Project 7

[MAN IN THE MIDDLE ATTACK}

ACMEGRADE | CYBERSECURITY | INTERSHIP PROGRAM

PROJECT 7: Man In The Middle Attack

Target: Any Windows Machine

[Windows XP Professional x64]

Tools: BetterCap and Wireshark In Kali Linux

STUDENT DETAILS:

Vedant Padsala	**padsalavedant04@gmail.com**	**9106597734**
Neerja Binu Vimalan	**neerjabinuvimalan@gmail.com**	**8590148231**
Subhajyoti Santra	**subhasantra555@gmail.com**	**9330168528**
Pavan Mahesh Patil	**pavanpatil23780@gmail.com**	**7776012881**
Rishab Raj	**rishabrajkmr4567@gmail.com**	**8092860626**

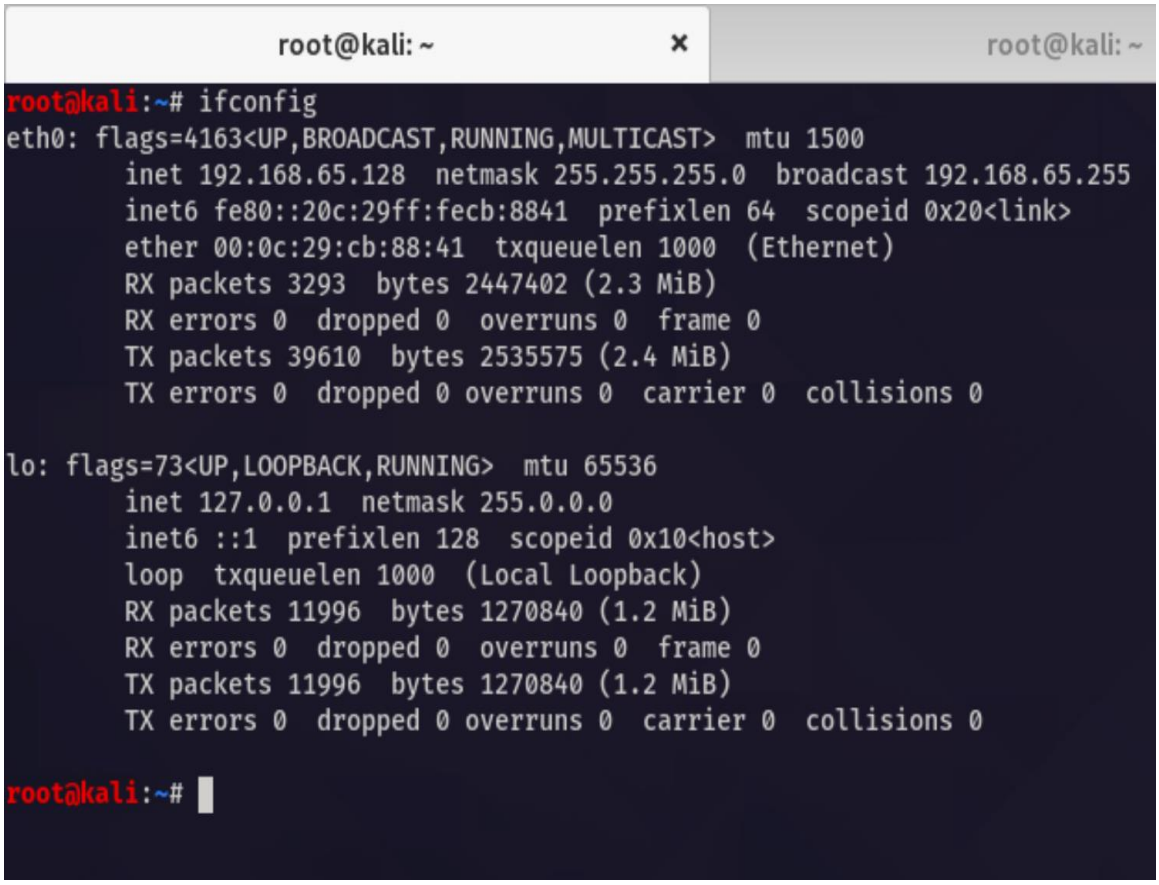
Bettercap Modules:

1. **HTTP Proxy Module**: This module enables you to perform various types of HTTP-related attacks. It allows you to intercept and manipulate HTTP traffic, which is especially useful for testing the security of web applications.
2. **DNS Spoofing Module**: This module enables DNS spoofing attacks, allowing you to redirect network traffic by spoofing DNS responses. This can be used to redirect users to malicious websites or intercept communication.
3. **SSLStrip Module**: SSLStrip is a module that can be used to bypass HTTPS security by downgrading secure connections to unencrypted HTTP connections, making it easier to intercept and manipulate the traffic.
4. **ARP Spoofing Module**: Address Resolution Protocol (ARP) spoofing is a technique used to intercept network traffic by associating the attacker's MAC address with a legitimate IP address on the network.
5. **WiFi Sniffer Module**: This module allows Bettercap to capture and analyze Wi-Fi traffic, including credentials and sensitive data exchanged over unsecured networks.
6. **Capture Module**: The capture module is used for packet capture and analysis. It can be used to intercept network traffic and analyze the packets for vulnerabilities or sensitive information.
7. **Proxy Authentication Module**: This module provides the capability to authenticate proxy connections, enhancing the security and control over the intercepted traffic.
8. **Proxy Authentication Capture Module**: Similar to the previous module, this one captures proxy authentication credentials and can be used to assess the security of proxy authentication mechanisms.

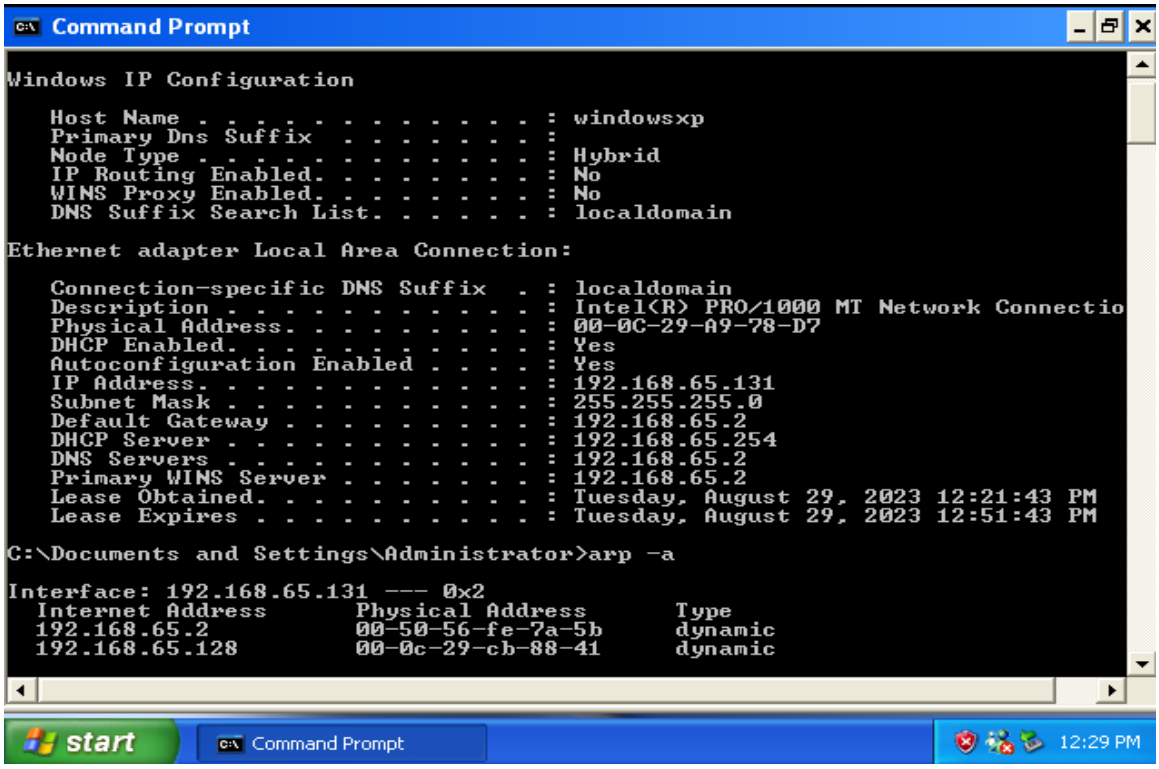
MAN IN THE MIDDLE ATTACK PROCEDURE AND STEPS:-

[1]. IP ADDRESS AND MACADDRESS:

