



slingshot college
(इस्लिङ्गटन कलेज)

Module Code & Module Title
CC5004NI Security in Computing

Assessment Weightage & Type
30% Individual Coursework

Year and Semester
2021 -22 Autumn

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: May 5, 2022

Assignment Submission Date: April 28, 2022

Word Count: 3270

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Abstract

The following paper is based on a theoretical and practical investigation of ethical hacking to identify vulnerabilities and improve the security of any organization's or institution's system. The report is divided into sections that must be completed in a specific order. The introduction to DNS and DNS spoofing is clearly detailed at first, as is the current DNS spoofing scenario. The goal of completing this report is described in detail. The article details the ethical hacking technique used to target Windows 7 using Kali Linux. The DNS server was hacked with the use of an inbuilt program in Kali Linux called Ettercap, which helped in the execution of the attack. DNS spoofing is demonstrated on a Windows computer, and the mitigation strategy is also presented with detailed explanations. Ettercap is an open-source sniffer and ARP cache poisoning tool, will be reviewed and analyzed in this study. Ettercap conducts man in the middle attacks on one or more targets by poisoning their ARP cache using the unsecure ARP protocol. On a switched local area network, it can sniff passwords, instant messaging, e-mails, and much more. The major goal of this paper is to inform administrators about packet sniffing techniques used on switched networks so that they may be prepared to deal with such tools.

Table of Contents

Abstract.....	i
Table of Contents.....	ii
Table of Figures.....	iv
1. Introduction.....	1
1.1 Problem Statement.....	2
1.2 IP Spoofing Statistics.....	2
1.3 Aims and Objectives.....	4
2. Background.....	5
2.1 History.....	5
2.2 Current Scenario.....	5
3. Demonstration.....	7
3.1 GNS3.....	7
3.2 Ettercap.....	7
3.3 Attack Process.....	8
3.3.1 Topology.....	8
4. Mitigation.....	21
4.1 Firewall.....	21
4.2 Access Control List (ACL).....	24
5. Evaluation.....	26
5.1 Pros of the applied mitigation strategy:.....	26
5.2 Cons of the applied mitigation strategy:.....	26
5.3 Cost Benefit Analysis (CBA).....	26
5.4 Application Area.....	28
6. Conclusion.....	29

7. References..... 30

Table of Figures

Figure 1: DNS Spoofing	1
Figure 2: Statistics of IP Spoofing	3
Figure 3: Statistics of DNS Attacks	6
Figure 4: GNS 3	7
Figure 5: Ettercap.....	7
Figure 6: Network Topology	8
Figure 7: Client's IP address	9
Figure 8: IP Information of Attacker.....	10
Figure 9: Ping scan to all hosts in the network	10
Figure 10: Routing table	11
Figure 11: Finding the location of etter.dns	11
Figure 12: Opening etter.dns with text editor.....	12
Figure 13: Locating index.html file.....	12
Figure 14: Opening index.html in text editor.....	12
Figure 15: Editing the index.html file	13
Figure 16: Opening Ettercap GUI from terminal	13
Figure 17: Sniffing in Unified mode from Ettercap.....	14
Figure 18: Selecting the network interface	15
Figure 19: List of hosts connected in the network	15
Figure 20: Adding 2 connected hosts as targets	16
Figure 21: Starting Apache web server	16
Figure 22: Initiating Man in the middle attack	17
Figure 23: Sniffing remote connections	17
Figure 24: Navigating to plugins.....	18
Figure 25: Selecting the dns_spoof plugin	18
Figure 26: Initiating the sniffing process	19
Figure 27: Accessing Facebook through IP address from victim's pc	19
Figure 28: Accessing Facebook through dns from victim's pc.....	20
Figure 29: Enabling Firewall.....	22
Figure 30: Spoofed packets blocked after turning on firewall	23

Figure 31: ACL Configuration.....	24
Figure 32: Spoofed packets blocked after ACL Configuration.....	25

1. Introduction

DNS stands for Domain Name System, which is one of the internet's essentials that is utilized by all internet users every day to accomplish their day-to-day jobs, check emails, or just spend time on their smartphone, although most people outside of networking are unaware of it. In simple terms, DNS is a dictionary of names that correspond to numbers, with the numbers in this case being IP addresses, which are used to communicate from one computer to another. In layman's terms, DNS is similar to our phone contact list, which links names to phone numbers or email addresses. As a result, each time the user types in the domain name, it is mapped to the associated unique IP address, allowing the web contents to be downloaded and shown in the browser.

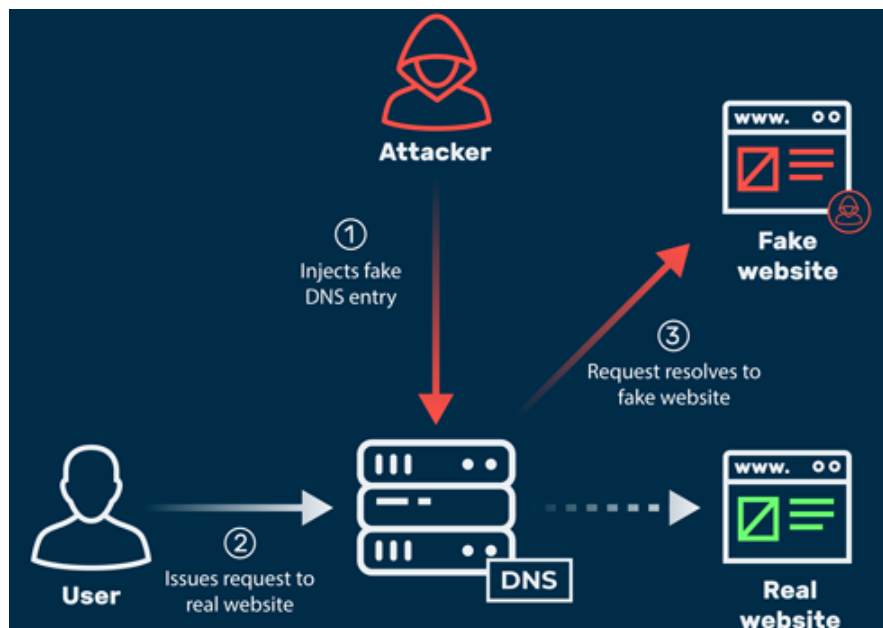


Figure 1: DNS Spoofing

(Sesni, 2021)

When an unauthorized individual changes the phone number of a certain person in our contact list and adds others who are unknown to us, we are inadvertently calling the wrong person whom the attacker wants us to call. That is, in fact, how DNS spoofing works. DNS spoofing happens when a hacker modifies the records in a name server's DNS resolver cache. This traffic redirection allows the attacker to transmit malware, steal data, and show unwelcome information, among other things. The attacker can even drive us to a fake website that is designed to seem like the actual site or an entirely other website.

1.1 Problem Statement

Any system based on trust has the advantage of being simple to create, but it also carries the risk of being exploited. This is highly beneficial for scaling systems since it allows all users to be tracked. However, the Internet has gone well beyond a small system with well-known users, and as a result, systems based on user trust no longer meet its requirements. DNS is a trifecta of security problems since it makes authentication optional while propagating information quickly and widely. Attackers have a lot to gain by taking advantage of the confidence that Internet users have in the DNS infrastructure. Attackers can utilize spoofed packets and changed cache entries to deceive users into revealing personal information to unreliable websites or installing malware that can damage their machine. It's critical that we reconsider our DNS usage and look at ways to defend ourselves against such attacks.

1.2 IP Spoofing Statistics

The charts below depict spoofing results using several types of aggregation. They only utilize the most recent test from each client IP address, as well as tests from the previous year. Because most tests are conducted behind a NAT, the findings are divided into tests conducted without a NAT and tests conducted with a NAT (with and without NAT). Excluded are tests that could not determine if spoofing or blocking occurs.

The rest of the tests are initially grouped into IP blocks (/24 for IPv4 and /40 for IPv6). Blocks with consistent results from different IP addresses are called "spoofable" or "unspoofable," whereas blocks with inconsistent results from different IP addresses are labeled "inconsistent" (Caida, 2022).

