Cyber seruity

HEF

- CHFI

Submitted By: Arbab Rauf

Submitted To: Muhammad Bila

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.

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.

EXEMPLE

```
┌──(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
```

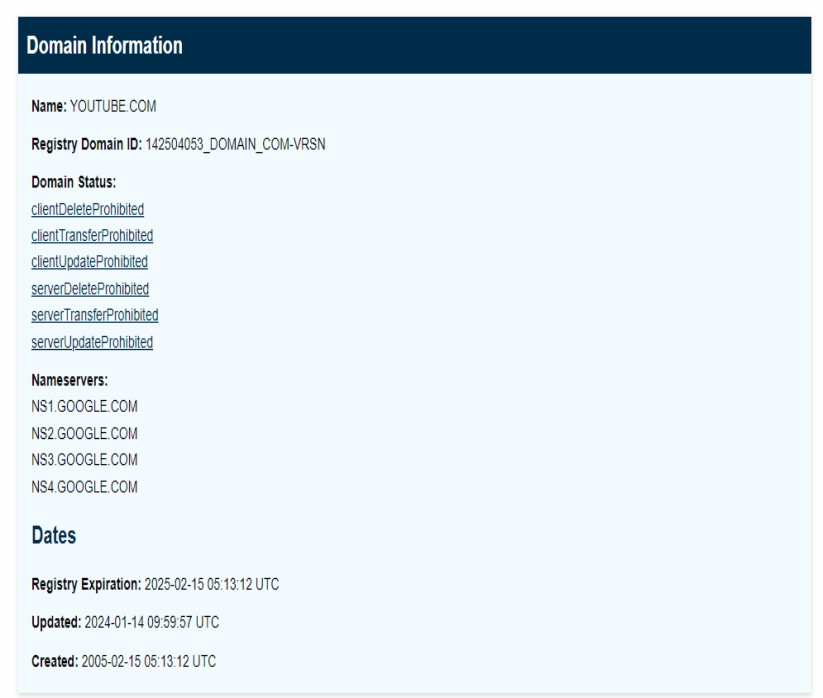
