LAB PERFORMED

8/7/2021

Table of Contents

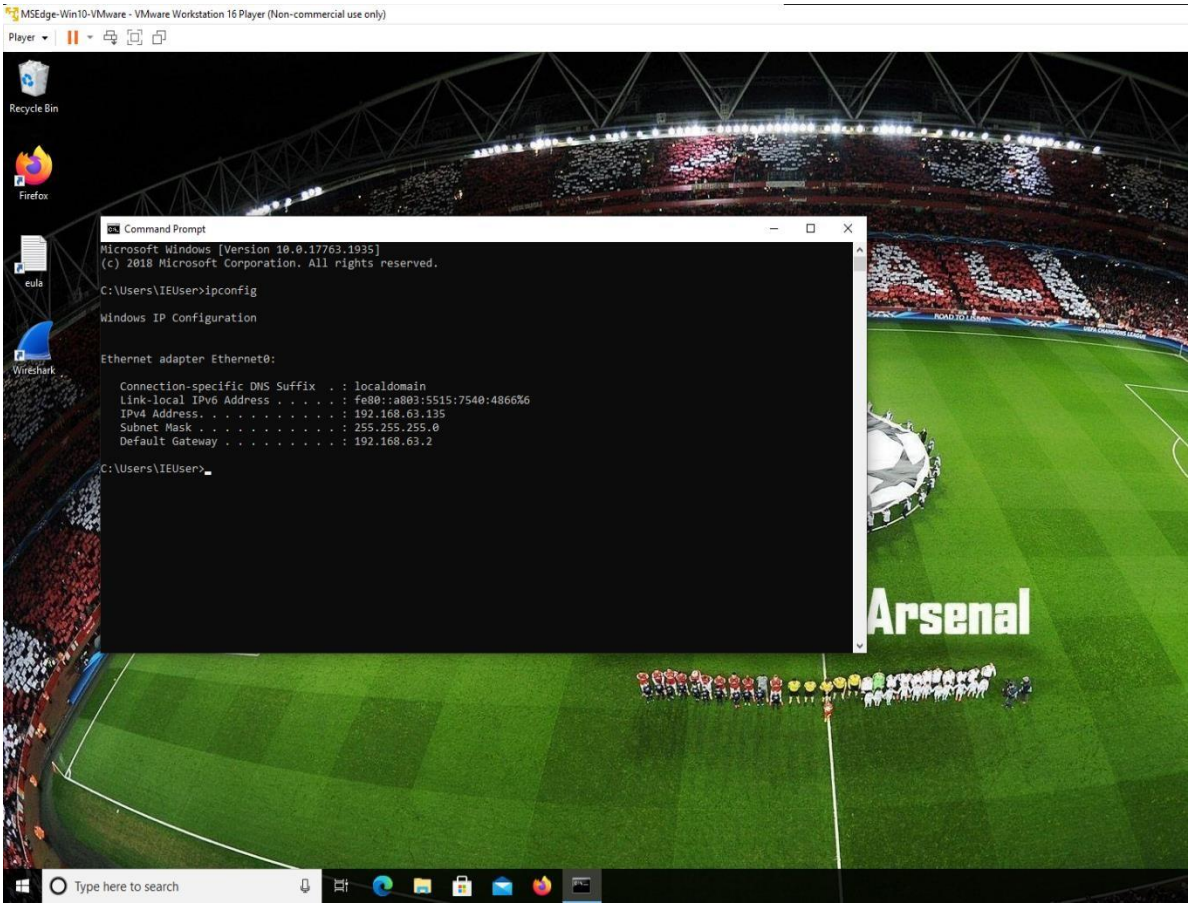
1 DNS SPOOFING

1.1 General Information collected before the attack

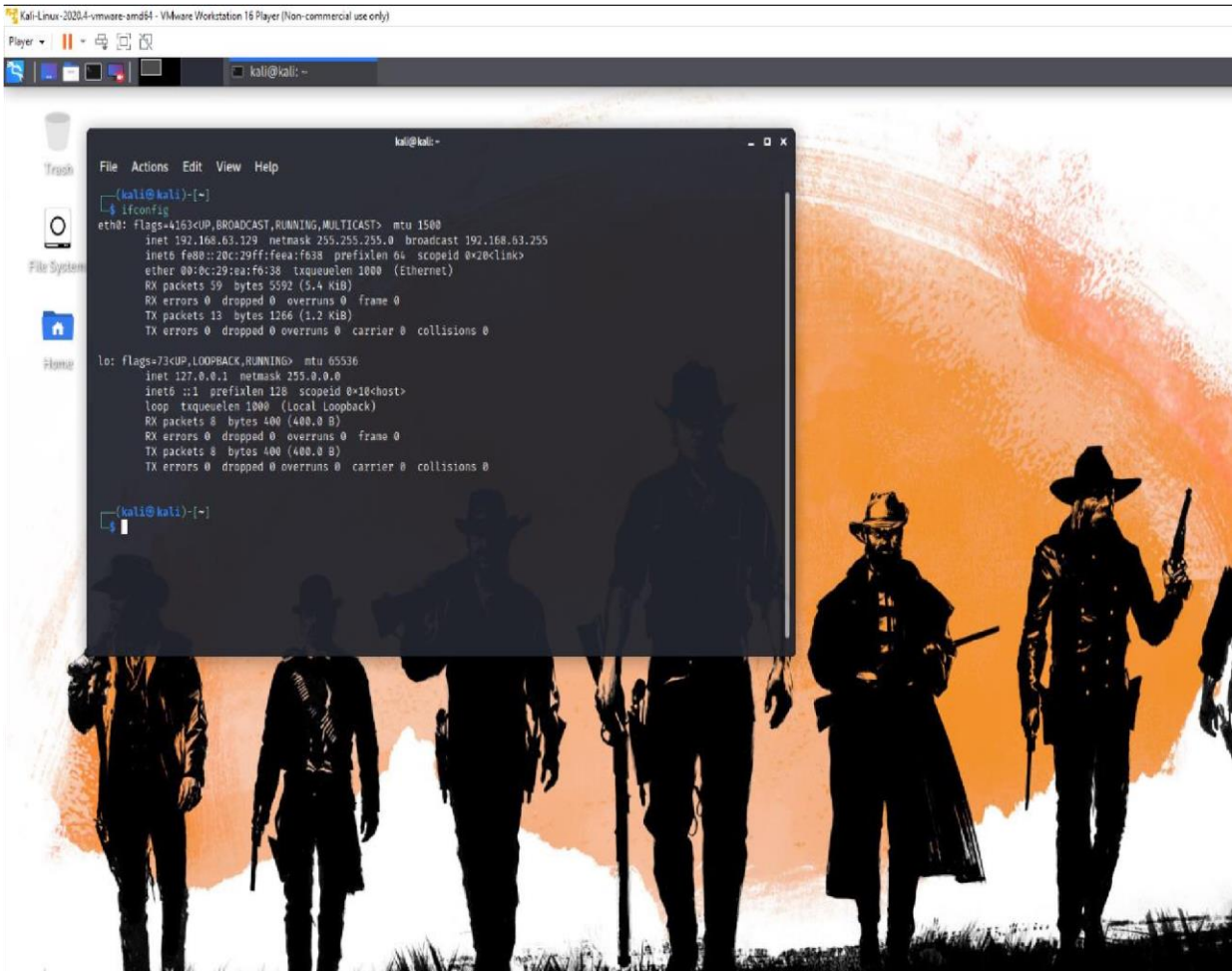
- DNS spoofing is a technique used by the attackers to direct traffic from a legitimate website to an altered website.
- DNS Cache poisoning is the other name of this technique.
- To use a fake or duplicate website to collect, and record user information like login credentials, credit card, bank details, etc.
- DNS server poisoning and Man-in-the-middle (MiTM) are the 2 different ways we can conduct this attack.
- For the scenario, we will use a man-in-the-middle attack base.