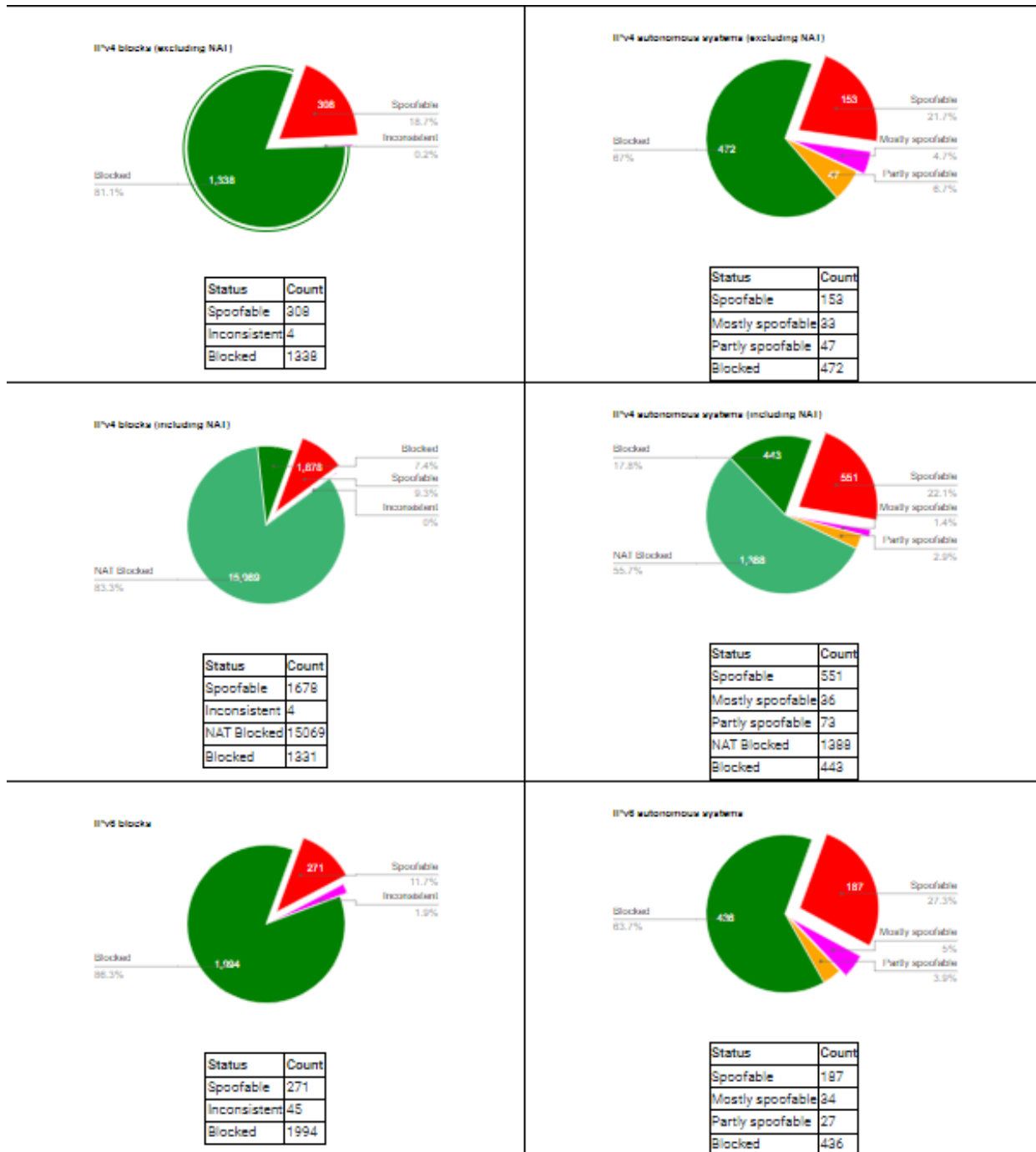


Figure 2: Statistics of IP Spoofing

(Caida, 2022)

1.3 Aims and Objectives

The goal of this report is to break down the cyber threat known as "Domain Name System (DNS) Cache Poisoning." The purpose of this report is to learn about the following:

- A definition of DNS cache poisoning.
- Real-world instances of DNS cache poisoning.
- An introduction to the DNS technology.
- The DNS Cache's function within DNS.
- Techniques used by cybercriminals to obtain information from unsuspecting users by exploiting DNS vulnerabilities.
- Best practices for avoiding such attacks.

2. Background

2.1 History

Christoph Schuba published the article "Addressing Weaknesses in the Domain Name System Protocol" in 1993. In it, he identified several flaws, including DNS cache poisoning as a strategy. It used to be possible to provide additional information in a DNS reply packet that would be cached by the daemon. An attacker might use this to insert bogus information into a network's DNS cache, allowing them to commit man-in-the-middle attacks or other mischief. CERT issued advice CA-1997-22 in 1997, identifying a vulnerability in BIND, the Berkeley Internet Name Domain software, which is used by practically all Internet nameservers. This time, a fundamental concept was finally realized: BIND's transaction IDs were not random, but rather sequential. The transaction ID is the only method of authentication for a DNS response, aside from layer 3 and 4 protocol checks (source and destination IP addresses and ports must match). A cache poisoning attack may be carried out via a faked query followed by a spoofed answer since an attacker could simply guess the next transaction ID after making their own request. To address issue, BIND was modified to utilize randomized transaction IDs in all new versions. In 2002, Vagner Sacramento issued an alert revealing another another flaw in BIND's DNS implementation. He discovered that BIND would make numerous recursive requests for the same IP address at the same time. As a result, a mathematical phenomenon known as the "Birthday Paradox" comes into play (Stewart, 2003).

2.2 Current Scenario

On November 27, 2018, Cisco's Talos research department published a report highlighting the depths of a sophisticated cyber espionage initiative it dubbed "DNSpionage." The report stated that the perpetrators of DNSpionage stole email and other login credentials from several government and private sector targets in Lebanon and the UAE by hijacking the DNS server from these targets, and that all these email and VPN targets were redirected to an internet address controlled by the hackers. Between 2017 and 2019, many assaults were carried out at various organizations, as seen in the table below (Krebs on Security, 2019).

Malicious IP Address	Active Time Period	Affected Organizations' Country (Sector)
142.54.179[.]69	February 2017	Jordan (Government)
89.163.206[.]26	February 2017	Jordan (Government)
185.15.247[.]140	December 2017 and January 2018	Kuwait (Government) Albania (Government)
146.185.143[.]158	August 2018	UAE (Government)
128.199.50[.]175	September 2018	UAE (Unidentified Sector)
185.20.187[.]8	September 2018	UAE (Law Enforcement) UAE (Government) Lebanon (Government) Lebanon (Civil Aviation)
82.196.8[.]43	October 2018	Iraq (Government)
188.166.119[.]57	October 2018 and November 2018	Egypt (Government) Libya (Government)
206.221.184[.]133	November 2018	Egypt (Government)
37.139.11[.]155	November 2018	UAE (Unidentified Sector)
199.247.3[.]191	November 2018	Iraq (Government) Albania (Government)
185.161.209[.]147	November 2018	Lebanon (Insurance)
139.162.144[.]139	December 2018	Jordan (Government)
37.139.11[.]155	December 2018	UAE (Unidentified Sector)
178.62.218[.]244	December 2018	UAE (Government) Cyprus (Government)
139.59.134[.]216	December 2018	Sweden (Internet Infrastructure) Saudi Arabia (Internet Services) Lebanon (Internet Services)
82.196.11[.]127	December 2018	Sweden (Internet Infrastructure) U.S. (Internet Infrastructure)
46.101.250[.]202	December 2018 and January 2019	Saudi Arabia (Government)

Figure 3: Statistics of DNS Attacks

(Krebs on Security, 2019)

The number of DNS attacks that have been reported in the media can be seen clearly in the graph above. So, a DNS attack is a potentially dangerous attack that causes problems for users by stealing information such as emails, usernames, as well as other login credentials.

3. Demonstration

3.1 GNS3

GNS3 (Graphical Network Simulator 3) is a program that allows users to create, setup, test, and debug virtual and real-world networks. It enables the users to operate a modest topology on your laptop with only a few devices to large topologies with many devices hosted on numerous servers or even in the cloud (Galaxy Technologies LLC, 2021).



Figure 4: GNS 3

(Galaxy Technologies LLC, 2021)

3.2 Ettercap

Ettercap is a strong Unix-based packet sniffer and ARP cache poisoning tool. It can sniff MAC and IP addresses, intercept and manipulate packets, decode passwords, and target other Ethernet hosts with a denial-of-service attack (Bashir, 2003).

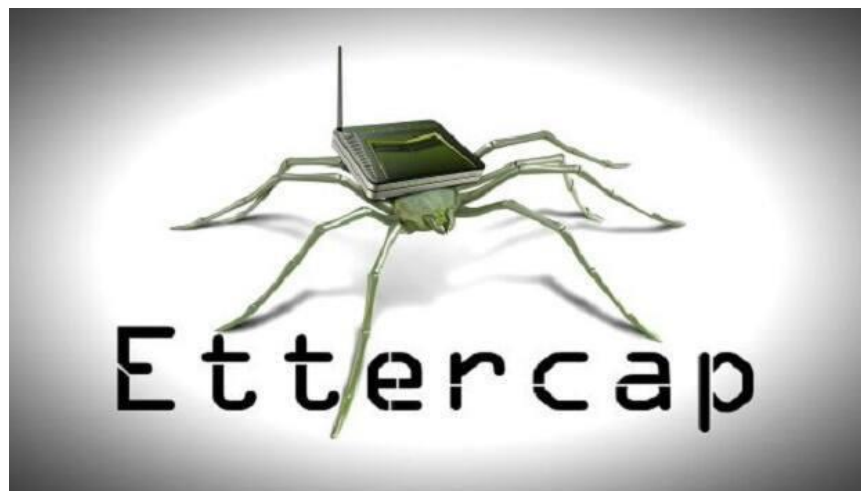
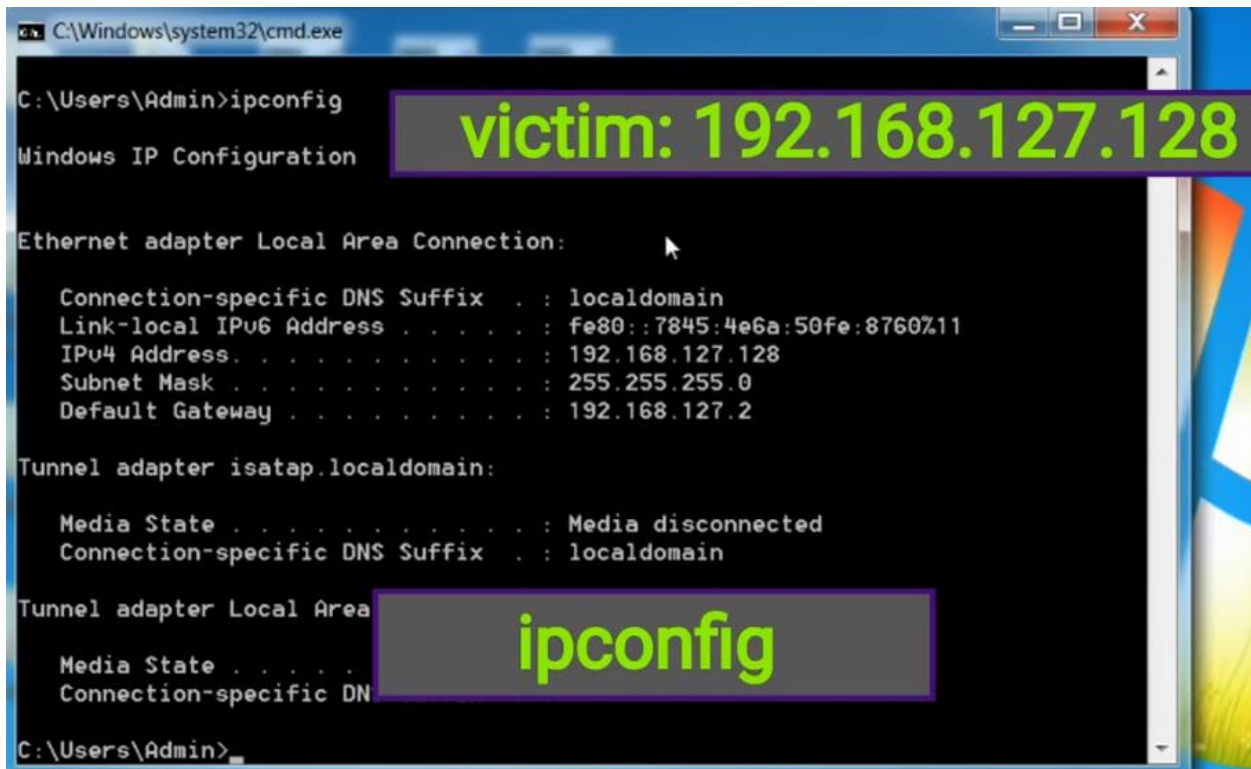