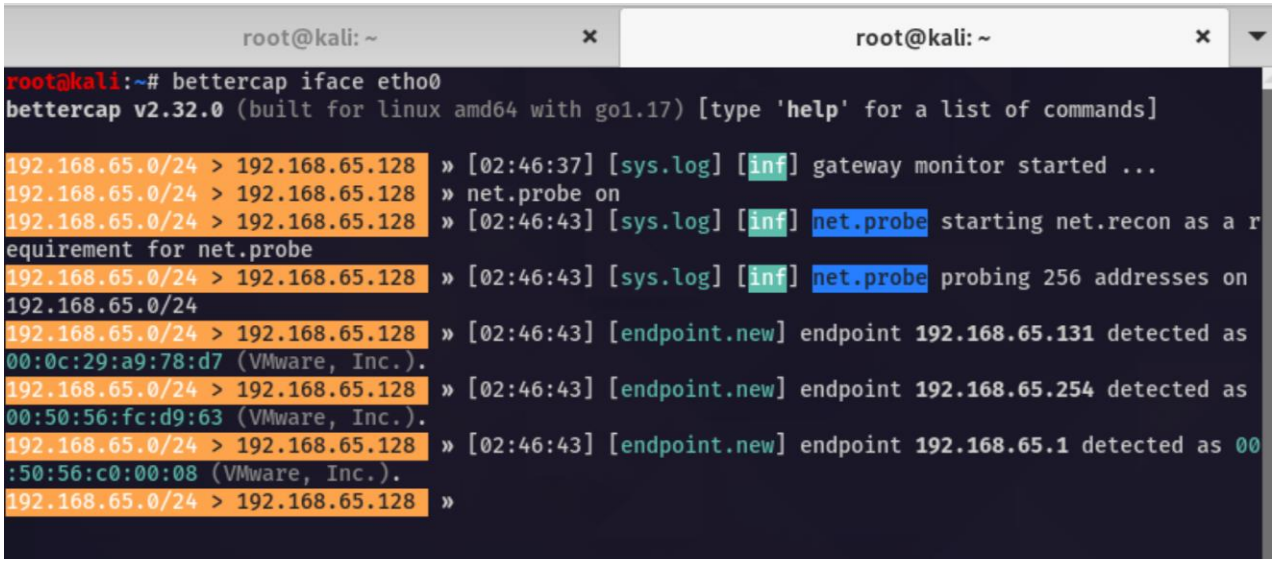
Zombie Machine(kali linux):-



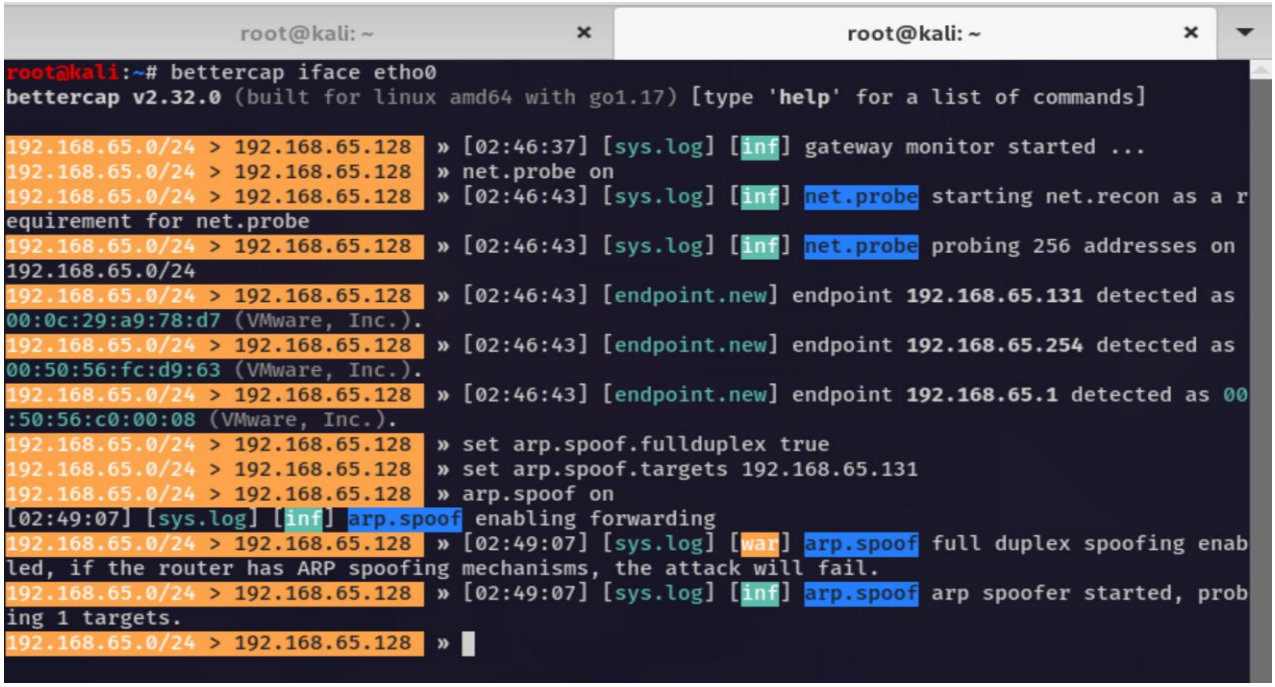
Target Machine(WindowsXP):-



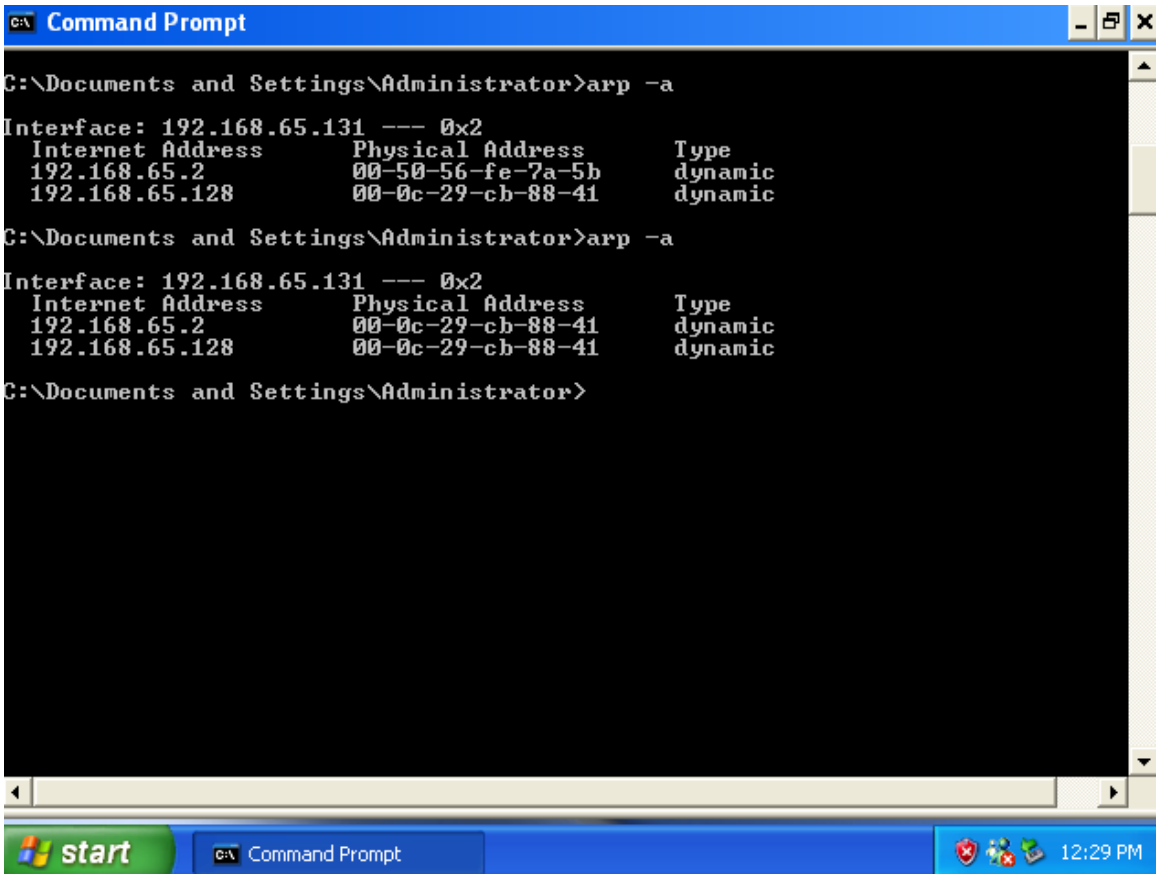
[2]. Initialising Bettercap tool with EthO and searching devices with net.probe module :-



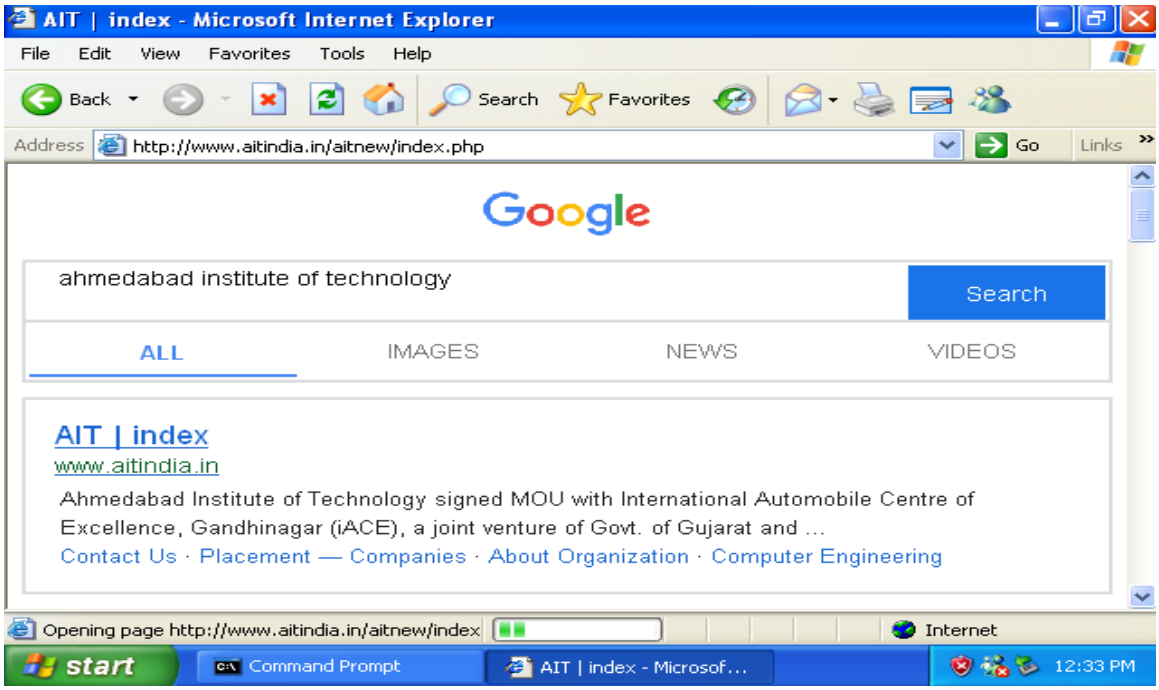
[3]. Using arp.spoof module, enabling fullduplex mode and setting target as WindowsXP :-