1.2 Attack Related Information

❖ Target is a Windows 10 VM that has an IP address **192.168.63.135**

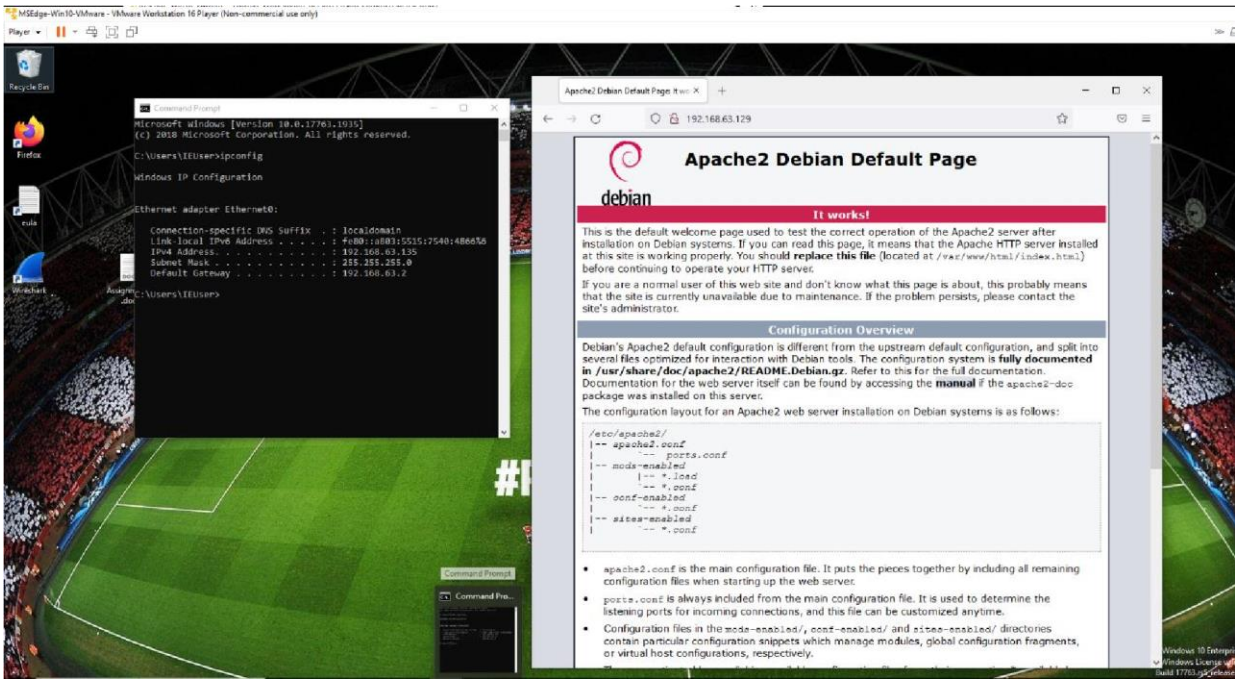


- The Attacker is a Kali VM that has an IP address **192.168.63.129**

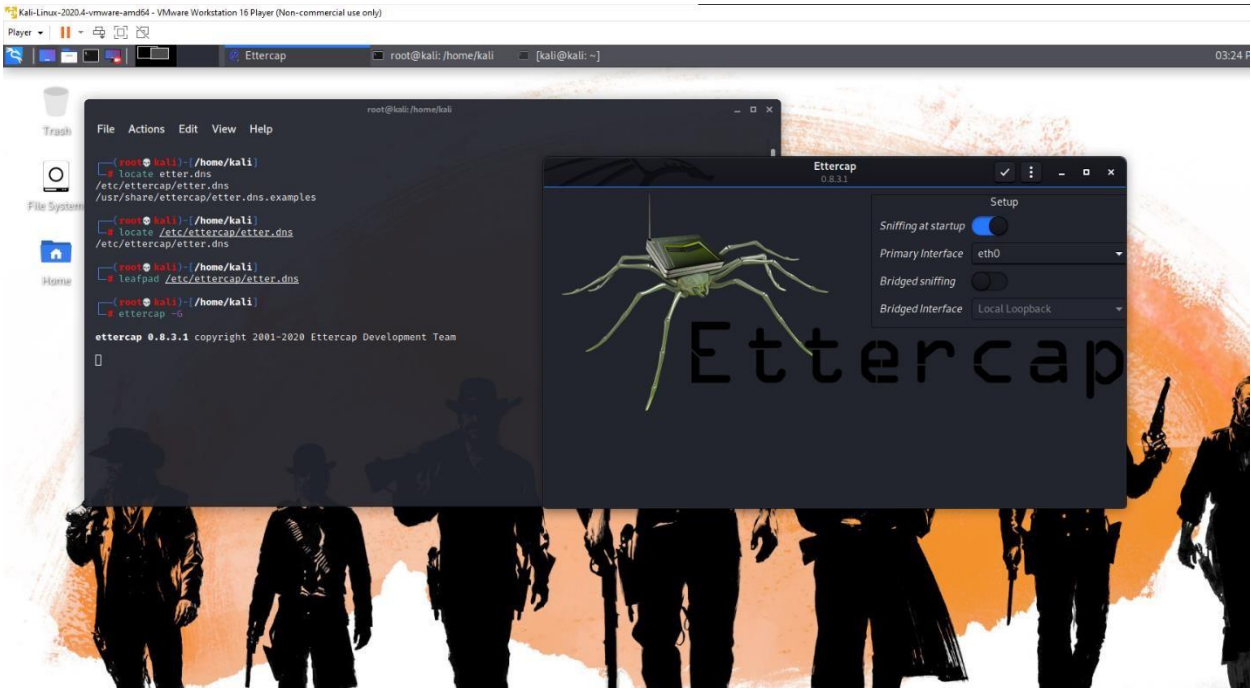


- No amplifiers were used for the attack
- The attack was successful
- **Note: The attack was successful because an illegitimate website was redirected for the user.**
- Redirection to a fake website from the original website is the result we intend to get.

- The result we got was a successful redirection to the site we intend to get i.e.



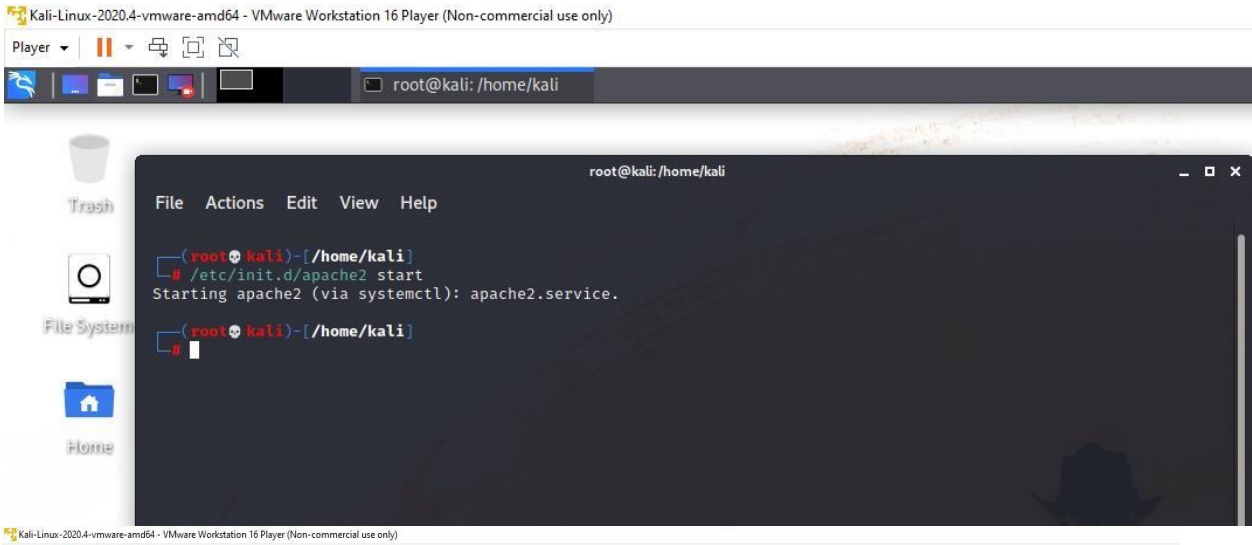
- The Tool used is **Ettercap**

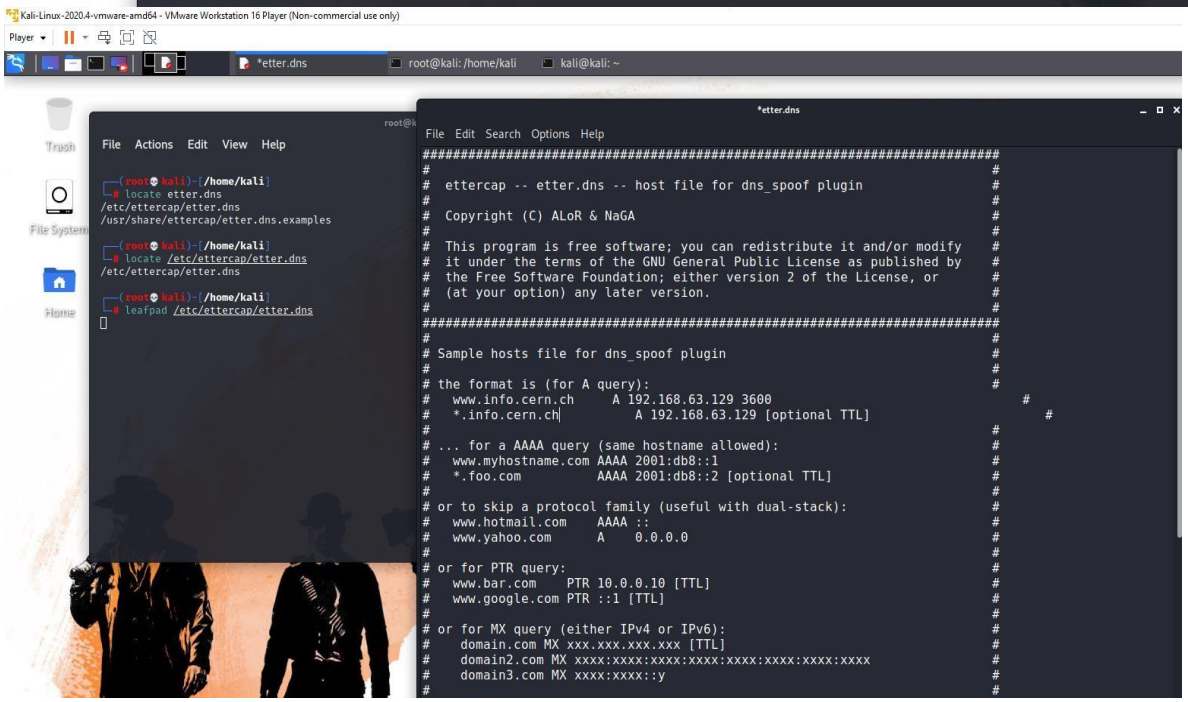


1.3 How the attack was conducted

- First, I started the Apache server with the command **/etc/init.d/apache2 start**

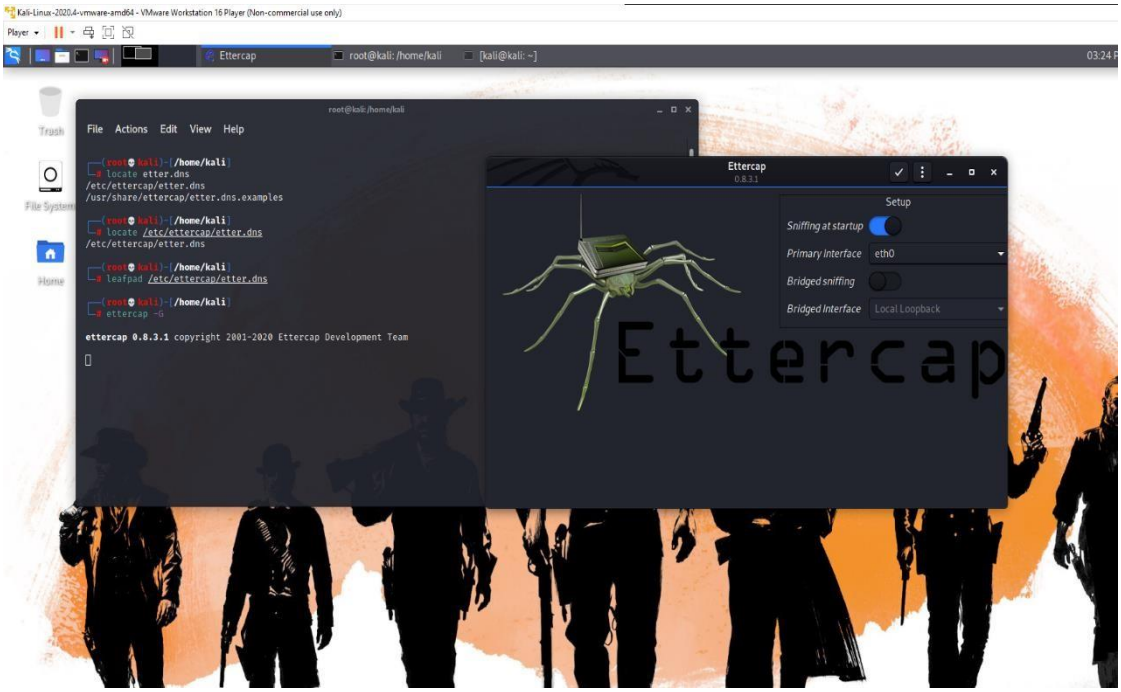
- Then I located and edited the etter.dns file with the website name I want to redirect it to. The website is www.info.cern.ch.



