

# Cyber security

---

HEF

• CHFI



Edit with WPS Office

**Submitted By: Arbab Rauf**  
**Submitted To: Muhammad Bila**



Edit with WPS Office

# Email & Domain Information Gathering

---

- It is also known as reconnaissance, involves collecting data from publicly available sources to understand the target's online presence and potential vulnerabilities.



Edit with WPS Office

## WHOIS Lookup

---

- WHOIS Lookup is a query and response protocol used to obtain information about the owner of a domain name, IP address, or an autonomous system on the Internet. It provides details such as the registrant's name, contact information, and the domain's registration and expiration dates.



Edit with WPS Office

# EXAMPLE

```
(rana@rana)-[~]
$ whois britannica.com
Domain Name: BRITANNICA.COM
Registry Domain ID: 3021450_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-06-09T05:06:21Z
Creation Date: 1995-06-14T04:00:00Z
Registry Expiry Date: 2025-06-13T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
d
Name Server: NS-1050.AWSDNS-03.ORG
Name Server: NS-1567.AWSDNS-03.CO.UK
Name Server: NS-243.AWSDNS-30.COM
Name Server: NS-829.AWSDNS-39.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-07-25T12:28:39Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
```



Edit with WPS Office

# DNS Records Analysis

- it involves examining the Domain Name System records to uncover details about domain ownership, IP addresses, and the mail servers associated with a domain.

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record



## **Techniques and Tools/Websites:-**

- WHOIS Lookup:
- who is britannica.com
- Website:
- <https://lookup.icann.org/en/lookup>
- <https://lookup.icann.org/en/lookuphttps://lookup.icann.org/en/lookup>

### **Domain Information**

**Name:** YOUTUBE.COM

**Registry Domain ID:** 142504053\_DOMAIN\_COM-VRSN

**Domain Status:**

[clientDeleteProhibited](#)

[clientTransferProhibited](#)

[clientUpdateProhibited](#)

[serverDeleteProhibited](#)

[serverTransferProhibited](#)

[serverUpdateProhibited](#)