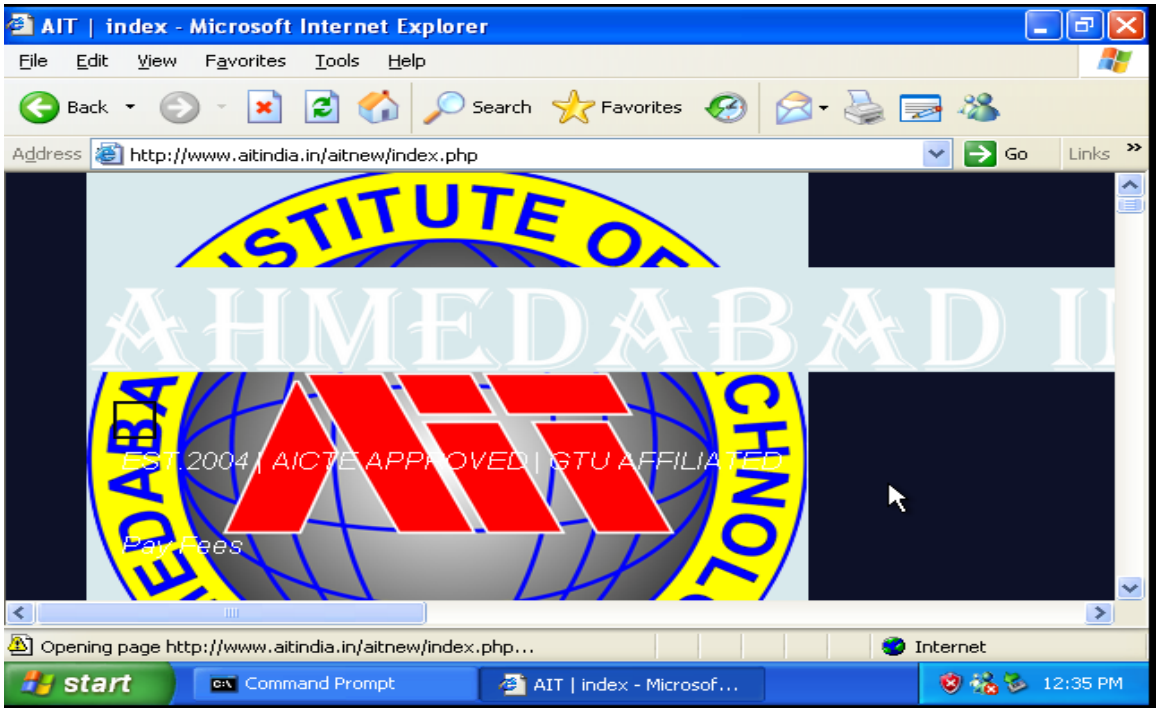


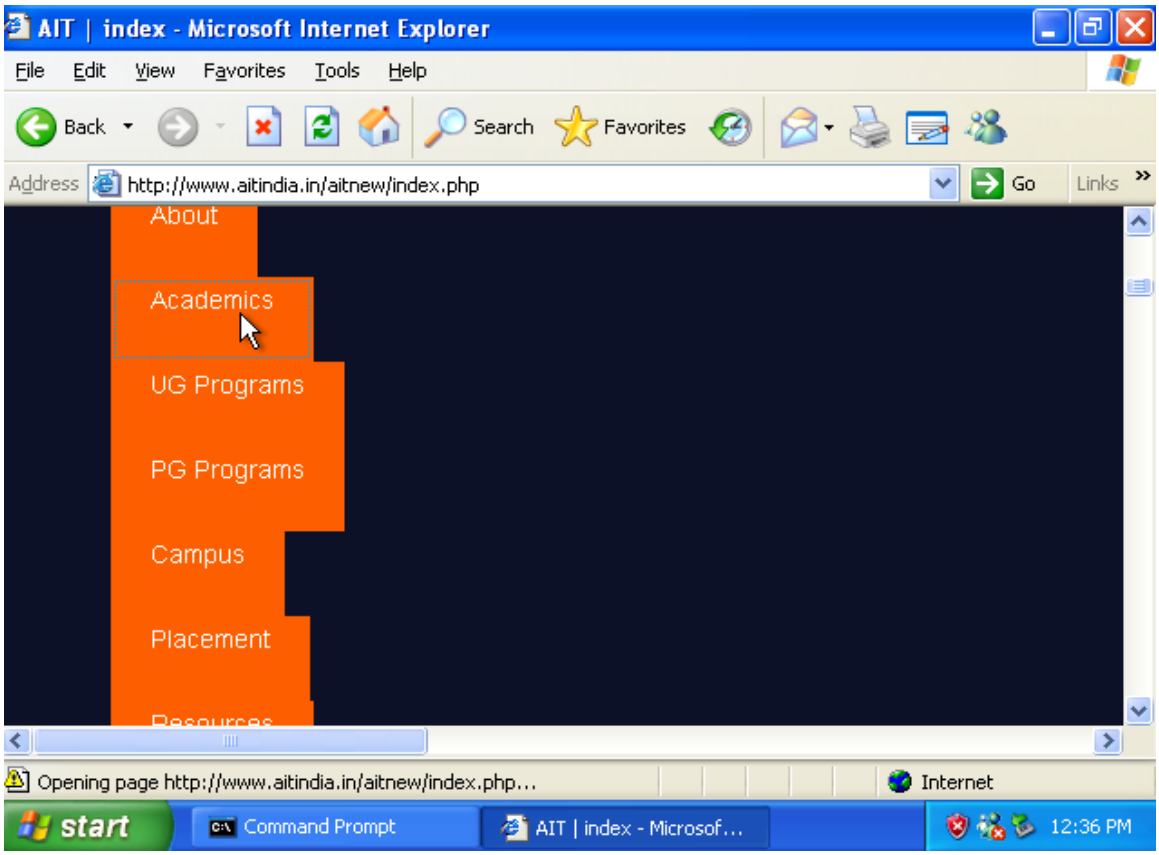
[4]. Verifying MacAddress of target:-

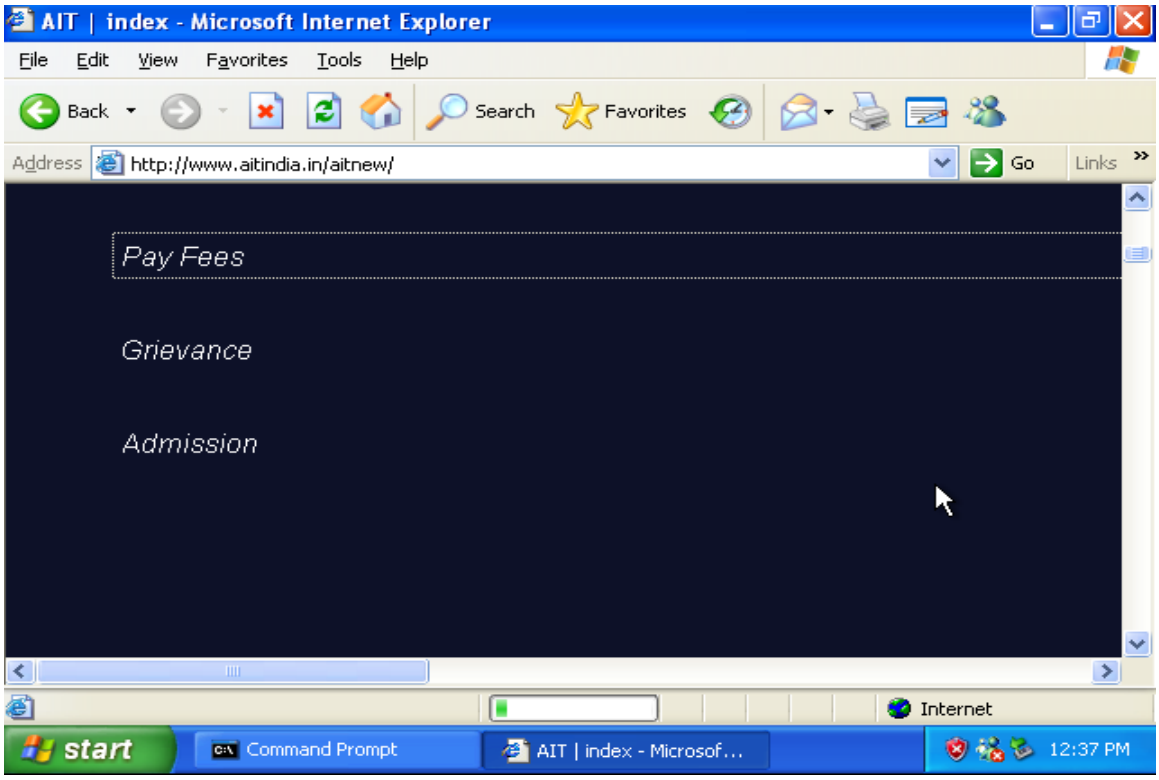


[5].Windows Activities :-

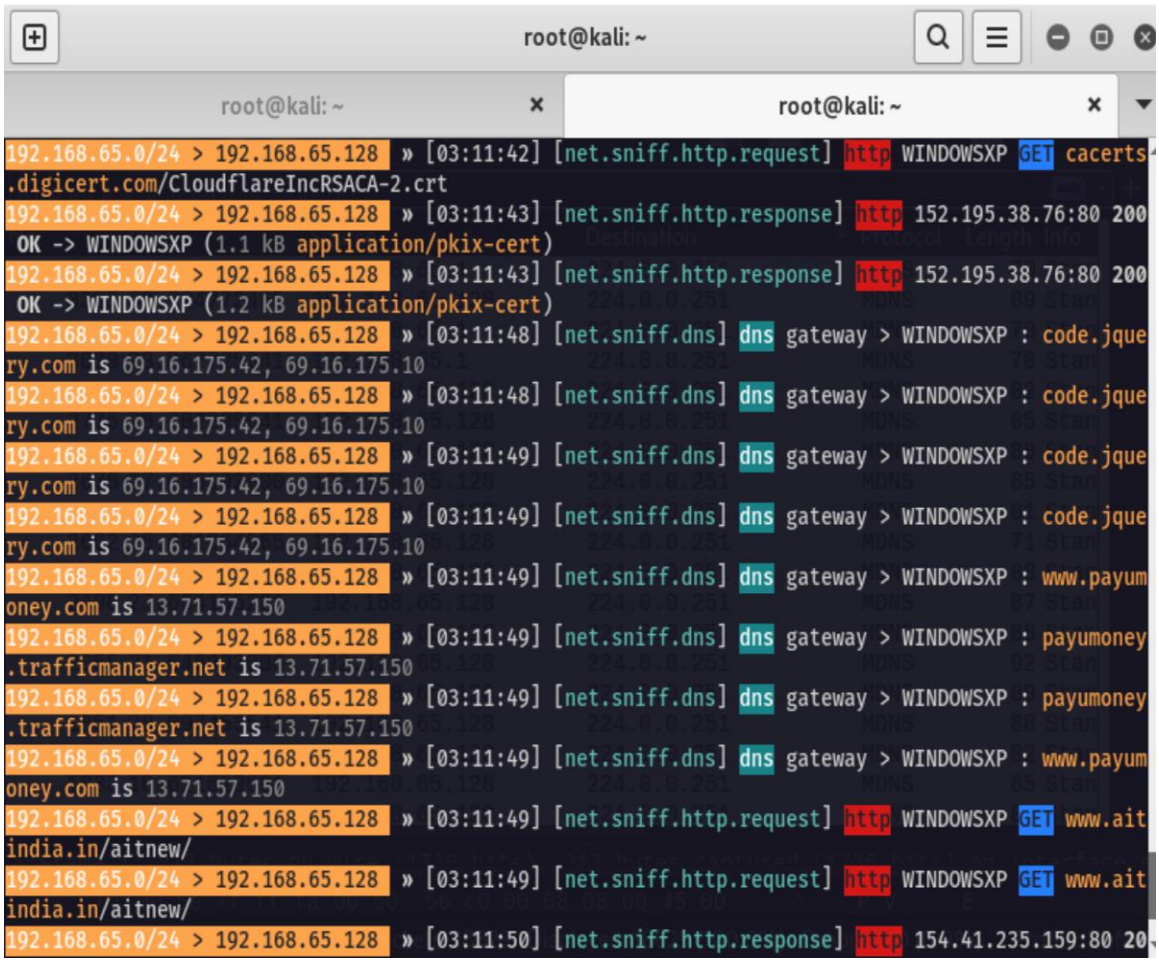


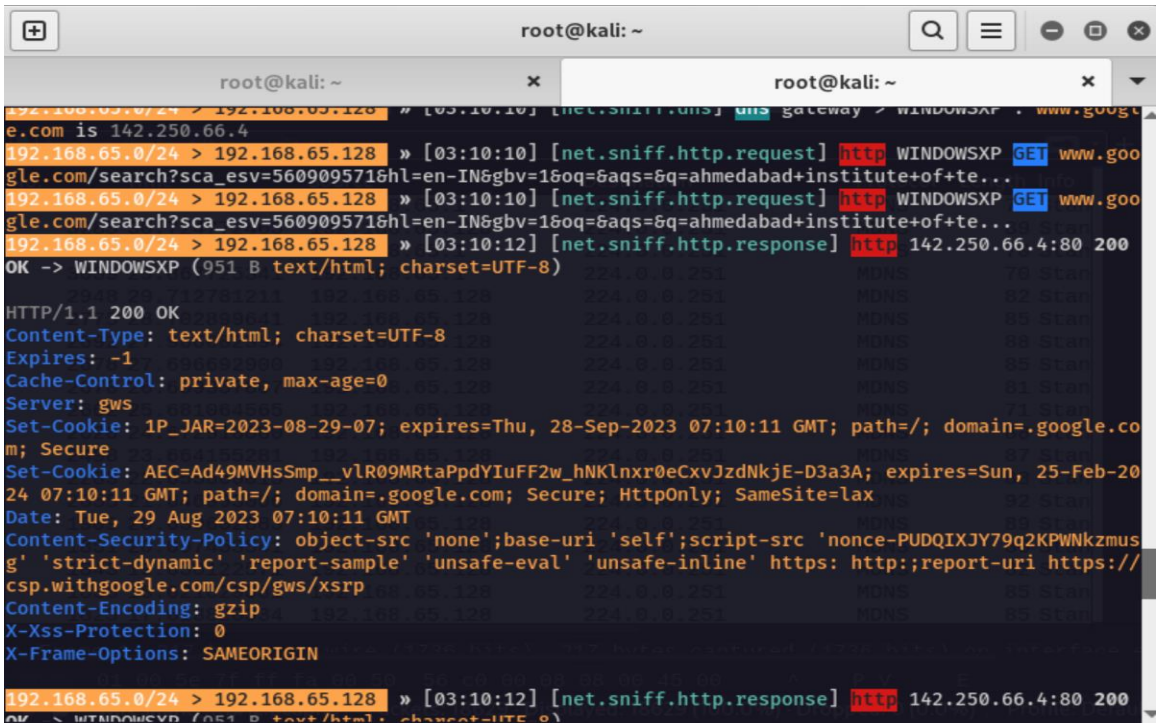


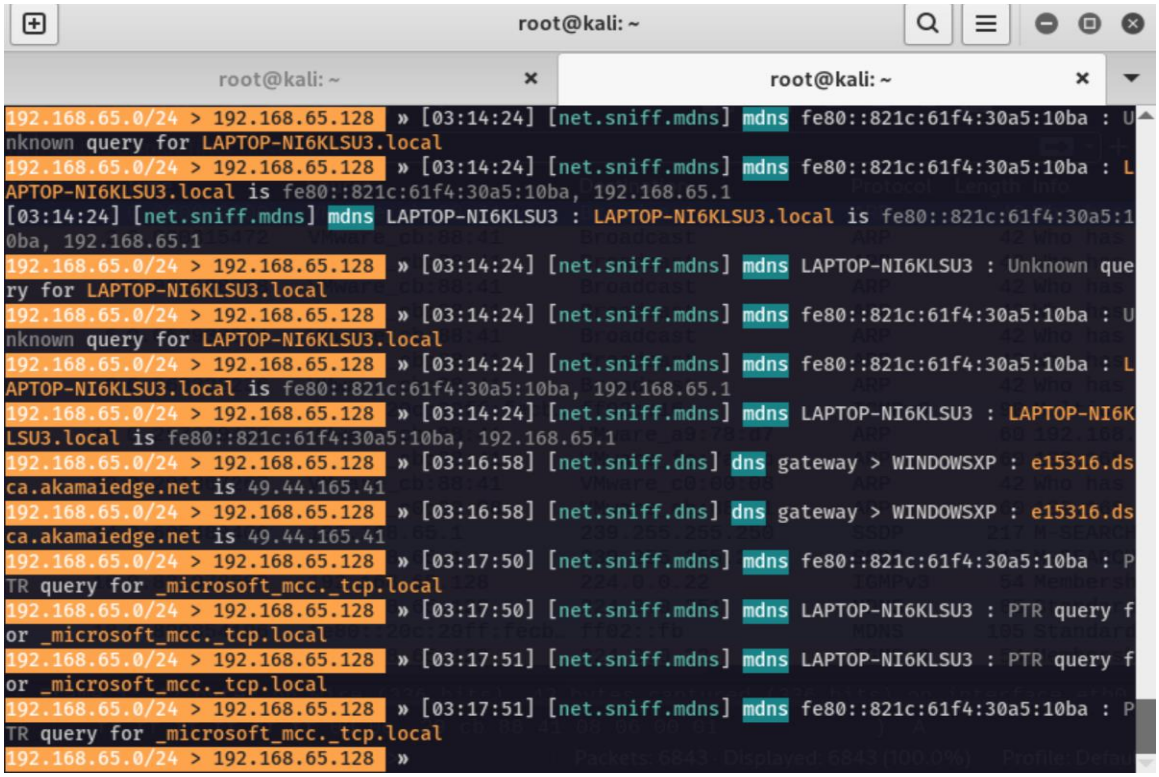

AIT | index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.aitindia.in/aitnew/index.php
Go Links
About
Academics
UG Programs
PG Programs
Campus
Placement
Opening page http://www.aitindia.in/aitnew/index.php...
Internet
start
Command Prompt
AIT | index - Microsof...
12:36 PM


AIT | index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.aitindia.in/aitnew/
Go Links
Pay Fees
Grievance
Admission
Internet
start
Command Prompt
AIT | index - Microsof...
12:37 PM

