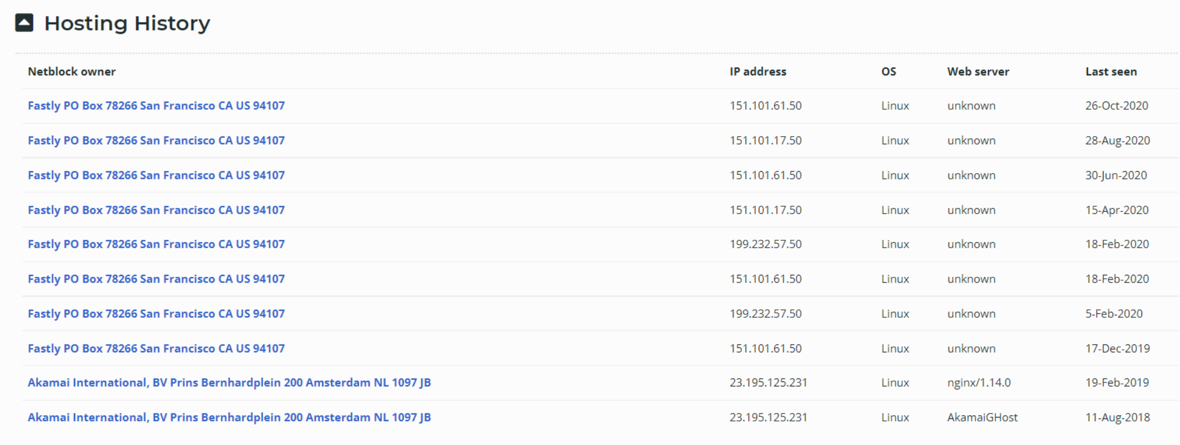
Certamen 1: Seguridad de sistemas

Rodrigo Cayazaya Marín

Rol: 201773538-4

1) Obtenga el "Hosting History" de los siguientes sitios web".

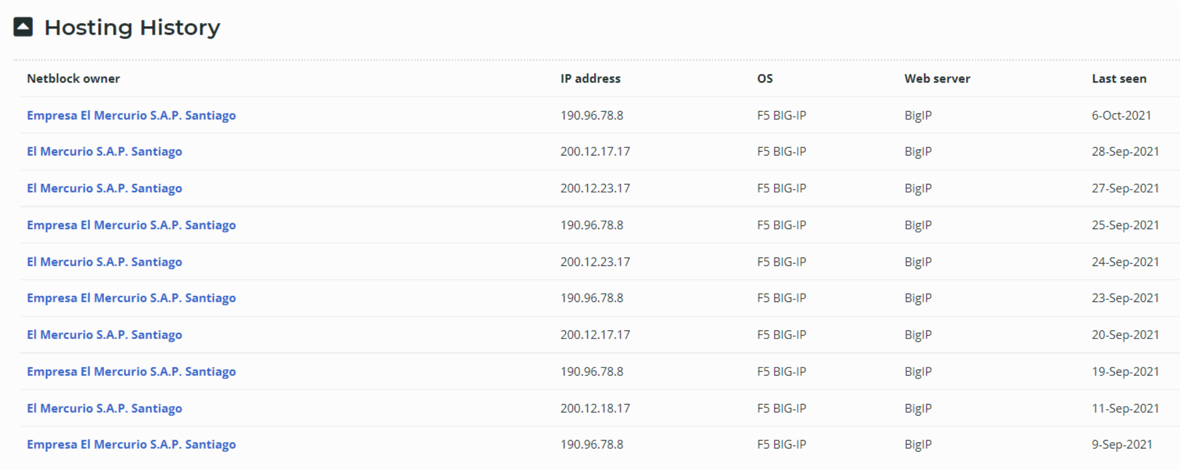
- https://www.marca.com/



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Fastly PO Box 78266 San Francisco CA US 94107	151.101.61.50	Linux	unknown	26-Oct-2020
Fastly PO Box 78266 San Francisco CA US 94107	151.101.17.50	Linux	unknown	28-Aug-2020
Fastly PO Box 78266 San Francisco CA US 94107	151.101.61.50	Linux	unknown	30-Jun-2020
Fastly PO Box 78266 San Francisco CA US 94107	151.101.17.50	Linux	unknown	15-Apr-2020
Fastly PO Box 78266 San Francisco CA US 94107	199.232.57.50	Linux	unknown	18-Feb-2020
Fastly PO Box 78266 San Francisco CA US 94107	151.101.61.50	Linux	unknown	18-Feb-2020
Fastly PO Box 78266 San Francisco CA US 94107	199.232.57.50	Linux	unknown	5-Feb-2020
Fastly PO Box 78266 San Francisco CA US 94107	151.101.61.50	Linux	unknown	17-Dec-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.125.231	Linux	nginx/1.14.0	19-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.125.231	Linux	AkamaiGHost	11-Aug-2018