Figure 5: Ettercap

(Pentest Magazine, 2017)

The “ipconfig” command is used to see the network details of the windows 7 machine.



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

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::7845:4e6a:50fe:8760%11
    IPv4 Address. . . . . : 192.168.127.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.127.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

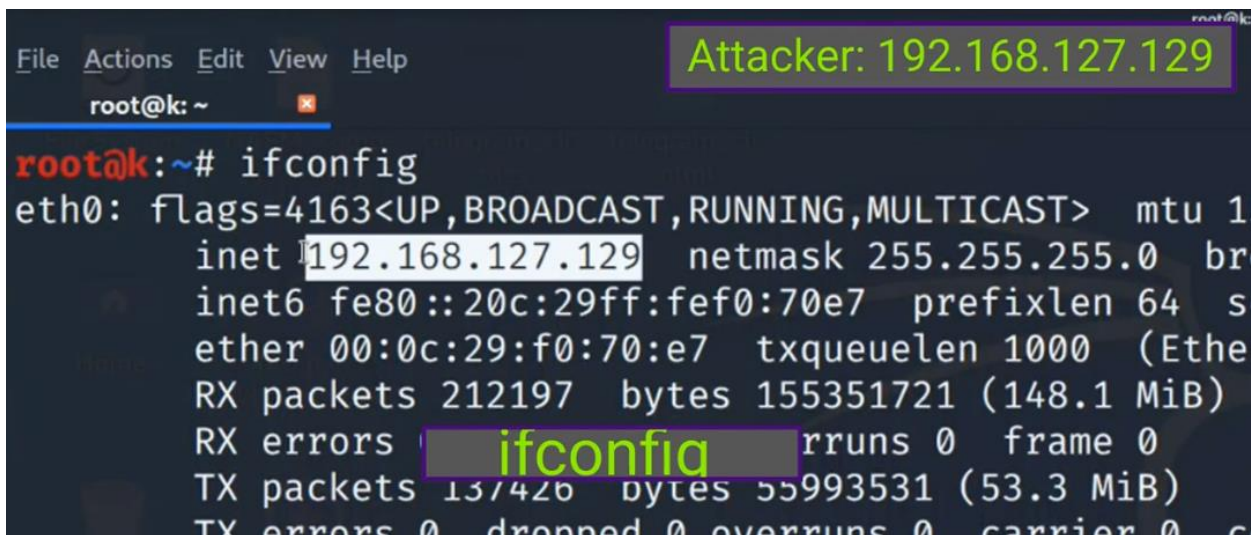
Tunnel adapter Local Area

    Media State . . . . .
    Connection-specific DN

C:\Users\Admin>
```

Figure 7: Client's IP address

The “ifconfig” command is used to see the network details of the kali linux machine.



```
File Actions Edit View Help
root@k: ~
root@k:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1
    inet 192.168.127.129 netmask 255.255.255.0 br
    inet6 fe80::20c:29ff:fef0:70e7 prefixlen 64 s
    ether 00:0c:29:f0:70:e7 txqueuelen 1000 (Ethe
    RX packets 212197 bytes 155351721 (148.1 MiB)
    RX errors ifconfig rruns 0 frame 0
    TX packets 137426 bytes 55993531 (53.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 c
```

Figure 7: Attacker's IP address

“ipcalc 192.168.127.129” command is used to calculate the IP information of required host which is the IP address of kali linux machine in this case.

```

root@k:~# ipcalc 192.168.127.129
Address:   192.168.127.129      11000000.10101000.01111111. 10
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00
Wildcard:  0.0.0.255           00000000.00000000.00000000. 11
⇒
Network:   192.168.127.0/24     11000000.10101000.01111111. 00
HostMin:   192.168.127.1       11000000.10101000.01111111. 00
HostMax:   192.168.127.254     11000000.10101000.01111111. 11
Broadcast: 192.168.127.255     11000000.10101000.01111111. 11
Hosts/Net: 254                  Class C, Private Internet

```

Figure 8: IP Information of Attacker

“nmap -sP 192.168.127.0/24” command is used to make a ping-only scan to all the hosts in the given network.

```

root@k:~# nmap -sP 192.168.127.0/24
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 192.168.127.2
Host is up (0.00019s latency).
MAC Address: 00:50:56:EF:4B:DE (VMware)
Nmap scan report for 192.168.127.128
Host is up (0.00044s latency).
MAC Address: 00:0C:29:DC:01:E1 (VMware)
Nmap scan report for 192.168.127.254
Host is up (0.00031s latency).
MAC Address: 00:50:56:EE:24:B6 (VMware)
Nmap scan report for 192.168.127.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.76 seconds
root@k:~#

```

Figure 9: Ping scan to all hosts in the network

“route -n” command is used to print out the routing table.

```
root@k:~# nmap -sP 192.168.127.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 17:17 +07
Nmap scan report for 192.168.127.2
Host is up (0.00019s latency).
MAC Address: 00:50:56:EF:4B:DE (VMware)
Nmap scan report for 192.168.127.128
Host is up (0.00044s latency).
MAC Address: 00:0C:29:DC:01:E1 (VMware)
Nmap scan report for 192.168.127.254
Host is up (0.00031s latency).
MAC Address: 00:50:56:EE:24:B6 (VMware)
Nmap scan report for 192.168.127.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.76 seconds
root@k:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          192.168.127.2 0.0.0.0        UG    100    0      0 eth0
192.168.127.0   0.0.0.0        255.255.255.0 U     100    0      0 eth0
root@k:~#
```

route -n --> print out routing table

Figure 10: Routing table

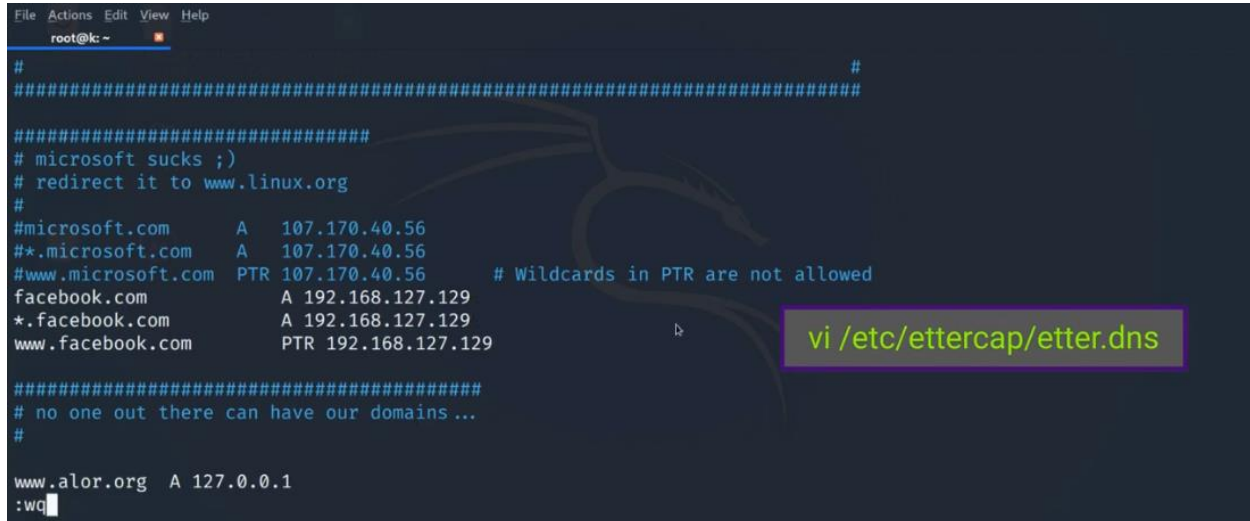
The etter.dns file is located using the “locate etter.dns” command.

```
root@k:~# locate etter.dns
/etc/ettercap/etter.dns
|
```

locate etter.dns

Figure 11: Finding the location of etter.dns

“vi /etc/ettercap/etter.dns” command is used to open the etter.dns file in a text editor. This hosts file, named etter.dns, is in charge of forwarding certain DNS requests. The target will be sent to Facebook's website if they type in facebook.com, but this file can change that.



