

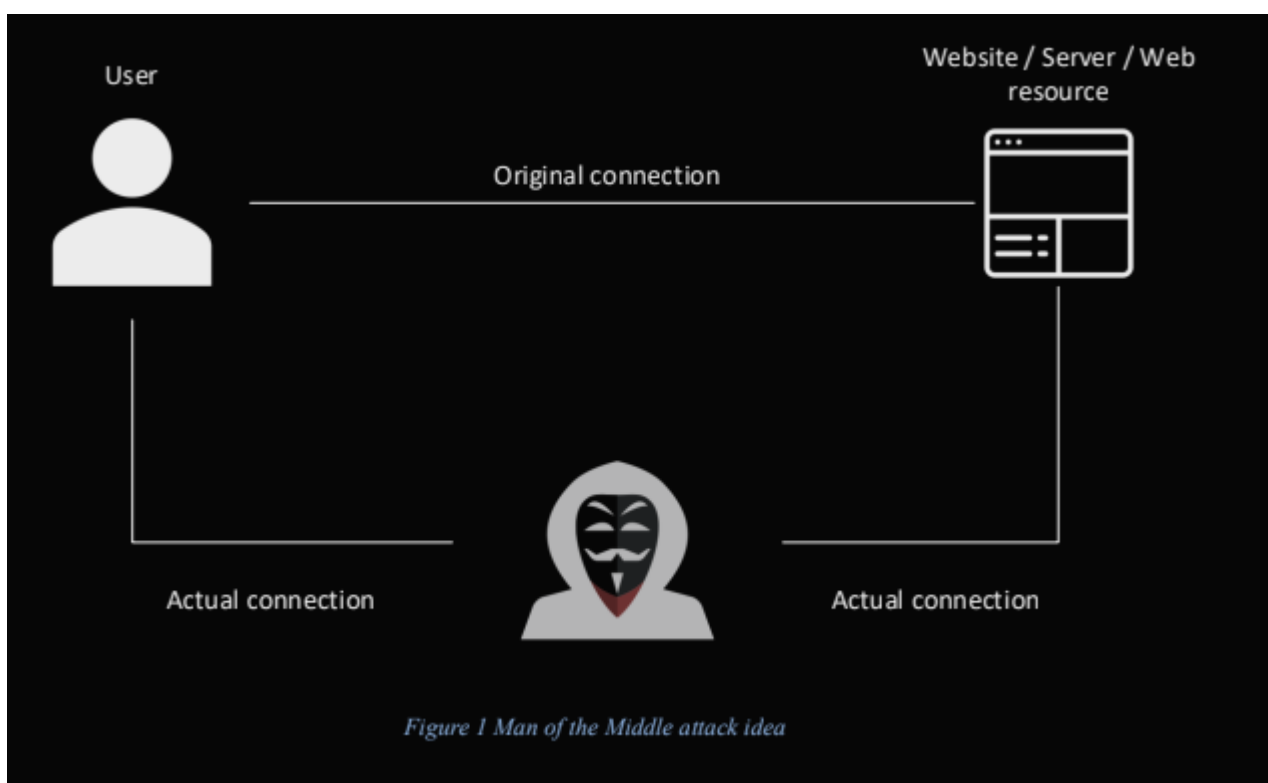
CYBERSECURITY

LAB 8

1. Introduction

Hacking attacks are not always associated with accessing your computer or data on the server. Increasing the importance of the Internet and the amount of transmitted data in the network has resulted in the development of attacks related to network communication, especially those belonging to the group of **Man in the Middle** attacks.

MitM is a group of attacks whose basic assumption is to eavesdrop communication between two devices in the network. As a result, the attacker gets access to the data transmitted during communication, can read it, modify it at will (altogether with a complete change of transmitted content, e.g. to transmit a fake website) and block it.



MitM attacks can be classified into several groups:

- **Wi-Fi eavesdropping** - a simple type of attack consisting of creating hotspots / access points of Wi-Fi networks impersonating known and safe networks (e.g. cafes, cinemas, public networks). Using this attack, the hacker has the ability to send any content to the network user (e.g. fake versions of known web services).
- **ARP poisoning** - attack utilizing lack of authentication during transmission using ARP protocol. By sending appropriate ARP messages the attacker poisons the ARP routing table by setting the MAC address of any devices in the attacked network with their own IP address. As a result of a change in the array, all the victim's network packets are sent to the attacker, at the same time the attacker is treated as the original recipient of the message and its replies as correct answers to any sent one.