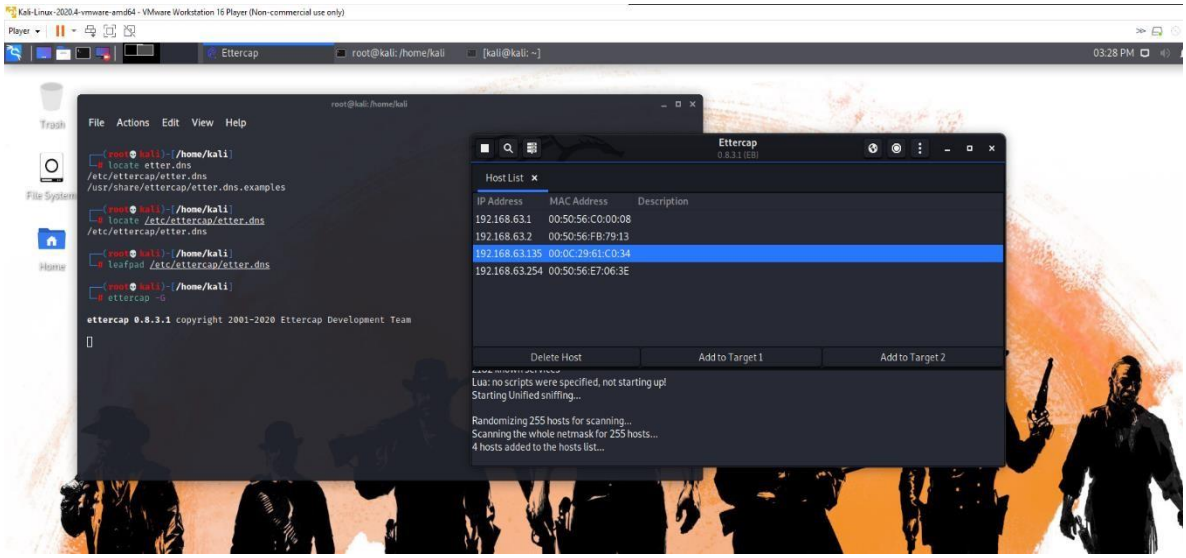


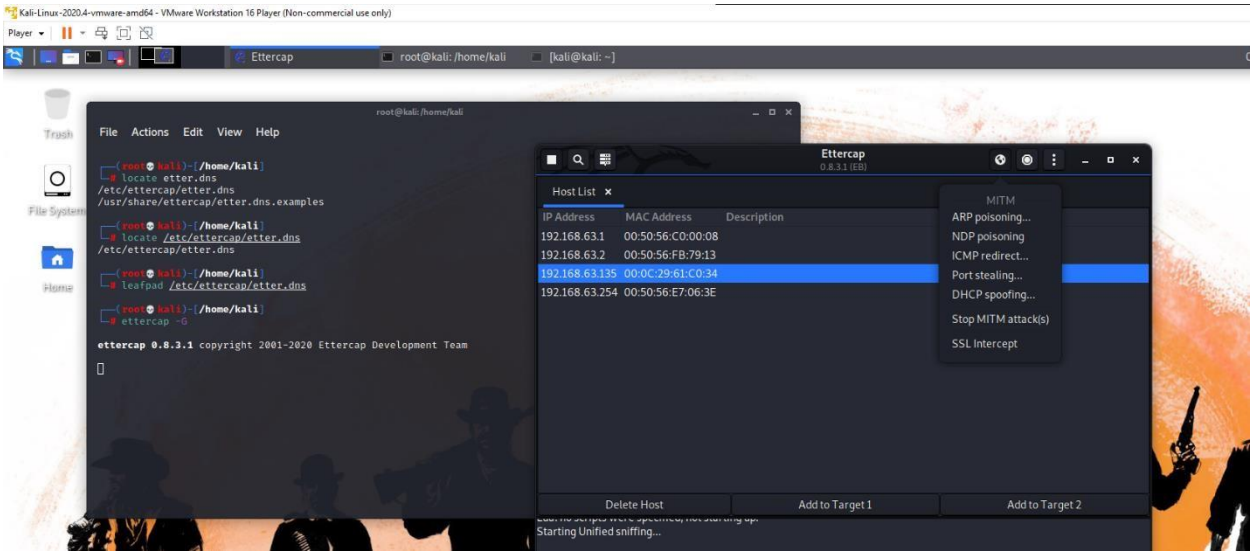
- The command I used for this is locate **etter.dns, locate /etc/Ettercap/etter.dns** and **leafpad /etc/Ettercap/etter.dns** to edit and save file.

- To start the Ettercap GUI, I ran the command **Ettercap -G.**

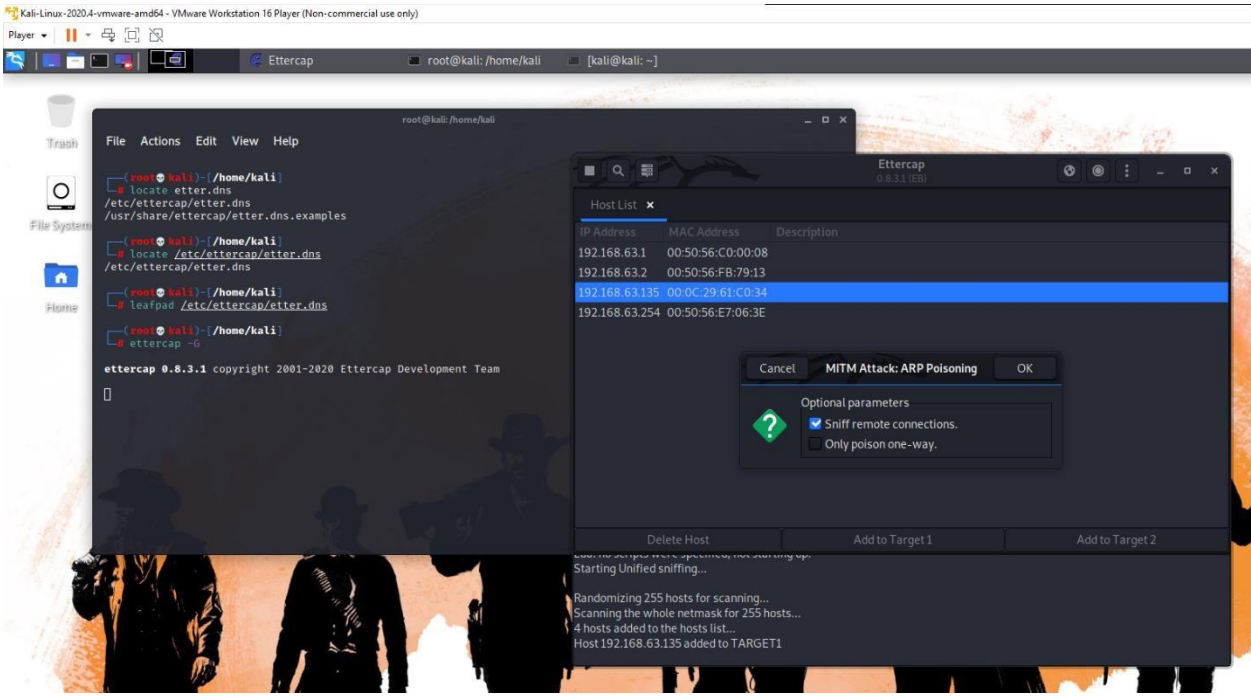


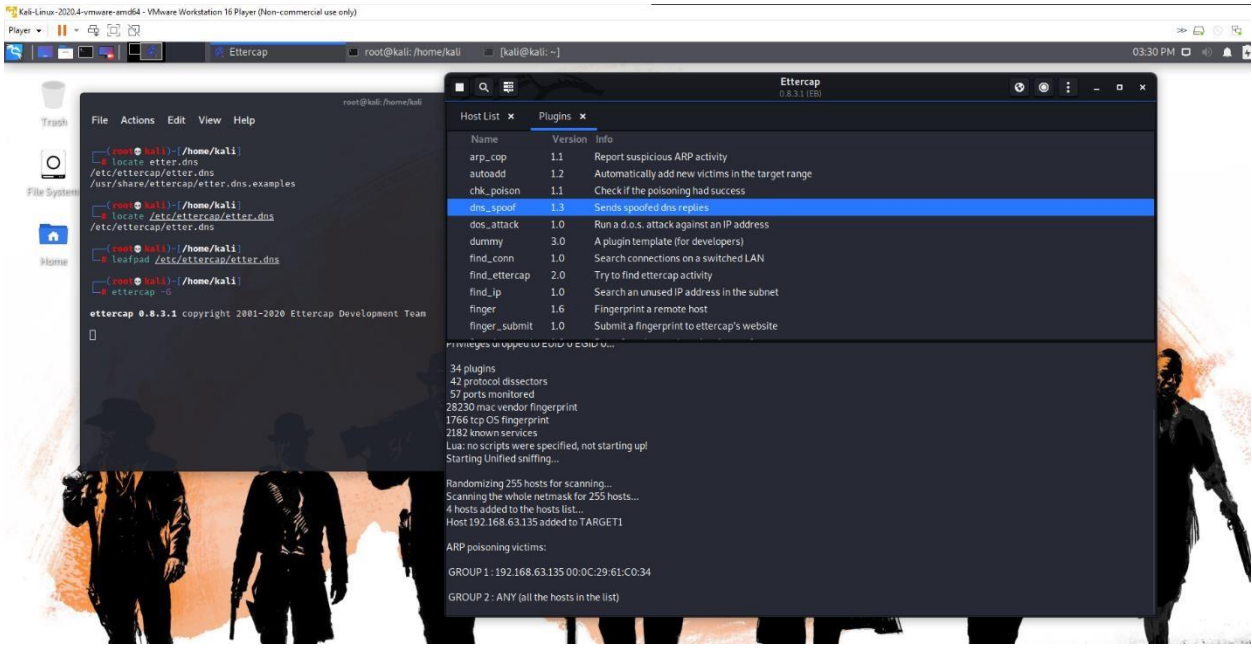
- Then I added the target machine IP to Target 1 list.