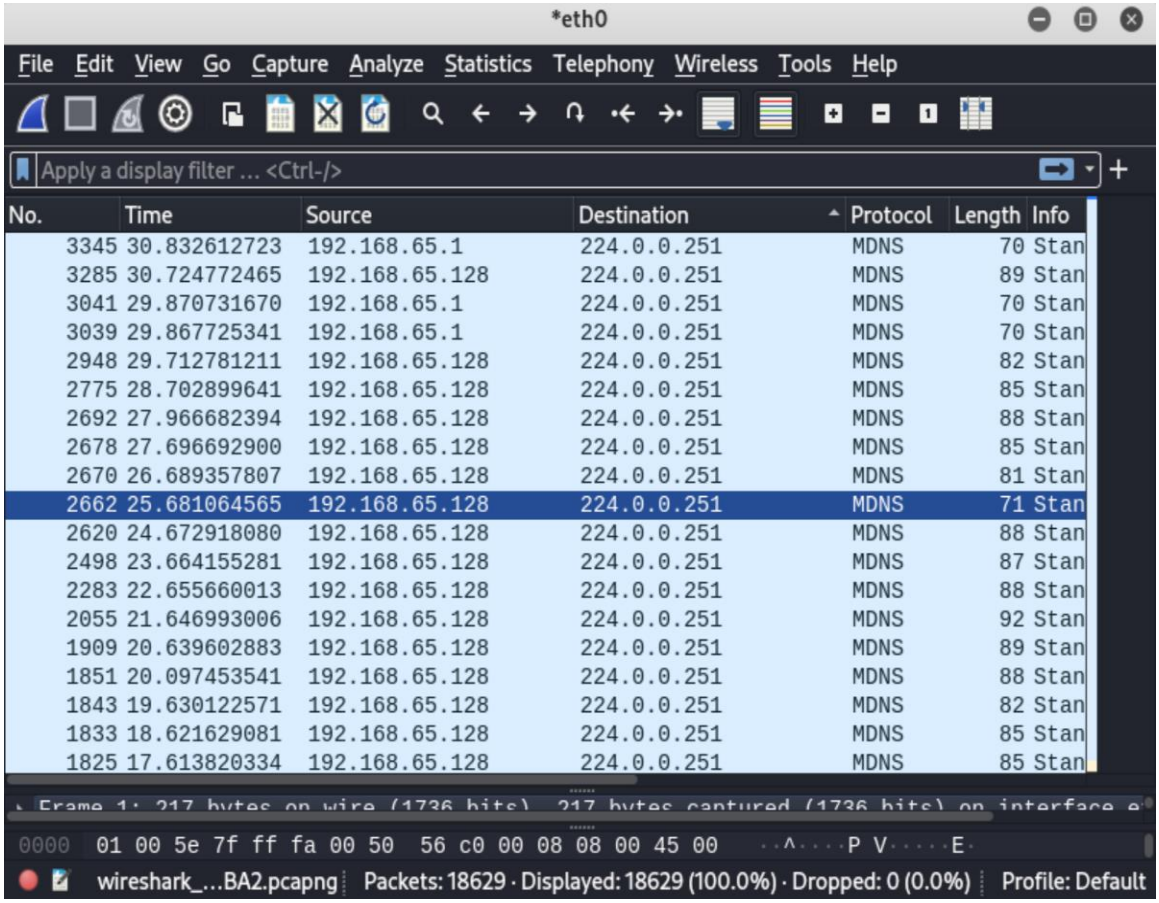
Sniffing through net.sniff module:-

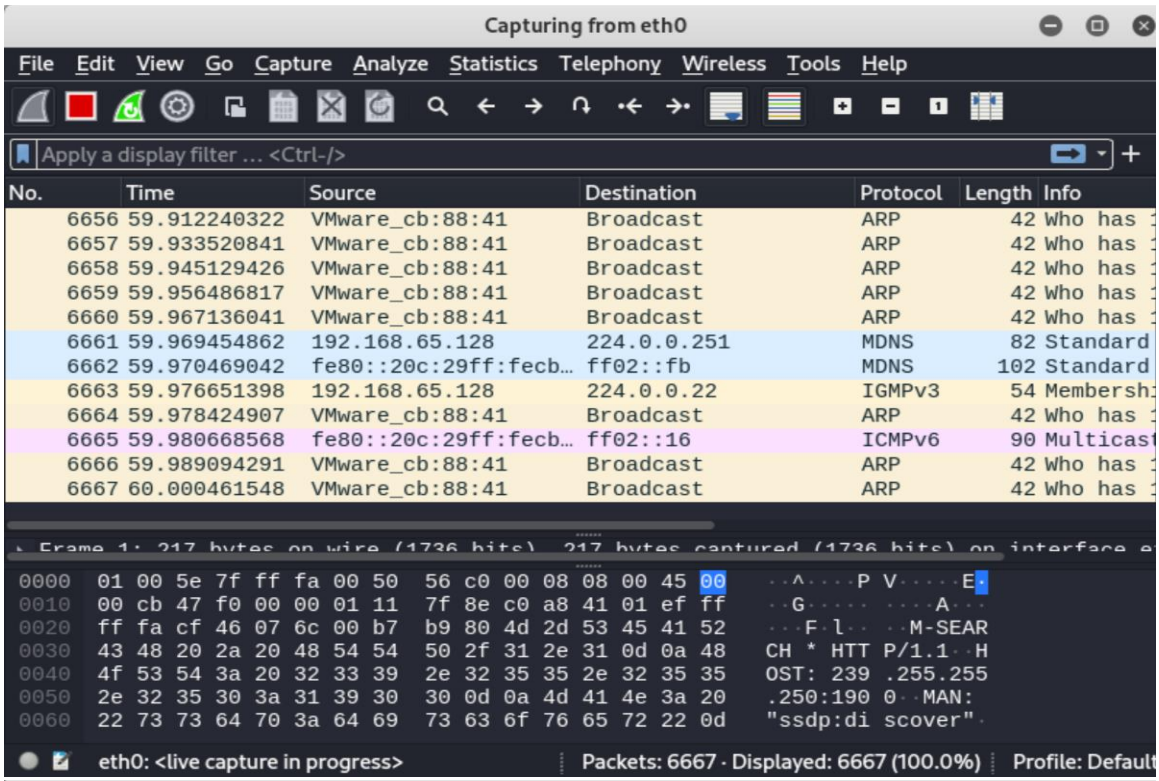


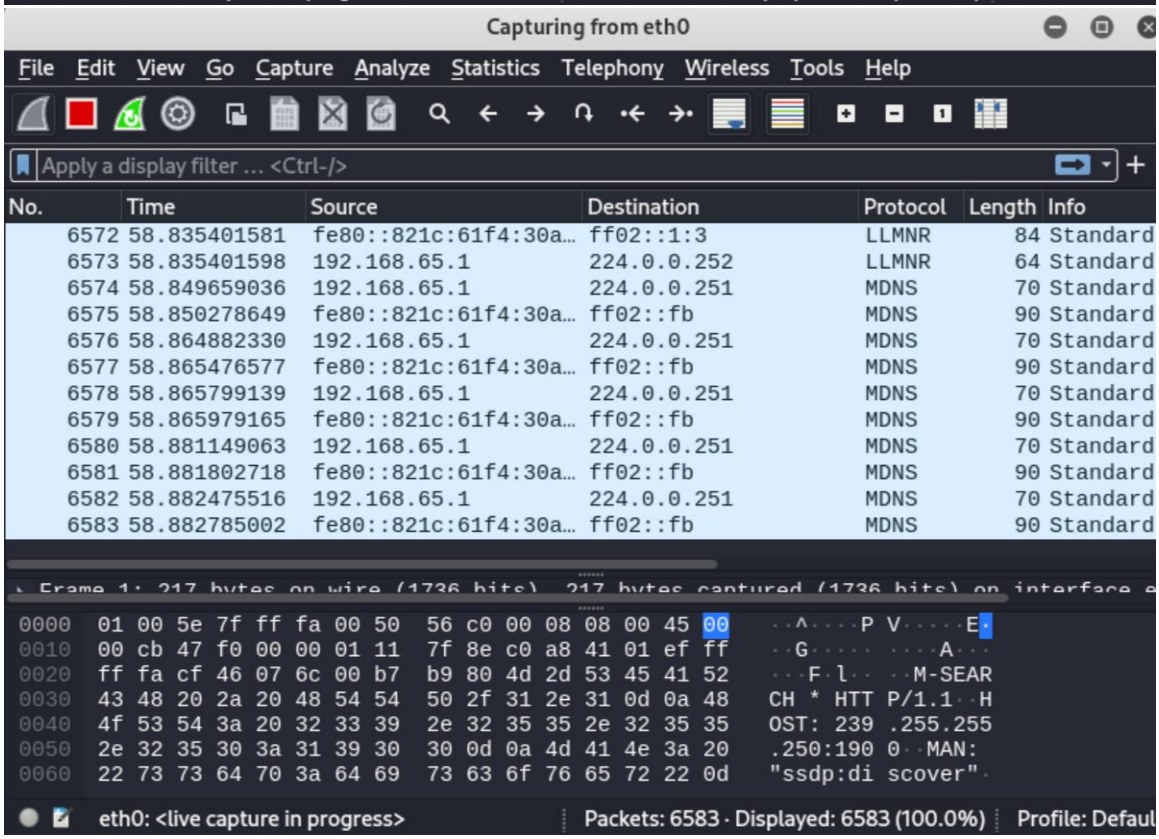

root@kali: ~
root@kali: ~
root@kali: ~
e.com is 142.250.66.4
192.168.65.0/24 > 192.168.65.128 » [03:10:10] [net.sniff.http.request] http WINDOWSXP GET www.goo
gle.com/search?sca_esv=560909571&hl=en-IN&gbv=1&oq=&aqs=&q=ahmedabad+institute+of+te...
192.168.65.0/24 > 192.168.65.128 » [03:10:10] [net.sniff.http.request] http WINDOWSXP GET www.goo
gle.com/search?sca_esv=560909571&hl=en-IN&gbv=1&oq=&aqs=&q=ahmedabad+institute+of+te...
192.168.65.0/24 > 192.168.65.128 » [03:10:12] [net.sniff.http.response] http 142.250.66.4:80 200
OK -> WINDOWSXP (951 B text/html; charset=UTF-8)
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Expires: -1
Cache-Control: private, max-age=0
Server: gws
Set-Cookie: 1P_JAR=2023-08-29-07; expires=Thu, 28-Sep-2023 07:10:11 GMT; path=/; domain=.google.co
m; Secure
Set-Cookie: AEC=Ad49MVHsSmp__vlR09MRtaPpdYIuFF2w_hNKlnxr0eCxvJzdNkjE-D3a3A; expires=Sun, 25-Feb-20
24 07:10:11 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Date: Tue, 29 Aug 2023 07:10:11 GMT
Content-Security-Policy: object-src 'none';base-uri 'self';script-src 'nonce-PUDQIXJY79q2KPWNkzmus
g' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://
csp.withgoogle.com/csp/gws/xsrp
Content-Encoding: gzip
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
192.168.65.0/24 > 192.168.65.128 » [03:10:12] [net.sniff.http.response] http 142.250.66.4:80 200