DNS Records Analysis

- 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

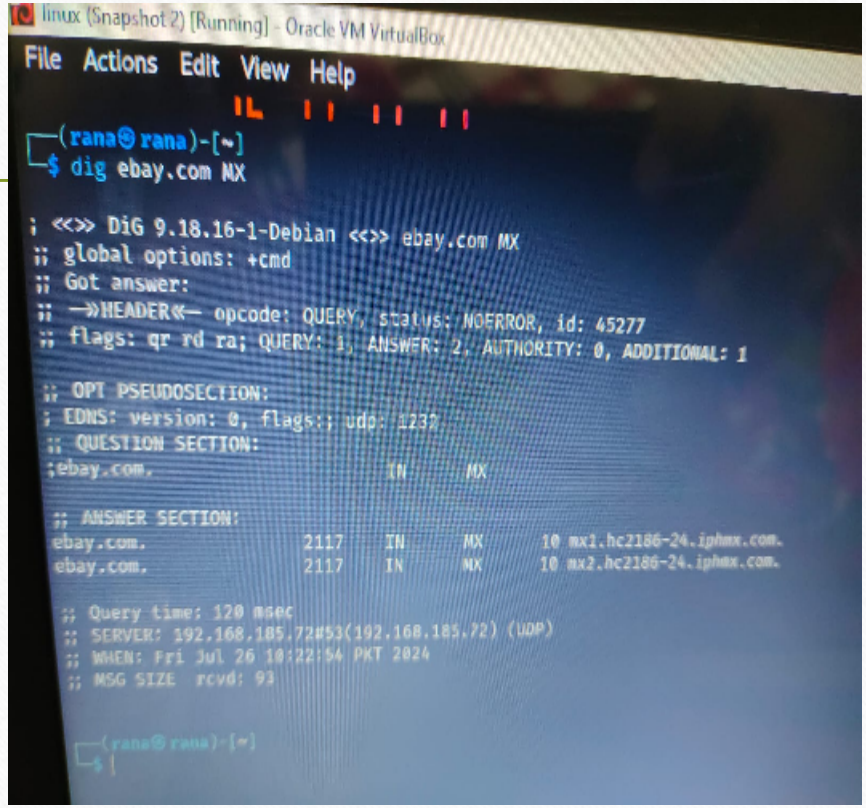
Techniques and Tools/Websites:-

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

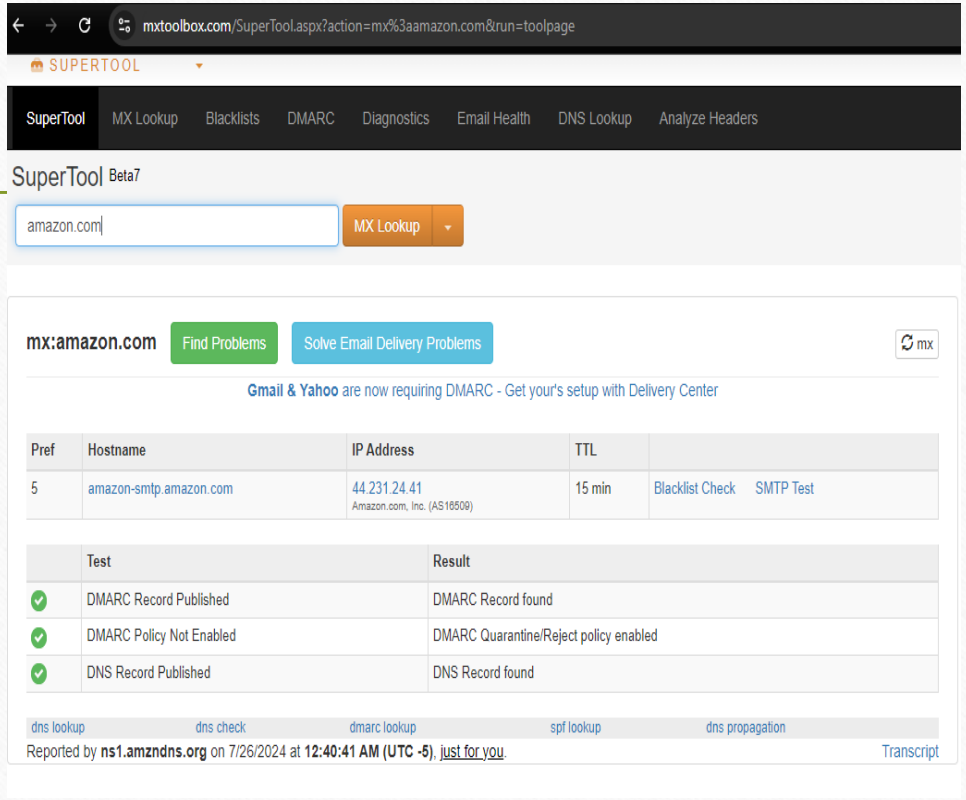


DNS Records Analysis:

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

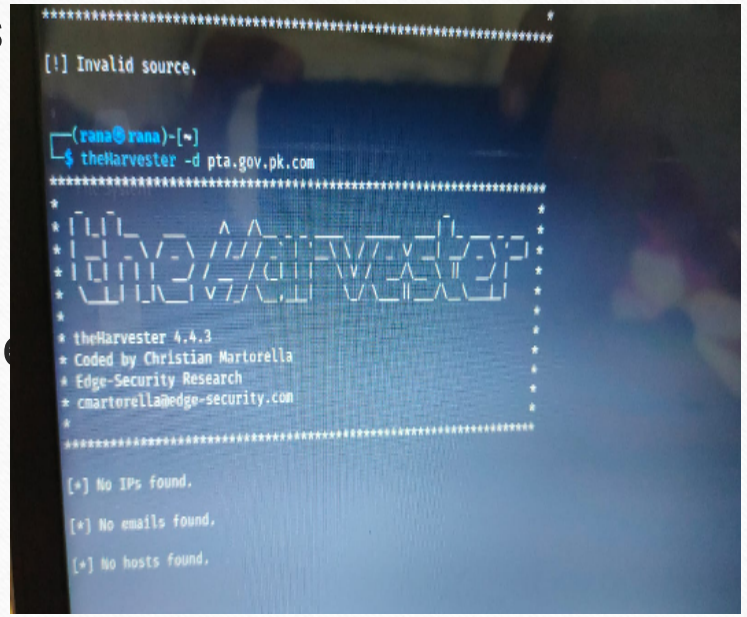


- Website:
- MXtoolbox



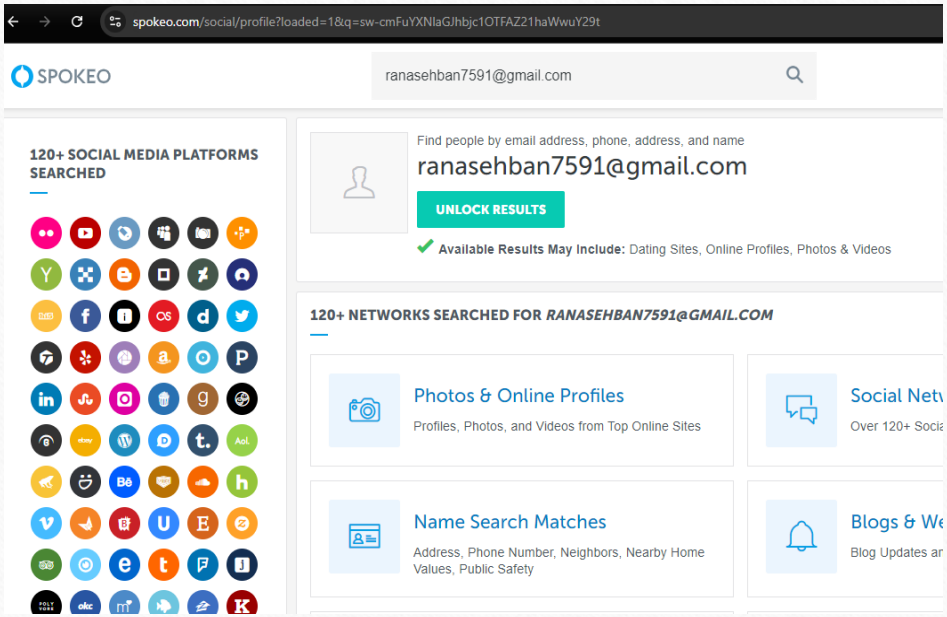
Email Address Search:

- 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



Reverse Email Lookup:-

- **Websites:**
- Pipl
- spokeo



Metadata Analysis:-

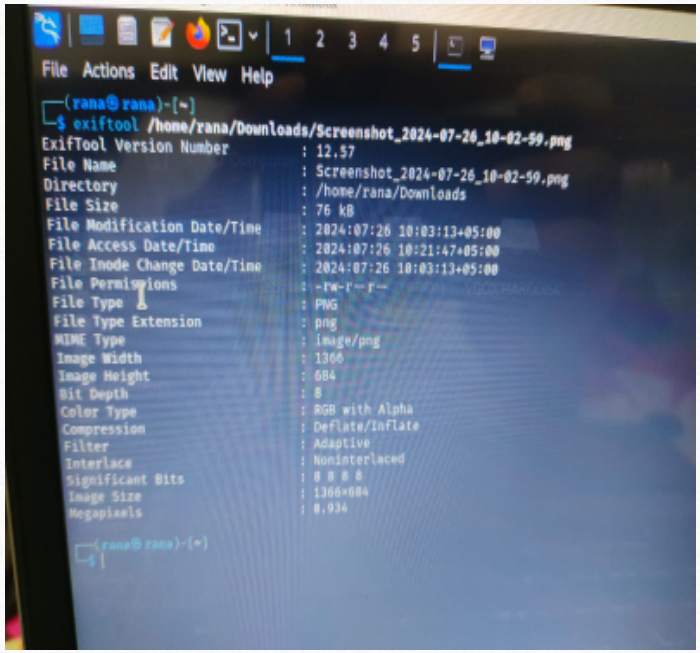
- It include information about the file creation date, author, software used, and other details that are embedded within the file.