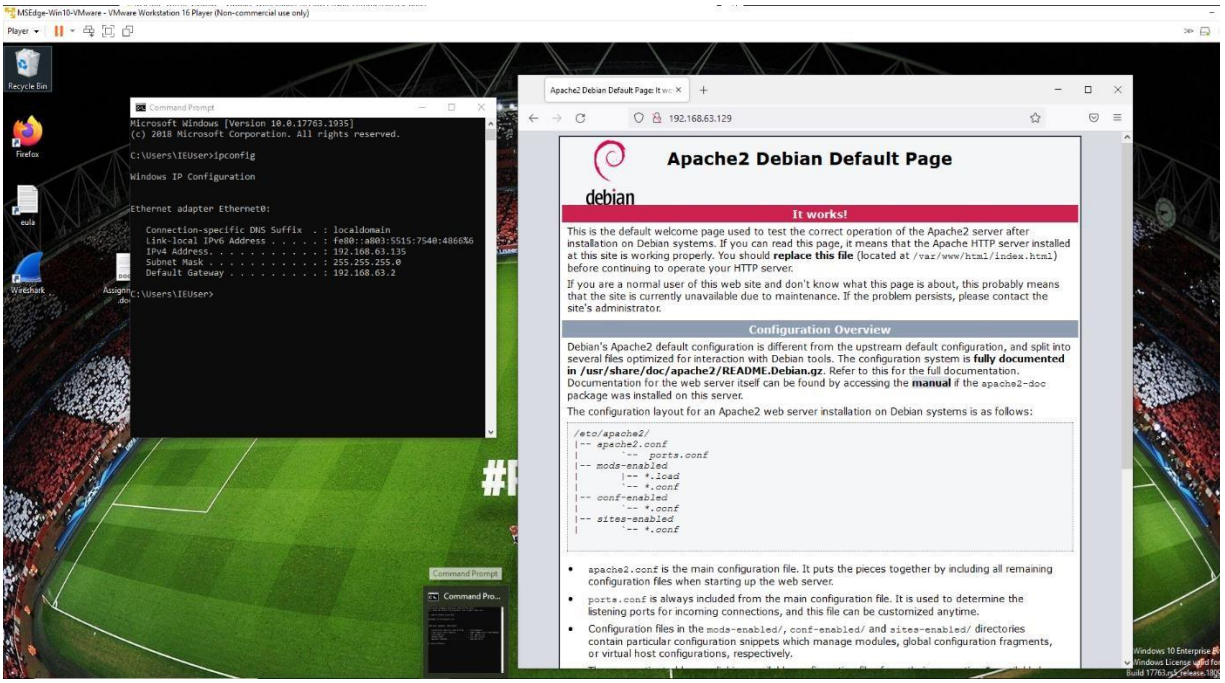
Then I started the ARP spoofing attack and then the min-in-the-middle module.





Next, I navigated to the plugins and selected dns_spoof version 1.3 to send spoofed DNS replies

- When launching the website in the Windows VM, the website was redirected to the illegitimate website.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Wireshark
Command Prompt
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\IEUser>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::a803:5515:7540:4866%6
IPv4 Address. . . . . : 192.168.63.135
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.63.2
C:\Users\IEUser>
Apache2 Debian Default Page: It wo
192.168.63.129
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
Command Prompt
Command Pro...

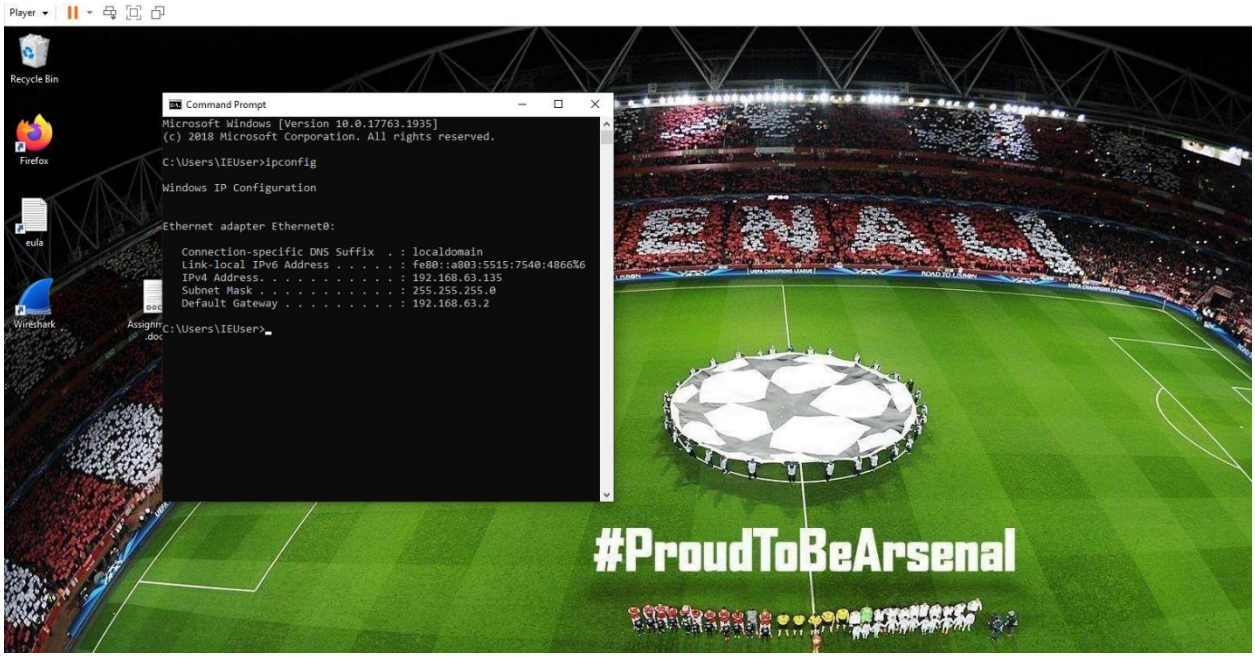
2 ARP SPOOFING

2.1 General Information collected before the attack

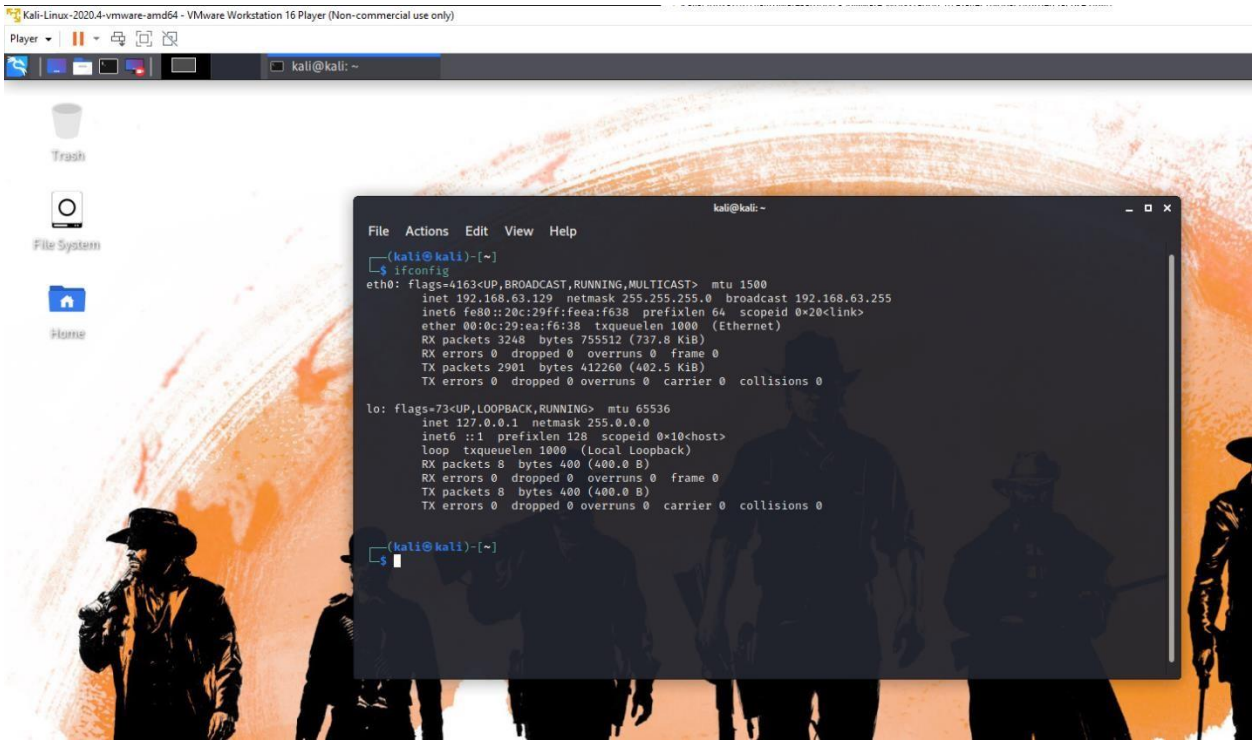
- The full form is ARP is Address Resolution Protocol. ARP's main task is to convert an IP address into MAC address or vice-versa making it possible to identify machines on different networks.
- The main use of the protocol as mentioned above is to redirect the user to a specific service the they requested or a specific machine on the network.
- If in case a request a some website is sent, the AR protocol will check the destination of the request with the ARP cache which is stored in the host machine.
- This acts as a bridge between MAC address and IP address.
- The protocol only works with 32-bit IPv4 addressing standards and was not built keeping in mind the factor of security.
- This attack requires the attacker to be in the same network as the target machine to conduct the attack.
- The attack is a MiTM attack without the use of any other plugins or filters.