- **DNS spoofing** - DNS cache poisoning allows an attacker to force the victim to download harmful data by trying to connect to known network services. An attacker sends a fake message containing a domain name and IP address of an e.g. malicious website. When a victim tries to connect to a website by providing a domain name, he is redirected to the attacker's website.
- **ICMP redirects** - using ICMP redirect packets, an attacker could instruct a router to forward packets destined for the victim through the attacker's own machine. The attacker can then monitor or modify the packets before sending them to their destination.
- **Port stealing** - an attack executed in local networks involving a change of information stored in the network switch forwarding table. Once this is done, all network packets addressed to the original port are redirected to the port to which the attacker's machine is connected.
- **STP mangling** - in the network each router assumes itself as the root bridge by default. However, it is possible to send Bridge Protocol Data Units (BPDUs) to establish a new root bridge. In the lack of support for adequate protection, all network traffic from the victim's switch starts to be transmitted by the switch indicated as root by the attacker.

2. Required virtual machines

- Kali
- Metasploitable2

3. Prerequisites

Get familiar with the following elements:

- Routing tables
- DNS
- APR
- DNS/ARP cache
- MAC
- Ettercap
- Arpspoof
- Wireshark

4. Problems and questions

I. What is the difference between active and passive MitM attacks?

> In an active Man-in-the-Middle (MitM) attack, the attacker intercepts and alters the communication between two parties without them being aware. In a passive MitM attack, the attacker simply monitors the communication without altering it.

II. How to protect your network against ARP poisoning attacks?

> ARP spoofing detection software or tools, such as ARPwatch, encryptions or filters as such.

III. Why is it important to use DNSSEC to prevent DNS spoofing attacks?

> It is used to prevent DNS spoofing attacks by providing authentication for DNS queries. It uses digital signatures to ensure that the DNS information received by the user is authentic and has not been tampered with by an attacker.

IV. What is monitor mode and how can you use it to eavesdrop network communication?

> Monitor mode is a feature of some wireless network adapters that allows them to capture all packets on a wireless network, regardless of whether they are intended for the adapter or not. This can be used by attackers to eavesdrop on network communication and steal sensitive information. To use monitor mode, you need a wireless network adapter that supports it and a software tool, such as Wireshark, to capture and analyze the packets.

5. Tasks

In some cases, the router's security mechanisms and the stored data in the cache may interfere with the observation of the result of the correct execution of the attack. In such a case, it may be necessary to correctly execute the attack:

- Connecting a computer to a hotspot launched with a smartphone
- Changing settings of VMs network cards to Bridged Adapter. Open VirtualBox -> Select each of yours VMs -> Settings -> Network -> Attached to: Bridged Adapter

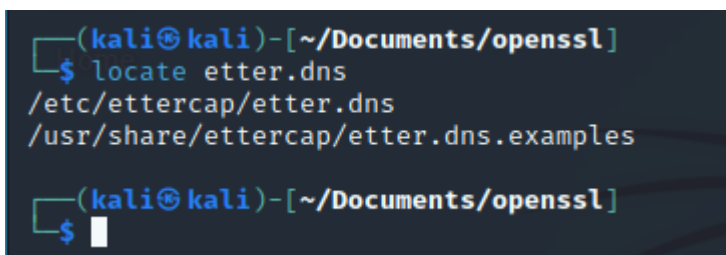
Please remember to restore the previous network adapter settings after completing the tasks!

The ARP table for your computer will be modified during the exercise. Remember to terminate the MitM attack after completing the exercises to reverse this process!!!

I. In this task, the victim machine is the Ubuntu Server VM. In addition, we will be using the Metasploitable 2 VM as a web server machine.

II. Open command line and locate `etter.dns` file in Kali VM

`locate etter.dns`



```
(kali㉿kali)-[~/Documents/openssl]
$ locate etter.dns
/etc/ettercap/etter.dns
/usr/share/ettercap/etter.dns.examples

(kali㉿kali)-[~/Documents/openssl]
$
```