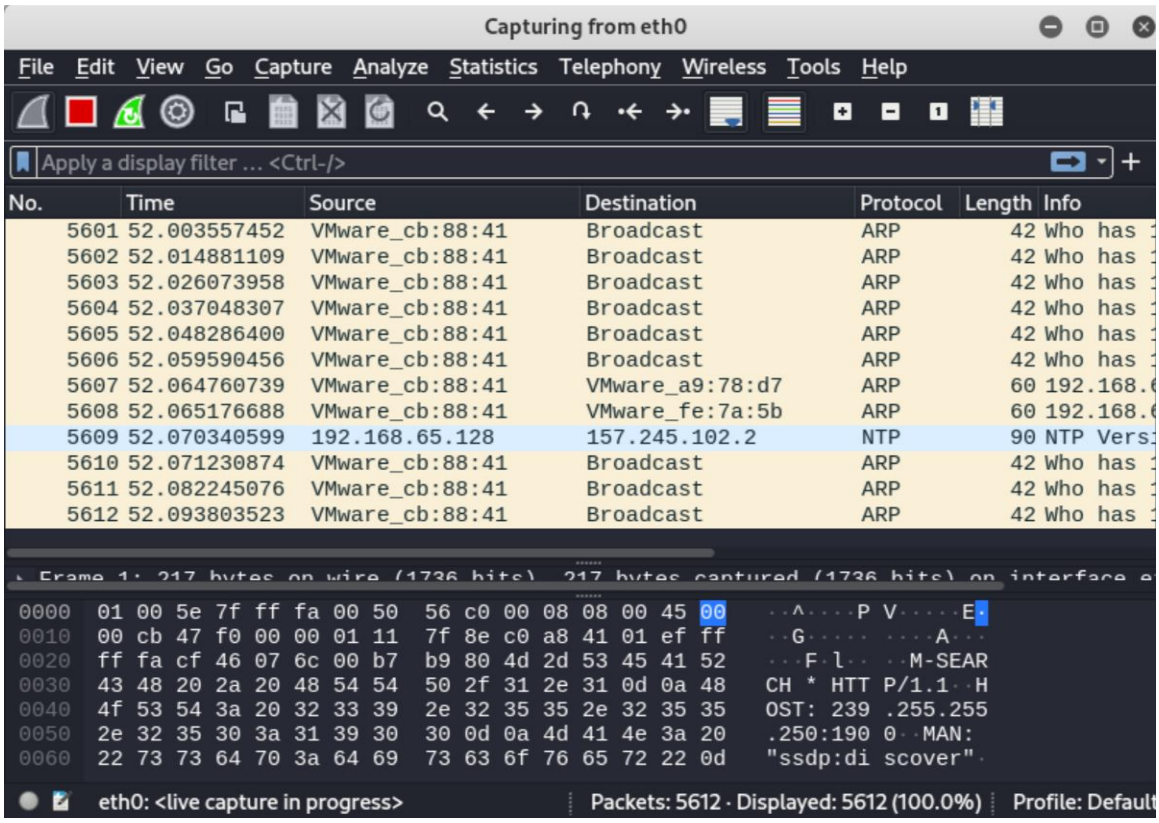

root@kali: ~
root@kali: ~
root@kali: ~
192.168.65.0/24 > 192.168.65.128 » [03:14:24] [net.sniff.mdns] mdns fe80::821c:61f4:30a5:10ba : U
nknown query for LAPTOP-NI6KLSU3.local
192.168.65.0/24 > 192.168.65.128 » [03:14:24] [net.sniff.mdns] mdns fe80::821c:61f4:30a5:10ba : L
APTOP-NI6KLSU3.local is fe80::821c:61f4:30a5:10ba, 192.168.65.1
[03:14:24] [net.sniff.mdns] mdns LAPTOP-NI6KLSU3 : LAPTOP-NI6KLSU3.local is fe80::821c:61f4:30a5:1
0ba, 192.168.65.1
192.168.65.0/24 > 192.168.65.128 » [03:14:24] [net.sniff.mdns] mdns LAPTOP-NI6KLSU3 : Unknown que
ry for LAPTOP-NI6KLSU3.local
192.168.65.0/24 > 192.168.65.128 » [03:14:24] [net.sniff.mdns] mdns fe80::821c:61f4:30a5:10ba : U
nknown query for LAPTOP-NI6KLSU3.local
192.168.65.0/24 > 192.168.65.128 » [03:14:24] [net.sniff.mdns] mdns fe80::821c:61f4:30a5:10ba : L
APTOP-NI6KLSU3.local is fe80::821c:61f4:30a5:10ba, 192.168.65.1
192.168.65.0/24 > 192.168.65.128 » [03:14:24] [net.sniff.mdns] mdns LAPTOP-NI6KLSU3 : LAPTOP-NI6K
LSU3.local is fe80::821c:61f4:30a5:10ba, 192.168.65.1
192.168.65.0/24 > 192.168.65.128 » [03:16:58] [net.sniff.dns] dns gateway > WINDOWSXP : e15316.ds
ca.akamaiedge.net is 49.44.165.41
192.168.65.0/24 > 192.168.65.128 » [03:16:58] [net.sniff.dns] dns gateway > WINDOWSXP : e15316.ds
ca.akamaiedge.net is 49.44.165.41
192.168.65.0/24 > 192.168.65.128 » [03:17:50] [net.sniff.mdns] mdns fe80::821c:61f4:30a5:10ba : P
TR query for _microsoft_mcc._tcp.local
192.168.65.0/24 > 192.168.65.128 » [03:17:50] [net.sniff.mdns] mdns LAPTOP-NI6KLSU3 : PTR query f
or _microsoft_mcc._tcp.local
192.168.65.0/24 > 192.168.65.128 » [03:17:51] [net.sniff.mdns] mdns LAPTOP-NI6KLSU3 : PTR query f
or _microsoft_mcc._tcp.local
192.168.65.0/24 > 192.168.65.128 » [03:17:51] [net.sniff.mdns] mdns fe80::821c:61f4:30a5:10ba : P
TR query for _microsoft_mcc._tcp.local
192.168.65.0/24 > 192.168.65.128 »

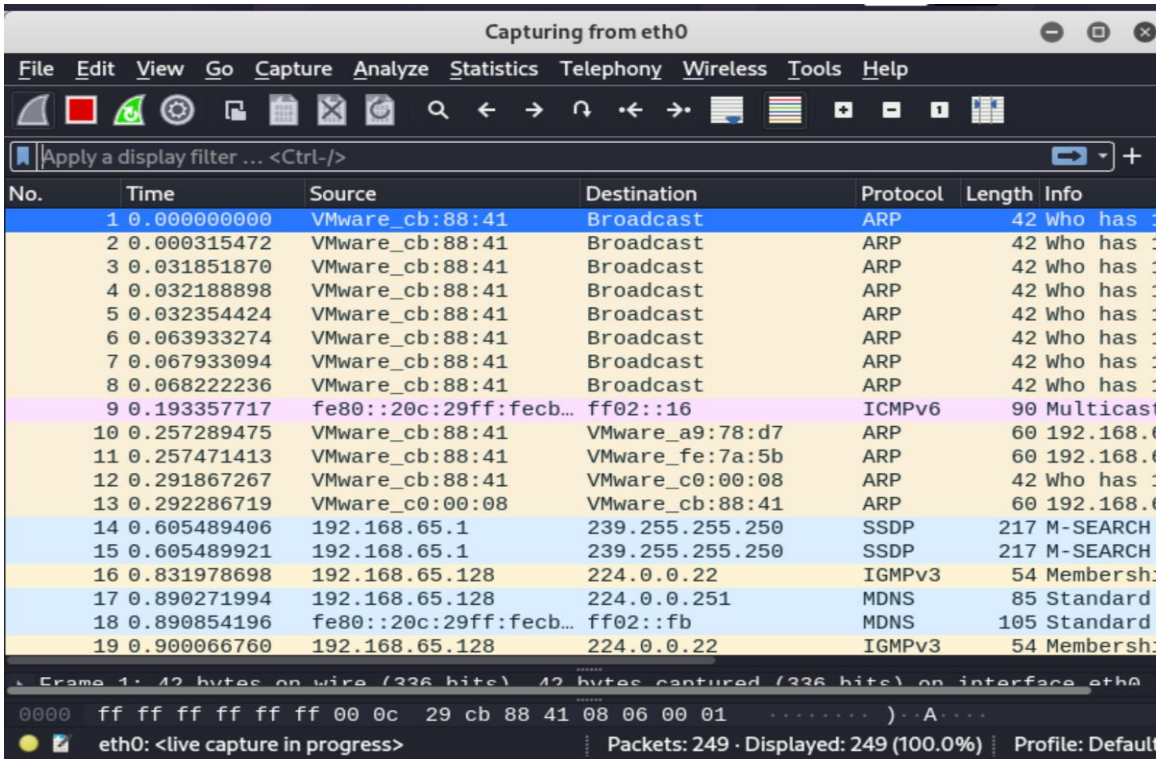
Sniffing thorugh WireShark tool:-



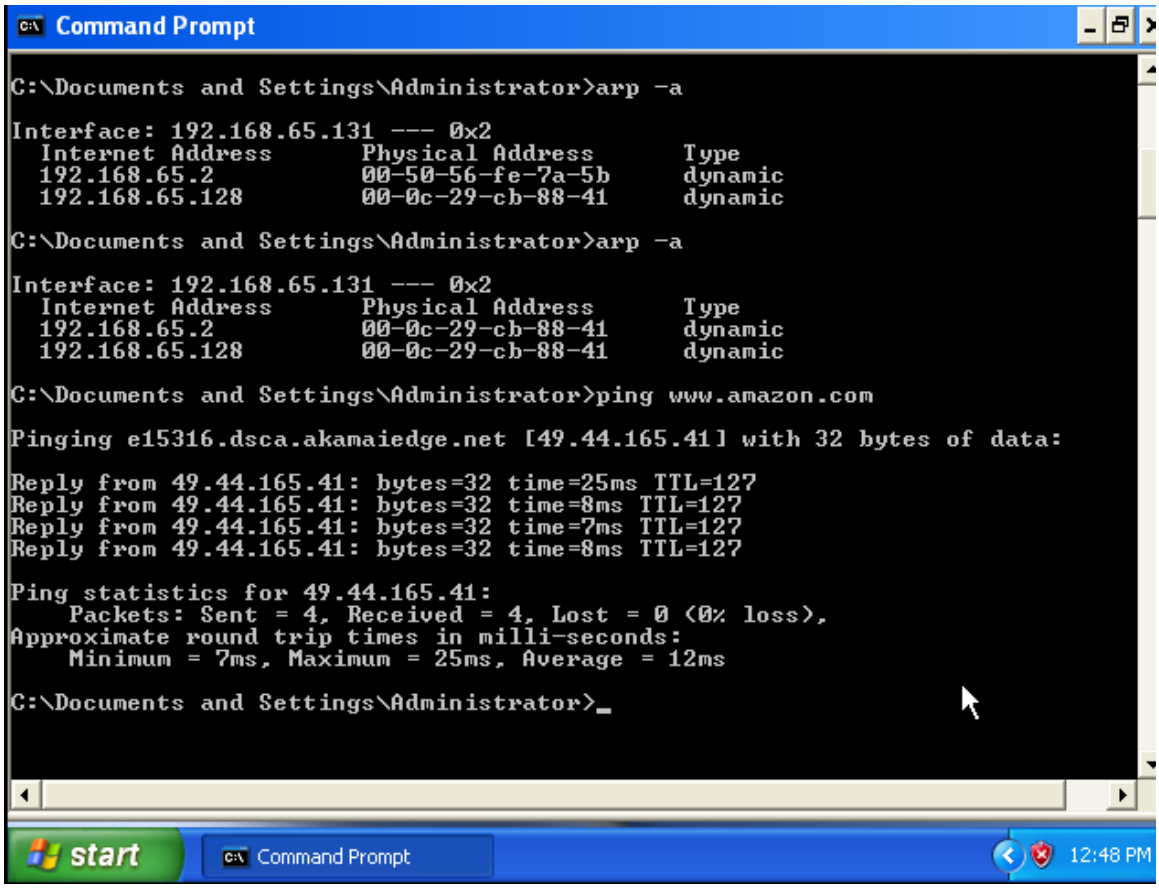

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
6656 59.912240322 VMware_cb:88:41 Broadcast ARP 42 Who has
6657 59.933520841 VMware_cb:88:41 Broadcast ARP 42 Who has
6658 59.945129426 VMware_cb:88:41 Broadcast ARP 42 Who has
6659 59.956486817 VMware_cb:88:41 Broadcast ARP 42 Who has
6660 59.967136041 VMware_cb:88:41 Broadcast ARP 42 Who has
6661 59.969454862 192.168.65.128 224.0.0.251 MDNS 82 Standard
6662 59.970469042 fe80::20c:29ff:fecb... ff02::fb MDNS 102 Standard
6663 59.976651398 192.168.65.128 224.0.0.22 IGMPv3 54 Membershi
6664 59.978424907 VMware_cb:88:41 Broadcast ARP 42 Who has
6665 59.980668568 fe80::20c:29ff:fecb... ff02::16 ICMPv6 90 Multicast
6666 59.989094291 VMware_cb:88:41 Broadcast ARP 42 Who has
6667 60.000461548 VMware_cb:88:41 Broadcast ARP 42 Who has
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00
0010 00 cb 47 f0 00 00 01 11 7f 8e c0 a8 41 01 ef ff
0020 ff fa cf 46 07 6c 00 b7 b9 80 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d
eth0: <live capture in progress>
Packets: 6667 · Displayed: 6667 (100.0%)
Profile: Default


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
6572 58.835401581 fe80::821c:61f4:30a... ff02::1:3 LLMNR 84 Standard
6573 58.835401598 192.168.65.1 224.0.0.252 LLMNR 64 Standard
6574 58.849659036 192.168.65.1 224.0.0.251 MDNS 70 Standard
6575 58.850278649 fe80::821c:61f4:30a... ff02::fb MDNS 90 Standard
6576 58.864882330 192.168.65.1 224.0.0.251 MDNS 70 Standard
6577 58.865476577 fe80::821c:61f4:30a... ff02::fb MDNS 90 Standard
6578 58.865799139 192.168.65.1 224.0.0.251 MDNS 70 Standard
6579 58.865979165 fe80::821c:61f4:30a... ff02::fb MDNS 90 Standard
6580 58.881149063 192.168.65.1 224.0.0.251 MDNS 70 Standard
6581 58.881802718 fe80::821c:61f4:30a... ff02::fb MDNS 90 Standard
6582 58.882475516 192.168.65.1 224.0.0.251 MDNS 70 Standard
6583 58.882785002 fe80::821c:61f4:30a... ff02::fb MDNS 90 Standard
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00
0010 00 cb 47 f0 00 00 01 11 7f 8e c0 a8 41 01 ef ff
0020 ff fa cf 46 07 6c 00 b7 b9 80 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d
eth0: <live capture in progress>
Packets: 6583 · Displayed: 6583 (100.0%)
Profile: Default


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5601 52.003557452 VMware_cb:88:41 Broadcast ARP 42 Who has
5602 52.014881109 VMware_cb:88:41 Broadcast ARP 42 Who has
5603 52.026073958 VMware_cb:88:41 Broadcast ARP 42 Who has
5604 52.037048307 VMware_cb:88:41 Broadcast ARP 42 Who has
5605 52.048286400 VMware_cb:88:41 Broadcast ARP 42 Who has
5606 52.059590456 VMware_cb:88:41 Broadcast ARP 42 Who has
5607 52.064760739 VMware_cb:88:41 VMware_a9:78:d7 ARP 60 192.168.
5608 52.065176688 VMware_cb:88:41 VMware_fe:7a:5b ARP 60 192.168.
5609 52.070340599 192.168.65.128 157.245.102.2 NTP 90 NTP Versi
5610 52.071230874 VMware_cb:88:41 Broadcast ARP 42 Who has
5611 52.082245076 VMware_cb:88:41 Broadcast ARP 42 Who has
5612 52.093803523 VMware_cb:88:41 Broadcast ARP 42 Who has
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00
0010 00 cb 47 f0 00 00 01 11 7f 8e c0 a8 41 01 ef ff
0020 ff fa cf 46 07 6c 00 b7 b9 80 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d
eth0: <live capture in progress>
Packets: 5612 · Displayed: 5612 (100.0%)
Profile: Default

