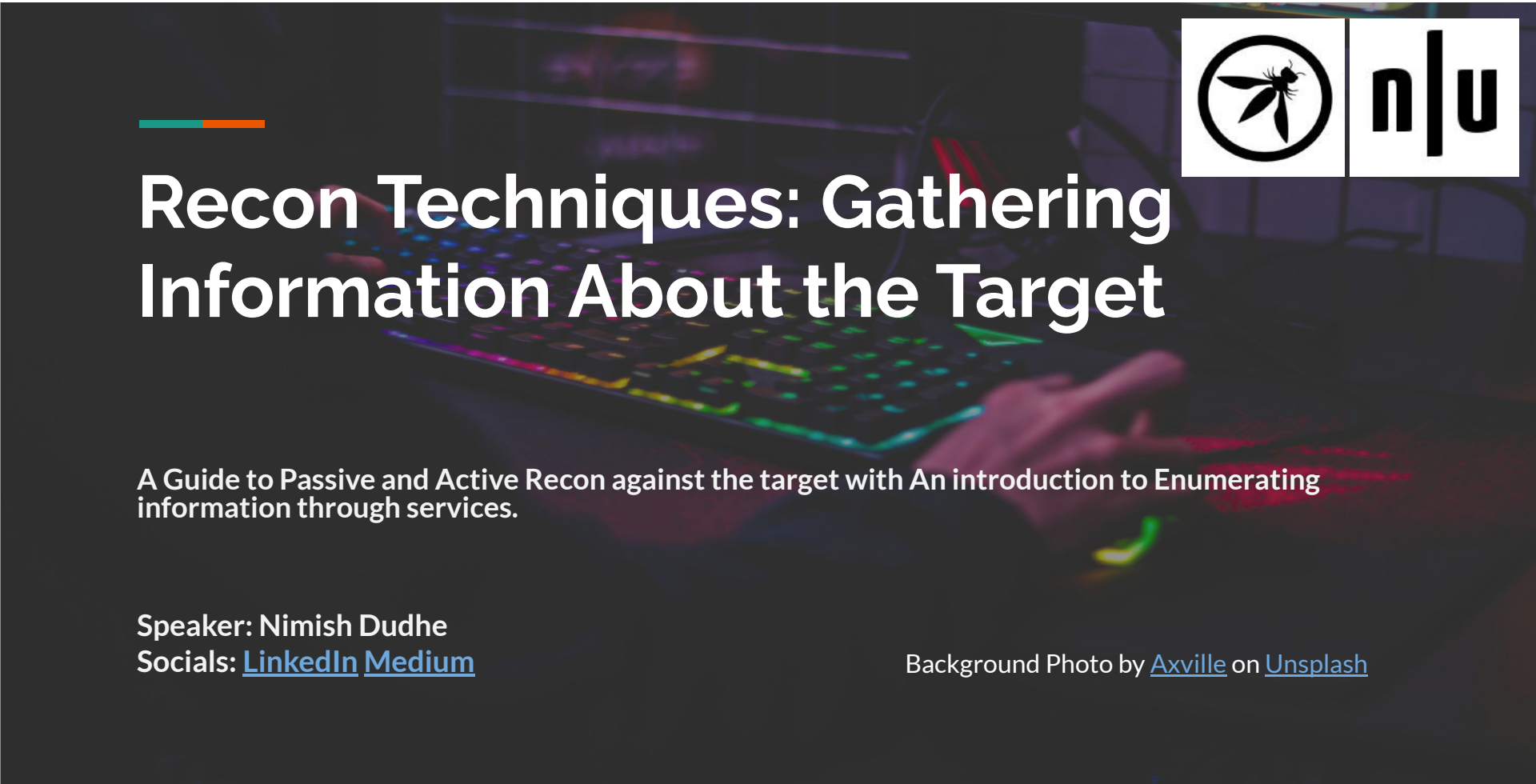


Recon Techniques: Gathering Information About the Target

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.

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.

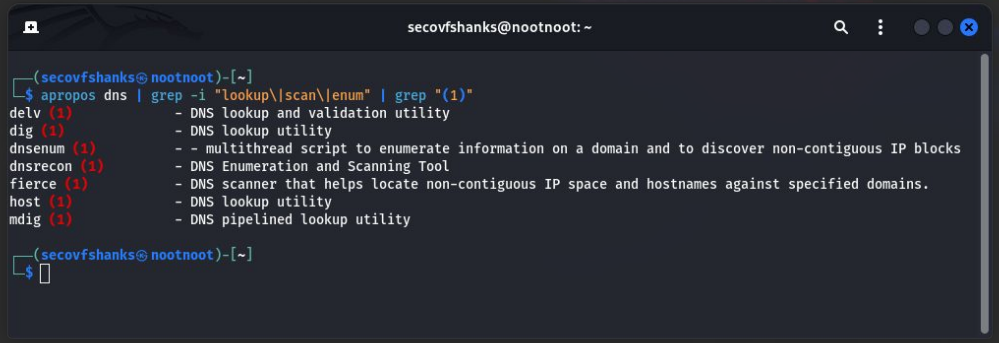
```
┌──(secovfshanks㉿nootnoot)-[~]
└─$ host null.community
null.community has address 104.21.7.192
null.community has address 172.67.187.250
null.community has IPv6 address 2606:4700:3032::6815:7c0
null.community has IPv6 address 2606:4700:3036::ac43:bbfa
null.community mail is handled by 5 alt1.aspmx.l.google.com.
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.
```