III. Navigate to this path and open the file

IV. Edit the file to spoof WUST domain name (add new line next to “microsoft.com ...”

`pwr.edu.pl A KALI_VM_IP_ADDRESS`

`*.pwr.edu.pl A KALI_VM_IP_ADDRESS`

`www.pwr.edu.pl PTR KALI_VM_IP_ADDRESS`

V. On Kali VM start Apache2

service apache2 start

VI. Run Ettercap on Kali VM

sudo ettercap -G

VII. Start sniffing

VIII. Use **Scan for hosts** and after finishing go to the **Hosts List** from the Hosts menu.

IX. Add your router/gateway IP to Target 1 (usually it will be IP address with 1 in last octet) and victim IP (Ubuntu Server VM) to Target 2

X. Start ARP Poisoning

Mitm menu -> ARP Poisoning -> Check Sniff remote connections

XI. Go to Plugins menu and activate dns_spoof plugin

Plugins -> Manage plugins -> double click on dsn_spoof

XII. Open the WUST website in the browser on your computer and observe the results
XIII. Stop last MitM attack, clear Target 1 and Target 2

XIV. Add a victim machine (Ubuntu Server VM) to Target 1 and Metasploitable VM to Target 2

XV. Start ARP Poisoning once again

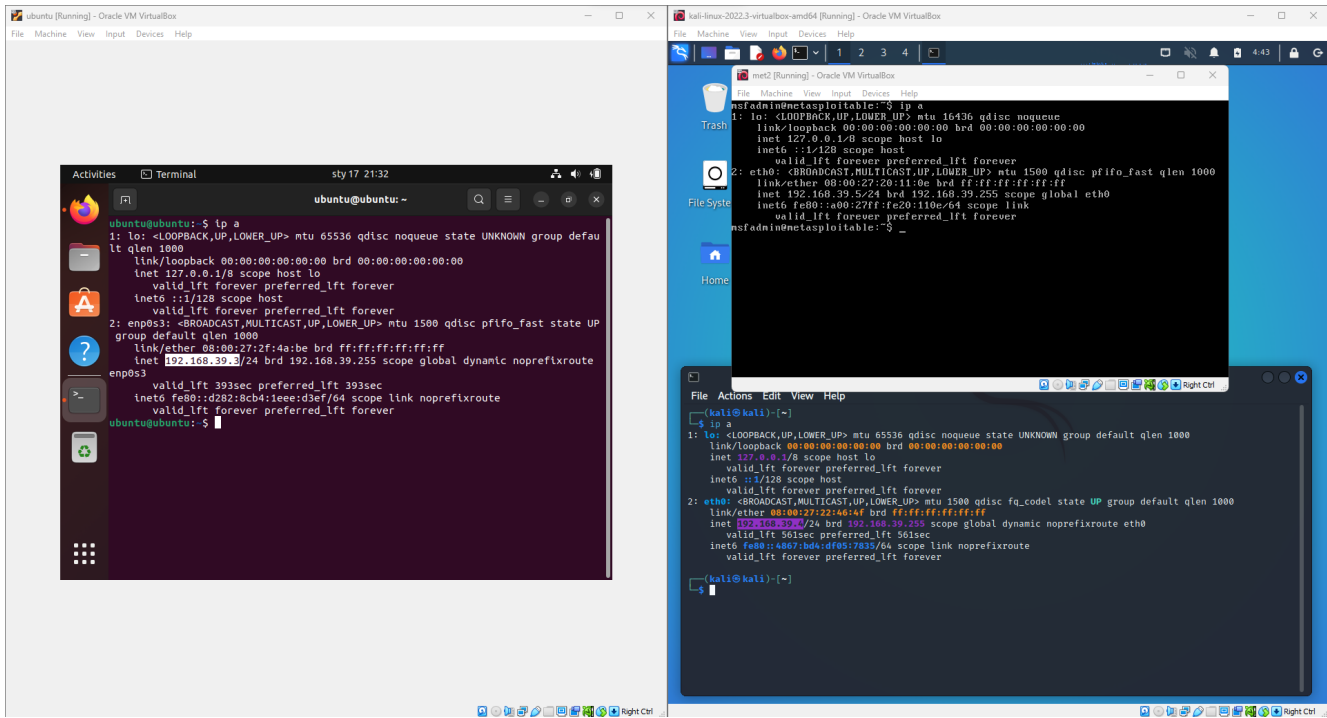
XVI. Connect to Metasploitable VM from web browser on victim machine