**Nameservers:**

NS1.GOOGLE.COM

NS2.GOOGLE.COM

NS3.GOOGLE.COM

NS4.GOOGLE.COM

### **Dates**

**Registry Expiration:** 2025-02-15 05:13:12 UTC

**Updated:** 2024-01-14 09:59:57 UTC

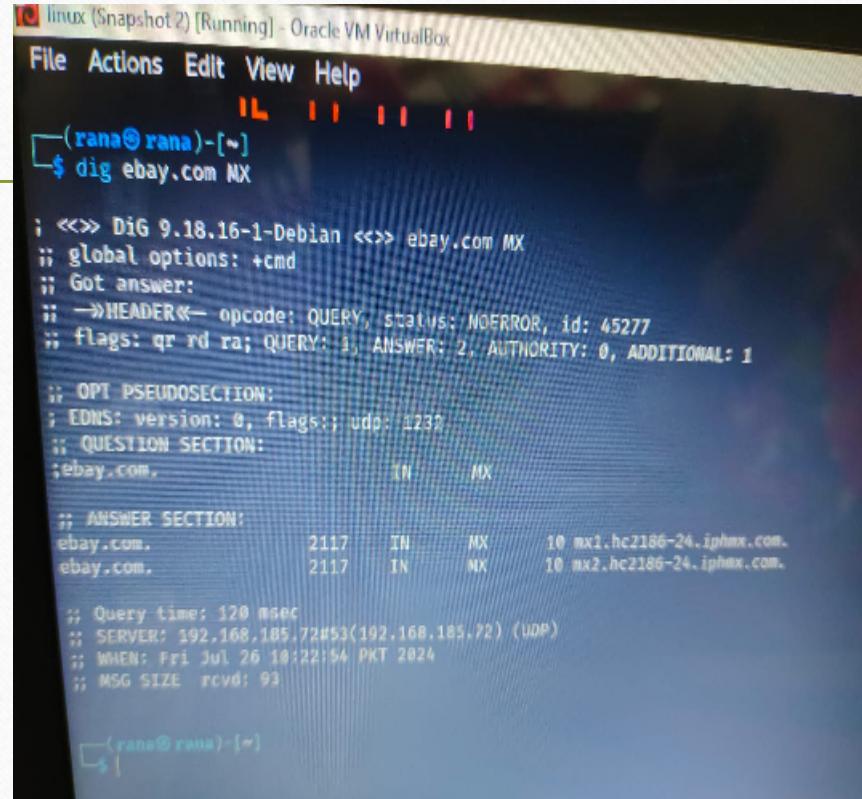
**Created:** 2005-02-15 05:13:12 UTC



Edit with WPS Office

# DNS Records Analysis:

- Techniques and Tools/Websites:
- Command: dig youtube.com MX



```
linux (Snapshot 2) [Running] - Oracle VM VirtualBox
File Actions Edit View Help
(rana@rana)-[~]
$ dig ebay.com NX

; <>> DiG 9.18.16-1-Debian <>> ebay.com NX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 45277
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;;
;; QUESTION SECTION:
;ebay.com.           IN      MX
;ANSWER SECTION:
ebay.com.        2117    IN      MX      10 mx1.hc2186-24.ipmx.com.
ebay.com.        2117    IN      MX      10 mx2.hc2186-24.ipmx.com.

;; Query time: 120 msec
;; SERVER: 192.168.185.72#53(192.168.185.72) (UDP)
;; WHEN: Fri Jul 26 10:22:54 PKT 2024
;; MSG SIZE rcvd: 93

(rana@rana)-[~]
```



Edit with WPS Office

- Website:
- MXtoolbox

The screenshot shows the MXtoolbox SuperTool interface. The URL in the address bar is `mxtoolbox.com/SuperTool.aspx?action=mx%3amazon.com&run=toolpage`. The page title is "SuperTool Beta7". A search bar contains "amazon.com" and an orange "MX Lookup" button. Below the search bar, there are three buttons: "mx:amazon.com" (highlighted), "Find Problems", and "Solve Email Delivery Problems". A message at the top right says "Gmail & Yahoo are now requiring DMARC - Get your's setup with Delivery Center".

Pref	Hostname	IP Address	TTL	Actions
5	amazon-smtp.amazon.com	44.231.24.41 Amazon.com, Inc. (AS18509)	15 min	Blacklist Check SMTP Test

Test	Result
✓ DMARC Record Published	DMARC Record found
✓ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓ DNS Record Published	DNS Record found

Below the tables are navigation links: dns lookup, dns check, dmarc lookup, spf lookup, dns propagation, and a Transcript link. At the bottom, it says "Reported by ns1.amzndns.org on 7/26/2024 at 12:40:41 AM (UTC -5). just for you."

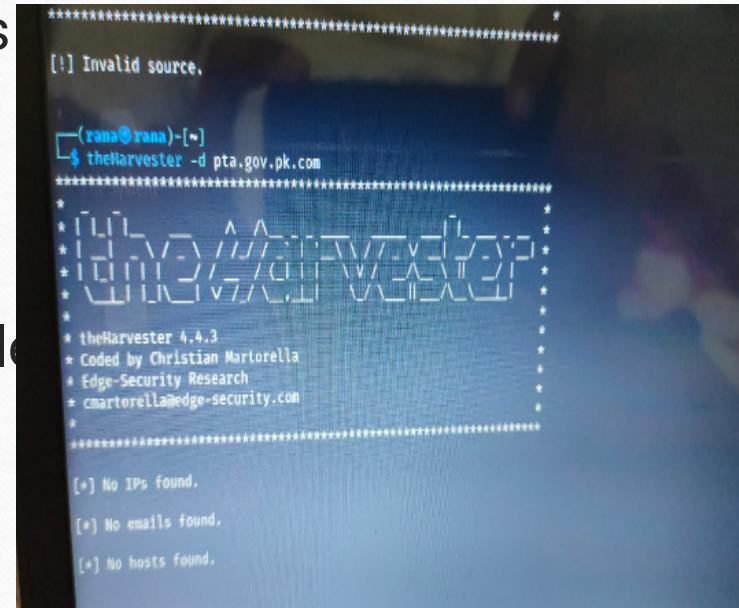


Edit with WPS Office

# Email Address Search:

---

- Techniques: Search for email addresses associated with a domain using public databases and search engines.
- Tool:
- theHarvester -d pta.gov.pk.com -b google
- Website:
- Hunter.io