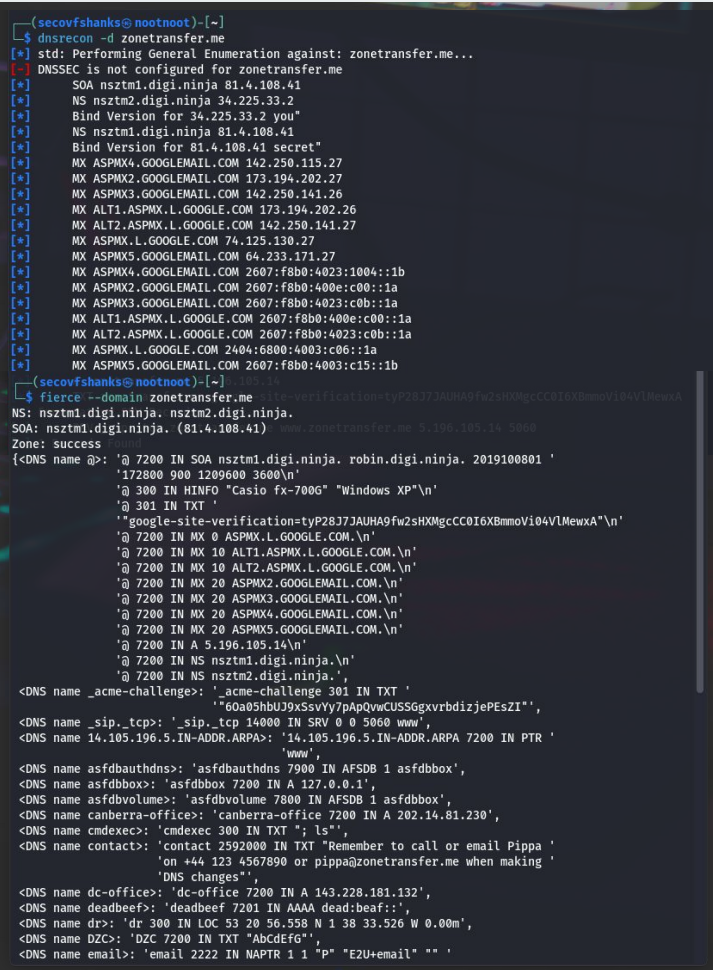
```
┌──(secovfshanks㉿nootnoot)-[~]
└─$ dig null.community

; <<>> 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

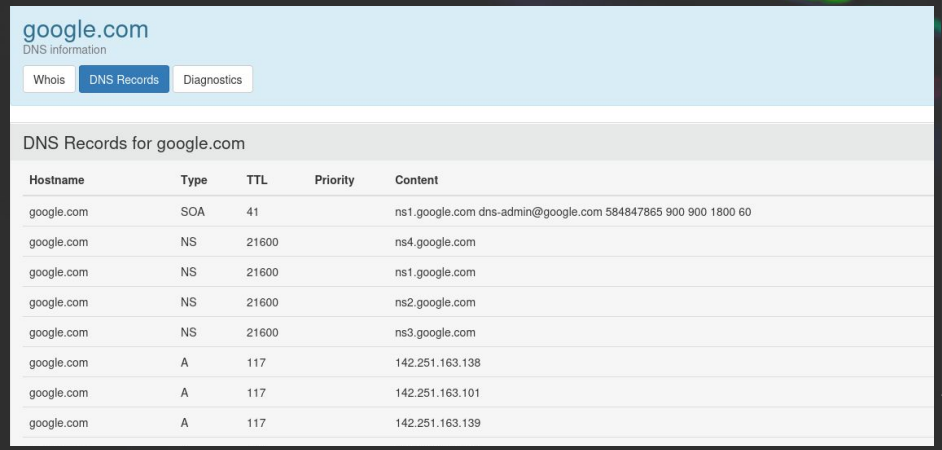


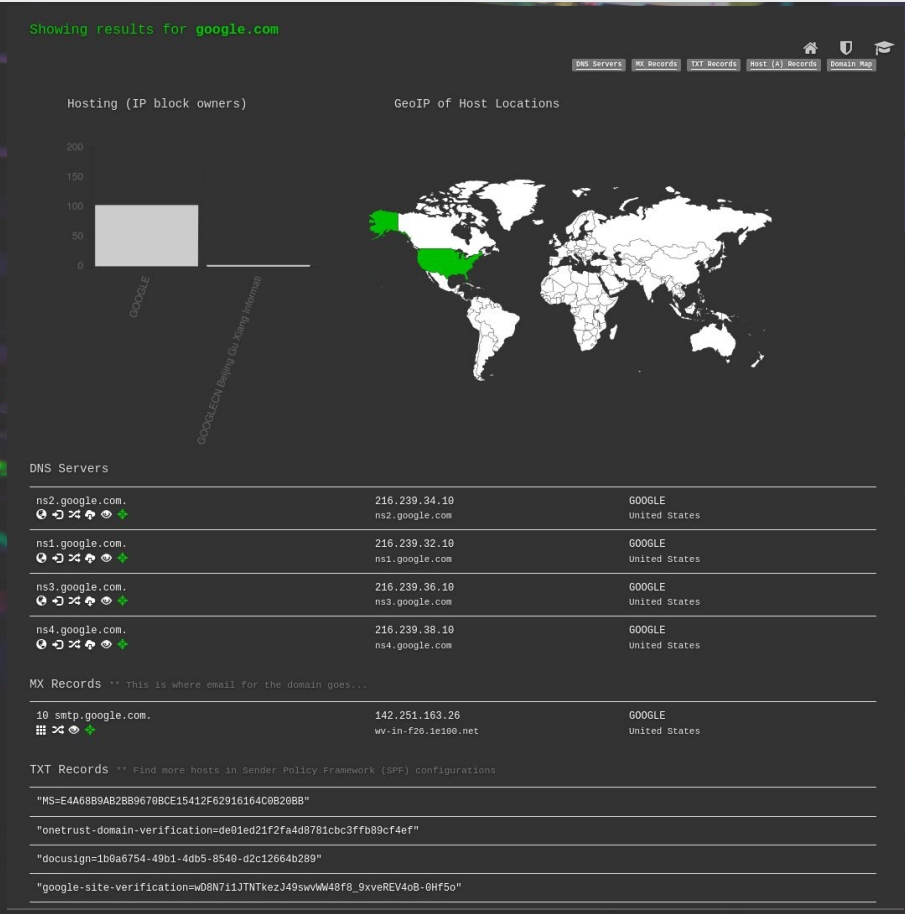


DNS Information (Records)

Web Tools:

- dnsdumpster.com
- who.is





Domain Ownership Info