2.2 Attack Related Information

- Target is a Windows 10 VM that has an IP address **192.168.63.135**



- Attacker is a Kali VM that has an IP address **192.168.63.129**

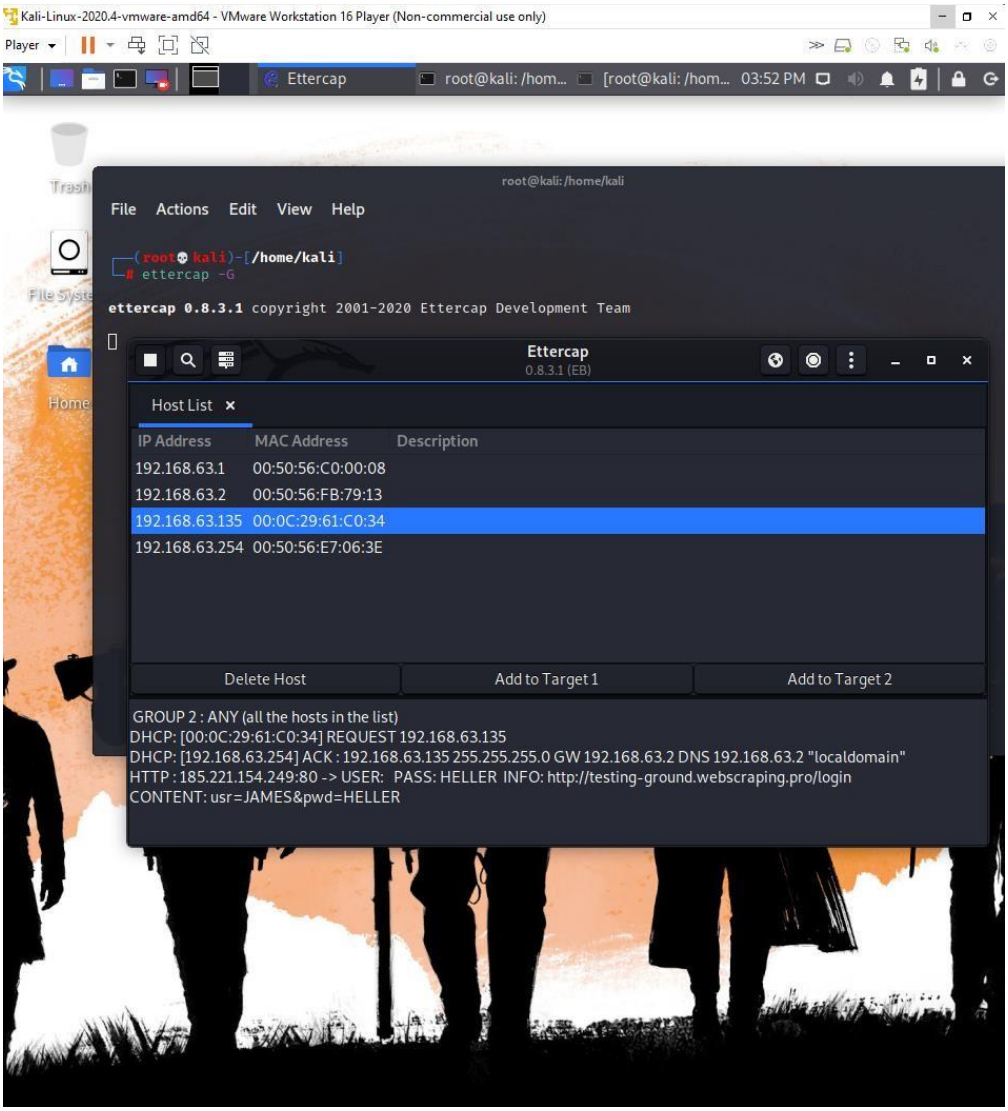


- The attack Status: Successful

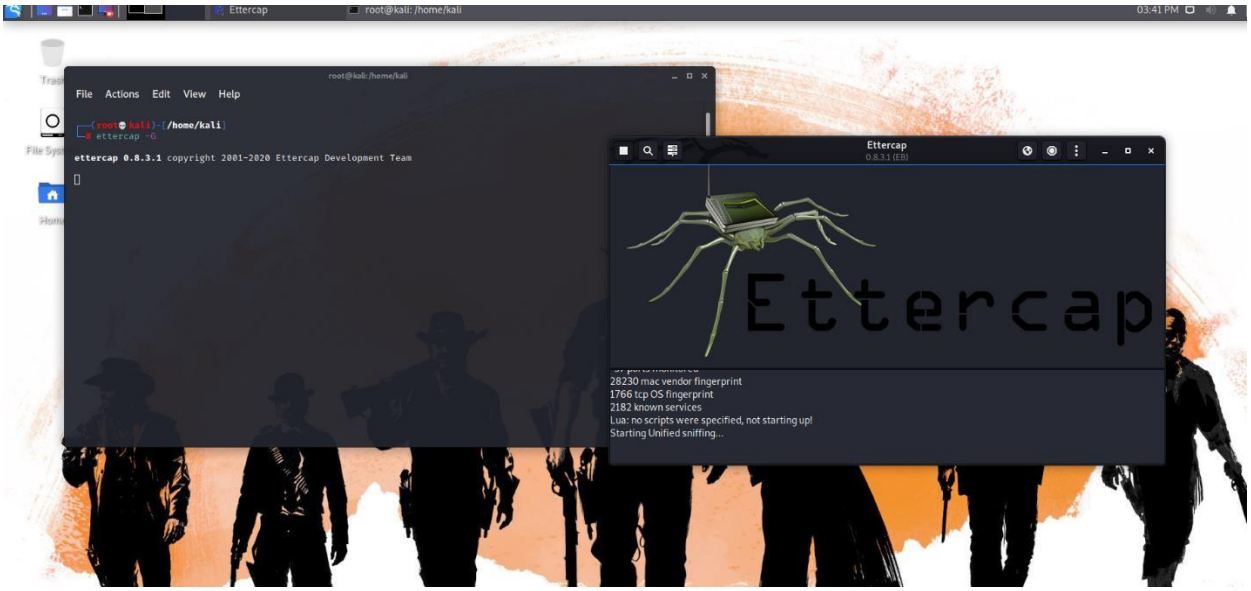
- **Note: The attack was successful because the credentials of the user were recorded in the Ettercap GUI.**

- The intended result of the attack was to be able to conduct a man-in-themiddle attack using ARP poisoning and later being able to see data accessed by the target and possibly extract and record any type of login credentials to any website.

- **Results achieved the credentials were recorded when the target logged in using the website. Listed on next page.**

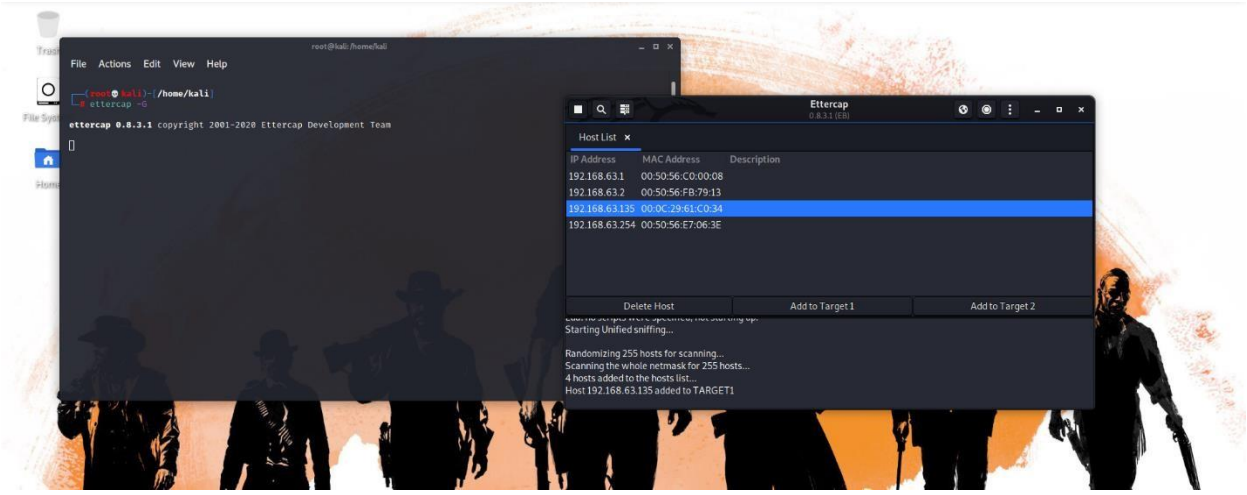

Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Ettercap
root@kali: /hom...
[root@kali: /hom...
03:52 PM
root@kali: /home/kali
File Actions Edit View Help
(root kali)-[/home/kali]
ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
Ettercap
0.8.3.1 (EB)
Host List
IP Address MAC Address Description
192.168.63.1 00:50:56:C0:00:08
192.168.63.2 00:50:56:FB:79:13
192.168.63.135 00:0C:29:61:C0:34
192.168.63.254 00:50:56:E7:06:3E
Delete Host
Add to Target 1
Add to Target 2
GROUP 2 : ANY (all the hosts in the list)
DHCP: [00:0C:29:61:C0:34] REQUEST 192.168.63.135
DHCP: [192.168.63.254] ACK : 192.168.63.135 255.255.255.0 GW 192.168.63.2 DNS 192.168.63.2 "localdomain"
HTTP : 185.221.154.249:80 -> USER: PASS: HELLER INFO: http://testing-ground.webscraping.pro/login
CONTENT: usr=JAMES&pwd=HELLER

- Tools used- Ettercap

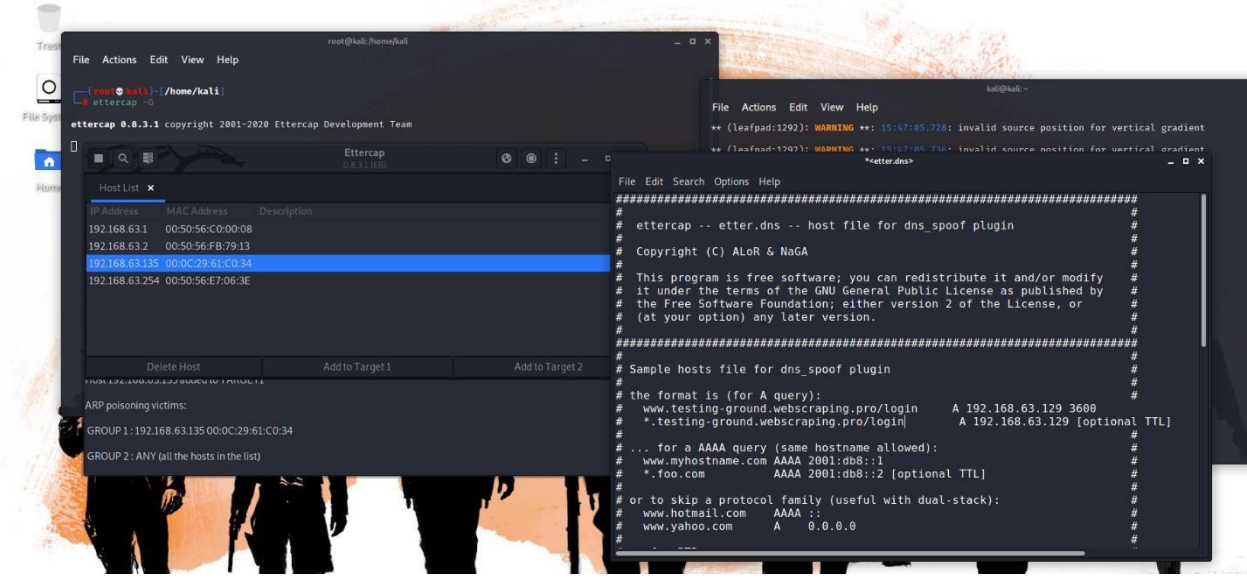


2.3 How the attack was conducted

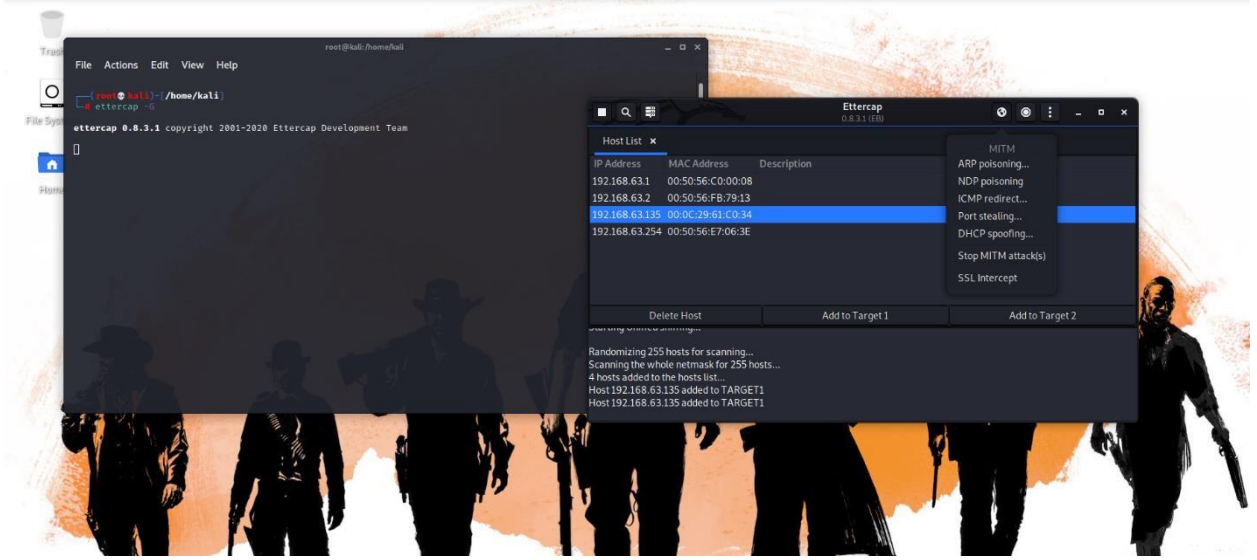
- The attack steps for ARP spoofing are somewhat similar to DNS spoofing.
  - No addition or changes are needed for the attack like in the previous attack.
- Because this attack focuses on just monitoring, nothing is needed to be tempered but the focus is more towards collecting information.
- First open Ettercap and Scan for hosts. Command: **ettercap -G**



- Edit the file **ettercap.dns and** add the website name u want to use to record credentials in the file which is **testing-ground.webscraping.pro/login** for this case.