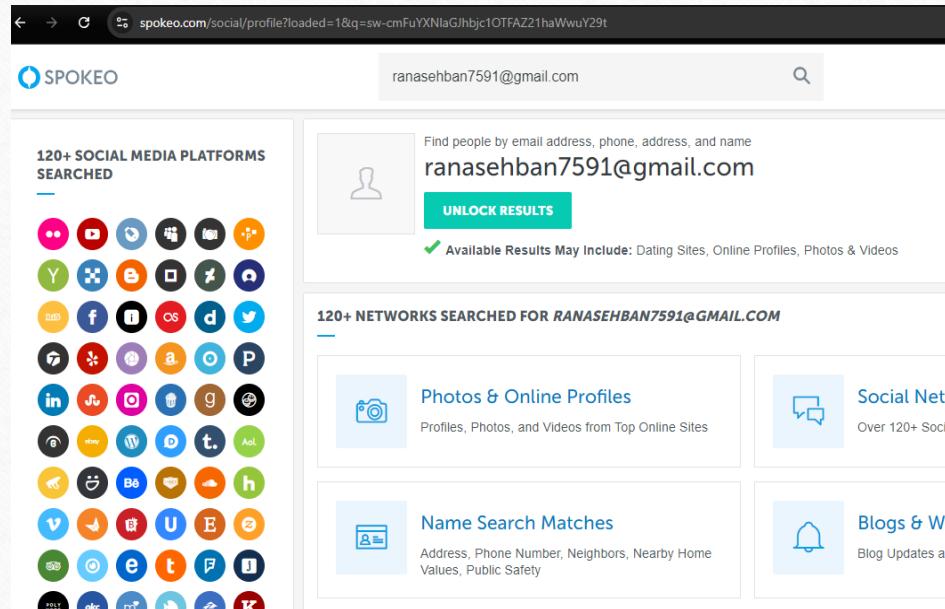


```
*****  
[!] Invalid source,  
[(rana@rana)-[*]] $ theHarvester -d pta.gov.pk.com  
*****  
* [!] No IPs found.  
* [!] No emails found.  
* [!] No hosts found.  
*****  
* theHarvester 4.4.3  
* Coded by Christian Martorella  
* Edge-Security Research  
* cmartorell@edge-security.com  
*  
*****
```



# Reverse Email Lookup:-

- Websites:
- Pipl
- spokeo



# **Metadata Analysis:-**

---

- It include information about the file creation date, author, software used, and other details that are embedded within the file.



Edit with WPS Office

# **Document Metadata Extraction:-**

---

- Extracting metadata from a PDF file to find out the author, creation date, and software used to create the document
- **Tools/Websites:**
- Tool: exiftool  
exiftool document.pdf
- Tool: FOCA  
foca-cli -f document.pdf

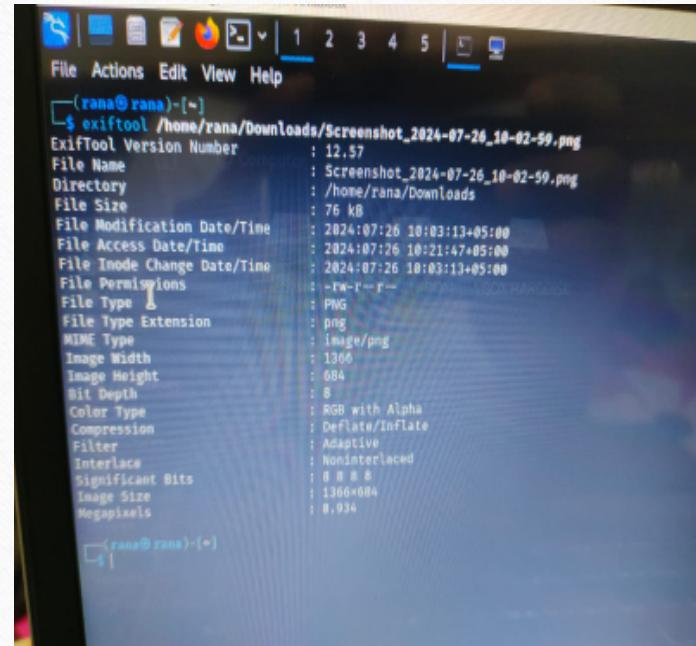


Edit with WPS Office

# Image Metadata Analysis:

---

- Extracting EXIF data from a JPEG image to find out the camera model, GPS location, and date/time the photo was taken.
- Tools/Websites:
- Tool: exiftool  
exiftool image.jpg
- Tool: FOCA  
foca-cli -f image.jpg