```

File Actions Edit View Help
root@k:~
#
#####
#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
#microsoft.com      A  107.170.40.56
#*.microsoft.com    A  107.170.40.56
#www.microsoft.com  PTR 107.170.40.56 # Wildcards in PTR are not allowed
facebook.com        A  192.168.127.129
*.facebook.com      A  192.168.127.129
www.facebook.com    PTR 192.168.127.129

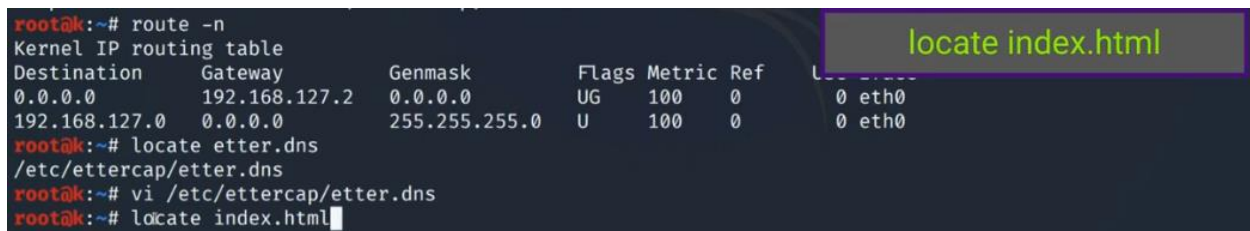
#####
# no one out there can have our domains...
#

www.alor.org A 127.0.0.1
:wq

```

Figure 12: Opening etter.dns with text editor

“locate index.html” command is used to locate the index.html file.



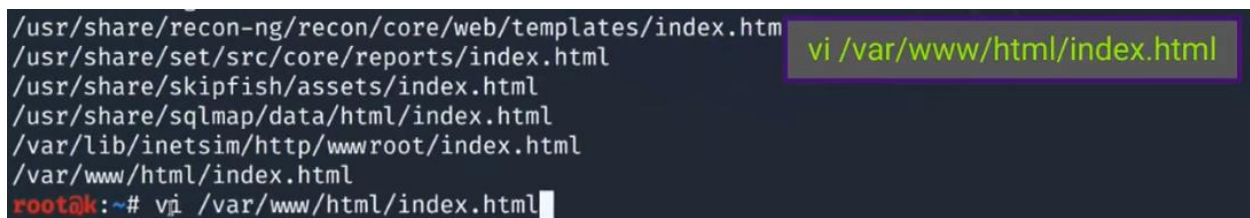
```

root@k:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Ifaces
0.0.0.0 192.168.127.2 0.0.0.0 UG 100 0 0 eth0
192.168.127.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
root@k:~# locate etter.dns
/etc/ettercap/etter.dns
root@k:~# vi /etc/ettercap/etter.dns
root@k:~# locate index.html

```

Figure 13: Locating index.html file

“vi /var/www/html/index.html” command is used to open the index.html file in a text editor.