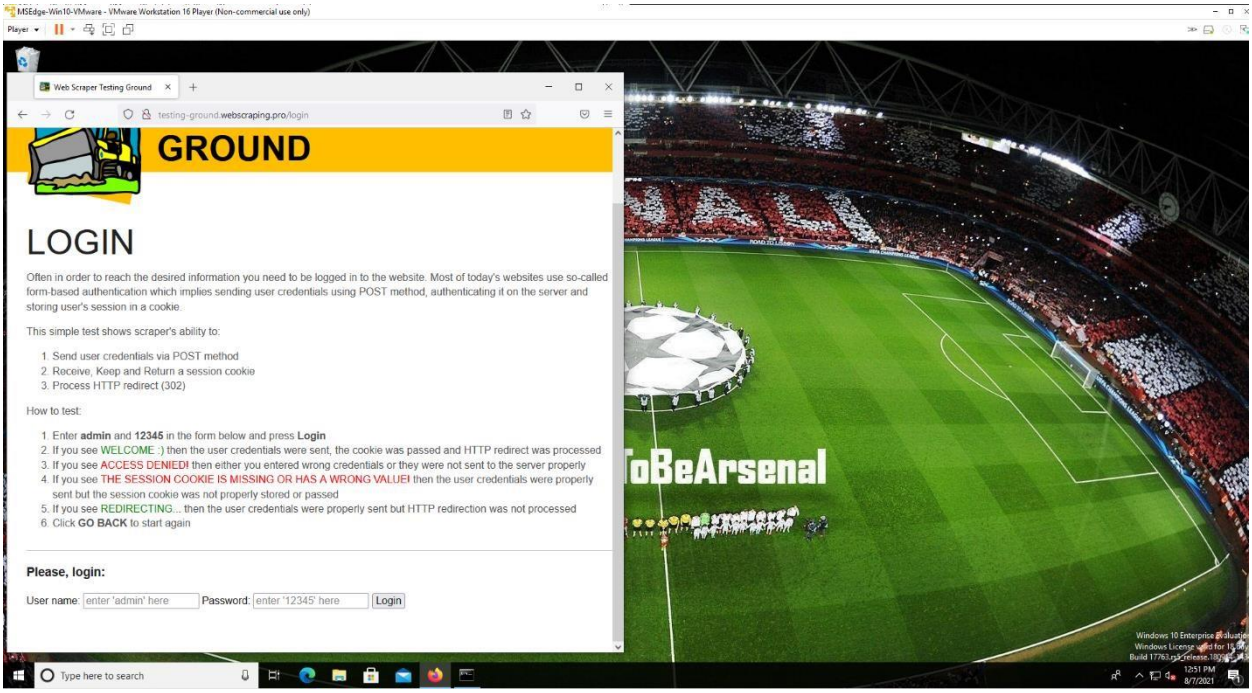


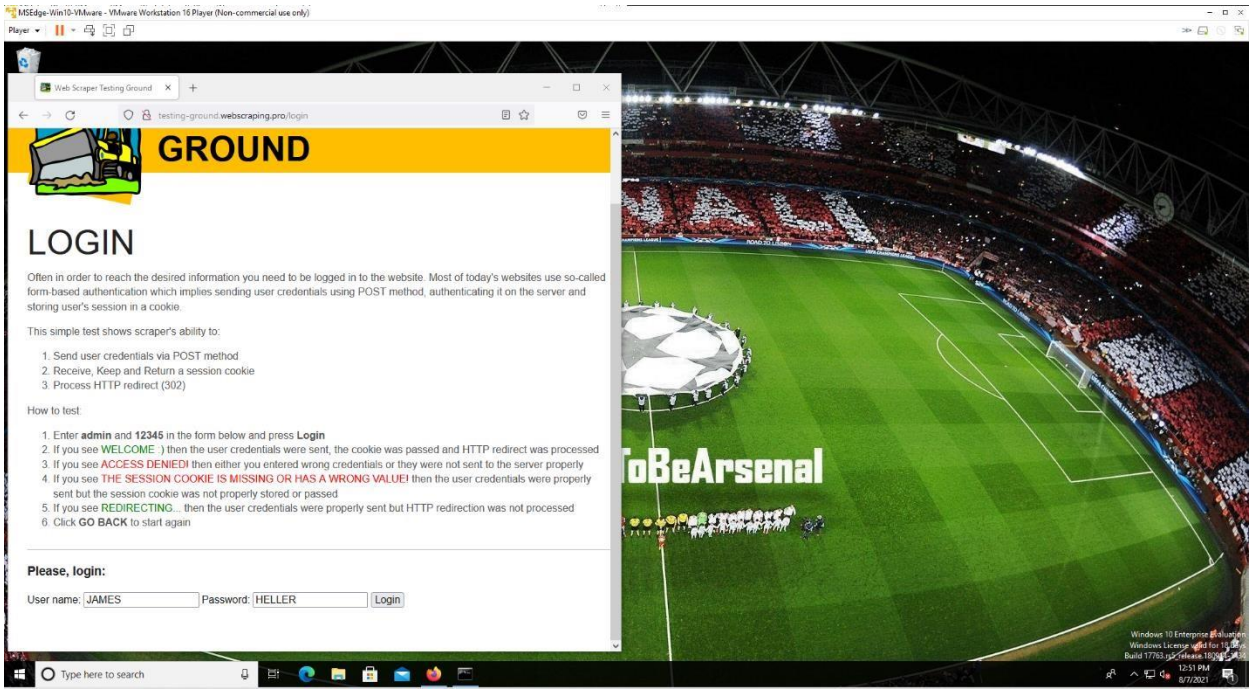
- Once the hosts are scanned and listed select the IP address of the target machine and add it to the target 1 list. Now, select ARP poisoning.



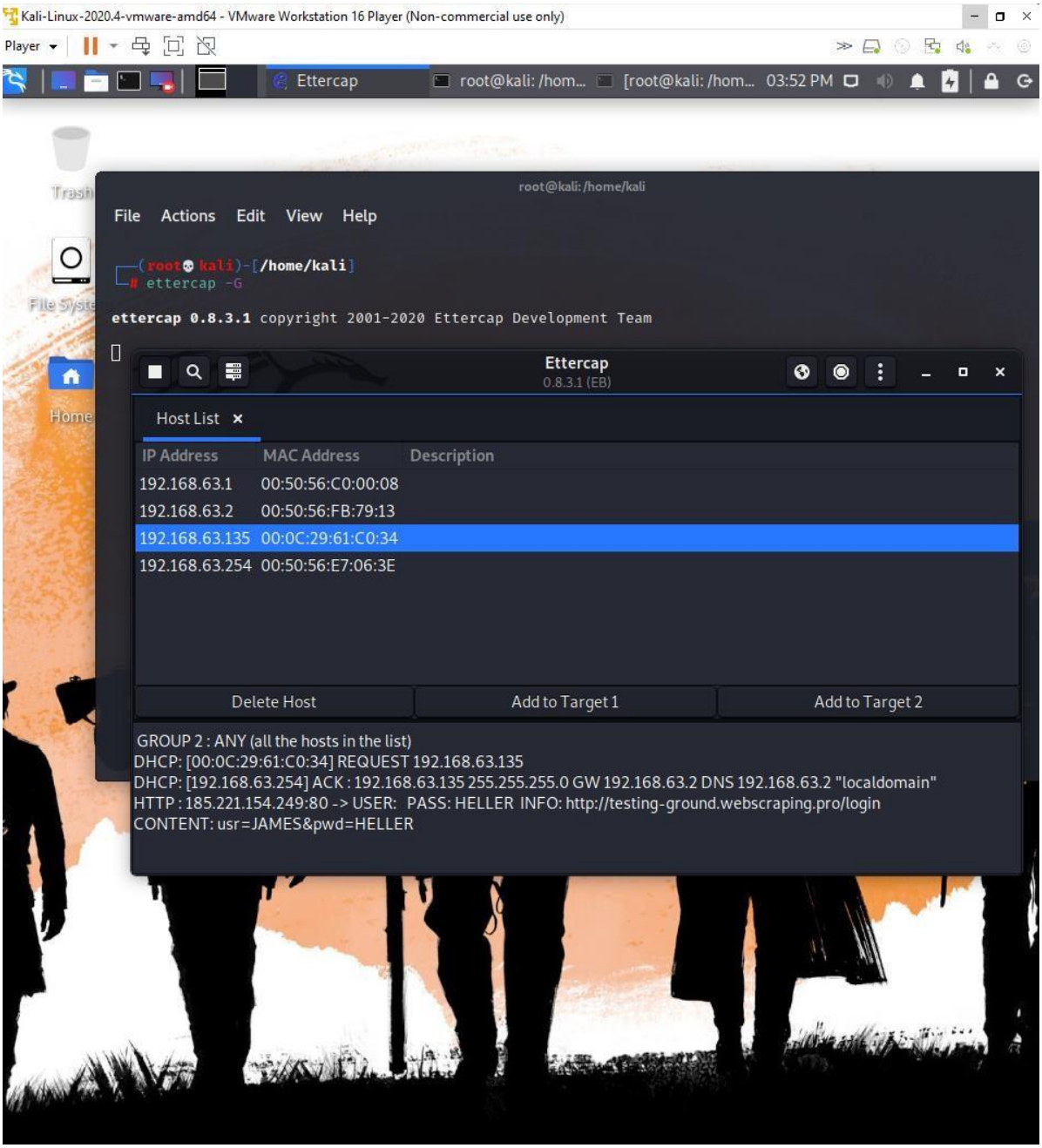
- **Now,** we will initiate ARP spoofing from the man-in-the-middle attack menu. No need to add any plugins for this attack.