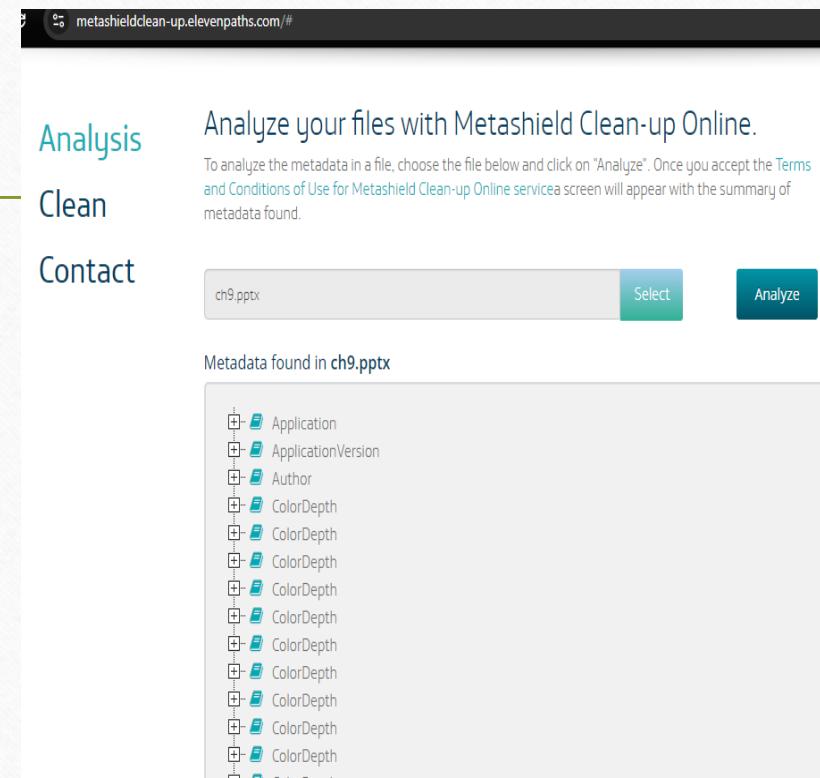
```
(rana@rana)-[~]
$ exiftool /home/rana/Downloads/Screenshot_2024-07-26_10-02-59.png
ExifTool Version Number : 12.57
File Name               : Screenshot_2024-07-26_10-02-59.png
Directory              : /home/rana/Downloads
File Size               : 76 KB
File Modification Date/Time : 2024:07:26 10:03:13+05:00
File Access Date/Time   : 2024:07:26 10:21:47+05:00
File Inode Change Date/Time : 2024:07:26 10:03:13+05:00
File Permissions        : -rw-r--r-
File Type               : PNG
File Type Extension    : png
MIME Type               : image/png
Image Width             : 1366
Image Height            : 684
Bit Depth               : 8
Color Type              : RGB with Alpha
Compression             : Deflate/Inflate
Filter                  : Adaptive
Interlace               : Noninterlaced
Significant Bits        : 0 0 0 0
Image Size              : 1366x684
Megapixels              : 0.934
```