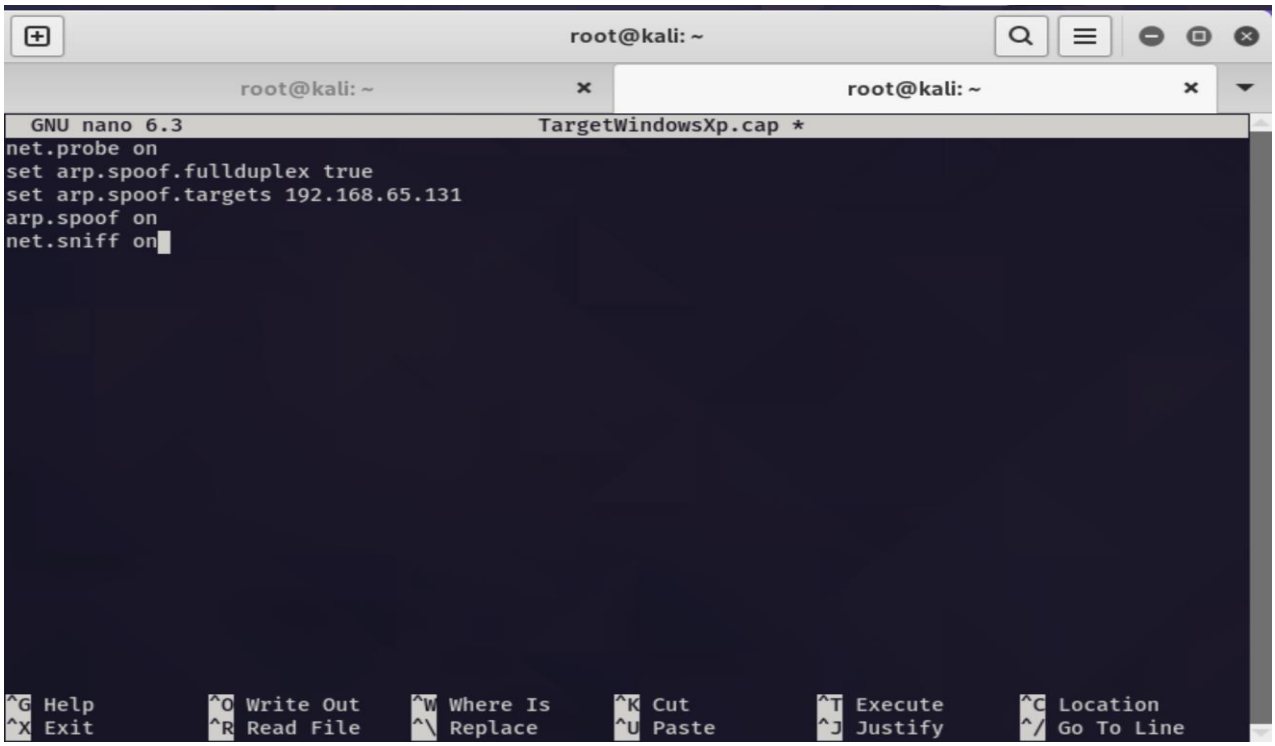

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 VMware_cb:88:41 Broadcast ARP 42 Who has
2 0.000315472 VMware_cb:88:41 Broadcast ARP 42 Who has
3 0.031851870 VMware_cb:88:41 Broadcast ARP 42 Who has
4 0.032188898 VMware_cb:88:41 Broadcast ARP 42 Who has
5 0.032354424 VMware_cb:88:41 Broadcast ARP 42 Who has
6 0.063933274 VMware_cb:88:41 Broadcast ARP 42 Who has
7 0.067933094 VMware_cb:88:41 Broadcast ARP 42 Who has
8 0.068222236 VMware_cb:88:41 Broadcast ARP 42 Who has
9 0.193357717 fe80::20c:29ff:fecb... ff02::16 ICMPv6 90 Multicast
10 0.257289475 VMware_cb:88:41 VMware_a9:78:d7 ARP 60 192.168.
11 0.257471413 VMware_cb:88:41 VMware_fe:7a:5b ARP 60 192.168.
12 0.291867267 VMware_cb:88:41 VMware_c0:00:08 ARP 42 Who has
13 0.292286719 VMware_c0:00:08 VMware_cb:88:41 ARP 60 192.168.
14 0.605489406 192.168.65.1 239.255.255.250 SSDP 217 M-SEARCH
15 0.605489921 192.168.65.1 239.255.255.250 SSDP 217 M-SEARCH
16 0.831978698 192.168.65.128 224.0.0.22 IGMPv3 54 Membersh
17 0.890271994 192.168.65.128 224.0.0.251 MDNS 85 Standard
18 0.890854196 fe80::20c:29ff:fecb... ff02::fb MDNS 105 Standard
19 0.900066760 192.168.65.128 224.0.0.22 IGMPv3 54 Membersh
0000 ff ff ff ff ff ff 00 0c 29 cb 88 41 08 06 00 01
eth0: <live capture in progress>
Packets: 249 · Displayed: 249 (100.0%)
Profile: Default