Open browser -> http://METASPLOITABLE_VM_IP_ADDRESS/dvwa

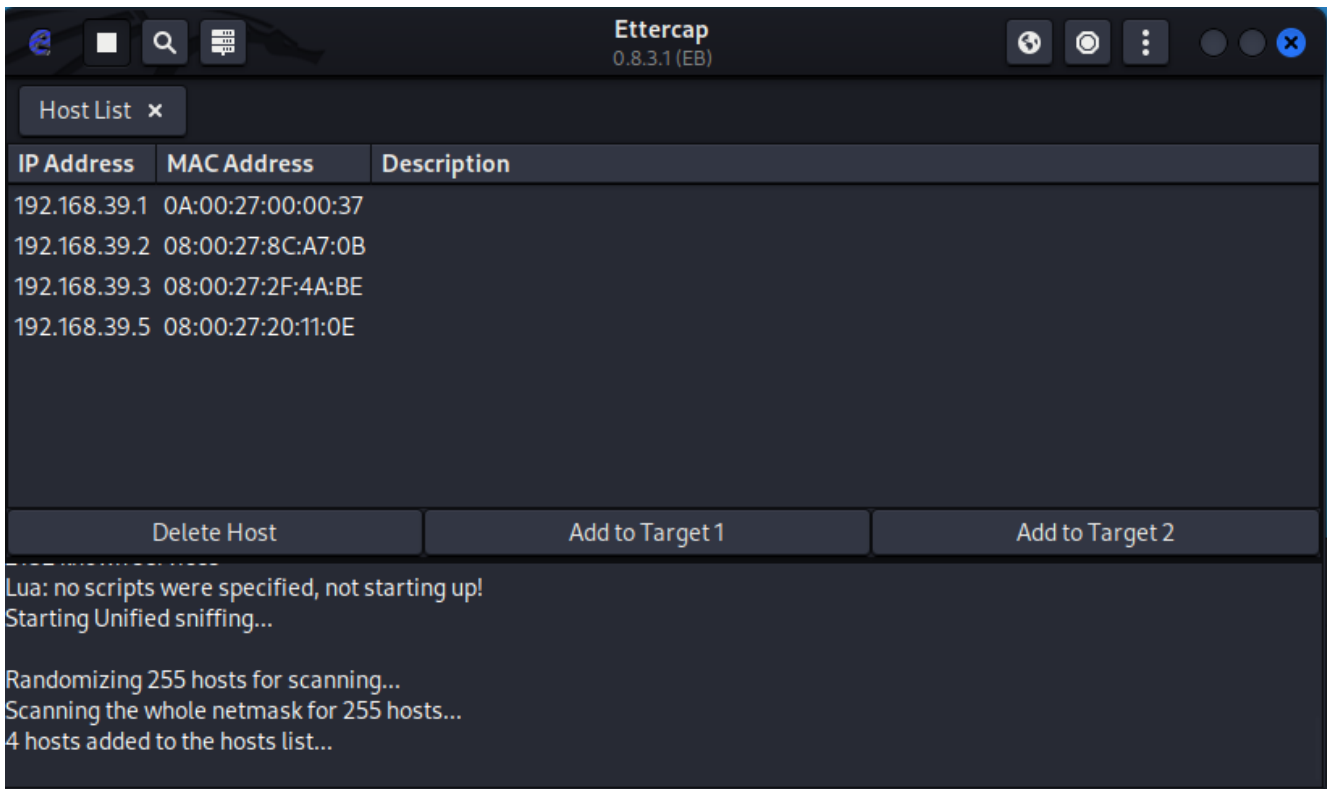
XVII. Open **DVWA** and try to log in with any login and password. Observe the results in ettercap.

XVIII. Open Wireshark on Kali VM, start capturing traffic on eth network interface and try to generate some network traffic on Metasploitable VM from Victim VM (try to log in again, open other applications on web server, try to connect with ssh). Observe the results.