Edit with WPS Office

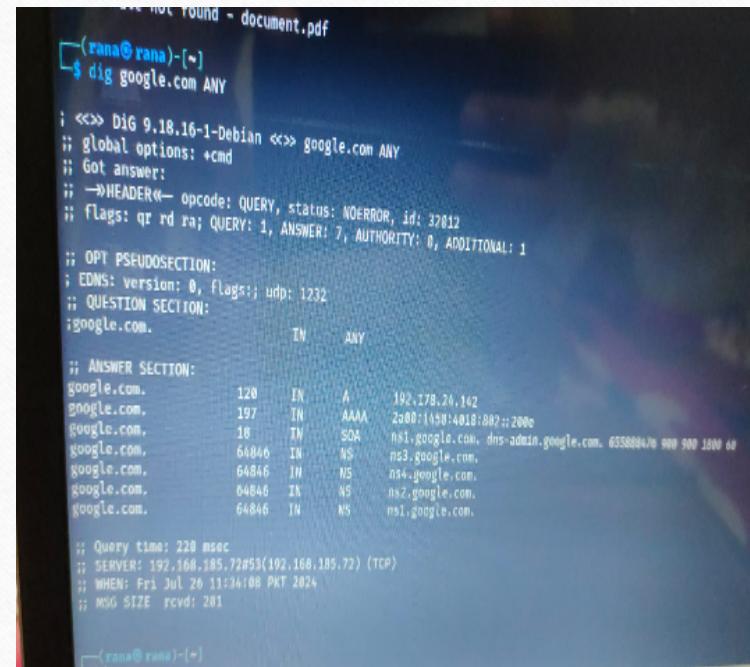
## Online Metadata Analyzers:

- Metashield analyzer
  - Get-MetaData



# DNS Enumeration:

- Process of collecting detailed information about a domain's DNS (Domain Name System) records.
- **DNS Queries:**
- Tools/Websites:
- Command: dig google.com ANY
- Command: nslookup -type=ANY google.com.com
- Website: MXToolbox



```
** not found - document.pdf
(rana@rana)-[~]
$ dig google.com ANY

; <>> DiG 9.18.16-1-Debian <>> google.com ANY
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32012
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.      IN      ANY

;; ANSWER SECTION:
google.com.        120    IN      A       192.178.24.142
google.com.        197    IN      AAAA    2a00:1450:4010:807::200e
google.com.        18     IN      SOA    ns1.google.com. dns-admin.google.com. 655880476 900 900 1500 60
google.com.        64846   IN      NS     ns3.google.com.
google.com.        64846   IN      NS     ns4.google.com.
google.com.        64846   IN      NS     ns2.google.com.
google.com.        64846   IN      NS     ns1.google.com.

;; Query time: 220 msec
;; SERVER: 192.168.185.72#53(192.168.185.72) (TCP)
;; WHEN: Fri Jul 26 11:34:08 PKT 2024
;; MSG SIZE rcvd: 281
```



# DNS Enumeration Tools:

---

- Tool: dnsenum
- dnsenum example.com
- Tool: dnsrecon
- dnsrecon -d google.com
- Tool: fierce
- fierce -dns example.com