```

/usr/share/recon-ng/recon/core/web/templates/index.htm
/usr/share/set/src/core/reports/index.html
/usr/share/skipfish/assets/index.html
/usr/share/sqlmap/data/html/index.html
/var/lib/inetsim/http/wwwroot/index.html
/var/www/html/index.html
root@k:~# vi /var/www/html/index.html

```

Figure 14: Opening index.html in text editor

Ettercap can sniff in both bridged and unified modes. In bridged mode, the attacker has many networking devices and is sniffing communication as it passes via a bridge between them. Unified employs a single network device that performs both sniffing and forwarding on the same network port.



Figure 17: Sniffing in Unified mode from Ettercap

The network interface is selected where the required machines are connected.

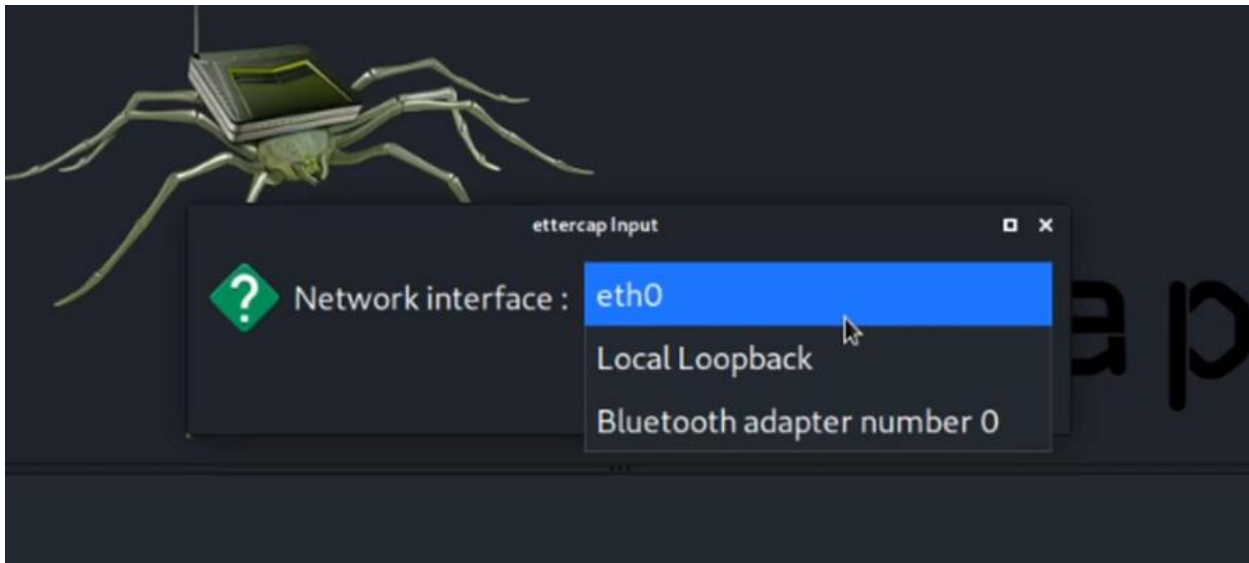


Figure 18: Selecting the network interface

A list of all the devices connected to the network should appear in the table as shown below.

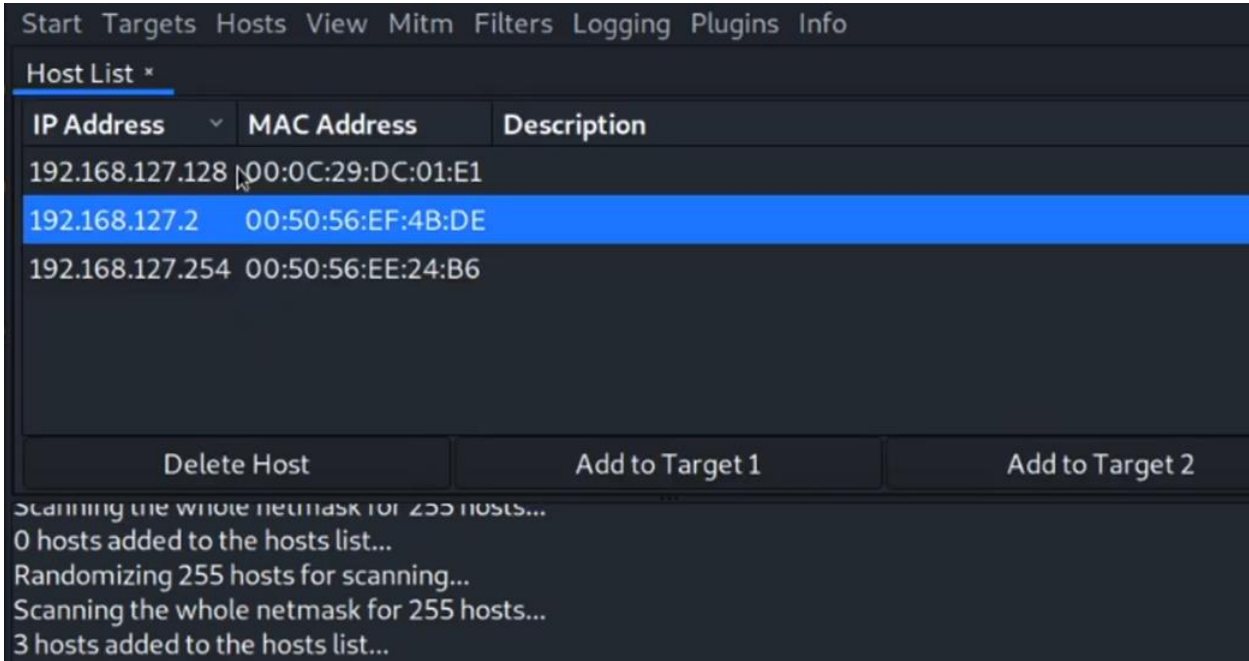


Figure 19: List of hosts connected in the network

Select the default gateway's IP address and add it to Target 1, as well as the IP address of the Target computer and add it to Target 2.

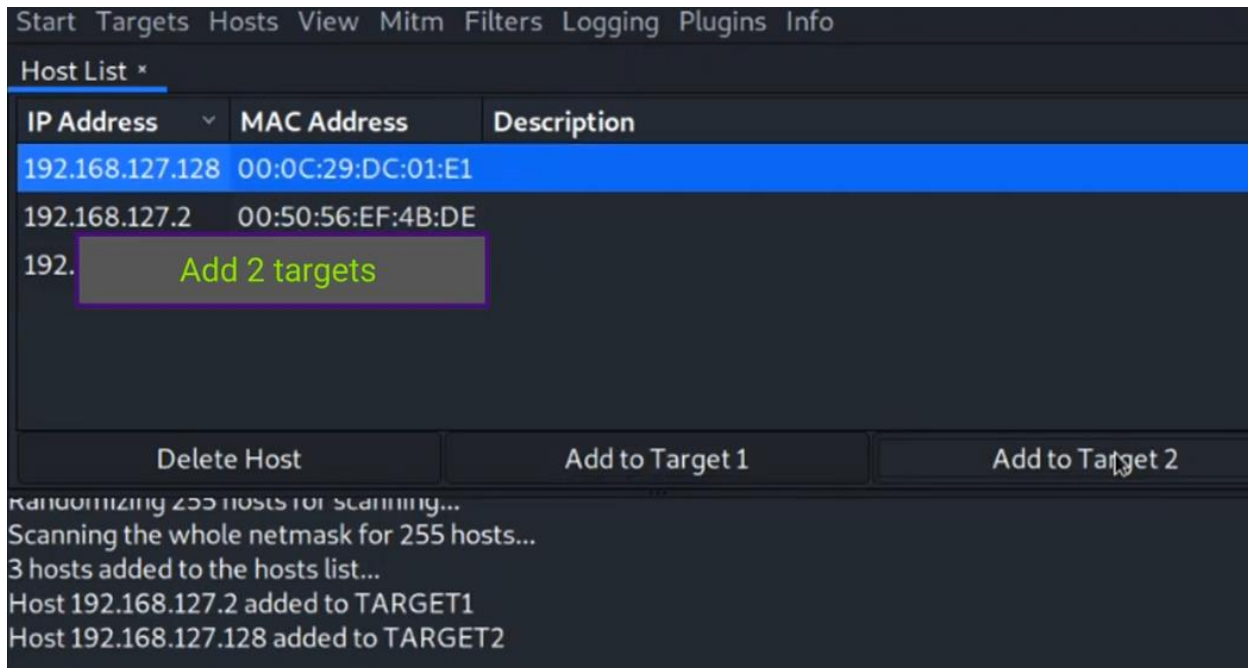


Figure 20: Adding 2 connected hosts as targets

“service apache2 start” command is used to start the apache web server so that the incoming traffic can be accepted.

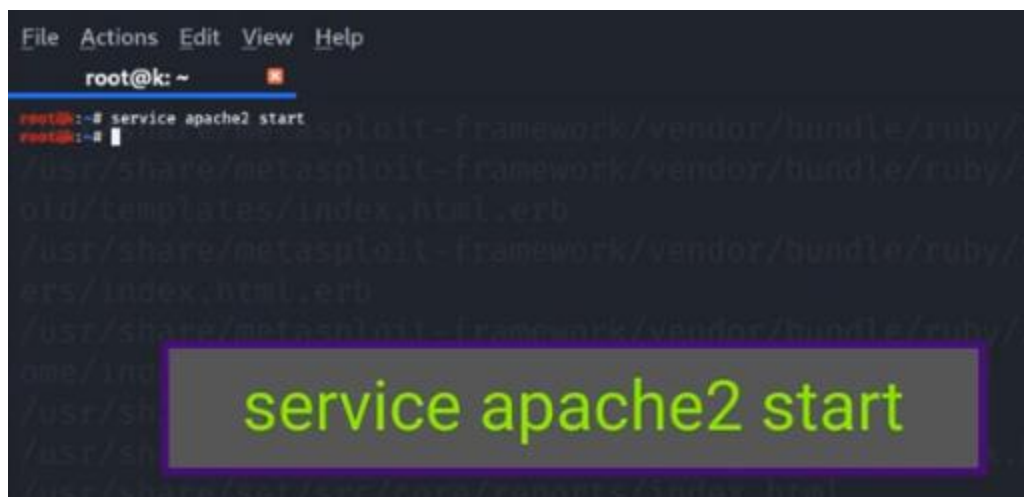


Figure 21: Starting Apache web server

In the Mitm menu bar, “ARP poisoning” is selected so that the communication between network devices can be intercepted.

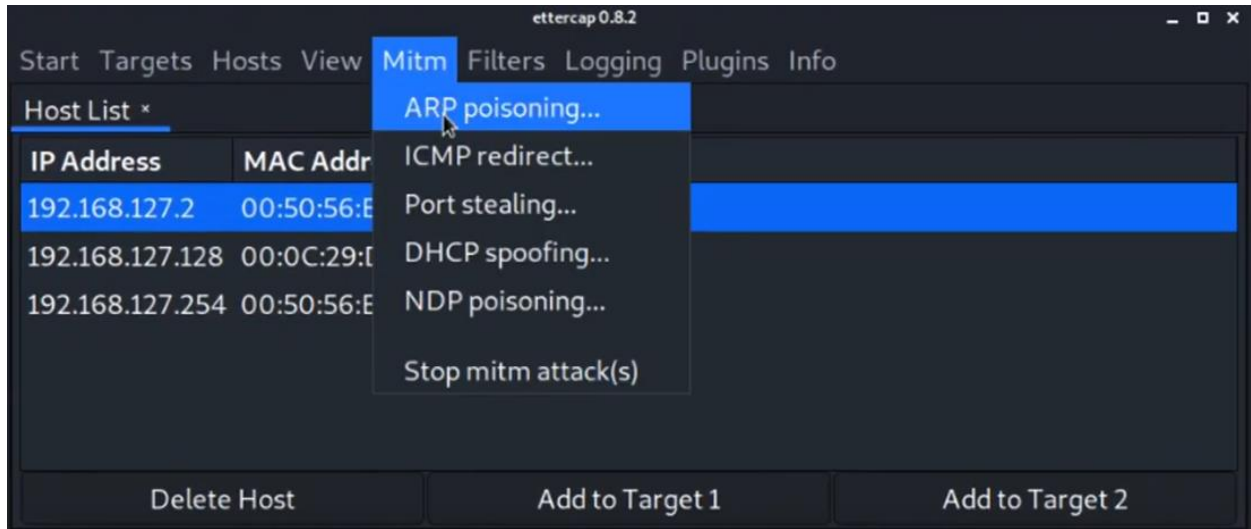


Figure 22: Initiating Man in the middle attack

The option to sniff remote connections is selected.

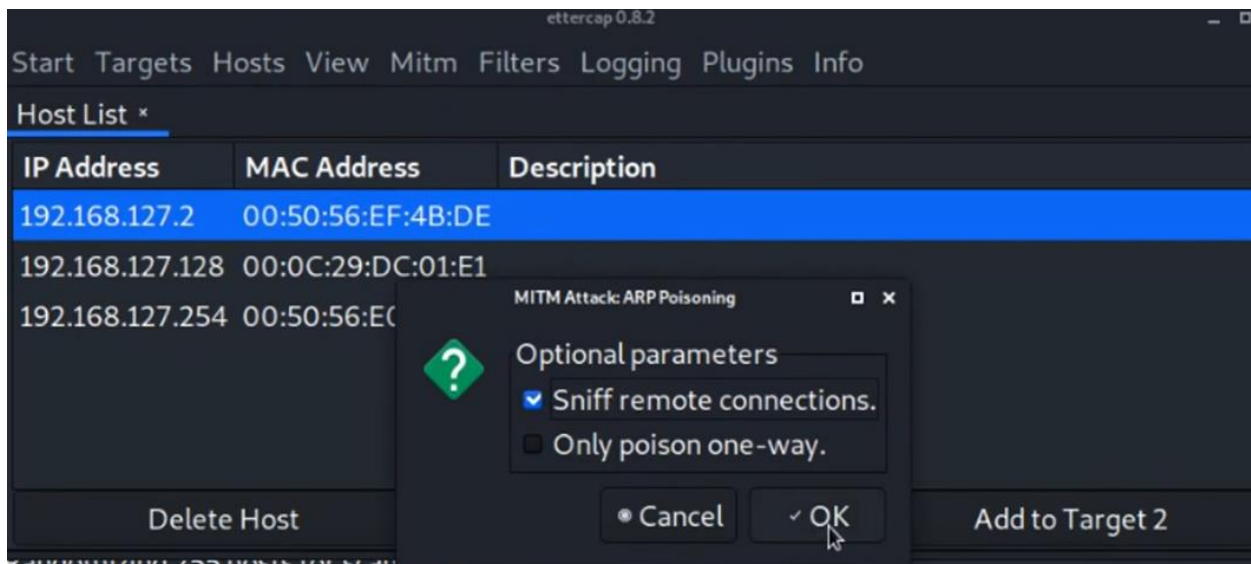


Figure 23: Sniffing remote connections

From the menu bar, the Plugins option is selected. Then the option named "Manage the plugins" is selected.

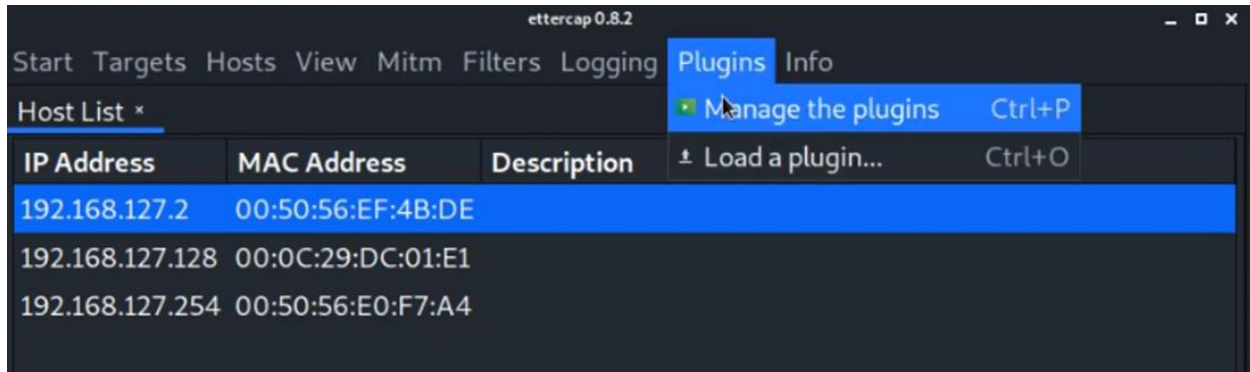