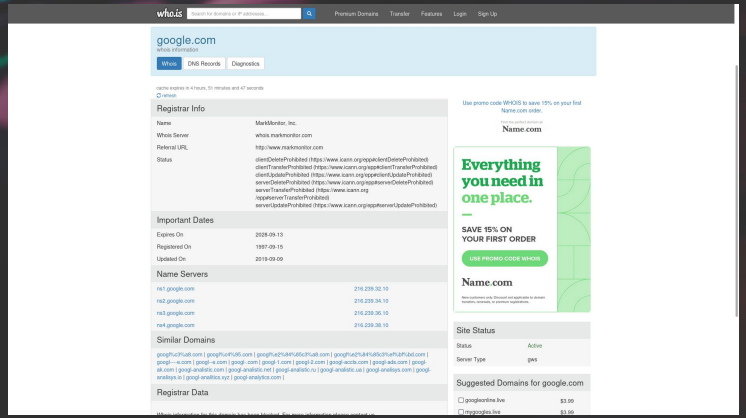
WHOIS is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees. These resources include domain names, IP address blocks and autonomous systems.

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:

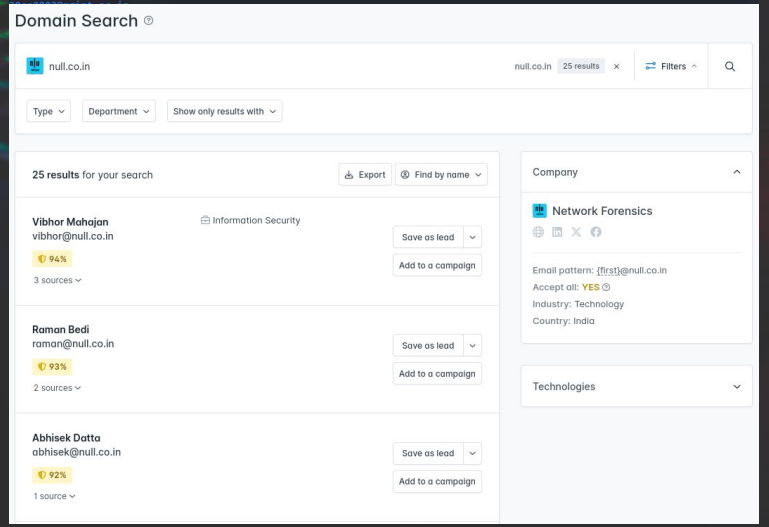
- whois Command Line Utility
- who.is webpage