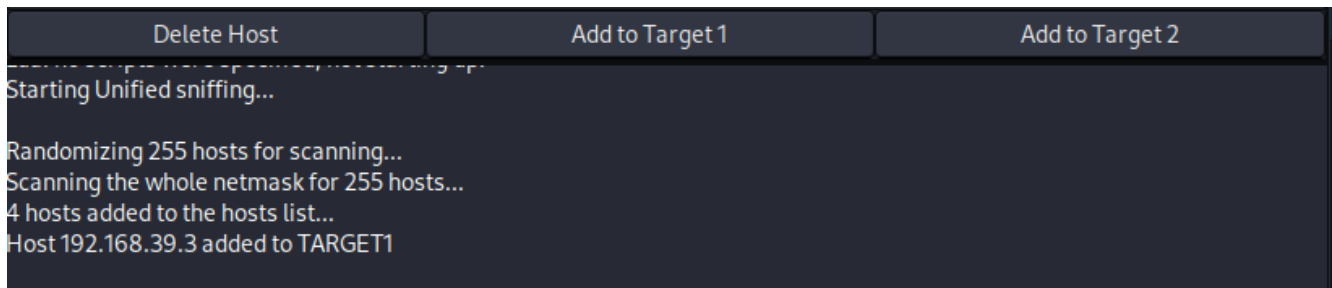
You can see the ip of the machines ,



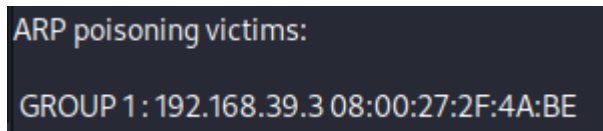
Started ettercap



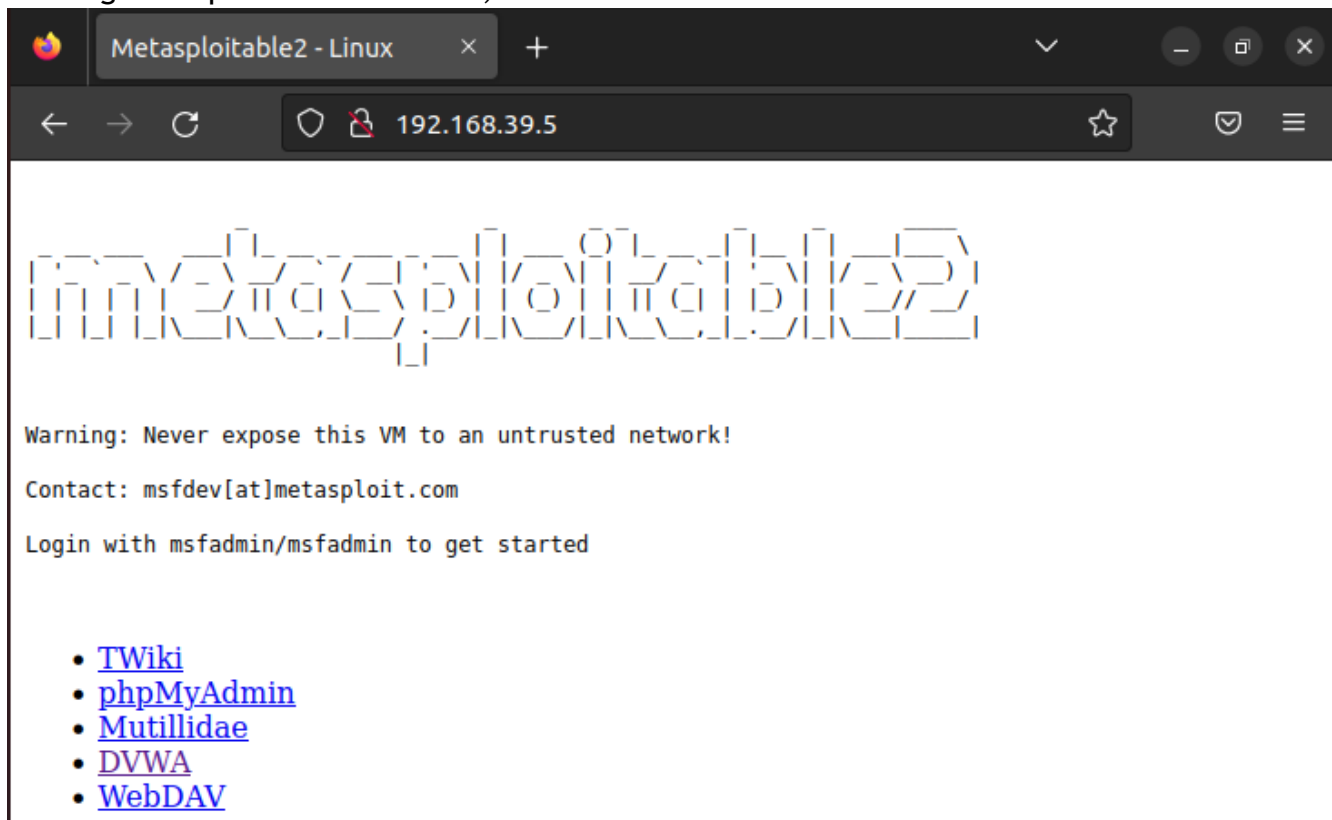
Added ubuntu to target 1

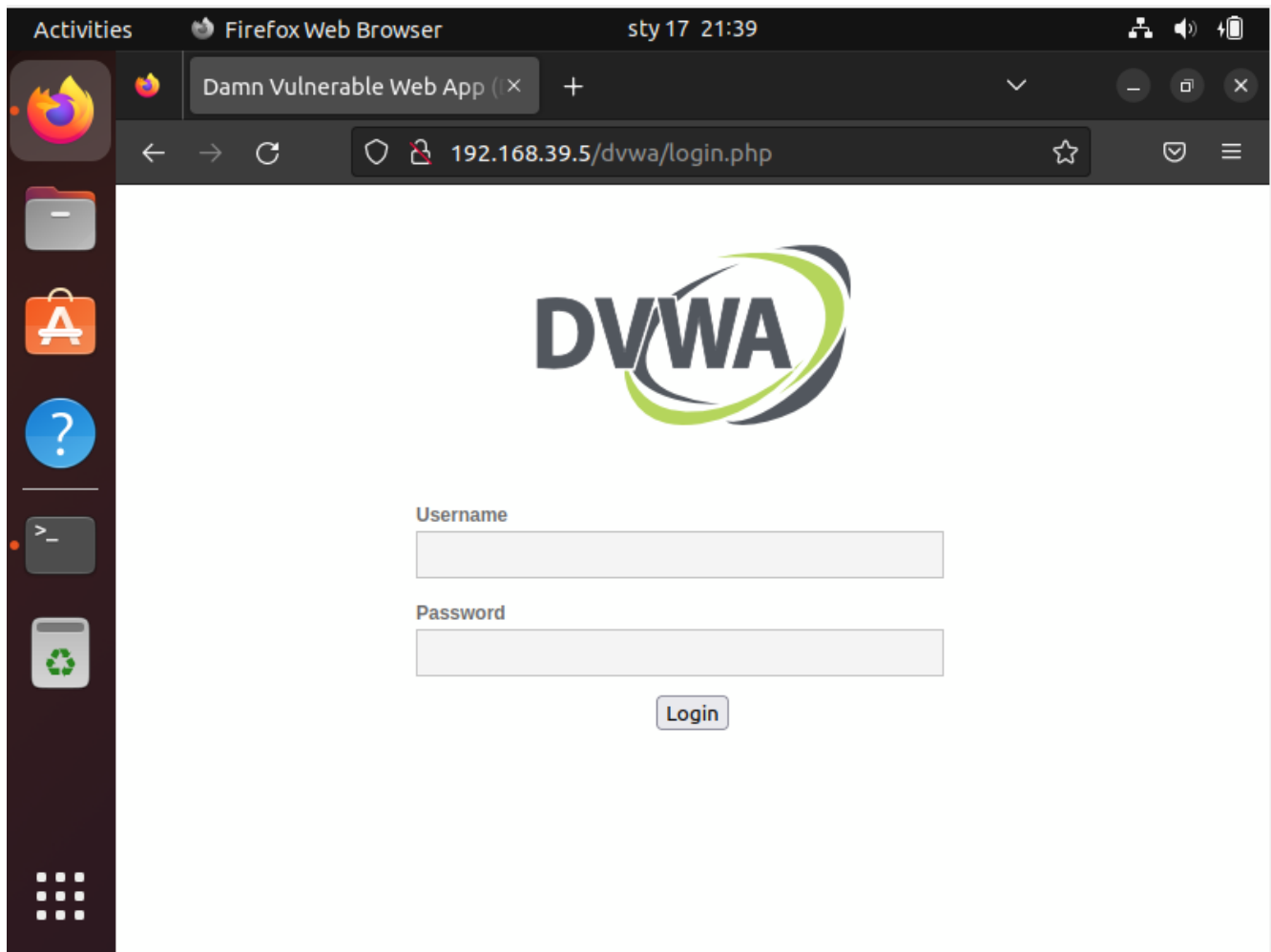


Started ARP poisoning



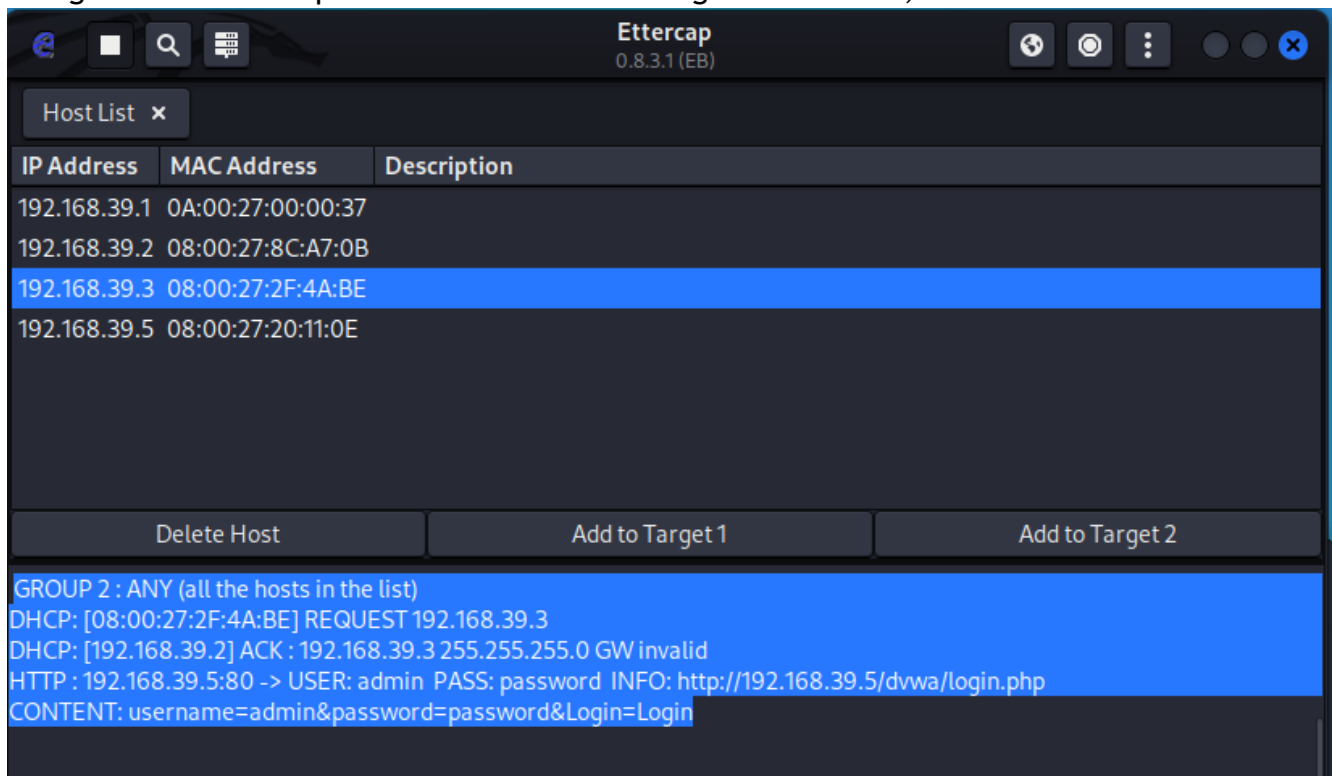
Running Metasploitable in ubuntu,





admin
password

Going back to ettercap in kali we can see the login credentials,



Next we capture some packets using wireshark,

No.	Time	Source	Destination	Protocol	Length	Info
66	20.076436740	PcsCompu_22:46:4f	PcsCompu_8c:a7:0b	ARP	42	192.168.39.3 is at 08:00:
67	20.086822385	PcsCompu_22:46:4f	PcsCompu_2f:4a:be	ARP	42	192.168.39.1 is at 08:00:
68	20.086942349	PcsCompu_22:46:4f	0a:00:27:00:00:37	ARP	42	192.168.39.3 is at 08:00:
69	25.552224986	192.168.39.3	192.168.39.5	TCP	66	[TCP Keep-Alive] 51700 →
70	25.558205375	192.168.39.3	192.168.39.5	TCP	66	[TCP Keep-Alive] 51700 →
71	25.559205734	192.168.39.5	192.168.39.3	TCP	66	[TCP Keep-Alive ACK] 80 →
72	25.566181073	192.168.39.5	192.168.39.3	TCP	66	[TCP Keep-Alive ACK] 80 →