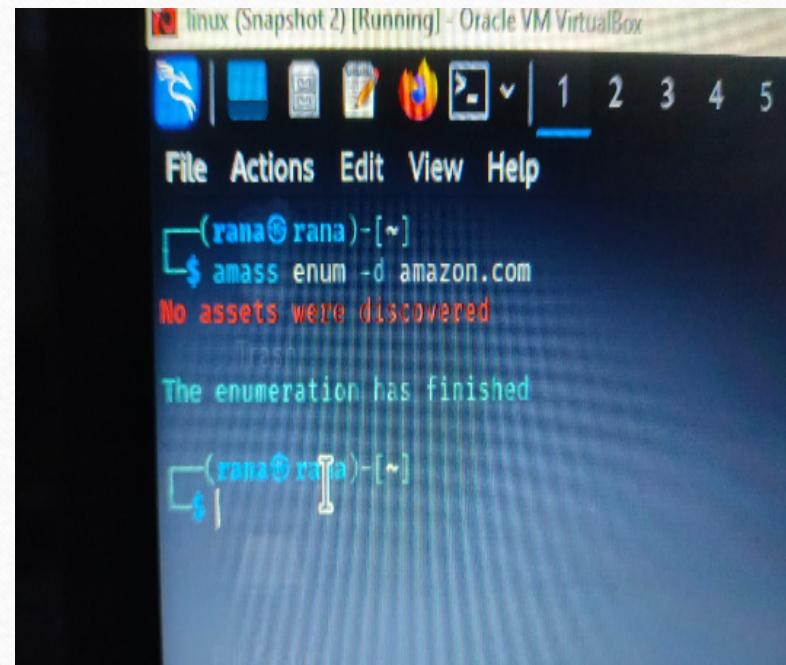
```
(rana㉿rana) ~
└─$ dnsrecon -d google.com
[*] std: Performing General Enumeration against: google.com ...
[!] DNSSEC is not configured for google.com
[*] SOA ns1.google.com 216.239.32.10
[*] SOA ns1.google.com 2001:4860:4802:32::a
[*] NS ns3.google.com 216.239.30.10
[*] NS ns3.google.com 2001:4860:4802:36::a
[*] NS ns4.google.com 216.239.30.10
[*] NS ns4.google.com 2001:4860:4802:38::a
[*] NS ns2.google.com 216.239.34.10
[*] NS ns2.google.com 2001:4860:4802:34::a
[*] NS ns1.google.com 216.239.32.10
[*] NS ns1.google.com 2001:4860:4802:32::a
[*] MX smtp.google.com 173.194.76.25
[*] MX smtp.google.com 173.194.76.27
[*] MX smtp.google.com 66.192.1.26
[*] MX smtp.google.com 66.192.1.27
[*] MX smtp.google.com 142.250.138.27
[*] MX smtp.google.com 2000:1150:4800:c00::1a
[*] MX smtp.google.com 2000:1150:4800:c00::1b
[*] MX smtp.google.com 2000:1150:4800:c00::1b
[*] MX smtp.google.com 2000:1150:4800:c00::1a
[*] A google.com 142.258.181.174
[*] AAAA google.com 2a00:1a58:1a61:8002::2000
[*] Enumerating SRV Records
[*] SRV _ldap._tcp.google.com ldap.google.com 216.239.32.58 389
[*] SRV _ldap._tcp.google.com ldap.google.com 2001:4860:4802:32::30 389
[*] SRV _caldav._tcp.google.com calendar.google.com 142.250.185.46 443
[*] SRV _caldav._tcp.google.com calendar.google.com 2000:1450:4803:8009::2000 443
[*] SRV _carddav._tcp.google.com google.com 142.250.181.174 443
[*] SRV _carddav._tcp.google.com google.com 2000:1450:4803:8002::2000 443
[*] SRV _caldav._tcp.google.com calendar.google.com 142.250.185.46 80
[*] SRV _caldav._tcp.google.com calendar.google.com 2000:1450:4803:8009::2000 80
8 Records Found
```



# Subdomain Enumeration:

---

- Tools:
- Tool: sublist3r  
sublist3r -d amazon.com
- Tool: amass  
amass enum -d amazon.com
- Website: VirusTotal (for discovering subdomains via DNS records)



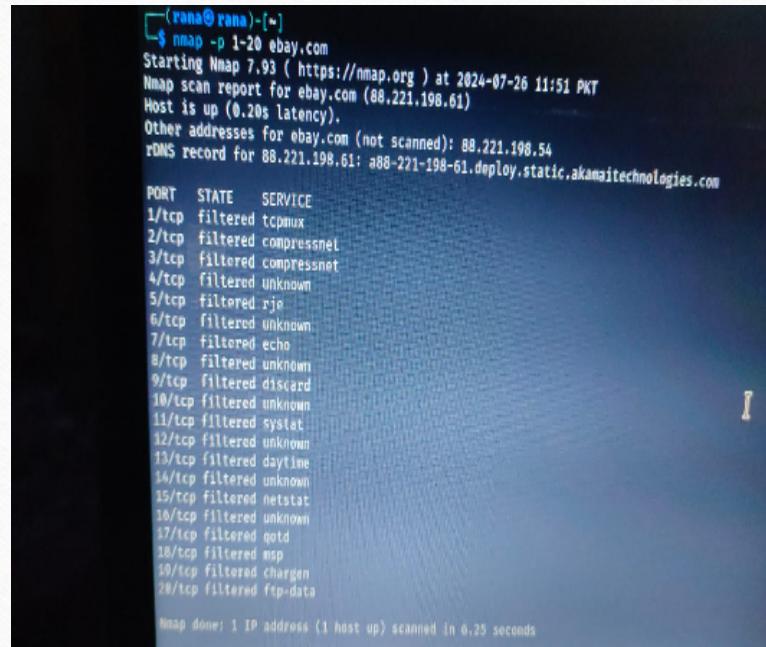
```
linux (Snapshot 2) [Running] - Oracle VM VirtualBox
File Actions Edit View Help
(rana@rana)-[~]
$ amass enum -d amazon.com
No assets were discovered
The enumeration has finished
(rana@rana)-[~]
$
```