```
┌──(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

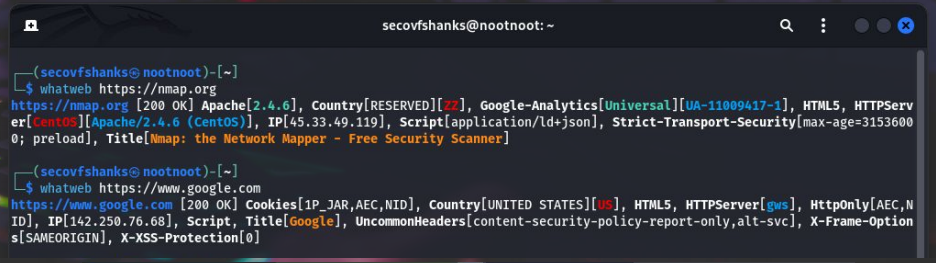
- theHarvester
  - An Open source tool that utilizes Open Source Intelligence (OSINT)
  - The tool gathers names, emails, IPs, subdomains, and URLs by using multiple public resources such as yahoo, google, crt.sh, dnsdumpster, etc.
- hunter.io
  - Hunter was created by Antoine Finkelstein and François 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.

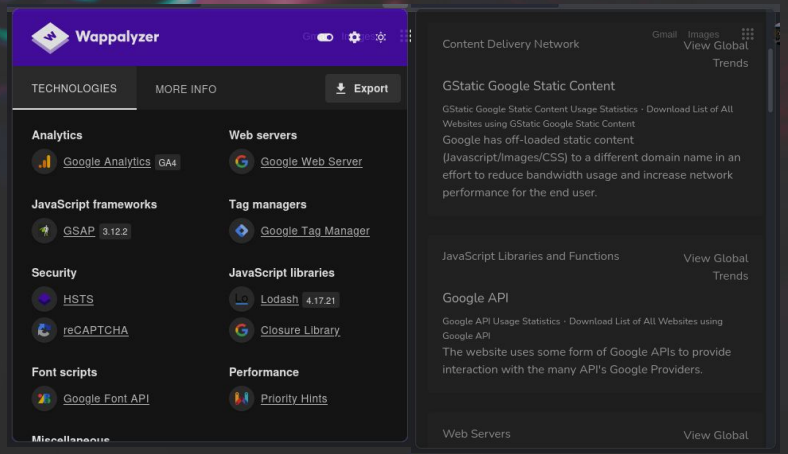


Web Technologies Used on a Site

Technology Profilers

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

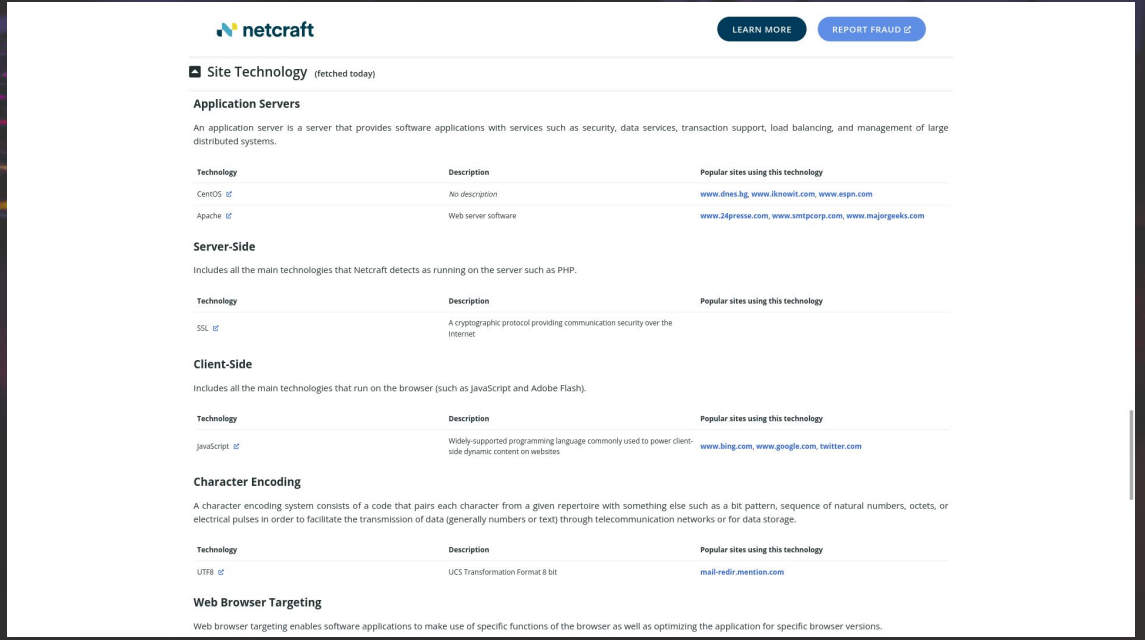




Web Technologies Used on a Site

Technology Profilers

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



netcraft

LEARN MORE REPORT FRAUD

Site Technology (fetched today)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

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

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

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

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

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

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

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

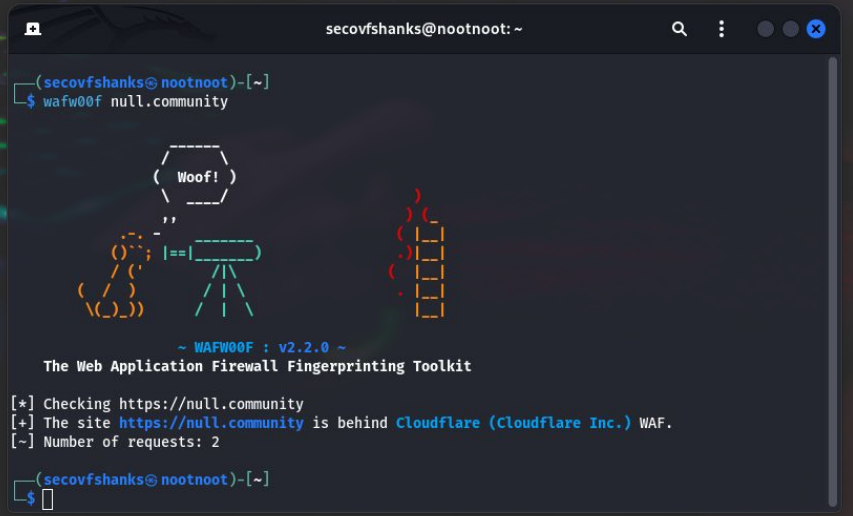
Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Detecting Firewalls Used by the Site