73	30.097972816	PcsCompu_22:46:4f	PcsCompu_2f:4a:be	ARP	42	192.168.39.5 is at 08:00:
74	30.098065257	PcsCompu_22:46:4f	PcsCompu_20:11:0e	ARP	42	192.168.39.3 is at 08:00:
75	30.108435853	PcsCompu_22:46:4f	PcsCompu_2f:4a:be	ARP	42	192.168.39.2 is at 08:00:
76	30.108529253	PcsCompu_22:46:4f	PcsCompu_8c:a7:0b	ARP	42	192.168.39.3 is at 08:00:
77	30.118925493	PcsCompu_22:46:4f	PcsCompu_2f:4a:be	ARP	42	192.168.39.1 is at 08:00:
78	30.119020078	PcsCompu_22:46:4f	0a:00:27:00:00:37	ARP	42	192.168.39.3 is at 08:00:
79	30.459674741	192.168.39.5	192.168.39.3	TCP	66	80 → 51700 [FIN, ACK] Seq=
80	30.462452024	192.168.39.5	192.168.39.3	TCP	66	[TCP Retransmission] 80 →
81	30.463536803	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [FIN, ACK] Seq=
82	30.470184304	192.168.39.3	192.168.39.5	TCP	66	[TCP Retransmission] 5170
83	30.471009811	192.168.39.5	192.168.39.3	TCP	66	80 → 51700 [ACK] Seq=1020
84	30.478170788	192.168.39.5	192.168.39.3	TCP	66	[TCP Dup ACK 83#1] 80 → 5

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured on interface eth0, 42 bytes from 08:00:27:2f:4a:be to 08:00:27:22:46:4f on interface eth0
Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: 08:00:27:22:46:4f, Length: 42