# Enumeration of Network Services:-

---

- Process of identifying active services running on a network, such as web servers, FTP servers, email servers, and other types of networked applications.
- Examples:-
- Port Scanning:
- Nmap:  
nmap -p 1-65535 google.com
- Masscan (for very large networks or fast scans):

masscan -p1-65535 192.168.1.0/24



```
(rana@rana)-[~]$ nmap -p 1-20 ebay.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-26 11:51 PKT
Nmap scan report for ebay.com (88.221.198.61)
Host is up (0.20s latency).
Other addresses for ebay.com (not scanned): 88.221.198.54
rDNS record for 88.221.198.61: a88-221-198-61.deploy.static.akamaitechnologies.com

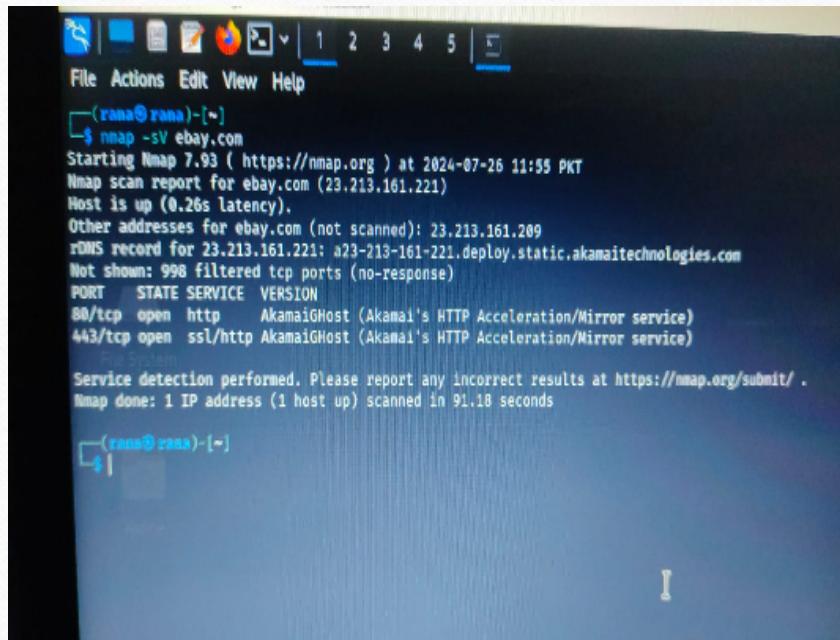
PORT      STATE    SERVICE
1/tcp     filtered  tcpmux
2/tcp     filtered  compressneg
3/tcp     filtered  compressneg
4/tcp     filtered  Unknown
5/tcp     filtered  rje
6/tcp     filtered  Unknown
7/tcp     filtered  echo
8/tcp     filtered  Unknown
9/tcp     filtered  discard
10/tcp    filtered  Unknown
11/tcp    filtered  systat
12/tcp    filtered  Unknown
13/tcp    filtered  daytime
14/tcp    filtered  Unknown
15/tcp    filtered  netstat
16/tcp    filtered  Unknown
17/tcp    filtered  qpid
18/tcp    filtered  nsp
19/tcp    filtered  chargen
20/tcp    filtered  ftp-data

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

# Service Version Detection:

---

- Tools:
- Nmap with version detection:  
nmap -sV google.com
- Banner Grabbing with Netcat:  
nc -v example.com 80



```
(rama@rama)-[~]
$ nmap -sV ebay.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-26 11:55 PKT
Nmap scan report for ebay.com (23.213.161.221)
Host is up (0.26s latency).
Other addresses for ebay.com (not scanned): 23.213.161.209
rDNS record for 23.213.161.221: a23-213-161-221.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

Nmap done: 1 IP address (1 host up) scanned in 91.18 seconds
```



Edit with WPS Office