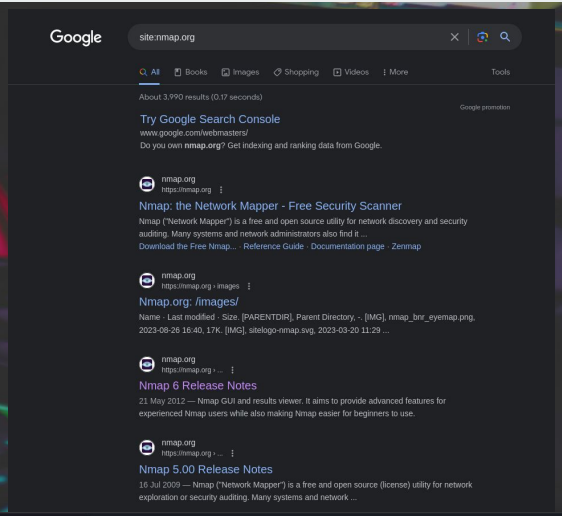
wafw00f

- 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

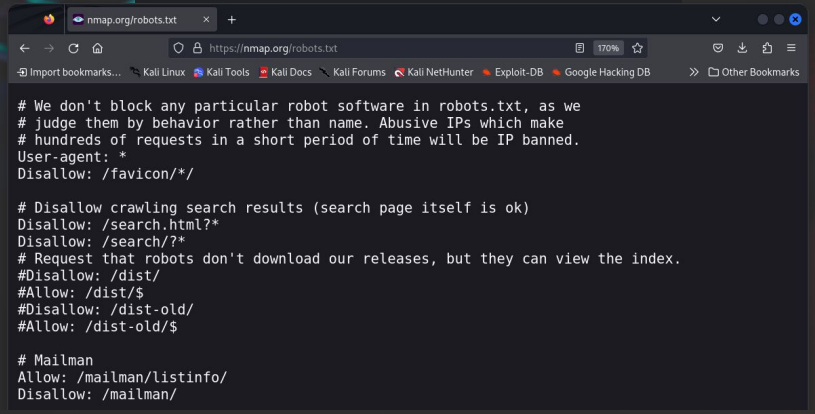


Directory Enumeration

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

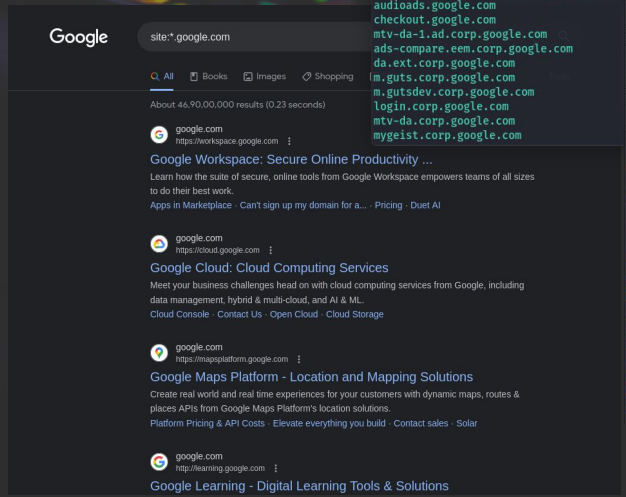



```
−<urlset xsi:schemaLocation="http://www.google.com/schemas/sitemap/0.84 http://www.google.com/schemas/sitemap/0.84/sitemap.xsd">
 −<url>
    <loc>https://nmap.org/</loc>
    <lastmod>2022-03-23T20:58:18Z</lastmod>
    <priority>0.5000</priority>
  </url>
 −<url>
    <loc>https://nmap.org/5/</loc>
    <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>
```



Subdomain Enumeration

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



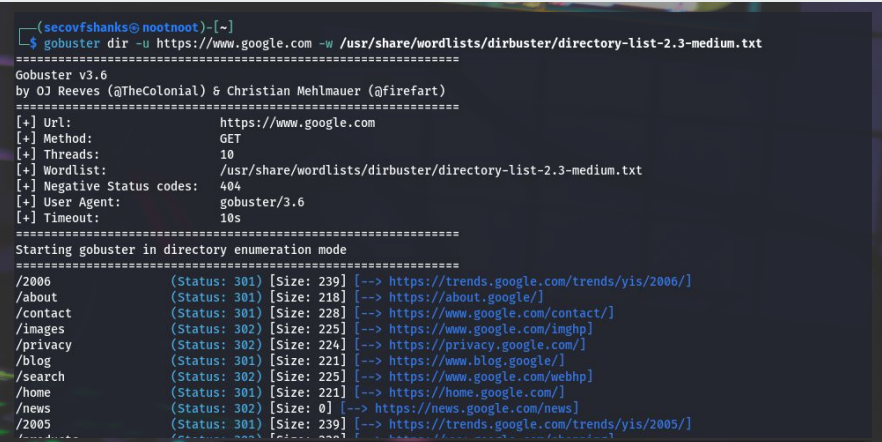
Active Information Gathering

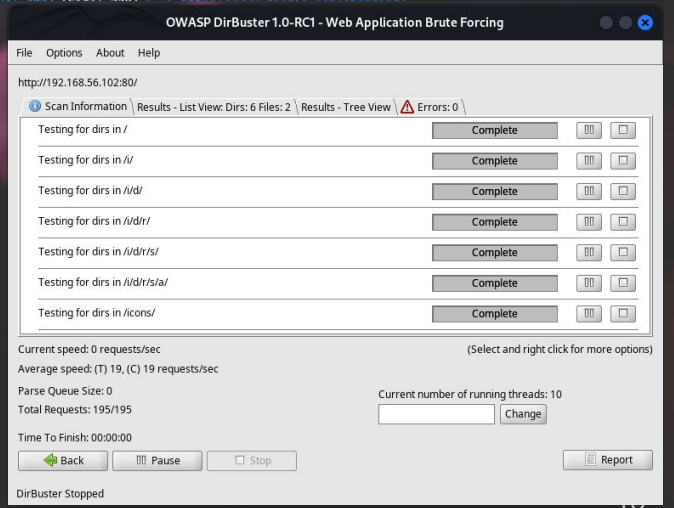
What do we look for?