Address Resolution Protocol (reply)

We can filter the ip of the targeted machine and see the protocol info,

No.	Time	Source	Destination	Protocol	Length	Info
7	6.475764177	192.168.39.3	192.168.39.5	TCP	74	51700 → 80 [SYN] Seq=0 Win=
8	6.478431681	192.168.39.3	192.168.39.5	TCP	74	[TCP Retransmission] [TCP
9	6.479388917	192.168.39.5	192.168.39.3	TCP	74	80 → 51700 [SYN, ACK] Seq=
10	6.486323698	192.168.39.5	192.168.39.3	TCP	74	[TCP Retransmission] 80 →
11	6.506942904	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [ACK] Seq=1 Ac
12	6.507397864	192.168.39.3	192.168.39.5	HTTP	536	GET /dvwa/index.php HTTP/
13	6.510372349	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [ACK] Seq=1 Ac
14	6.510700185	192.168.39.3	192.168.39.5	TCP	536	[TCP Retransmission] 5170
15	6.511883955	192.168.39.5	192.168.39.3	TCP	66	80 → 51700 [ACK] Seq=1 Ac
16	6.518217346	192.168.39.5	192.168.39.3	TCP	66	[TCP Dup ACK 15#1] 80 → 5
17	6.525924152	192.168.39.5	192.168.39.3	TCP	1514	80 → 51700 [ACK] Seq=1 Ac
18	6.525924405	192.168.39.5	192.168.39.3	TCP	1514	80 → 51700 [ACK] Seq=1449