Figure 24: Navigating to plugins

"dns spoof" from the list of plugins is selected.

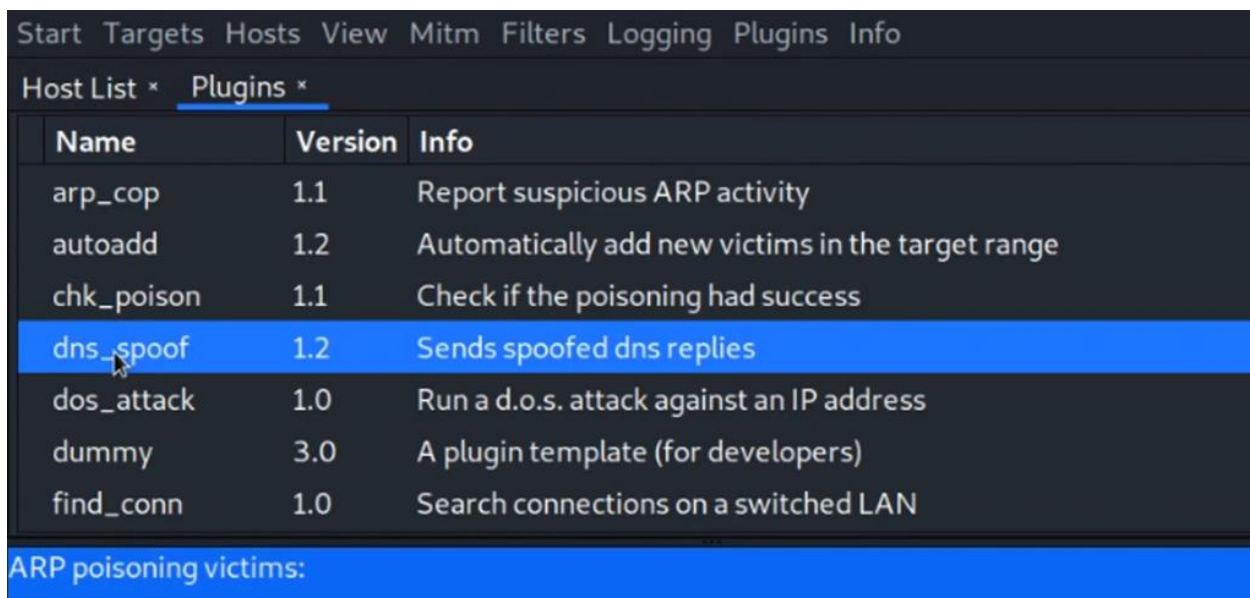


Figure 25: Selecting the dns_spoof plugin

Then the “Start sniffing” option is selected from the Start option in the menu bar.

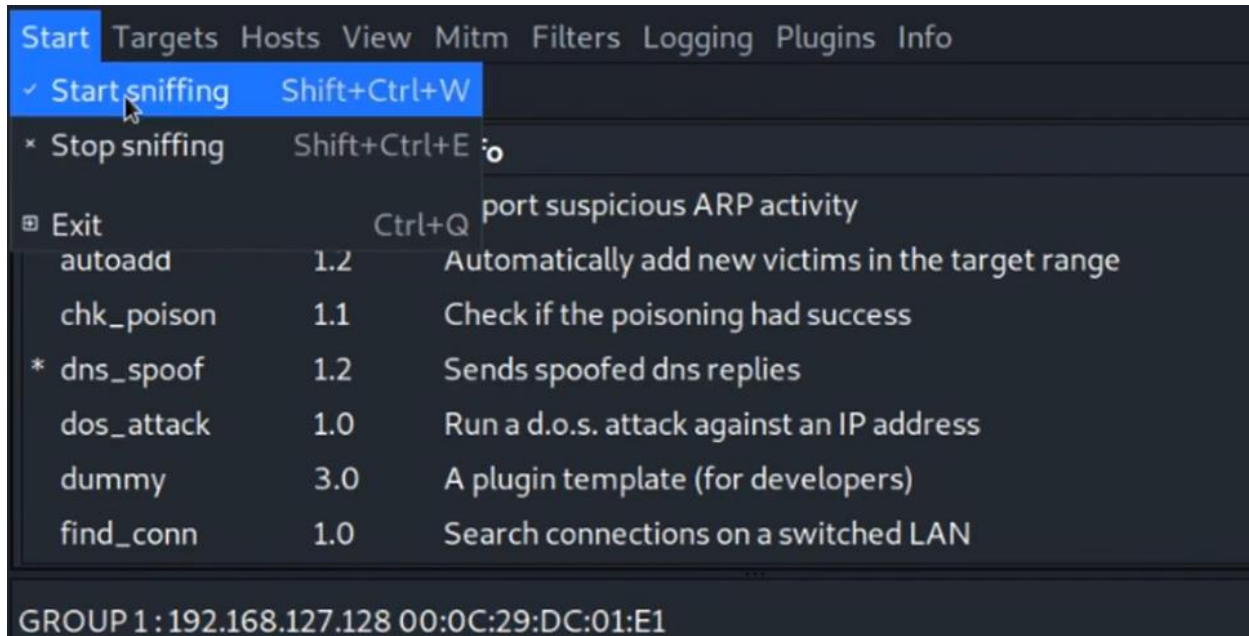


Figure 26: Initiating the sniffing process

When the IP address of facebook.com is entered in the URL bar, the spoofed page appears.

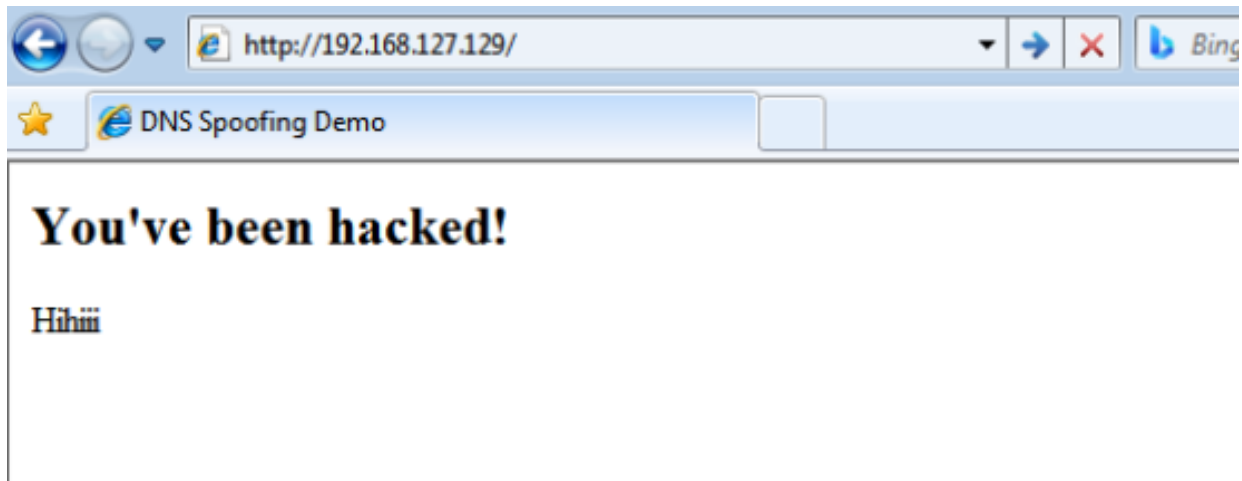


Figure 27: Accessing Facebook through IP address from victim's pc

Similarly, when facebook.com is entered in the URL bar, the spoofed page appears.

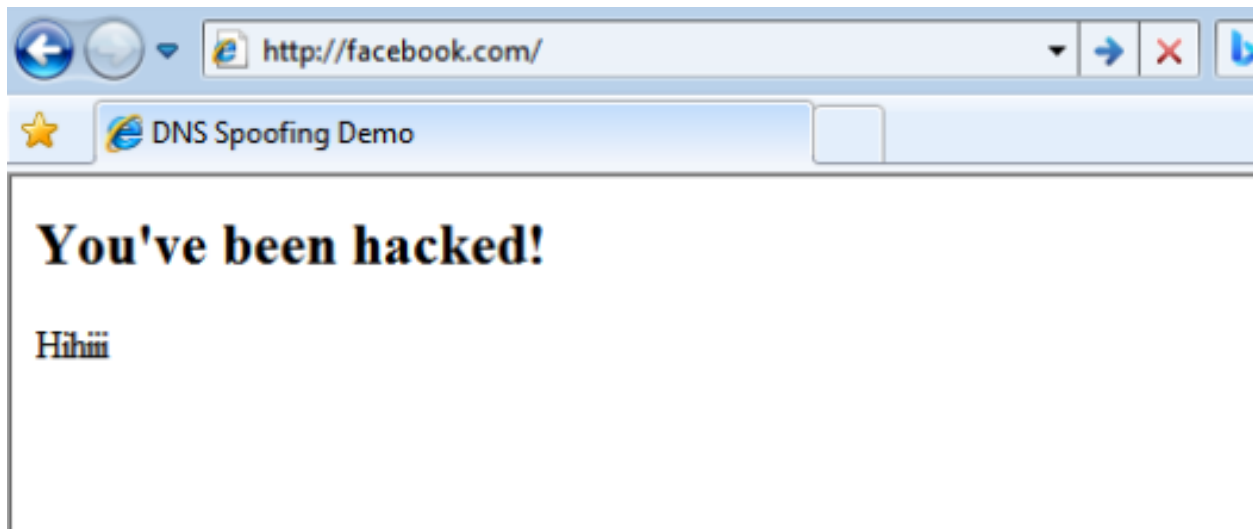


Figure 28: Accessing Facebook through dns from victim's pc

4. Mitigation

DNS spoofing attacks may be mitigated in a number of ways. Some of them are listed as follows:

4.1 Firewall

A firewall is a security component that monitors incoming and outgoing (inbound and outbound) traffic and protects the network from illegal access. It enforces a network-to-network access control policy. It operates as a network guard, filtering permitted traffic and preventing harmful or suspicious traffic according to specified rules/policies. It conducts Network Address Translator (NAT) by routing outbound traffic through the firewall rather than through the network. TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol) are the most common communication protocols used by firewalls, as they all contain source and destination addresses.

Firewalls also function on internet traffic, which typically follows these three protocols. The firewall is based on packet filtering, which is a technique for monitoring and controlling network traffic. It analyzes a unique TCP packet header, comprising source IP, destination IP, Source Port, and Destination Port, to determine if a packet should be forwarded or deleted. IP address spoofing, source routing attacks, denial of service attacks, and TCP assaults are all examples of attacks against firewalls (Abdulwasiu, 2022).