- **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

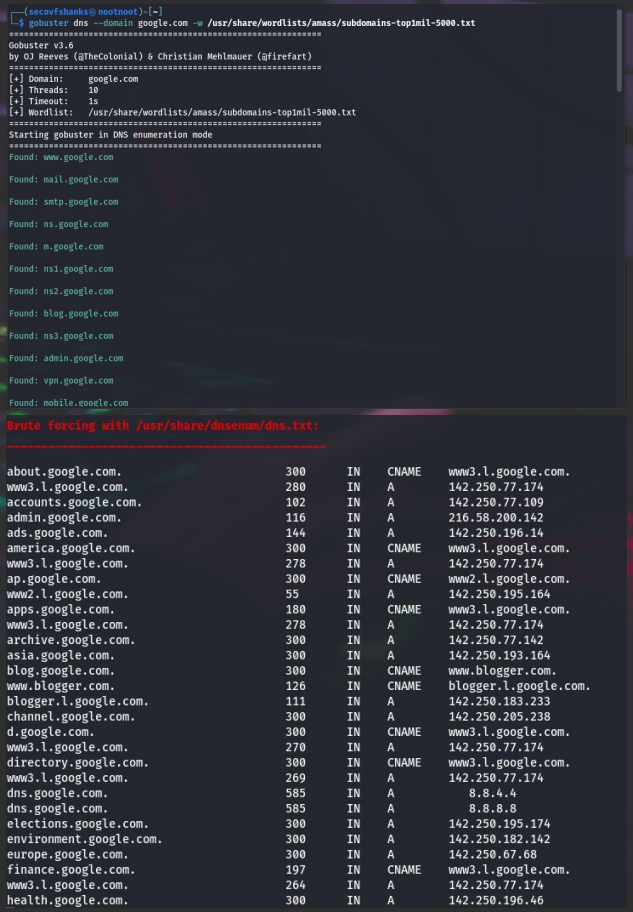
- gobuster
  - Is written in go.
  - Used to brute force URIs (Directories and Files), subdomains, etc.
- dirbuster
  -
  - Developed at OWASP Lead by James Fisher.
  - A multithreaded Java application
  - Designed to brute force files and directories on web/application servers





Subdomain Listing

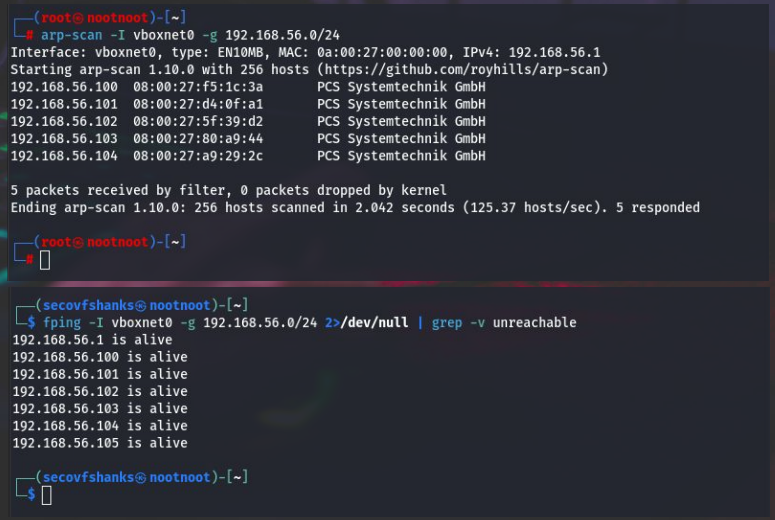
- gobuster
  - Is written in go.
  - Used to brute force URIs (Directories and Files), subdomains, etc.
- dnsenum
  - Multithread script to enumerate information on a domain and to discover non-contiguous IP blocks.



Section II: Scanning

Listing Live Machines on a Network

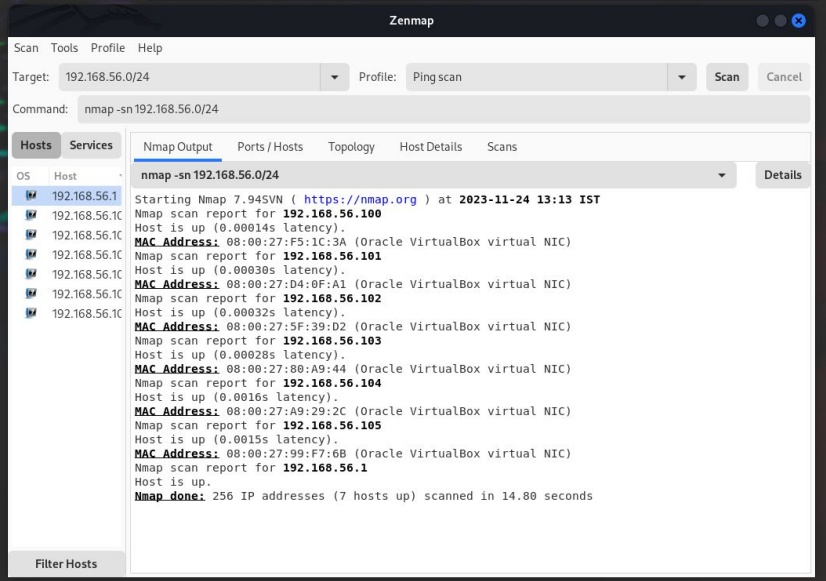
- ARP (Address Resolution Protocol)
  - arp-scan (root privileges required)
- ICMP (Internet Control Message Protocol)
  - fping command
  - NMap Host Discovery
    - ICMP Echo Request Scan
    - Doesn't scan for open ports
  - ZenMap Host Discovery
    - Same as NMap but in GUI >_<