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

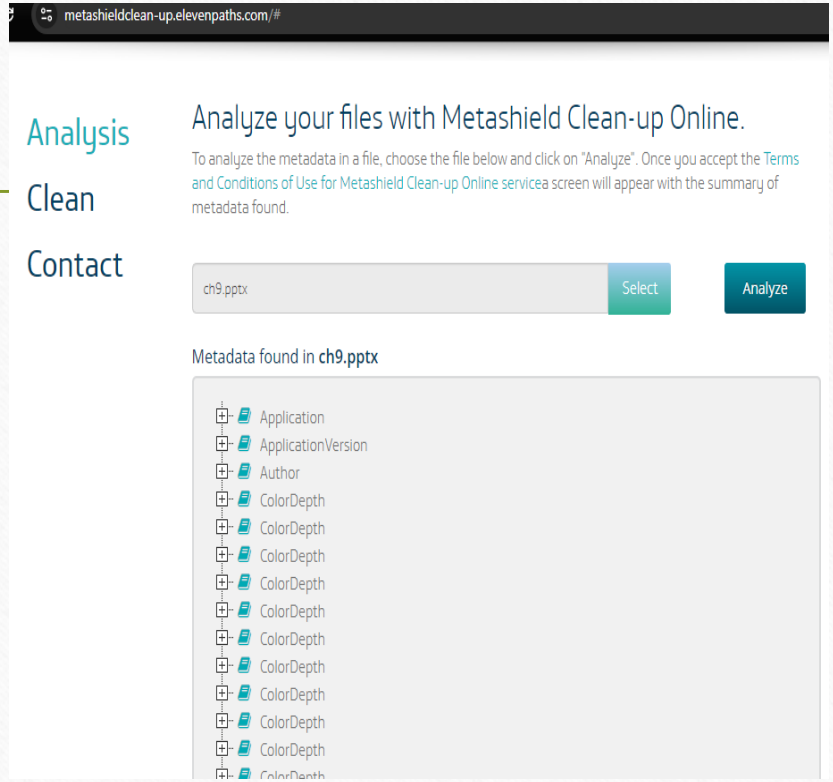
Image Metadata Analysis:

- 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



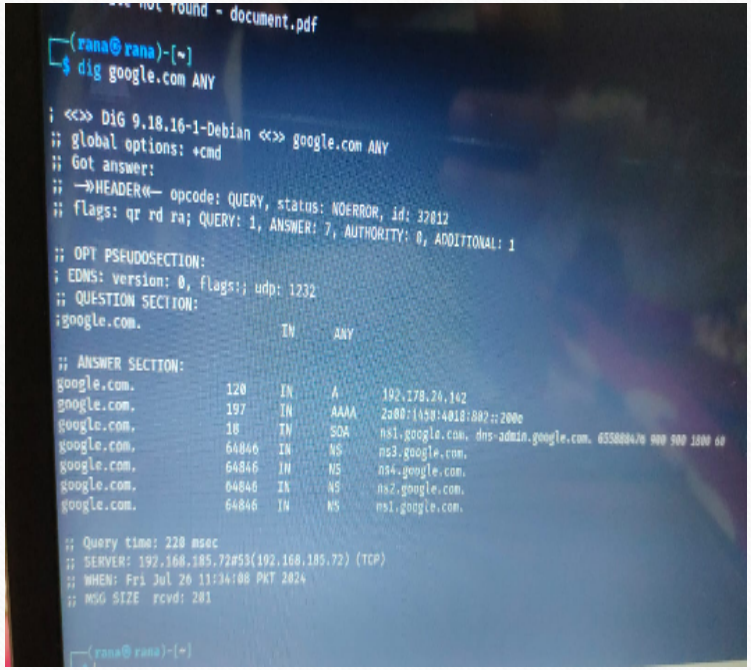
Online Metadata Analyzers:

- Metashield analyzer
- Get-MetaData



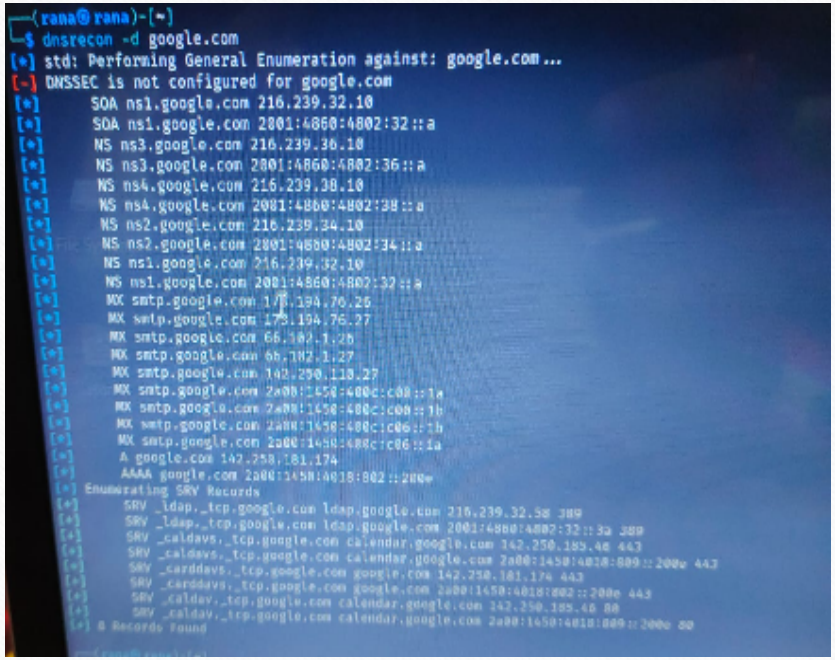
DNS Enumeration:

- 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



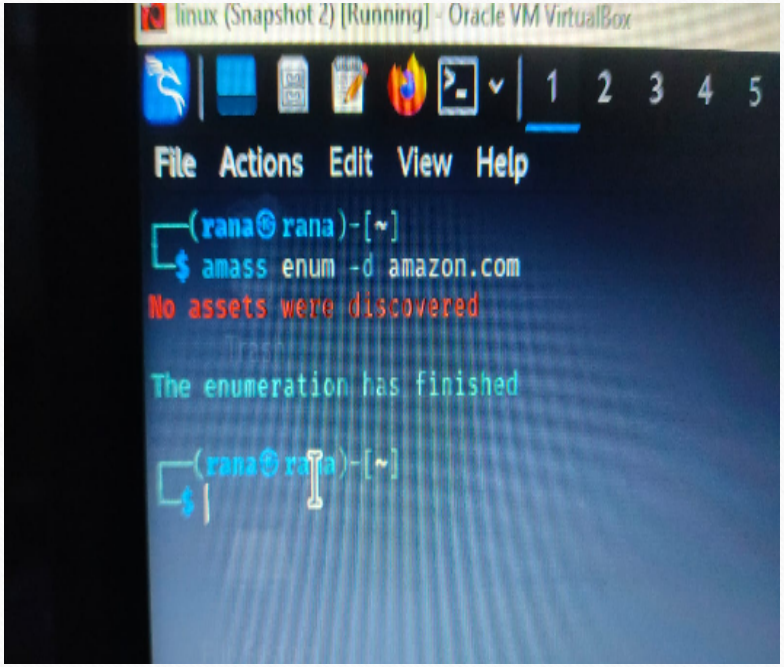
DNS Enumeration Tools:

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



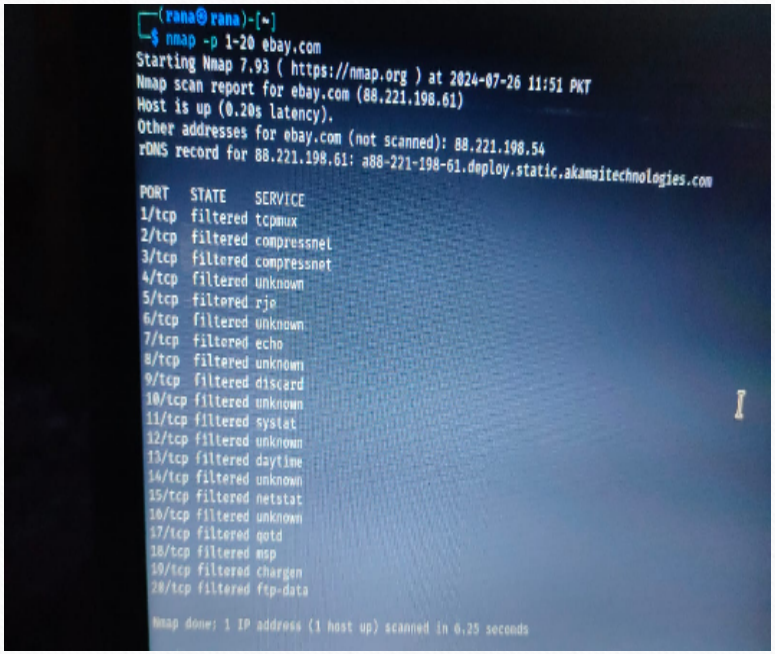
Subdomain Enumeration:

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



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



Service Version Detection:

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