In our case, a firewall is used to prevent Kali Linux from sending packets across the router to Windows 7. As a result, the spoofing won't affect the fake Facebook server. To block unwanted packets in the Windows 7 computer, the firewall for both the private and public networks is switched on as shown in the image below.

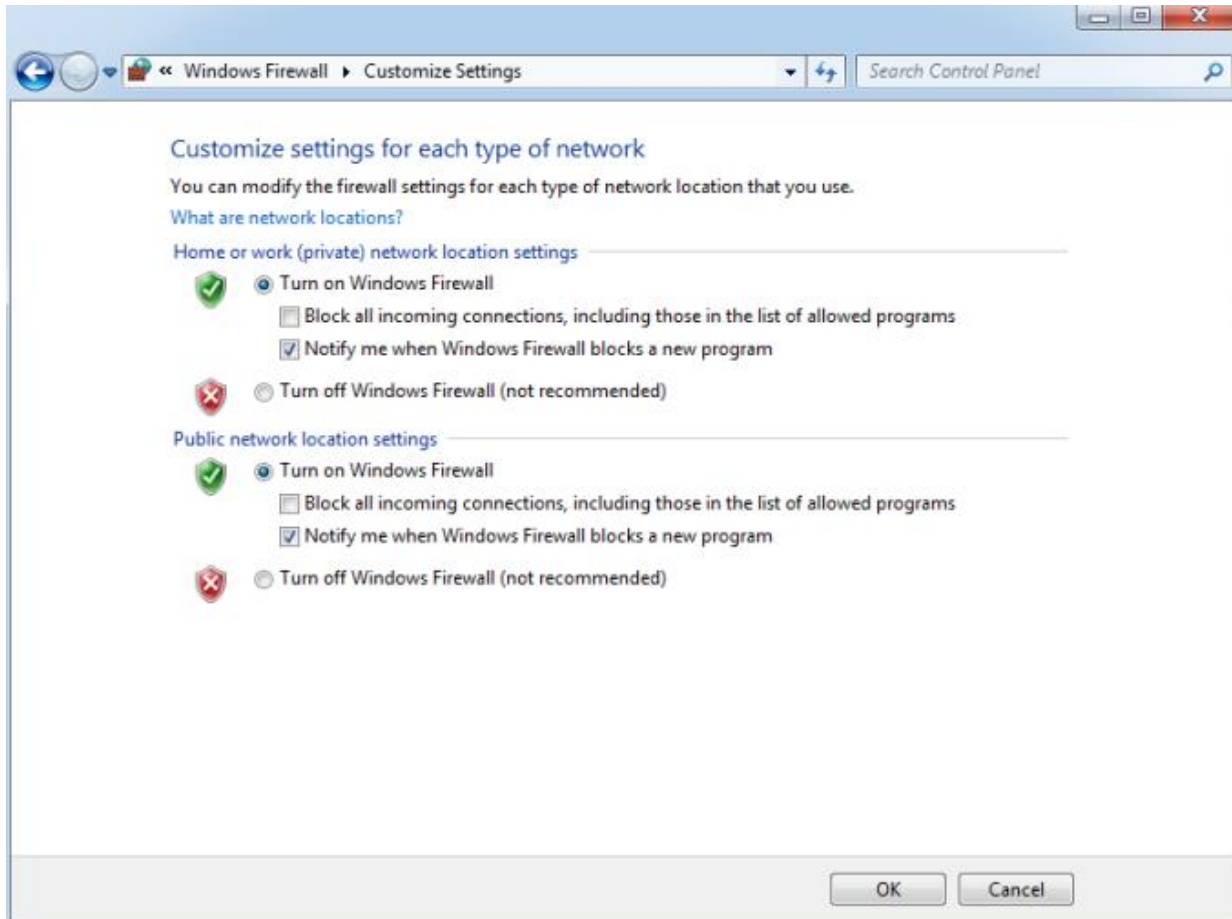


Figure 29: Enabling Firewall

Spoofed packets are prevented by the firewall, as seen in the image below. To avoid DNS spoofing, the best and cheapest option is to use a firewall. It contributes to the system's enhanced security.

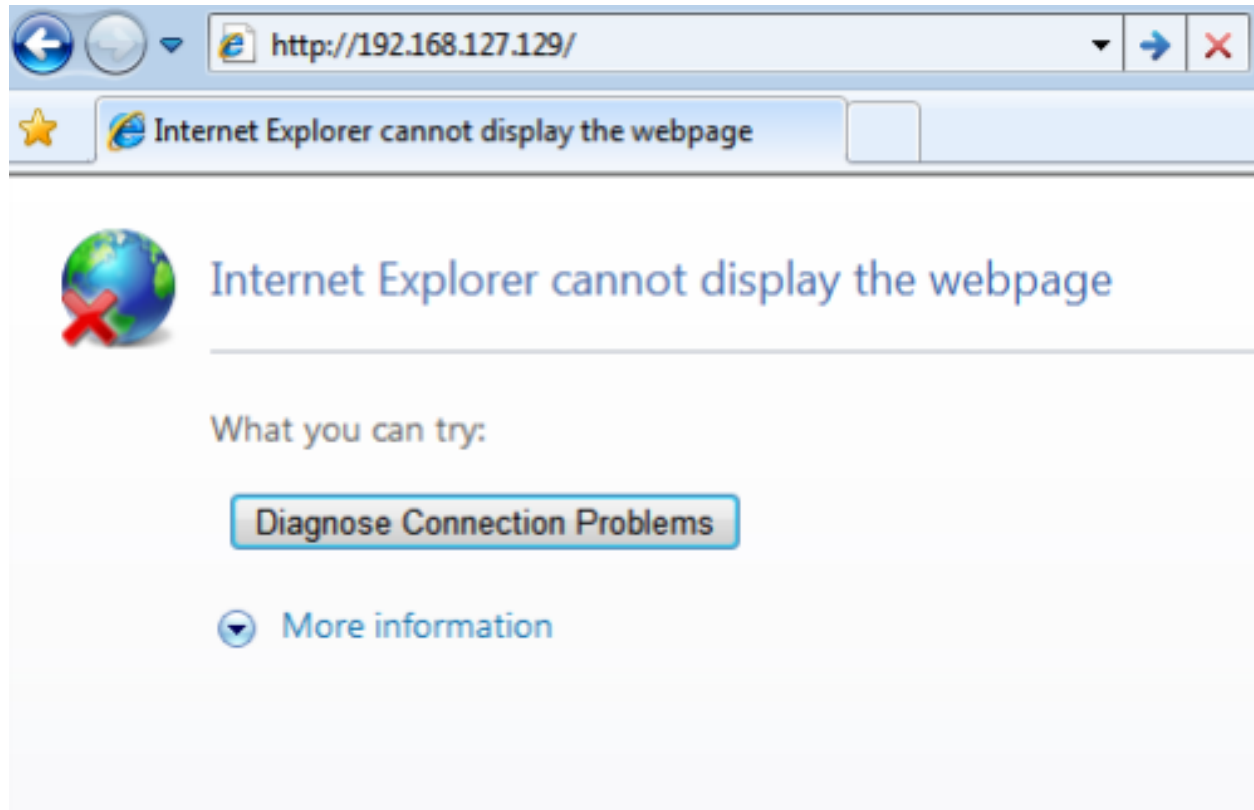


Figure 30: Spoofed packets blocked after turning on firewall

4.2 Access Control List (ACL)

Access Control Lists, or simply Access-Lists, are a collection of allow and deny commands that give a powerful mechanism to control traffic into and out of a network. When a router allows or denies packets based on filtering rules configured by network administrators on the router's interface, it operates as a packet filter. An interface's ACL can manage two types of traffic: incoming and outgoing traffic to and from a router, which are referred to as inbound and outbound traffic, respectively. A packet-filtering router, as a layer 3 device, utilizes rules to decide whether to allow or reject traffic based on source and destination IP addresses, source port and destination port, and packet protocol (Vishesh, 2017).

In this case, ACL may be used to prevent unwanted packets from entering the private network. In the router, an ACL called SUJEN is created. Only the Windows PC host 192.168.127.128 is allowed, and all other networks are restricted. By doing so, we can protect ourselves from the fake packets that an attacker's computer delivers to our victim computer. This helps to the enhance entire network's security.