- Then using the website, a new user will be created for e.g. I created the user: JAMES and password: HELLER





- **The main motive of this attack was to record the user credentials in the Ettercap GUI which can be seen in the image below.**



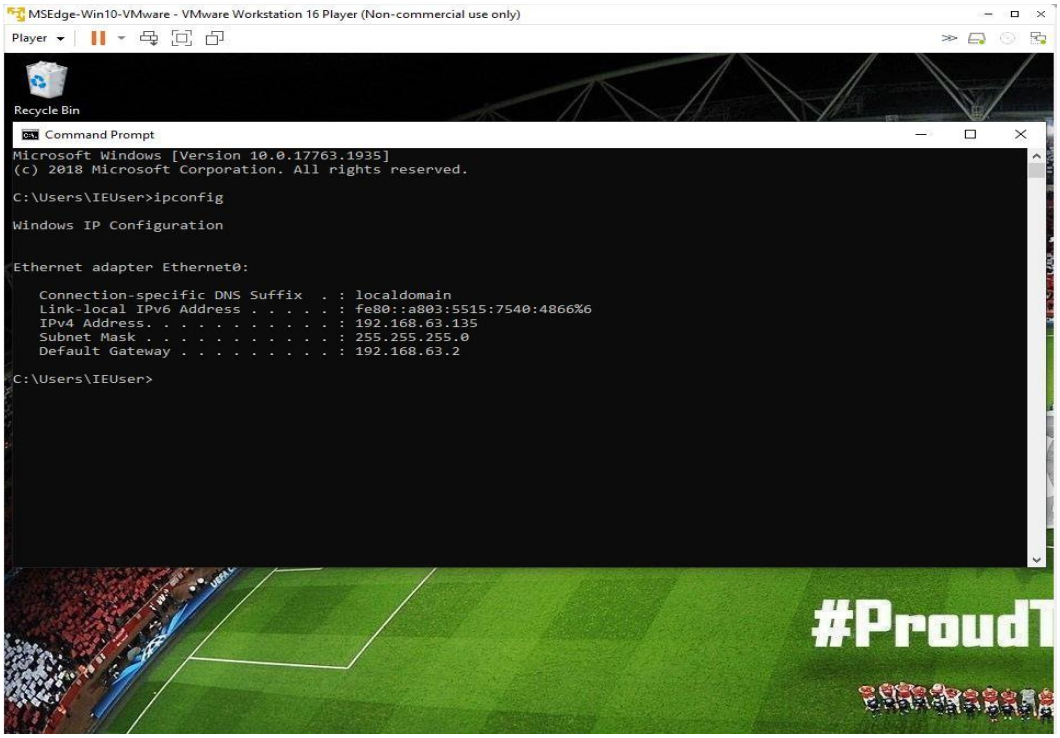
3. Smurf DoS Attack

3.1 Before Attack General information

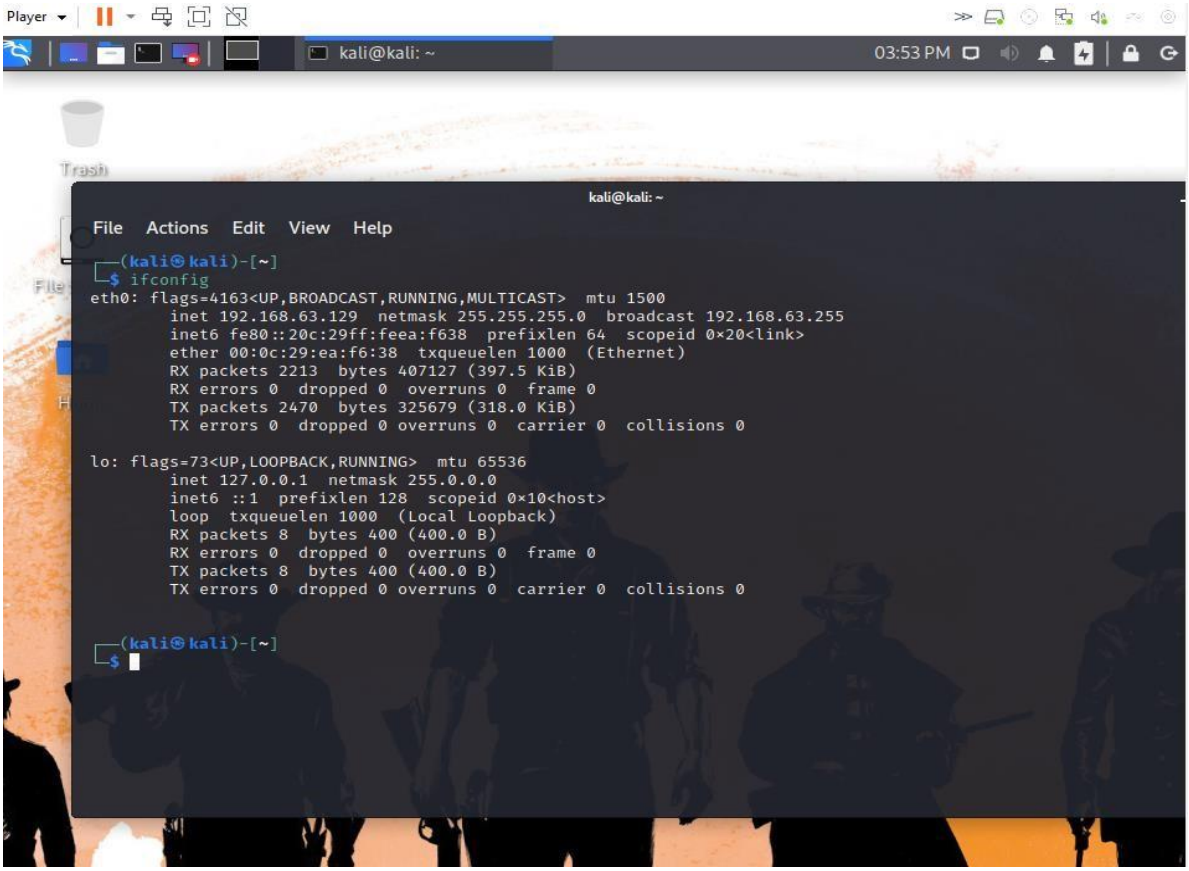
- Distributed Denial of Service (DDoS) attack is the type of attack smurf is related to.
- In the attack, Internet Control Message Protocol ping flooding is used instead of SYN packet flooding.
- However, the ping flooding part like the other DDoS attack is the same, but the protocol is altered to ICMP from common SYN.
- To determine if the packet is transmitted to the destination, ICMP is responsible and it also keeps a track how much data was lost or received.
- The potential of the attack to exploit IP and ICMP vulnerabilities this attack is very dangerous.

3.2 Attack Related Information

- Target is a Windows 10 VM that has an IP address **192.168.63.135**

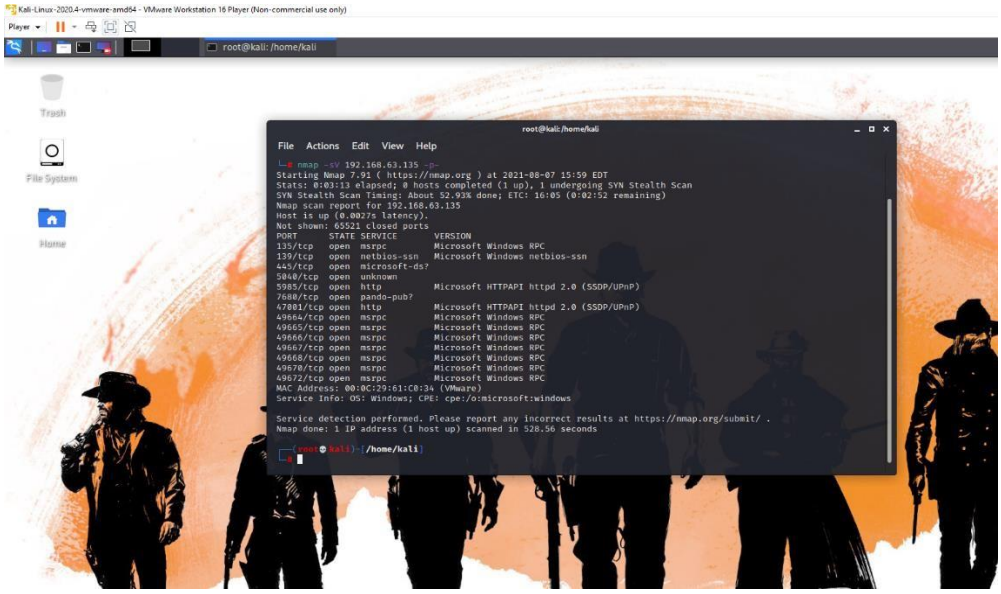


- Attacker is a Kali VM that has an IP address **192.168.63.129**



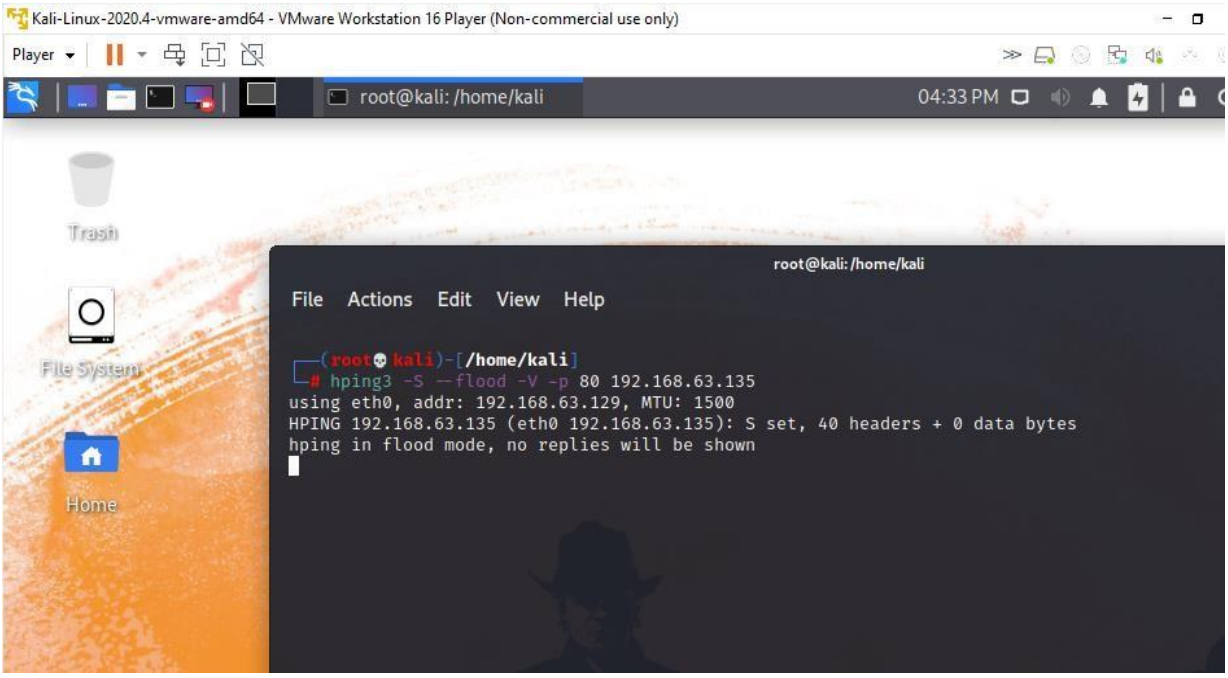
- For the attack the Amplifier is ICMP (Internet Control Message Protocol) ○ The attack Status: Successful
- **Note: The attack was successful because the system slowed down after millions of packets were sent using HPing3 command.**

