08:00:27:A9:29:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.23 seconds
```

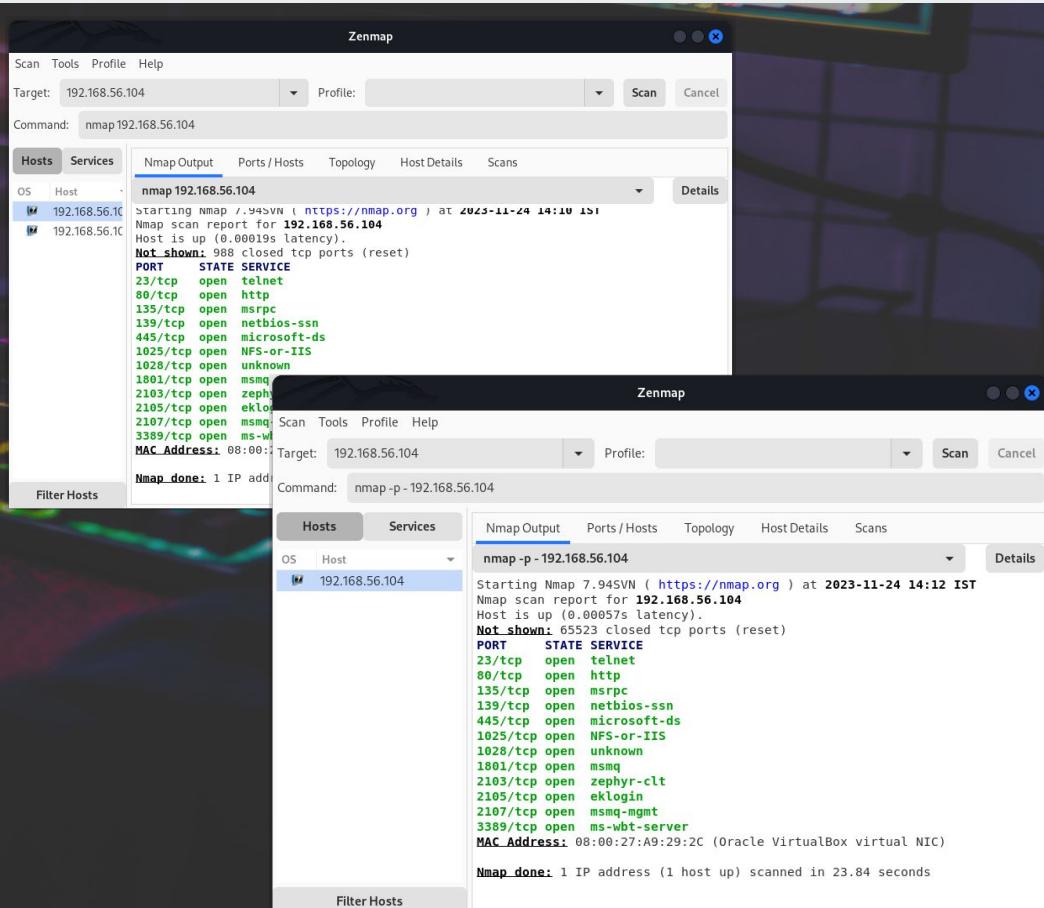
ZenMap: Scanning TCP Ports on a Single Host

Default Scan:

- Same As In NMap
- But in a GUI >_<

All Port Scan:

- Same As In NMap
- But In A GUI >_<



The screenshot shows the Zenmap interface with a scan report for host 192.168.56.104. The 'Services' tab is selected, displaying open ports and their corresponding services. The output pane shows the command run: nmap 192.168.56.104. The report details 988 closed TCP ports (reset) and lists numerous open ports with their services, including telnet, http, msrpc, netbios-ssn, microsoft-ds, NFS-or-IIS, unknown, ms-wbt-server, and others. The MAC address of the host is listed as 08:00:27:A9:29:2C.

Scan Tools Profile Help

Target: 192.168.56.104 Profile: Scan Cancel

Command: nmap 192.168.56.104

Hosts Services

OS Host

nmap 192.168.56.104

starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 14:10 IST

Nmap scan report for 192.168.56.104

Host is up (0.00019s latency).

Not shown: 988 closed tcp ports (reset)

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1028/tcp open unknown

1801/tcp open msmq

2103/tcp open zephyr

2105/tcp open eklogin

2107/tcp open msmq

3389/tcp open ms-wbt-server

MAC Address: 08:00:27:A9:29:2C

Filter Hosts

Scan Tools Profile Help

Target: 192.168.56.104 Profile: Scan Cancel

Command: nmap -p - 192.168.56.104

Hosts Services

OS Host

nmap -p - 192.168.56.104

Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 14:12 IST

Nmap scan report for 192.168.56.104

Host is up (0.00057s latency).

Not shown: 65523 closed tcp ports (reset)

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1028/tcp open unknown

1801/tcp open msmq

2103/tcp open zephyr-clt

2105/tcp open eklogin

2107/tcp open msmq-mgmt

3389/tcp open ms-wbt-server

MAC Address: 08:00:27:A9:29:2C (Oracle VirtualBox virtual NIC)

Filter Hosts

Scan Tools Profile Help

Target: 192.168.56.104 Profile: Scan Cancel

Command: nmap -p - 192.168.56.104

Hosts Services

OS Host

nmap -p - 192.168.56.104

Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 14:12 IST

Nmap scan report for 192.168.56.104

Host is up (0.00057s latency).