```
R1(config)#ip access-list standard SUJEN
R1(config-std-nacl)#permit host 192.168.127.128
R1(config-std-nacl)#deny any
R1(config-std-nacl)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#int fa0/1
R1(config-if)#ip access-group SUJEN in
R1(config-if)#ex
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

Figure 31: ACL Configuration

After establishing the ACL on the router linking the pcs using NAT, the Spoof packet is prevented, as seen in the figure below.

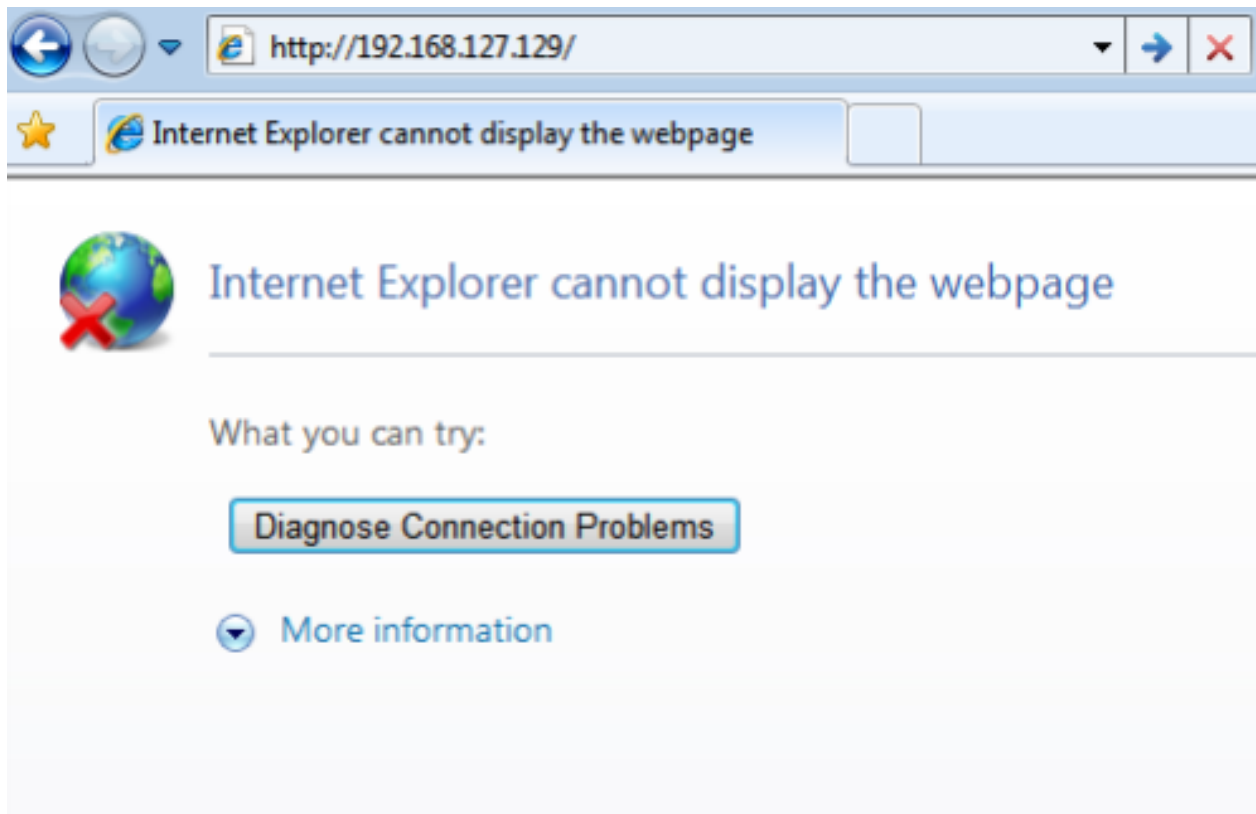


Figure 32: Spoofed packets blocked after ACL Configuration

5. Evaluation

The proposed mitigation measures are thoroughly examined to determine their benefits and drawbacks.

5.1 Pros of the applied mitigation strategy:

Mentioned below is a list of strengths of this new cryptographic algorithm:

- The attacker's DNS spoof packets are blocked by the firewall from reaching the internal computer network.
- A firewall distinguishes between trustworthy and untrusted networks in a network and determines who should be granted permission and who should not.
- ACL enables us to create rules for network devices to allow or restrict traffic in the needed network, hence preventing superfluous packets.

5.2 Cons of the applied mitigation strategy:

Mentioned below is a list of weakness of this new cryptographic algorithm:

- The basic firewall cannot prevent large and powerful spoofs from entering the network, and sophisticated firewalls are out of reach for most consumers and small businesses.
- ACL configuration is simple, however adding or removing users is a little more difficult. To remove a single user, the entire ACL must be removed.

5.3 Cost Benefit Analysis (CBA)

Cost-benefit analysis is a decision-making process that is best suited to concerns of a social nature, which are usually the subject of choices, whether private or public. Whatever the choice, regardless of its type, incorporates social benefits and costs, the cost-benefit analysis should or should be used to verify the extent to which that (private or public) decision is beneficial from a social standpoint (Caleiro, 2021).

CBA can be used for short-term choices, but it is most utilized when a corporation or individual must make a long-term decision. Organizations are advised to begin a cost-benefit analysis by assessing the value of the information assets to be protected as well

as the loss of value if those information assets are compromised. CBA is used to determine whether the risk-control choices are worth the related cost. A mathematical technique is used to calculate cost benefit analysis.

CBA = ALE (prior) – ALE (post) – ACS

- ALE (prior) is the annualized loss expectancy of the risk prior to the execution of the control measure or alternative.
- ALE (post) is the evaluation of countermeasure after the control or alternative has been in place over a length of time.
- ACS is the annualized cost of the safeguard/control.

For this case, the attack was carried out in a controlled environment, so all the mitigating strategies listed above are completely free. The default firewall is Firewall, and ACL may be configured on the router for free. As a result, the cost of implementing the mitigation strategies will be zero.

For calculating the CBA in a real organization, let us assume the value of data of an organization is \$20000. The annual loss expectancy due to DNS and other such attacks is \$10000. The cost for installing the firewall and powerful router with ACL is \$2000 per year. Using this countermeasure, the ALE will be reduced to \$4000.

For this case, the cost benefit analysis can be done using the formula,

$$\text{CBA} = \text{ALE (prior)} - \text{ALE (post)} - \text{ACS}$$

$$\text{CBA} = \$10000 - \$4000 - \$2000$$

$$\text{CBA} = \$10000 - \$6000$$

$$\text{CBA} = \$4000$$

In this case, the cost of firewall and router plus their annual cost is less than the loss expectancy due to DNS attacks. Therefore, there are positive benefits of installing the countermeasure.

5.4 Application Area

An implementation of this cryptographic algorithm is that it can be applied to encrypt an electronic file such as student records, email, and classified documents. It may be implemented in a variety of cryptographic libraries, including OpenSSL, wolfCrypt, cryptlib, and many others. Encrypting and decrypting a huge file takes a long time. As a result, it's ideal for small files. RSA established the foundation for most of current secure communications as one of the earliest public-key encryption systems that was extensively utilized. It was the first method used in PGP encryption and was traditionally used in TLS. Many internet browsers, VPNs, email, chat, and other communication methods still use the RSA. Secure connections between VPN clients and VPN servers are commonly produced using RSA. RSA encryption can be used in TLS handshakes for exchanging keys and establishing a secure link under protocols like OpenVPN.

6. Conclusion

If network administrators are unaware of ARP cache poisoning and are not prepared to identify malicious activities on their network, ARP spoofing and poisoning might catch them off guard. If the attacker is clever enough, tools like Ettercap can be launched on a network without being detected. There is nothing stopping an attacker from sniffing passwords, confidential information, company secrets, instant messaging, e-mails, and any other traffic they want once they get a list of IP and MAC addresses. A well-executed attack might go unnoticed for a long period.

The improvement of security defenses has resulted in the development of new attack and defense strategies. Hackers are constantly improving their skills and breaching security defenses. Since the last three decades, DNS has been a core standard of web architecture and the internet in general. Vulnerabilities in the protocols are thoroughly investigated to make them more resilient, and as a result, attacks such as DNS spoofing and DNS amplification have become more difficult to dispatch and can be recognized successfully.

In this research, we suggest a DNS spoofing attack that takes advantage of the weakness of the DHCP server-side IP address conflict recognition mechanism. When compared to recently known methods, this research shows that the suggested attack is easier to execute and far more subtle. This research demonstrates how existing detection and mitigation methods are ineffective in preventing the attack. Strong identification and mitigation systems could be developed using this method, which helps to differentiate the proposed attack and, in general, makes DNS a secure protocol.

7. References

Abdulwasiu, J., 2022. *Firewall*, Chicago: Illinois Institute of Technology.

Bashir, M. S., 2003. *ARP Cache Poisoning with Ettercap*, Bethesda: SANS Institute.

Caida, 2022. *State of IP Spoofing*. [Online]

Available at: <https://spoofer.caida.org/summary.php>

[Accessed 28 April 2022].

Caleiro, A. B., 2021. *Rawlsian Cost-Benefit Analysis*. Évora: Escola de Ciências Sociais da Universidade de Évora.

Galaxy Technologies LLC, 2021. *Getting Started with GNS3 | GNS3 Documentation*.

[Online]

Available at: <https://docs.gns3.com/docs/>

[Accessed 20 April 2022].

Krebs on Security, 2019. *A Deep Dive on the Recent Widespread DNS Hijacking Attacks*. [Online]

Available at: <https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/>

[Accessed 16 April 2022].

Pentest Magazine, 2017. *Ettercap and middle-attacks tutorial*. [Online]

Available at: <https://pentestmag.com/ettercap-tutorial-for-windows/>

[Accessed 20 April 2022].

Sesni, I., 2021. *Introduction to DNS Spoofing*. [Online]

Available at: <https://pmi-sesni.medium.com/introduction-to-dns-spoofing-c1abf8e67e2d>

[Accessed 23 April 2022].

Stewart, J., 2003. *DNS Cache Poisoning - The Next Generation*, s.l.: GCIH.

Vishesh, S., 2017. Access Control List: Route-Filtering and Traffic Control. *International Journal of Advanced Research in Computer and Communication Engineering*, 6(7), pp. 364-369.