Zombie Machie Activity:-

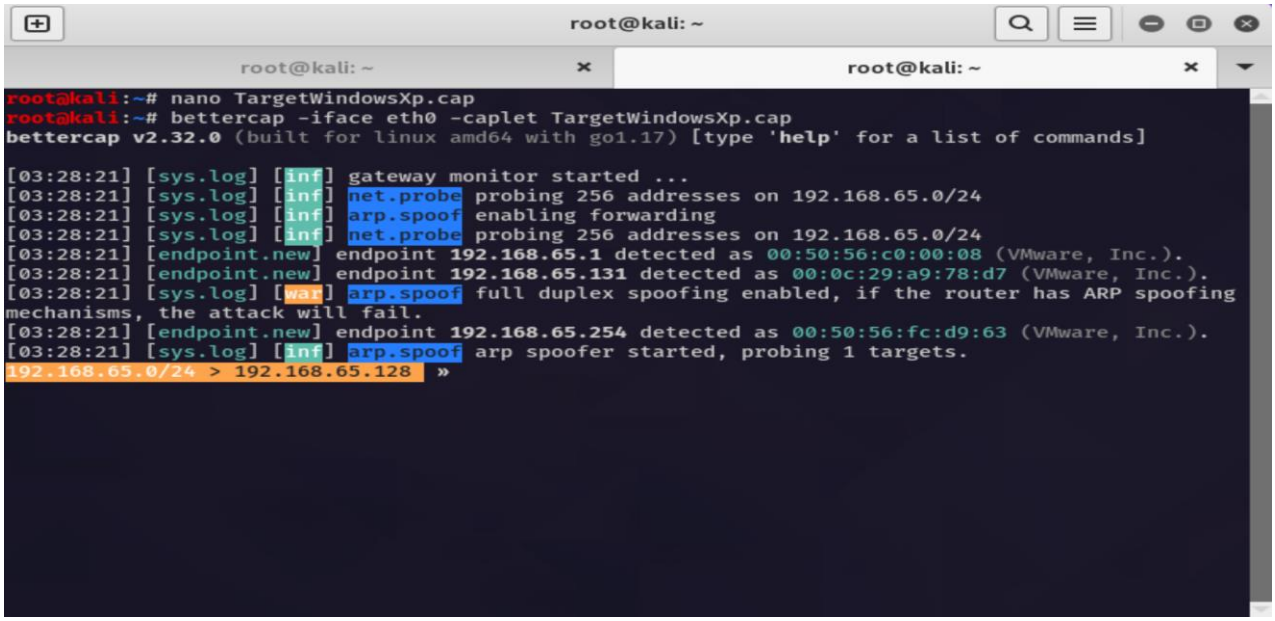


[6]. MITM Attack using Caplets Function:-

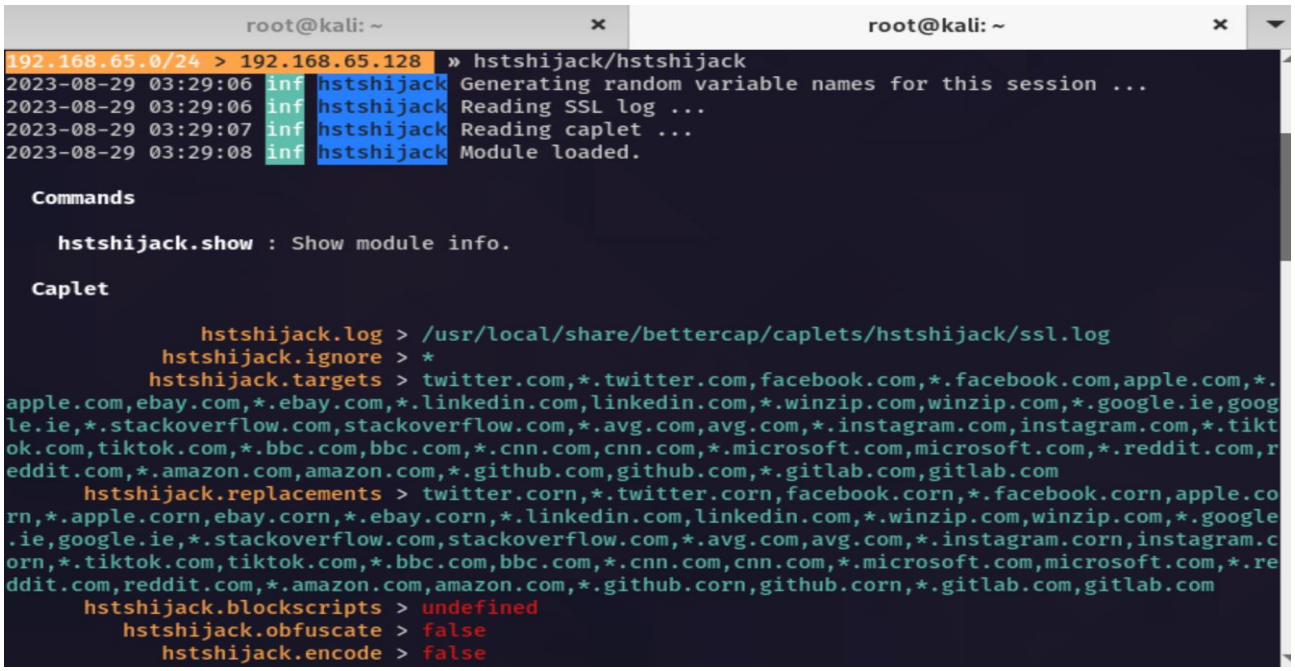
Creating .cap file using nano module:-

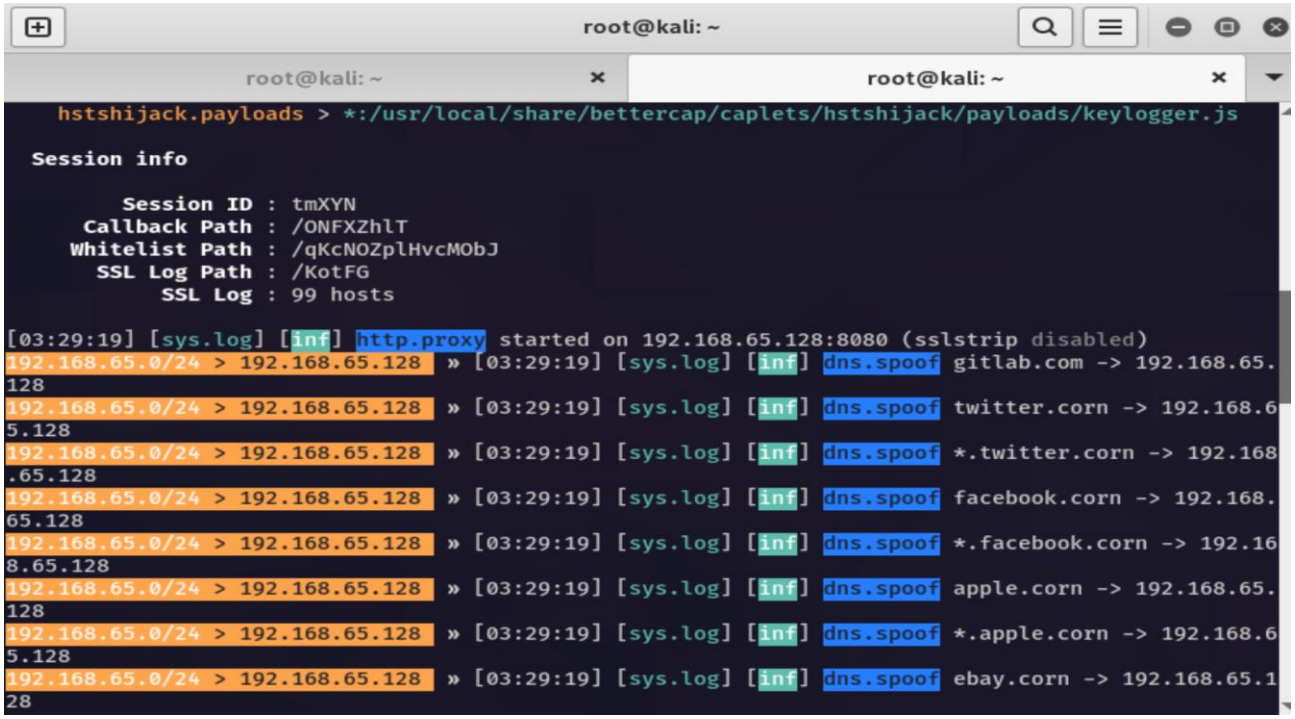


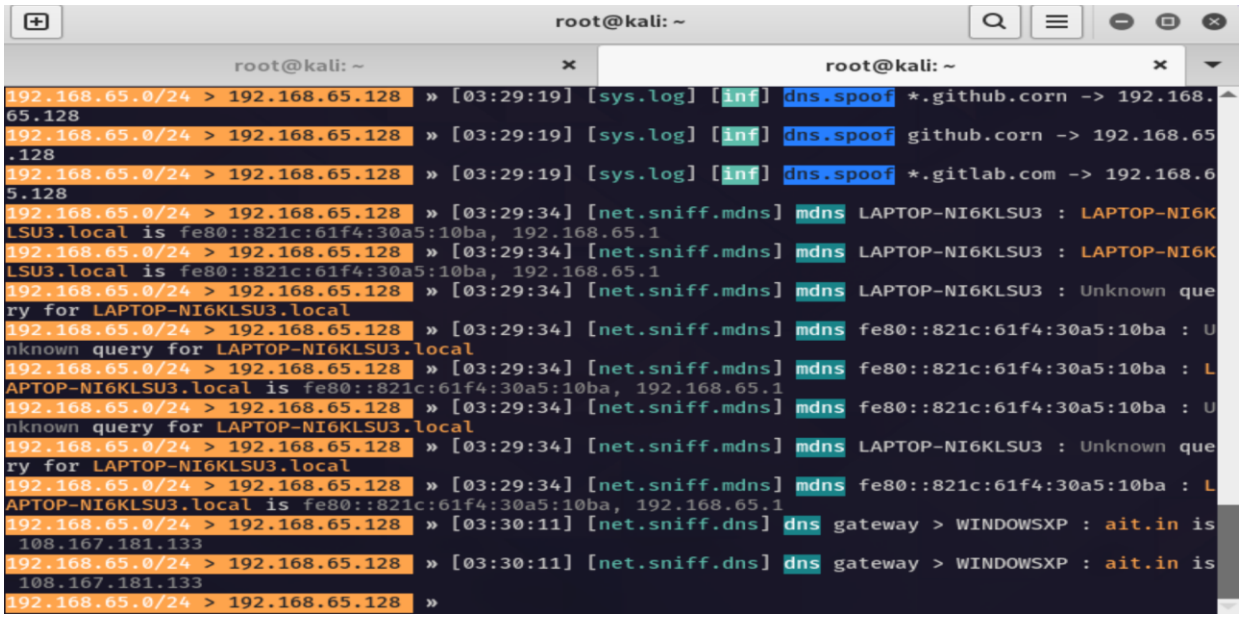
INITIALISING USING .cap FILE:-



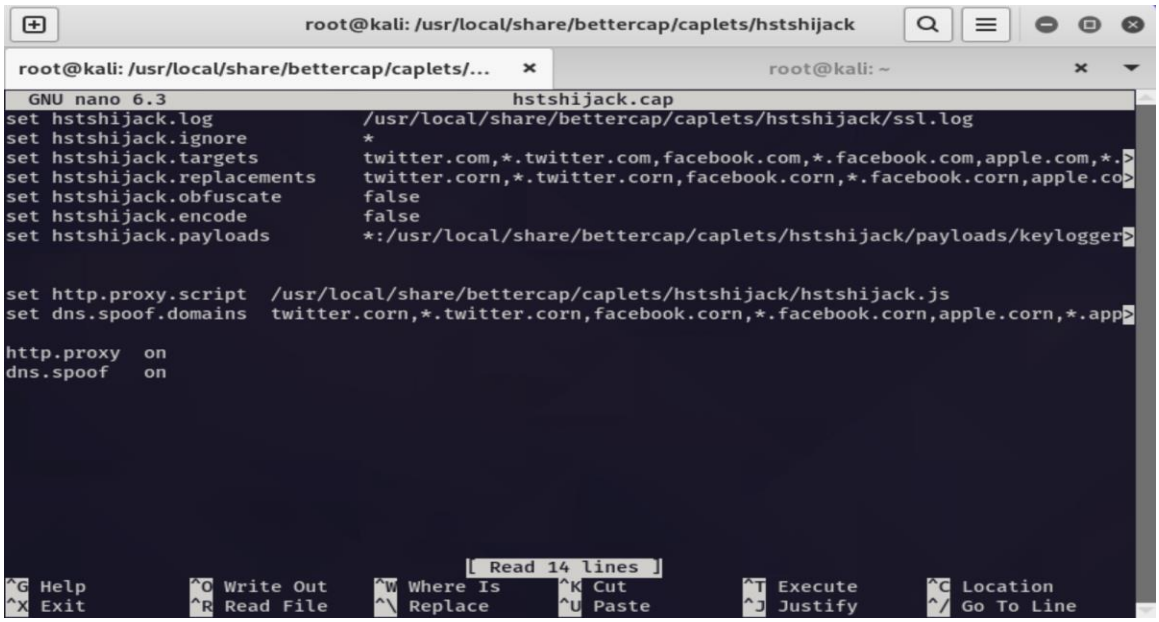
[7]. MIGRATING HTTPS TRAFFIC TO HTTP USING HSTSHIJACK CAPLET FUNCTION:-



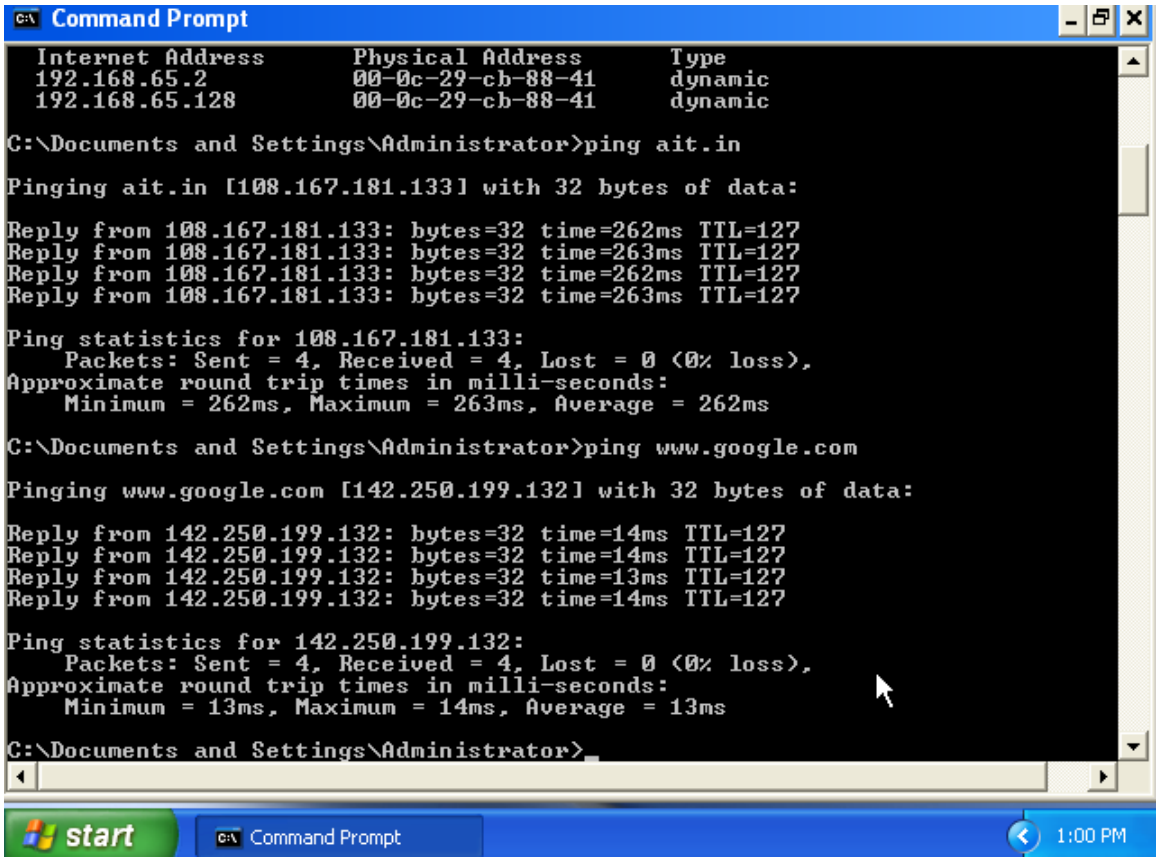


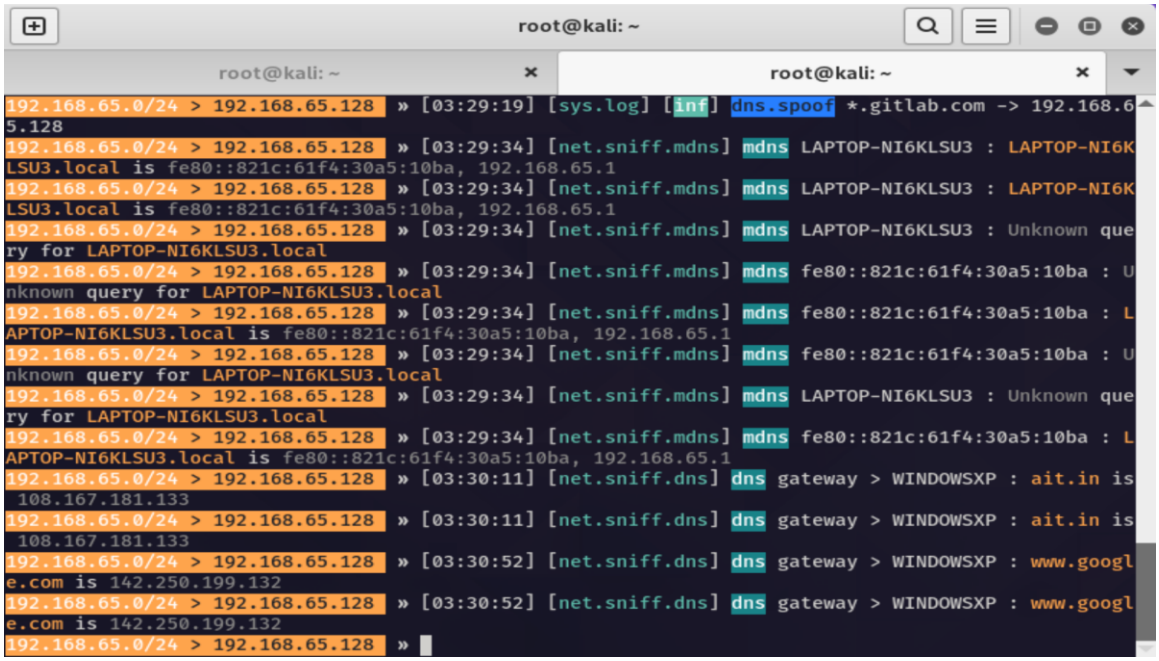


HSTSHIJACK.CAP FILE:-

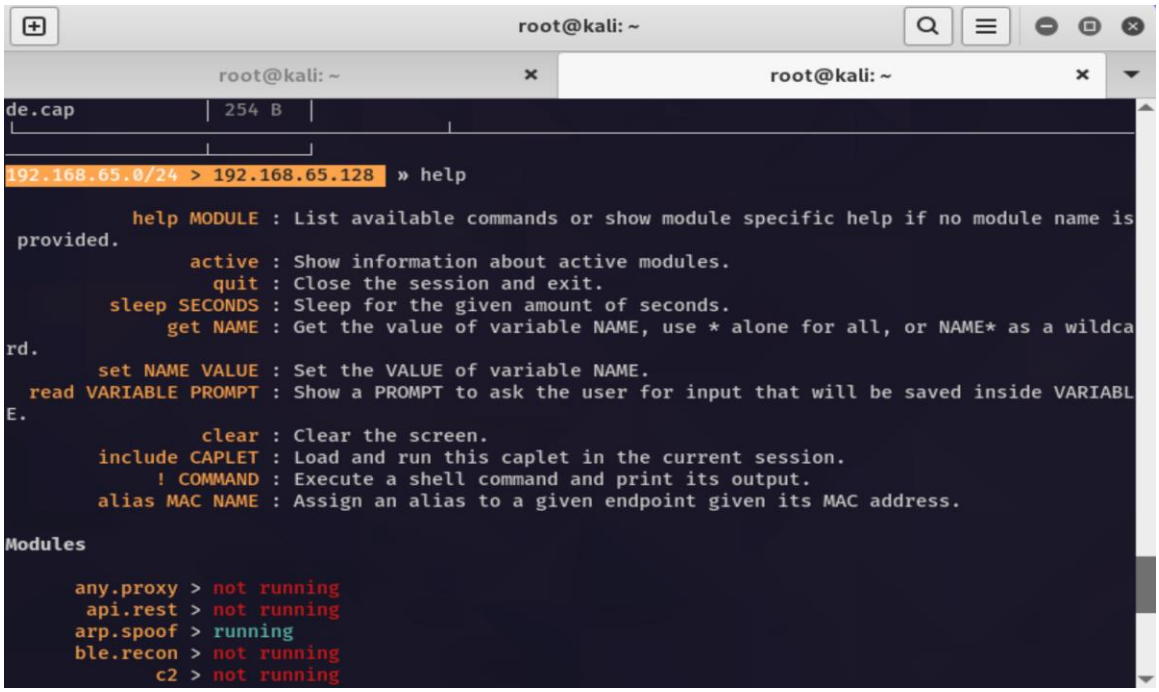


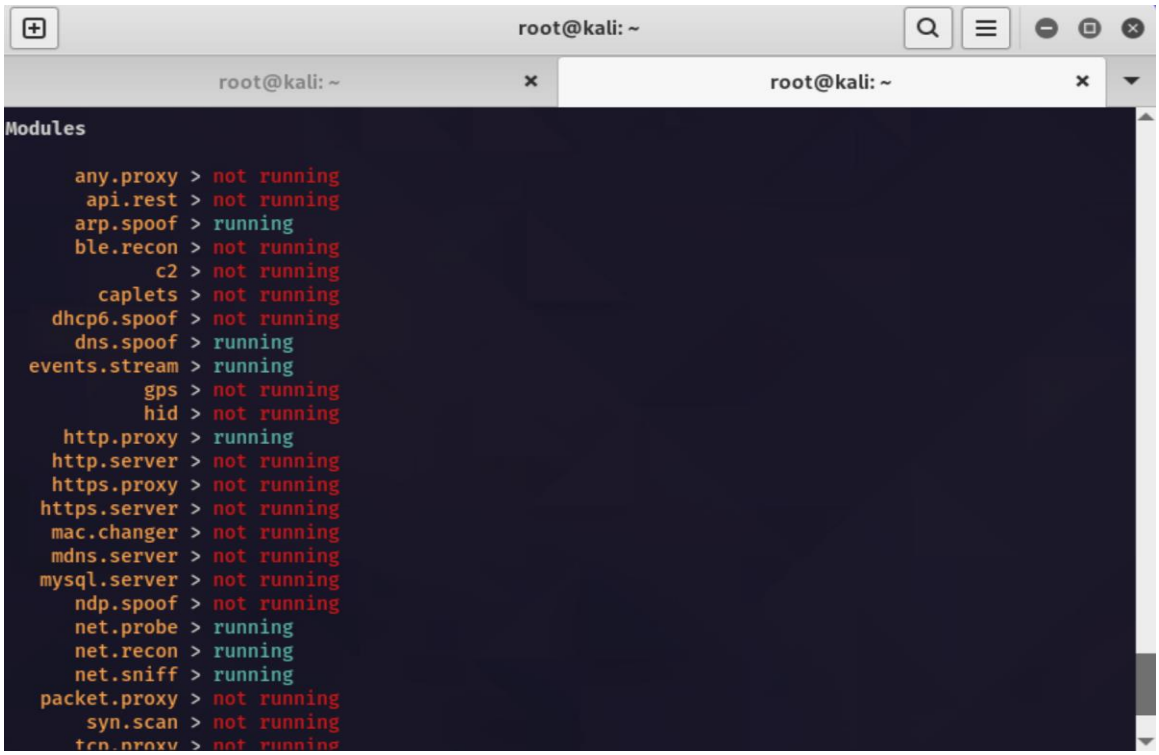
MIGRATION OF HTTPS TRAFFIC TO HTTP:-



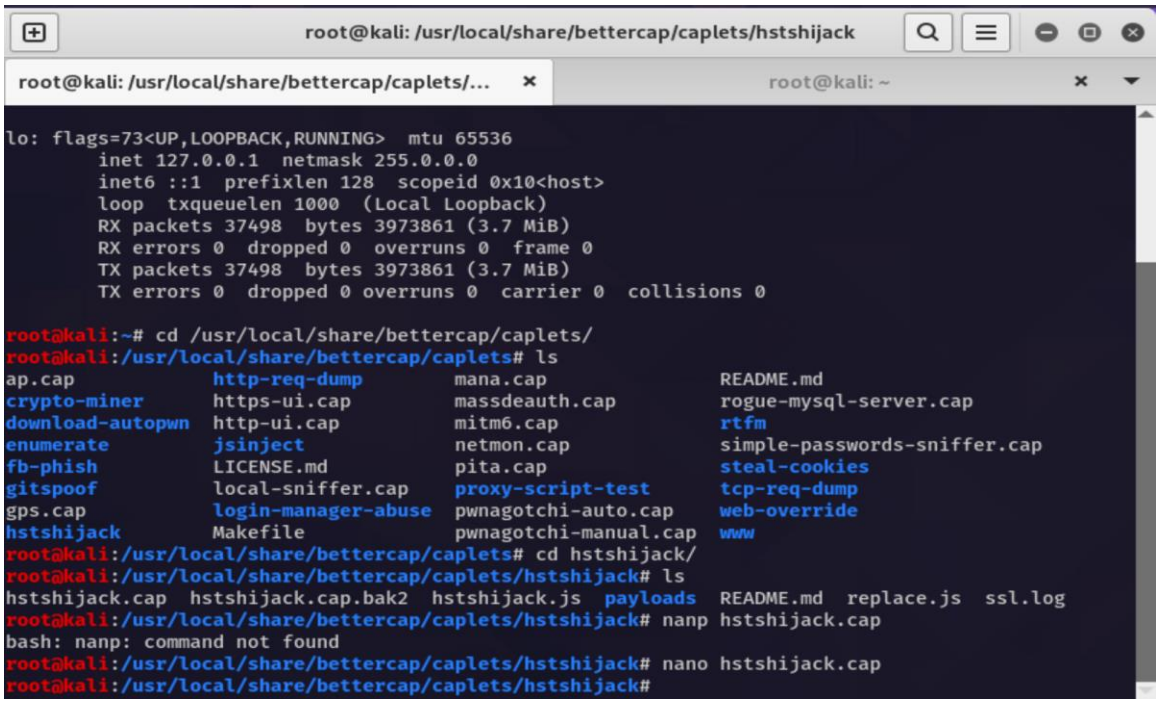


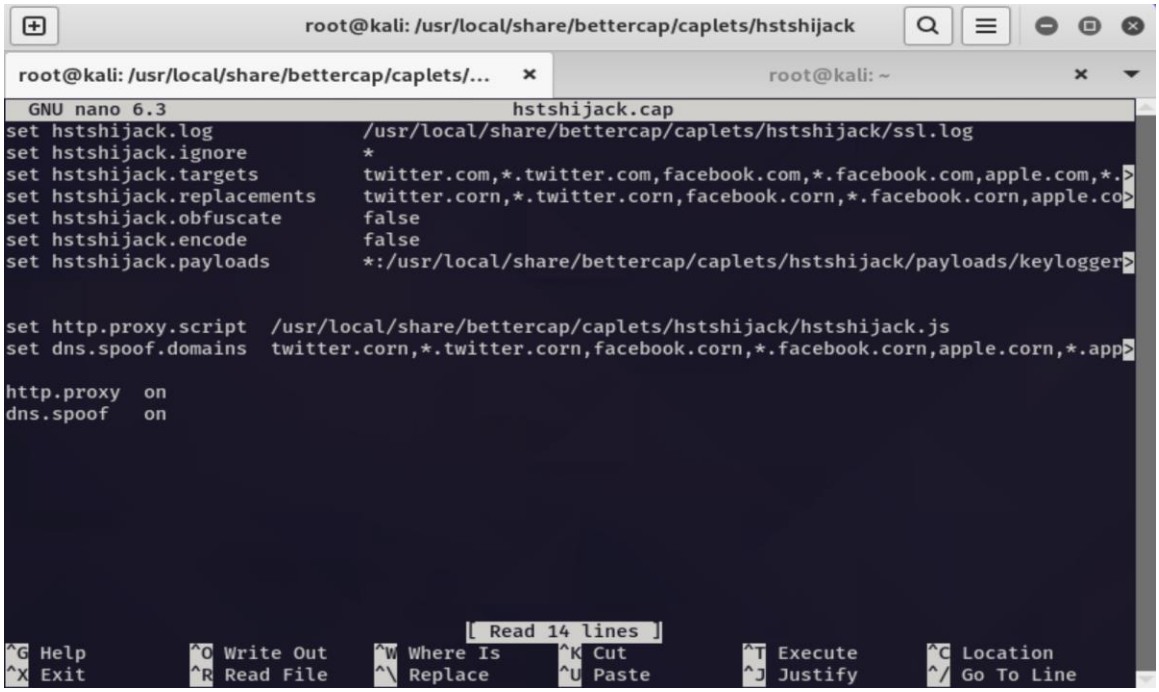
MODULES RUNNING UNDER BETTERCAP TOOL :-



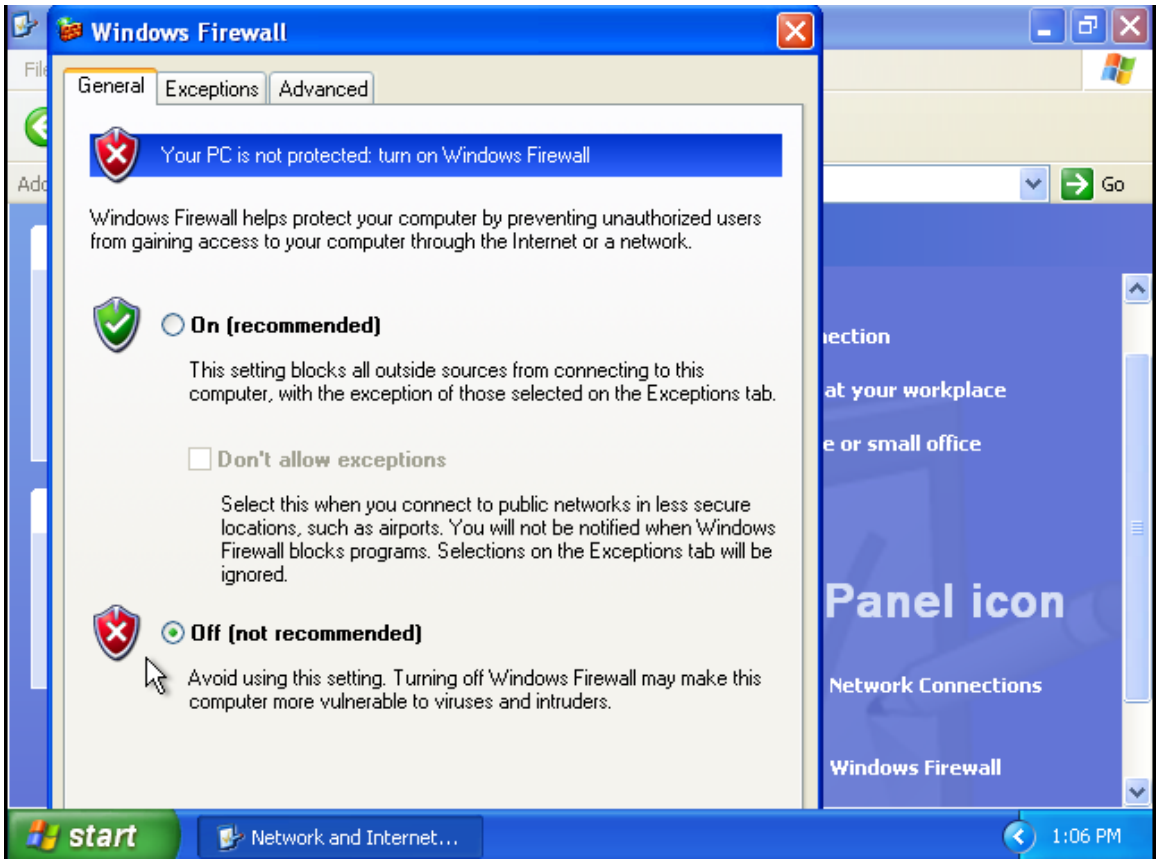


VARIOUS CAPLET FILES:-





DISABLING FIREWALL FOR WINDOWS SYSTEM:-



[8]. Title: Project Report Summary - Man-in-the-Middle Attack using BetterCap and Wireshark on Windows XP using Kali Linux

Project Overview:

Project 7 aimed to execute a Man-in-the-Middle (MitM) attack on a Windows XP target system using the tools BetterCap and Wireshark. The objective was to gain practical experience in conducting a MitM attack, understand the modules offered by BetterCap, and analyze intercepted network packets using Wireshark.

Target System:

Windows XP Professional x64

Tools Used:

1. BetterCap: A versatile network manipulation tool used for various network security tasks.

2. Wireshark: A widely-used packet analysis tool for capturing and dissecting network packets.

Project Steps:

1. Setting Up the Environment:

- A controlled lab environment was established, consisting of three machines - the attacker, the victim (Windows XP), and a third-party device.

2. BetterCap Modules:

- ARP Spoofing (arp.sniff): The attacker used ARP spoofing to trick the victim into sending its traffic through the attacker's machine.