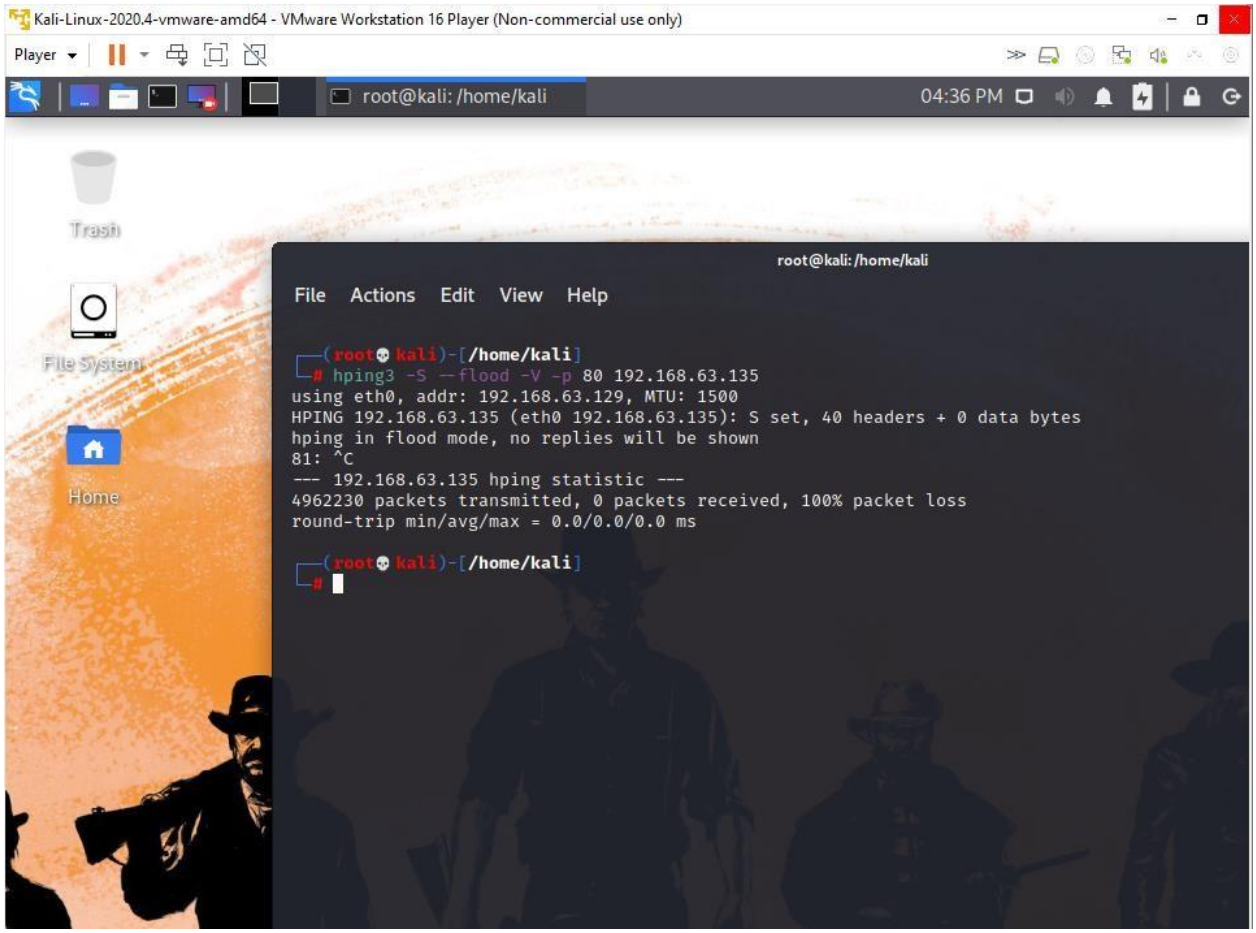
- Port number 135 msrpc(Remote Procedure Call) was targeted with the help of a nmap scan as shown in the image below



- The intended Result was a slowdown of the target Machine till the machine collapses
- Achieved result was however different from the expected result as the machine slowed down but not collapsing.

- Tool used for the attack is Hping3. Around 5 million packets were sent.



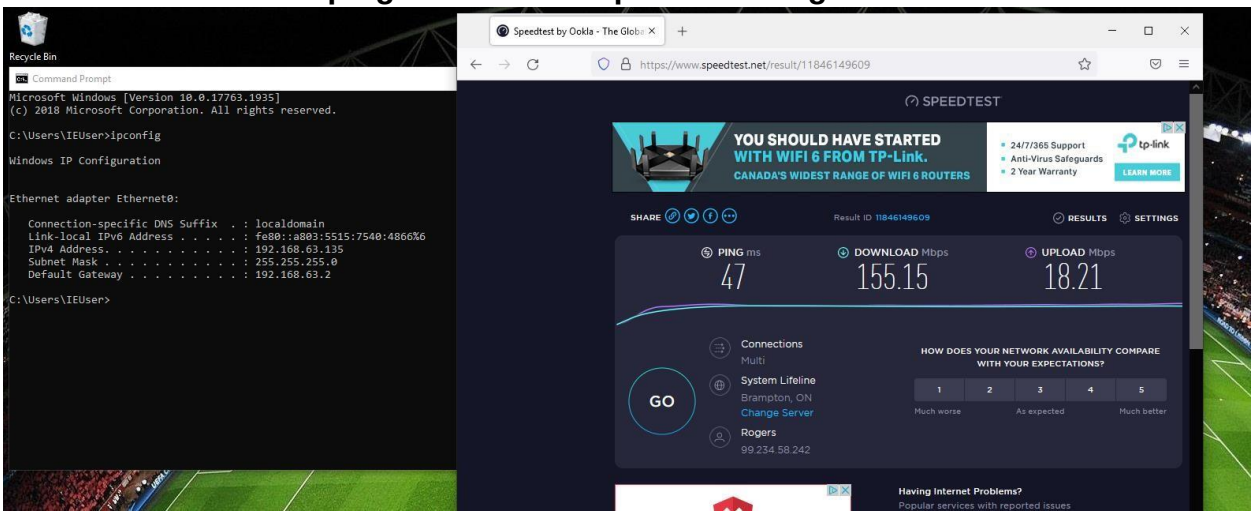


3.3 How the attack was conducted

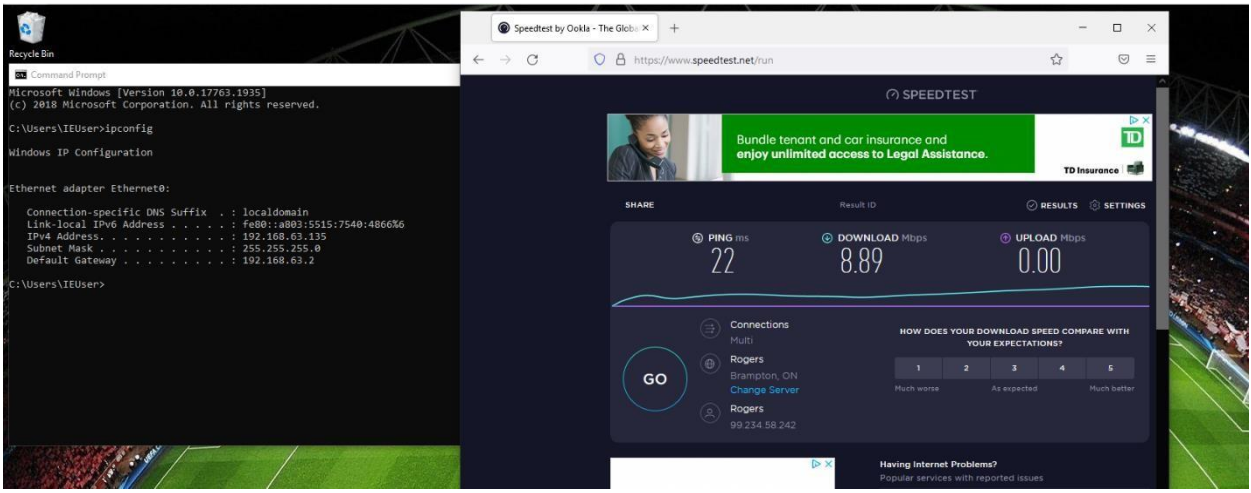
1. First on the Target machine, IP address configuration was extracted using the ipconfig command.
2. Secondly, Nmap scan was performed from the attacker machine for the target machine which is Windows VM in this case. ALL the open services and ports were identified from this scan.
3. Next, Hping3 which is used to send an ICMP flood was run in the kali VM on port number 135.
4. The command used for this was: **hping3 -1 –flood -V -p 135 192.168.63.135**
    a. The number 1 indicates ICMP packets
    b. –flood is used here to mention the initiation of the DoS attack.
    c. -V here indicates verbosity
    d. -p indicates port which is 135 in this case.
    e. And the end of the command the IP address is mentioned

5. **Result can be seen immediately, however the hping3 impacts ipv6 more than ipv4 in the Windows 10 platform but on comparing the internet speed before the attack and after the attack we can see the difference.**

a. Before the attack the ping and internet speed were high.



b. After the attack the ping decreased due to more incoming packets and internet speed dropped.



4 Conclusion

All 3 attacks were successful and the reasons for their success and how it works are listed in the respective attack data above.

5 References

- https://www.veracode.com/security/arp-spoofing
- https://en.wikipedia.org/wiki/ARP_spoofing
- https://www.okta.com/identity-101/arp-poisoning/
- https://en.wikipedia.org/wiki/DNS_spoofing

https://www.imperva.com/learn/application-security/dns-spoofing/ ○ https://www.varonis.com/blog/dns-cache-poisoning/

○ https://www.imperva.com/learn/ddos/smurf-attack-ddos/ ○ https://en.wikipedia.org/wiki/Smurf_attack ○ https://tools.kali.org/information-gathering/hping3