Not shown: 65523 closed tcp ports (reset)

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

1028/tcp open unknown

1801/tcp open msmq

2103/tcp open zephyr-clt

2105/tcp open eklogin

2107/tcp open msmq-mgmt

3389/tcp open ms-wbt-server

MAC Address: 08:00:27:A9:29:2C (Oracle VirtualBox virtual NIC)

Filter Hosts

ZenMap: Scanning UDP Ports on a Single Host

UDP Scan:

- Same As In NMap
- But in a GUI >_<

UDP All Port Scan:

- Same As In NMap
- But In A GUI >_<

Scan Tools Profile Help
Target: 192.168.56.104 Profile: Scan Cancel
Command: nmap -sU 192.168.56.104

Hosts Services
OS Host
192.168.56.104

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sU 192.168.56.104
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 14:19 IST
Nmap scan report for 192.168.56.104
Host is up (0.00073s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT STATE SERVICE
123/udp open|filtered ntp
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
161/udp open|filtered snmp
500/udp open|filtered isakmp
1027/udp open|filtered unknown
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 08:00:27:A9:29:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds

Scan Tools Profile Help
Target: 192.168.56.104 Profile: Scan Cancel
Command: nmap -sU-p - 192.168.56.104

Hosts Services
OS Host
192.168.56.104

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sU-p - 192.168.56.104
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-24 14:20 IST
Nmap scan report for 192.168.56.104
Host is up (0.00036s latency).
Not shown: 65526 closed udp ports (port-unreach)
PORT STATE SERVICE
123/udp open|filtered ntp
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
161/udp open|filtered snmp
500/udp open|filtered isakmp
1027/udp open|filtered unknown
1900/udp open|filtered upnp
3527/udp open|filtered beserver-msg-q
4500/udp open|filtered nat-t-ike
MAC Address: 08:00:27:A9:29:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds

NMap: Scanning Ports on Multiple Hosts

Multiple Host Port Scan:

- Scans The 1000 Most Common TCP Ports on Multiple Hosts
- Command: **nmap <ip range>**

Multiple Host UDP Port Scan:

- Scans The 1000 Most Common UDP Ports on Multiple Hosts
- Command: **sudo nmap -sU <ip range>**