- Network Sniffing (net.sniff): This module allowed the attacker to capture and analyze network traffic passing through the MitM setup.

- hstshijack: A specialized module to redirect HTTP traffic to the attacker's machine.

3. Capturing Packets:

- BetterCap was configured to intercept traffic using the mentioned modules, ensuring all packets passing through the MitM setup were captured.

4. Wireshark Analysis:

- Captured packets were saved and imported into Wireshark.

- The Wireshark interface was used to analyze the captured packets, focusing on identifying sensitive information and understanding the flow of communication.

5. Caplets Function:

- Caplets in BetterCap were used to create scripts containing commands for specific tasks.

- Commands used in the caplets were documented to ensure clear understanding and reproducibility.

6. hstshijack Caplet:

- The hstshijack caplet function was employed to hijack and redirect HTTP traffic to the attacker's machine, allowing interception and analysis of unencrypted HTTP data.

Results:

1. Successful execution of a Man-in-the-Middle attack on the Windows XP machine.

2. Captured a range of network packets, including unencrypted HTTP traffic.

3. Analyzed intercepted packets using Wireshark to identify sensitive data and understand the communication patterns.

Discussion:

The project provided hands-on experience in executing a MitM attack using BetterCap on a Windows XP target. It highlighted the potential risks of unencrypted network traffic and underscored the importance of implementing security measures to prevent such attacks.

Conclusion:

Project 7 successfully demonstrated the process of conducting a Man-in-the-Middle attack on a Windows XP machine using BetterCap and Wireshark. This project enhanced understanding of network security concepts, MitM attack methods, and packet analysis techniques using Wireshark.