19	6.526614384	192.168.39.5	192.168.39.3	TCP	1514	80 → 51700 [ACK] Seq=2897
20	6.526916057	192.168.39.5	192.168.39.3	TCP	1514	[TCP Out-Of-Order] 80 → 5
21	6.527246949	192.168.39.5	192.168.39.3	TCP	1514	[TCP Out-Of-Order] 80 → 5
22	6.527704801	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [ACK] Seq=471
23	6.528122003	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [ACK] Seq=471
24	6.536031197	192.168.39.5	192.168.39.3	TCP	1514	[TCP Retransmission] 80 →
25	6.536672757	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [ACK] Seq=471
26	6.536840750	192.168.39.3	192.168.39.5	TCP	66	51700 → 80 [ACK] Seq=471

Frame 7: 74 bytes on wire (592 bits), 74 bytes captured on interface eth0, 74 bytes from 08:00:27:2f:4a:be to 08:00:27:22:46:4f on interface eth0
Ethernet II, Src: PcsCompu_2f:4a:be (08:00:27:2f:4a:be), Dst: 08:00:27:22:46:4f, Length: 74
Internet Protocol Version 4, Src: 192.168.39.3, Destination: 192.168.39.5
Transmission Control Protocol, Src Port: 51700, Dst Port: 80

Thank you, the enlisted guide from university was a bit hard to grasp so i took help from a given video from ms teams! It was much easier to understand.