```
(secovfshanks㉿rootroot)-[~]
└─$ nmap 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-24 15:00 IST
Nmap scan report for 192.168.56.1
Host is up (0.000067s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 192.168.56.101
Host is up (0.00051s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3000/tcp  closed ppp
3306/tcp  open  mysql
8080/tcp  open  http-proxy
8181/tcp  closed intermapper

Nmap scan report for 192.168.56.102
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
```

NMap: Using Default Scripts for Services

Multiple Host Script Scan:

- Scans The 1000 Most Common TCP Ports on Multiple Hosts
- Performs a script scan using the default set of scripts. It is equivalent to --script=default.
- Command: `nmap -sC <ip range>`

Some of the scripts in this category are considered intrusive and should not be run against a target network without Permission

```
[secovfshanks@nootnoot] ~]$ nmap -sC 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 07:23 IST
Nmap scan report for 192.168.56.1
Host is up (0.00014s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html).

Nmap scan report for 192.168.56.101
Host is up (0.0012s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:b8:a3:44:ab:b3:d3:0a:5c:6a (RSA)
|   256 c0:a9:cc:18:7b:27:a4:07:0d:2a:0d:bb:a2:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:04:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp    open  http
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME                FILENAME
| -     2020-10-29 19:37    chat/
| -     2011-07-27 20:17    drupal/
| 1.7K  2020-10-29 19:37    payroll_app.php
| -     2013-04-08 12:06    phpmyadmin/
|-
445/tcp  open  microsoft-ds
631/tcp  open  ipp
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-10-29T19:28:07
| Not valid after:  2030-10-27T19:28:07
| http-methods:
|   Potentially risky methods: PUT
|_ssl-date: 2023-11-23T21:31:17+00:00; -1d04h22m16s from scanner time.
| http-robots.txt: 1 disallowed entry
```

NMap: Using Service Version Detection

Multiple Host Service Version Scan:

- For any of the ports found open, version detection is used to determine what application is running.
- Command: `nmap -sV <ip range>`

```
(secovfshanks㉿rootroot)-[~]
$ nmap -sV 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 07:34 IST
Nmap scan report for 192.168.56.1
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.58 ((Debian))

Nmap scan report for 192.168.56.101
Host is up (0.00065s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    ProFTPD 1.3.5
22/tcp    open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.7
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp   CUPS 1.7
3000/tcp  closed  ppp
3306/tcp  open  mysql MySQL (unauthorized)
8080/tcp  open  http   Jetty 8.1.7.v20120910
8181/tcp  closed  intermapper
Service Info: Hosts: 127.0.0.1, METASPOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.56.102
Host is up (0.00039s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.56.103
Host is up (0.00048s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Microsoft Windows XP telnetd
80/tcp    open  http   Microsoft IIS httpd 7.0
135/tcp   open  msrpc  Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
```

NMap: Using OS Scan For Guessing OSes

OS Scan:

- Tries guessing OS Based on the responses received from the target machine. And compares the results to its database.
- Command: `sudo nmap -O <ip range>`

Nmap sends a series of TCP and UDP packets to the remote host and examining the responses.

```
(secovfshanks㉿nootroot)-[~]
└$ sudo nmap -O 192.168.56.0/24
[sudo] password for secovfshanks:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 07:33 IST
Nmap scan report for 192.168.56.100
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:F5:1C:3A (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.56.101
Host is up (0.00059s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3000/tcp  closed ppp
3306/tcp  open  mysql
8080/tcp  open  http-proxy
8181/tcp  closed intermapper
MAC Address: 08:00:27:D4:0F:A1 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18), or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Linux 3.2 - 3.10 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.56.102
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:5F:39:D2 (Oracle VirtualBox virtual NIC)
```

OS DETECTION

One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its `nmap-os-db` database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. Each fingerprint includes a freeform textual description of the OS, and a classification which provides the vendor name (e.g. Sun), underlying OS (e.g. Solaris), OS generation (e.g. 10), and device type (general purpose, router, switch, game console, etc). Most fingerprints also have a Common Platform Enumeration (CPE) representation, like `cpe:/o:linux:linux_kernel:2.6`.

Thank You