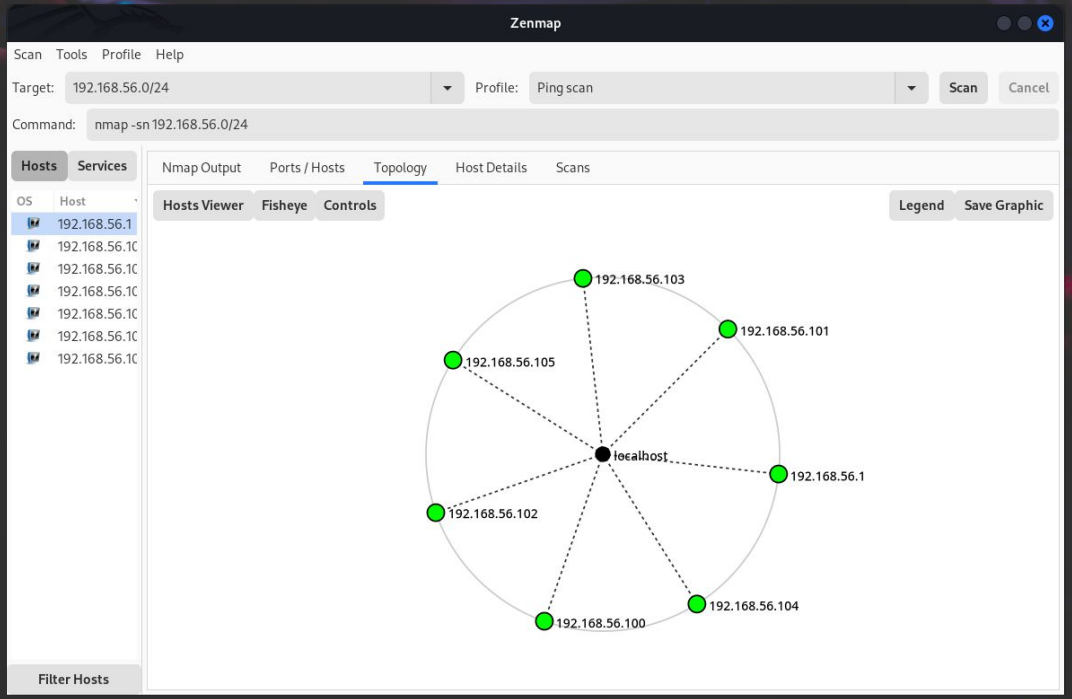
Listing Live Machines on a Network

- 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 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  wsdapi
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
```

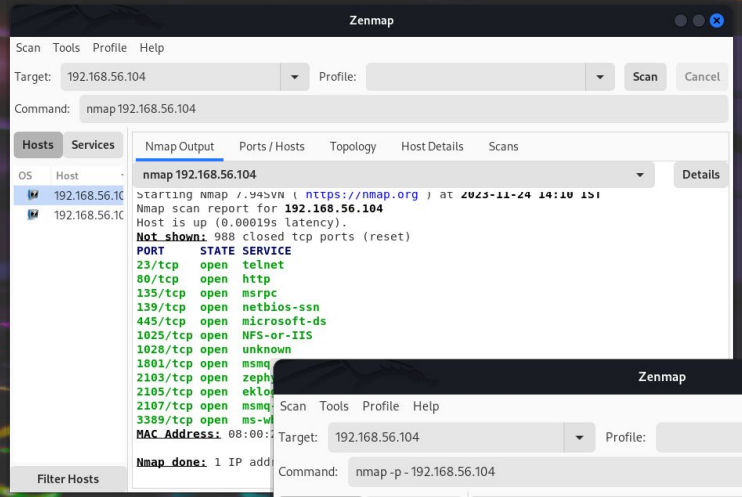
ZenMap: Scanning TCP Ports on a Single Host

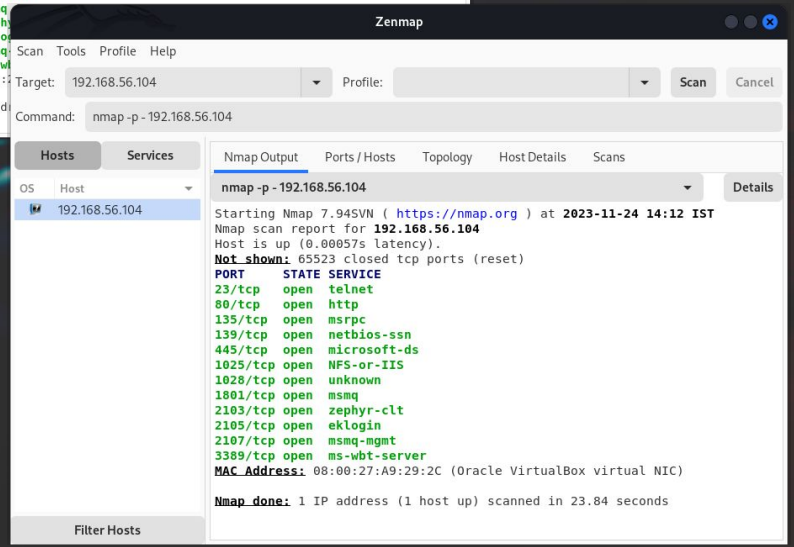
Default Scan:

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

All Port Scan:

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





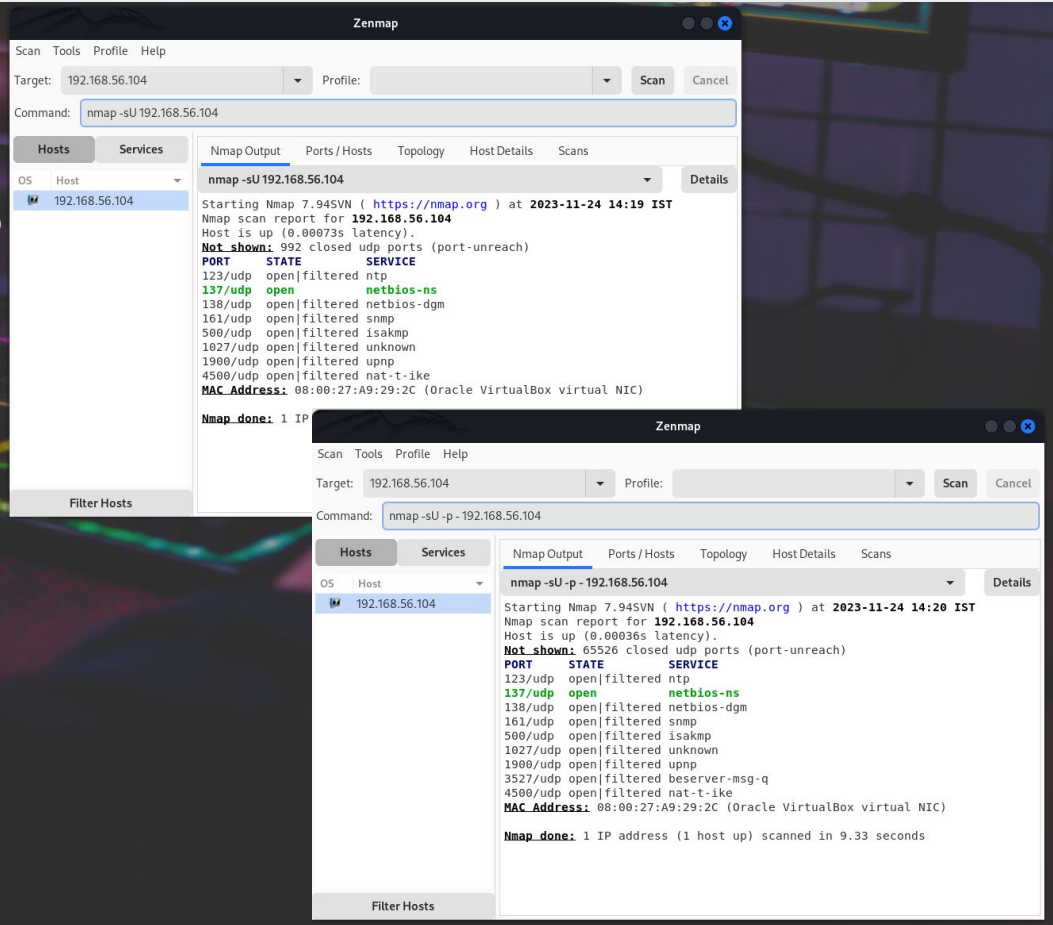
ZenMap: Scanning UDP Ports on a Single Host

UDP Scan:

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

UDP All Port Scan:

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



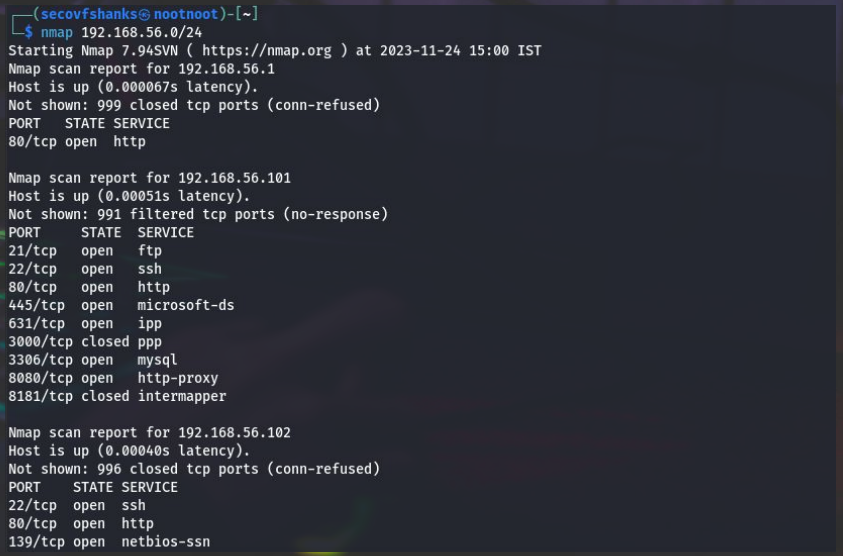
NMap: Scanning Ports on Multiple Hosts

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>`**



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:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d: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㉿nootnoot)-[~]
└─$ 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, METASPLOITABLE3-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㉿nootnoot)-[~]
└─$ 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%),
 Linux 3.2 - 3.16 (94%), Linux 4.5 (93%), Linux 3.13 - 3.16 (93%)
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