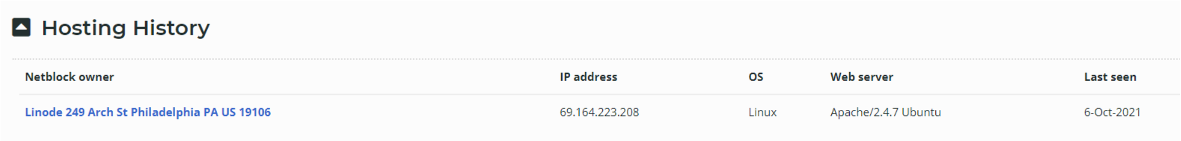
- http://www.lun.com/



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Empresa El Mercurio S.A.P. Santiago	190.96.78.8	F5 BIG-IP	BigIP	6-Oct-2021
El Mercurio S.A.P. Santiago	200.12.17.17	F5 BIG-IP	BigIP	28-Sep-2021
El Mercurio S.A.P. Santiago	200.12.23.17	F5 BIG-IP	BigIP	27-Sep-2021
Empresa El Mercurio S.A.P. Santiago	190.96.78.8	F5 BIG-IP	BigIP	25-Sep-2021
El Mercurio S.A.P. Santiago	200.12.23.17	F5 BIG-IP	BigIP	24-Sep-2021
Empresa El Mercurio S.A.P. Santiago	190.96.78.8	F5 BIG-IP	BigIP	23-Sep-2021
El Mercurio S.A.P. Santiago	200.12.17.17	F5 BIG-IP	BigIP	20-Sep-2021
Empresa El Mercurio S.A.P. Santiago	190.96.78.8	F5 BIG-IP	BigIP	19-Sep-2021
El Mercurio S.A.P. Santiago	200.12.18.17	F5 BIG-IP	BigIP	11-Sep-2021
Empresa El Mercurio S.A.P. Santiago	190.96.78.8	F5 BIG-IP	BigIP	9-Sep-2021

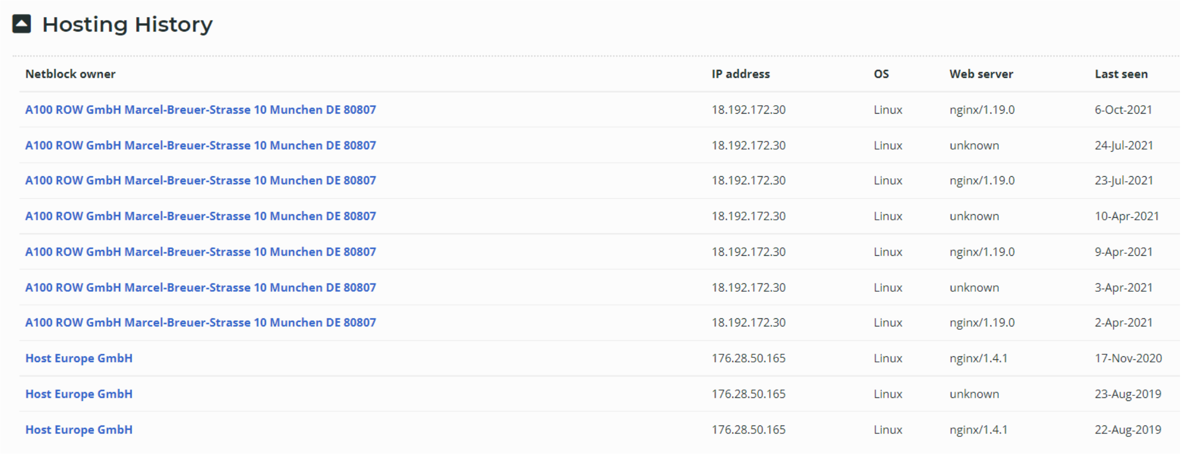
- https://www.webscantest.com/



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Linode 249 Arch St Philadelphia PA US 19106	69.164.223.208	Linux	Apache/2.4.7 Ubuntu	6-Oct-2021

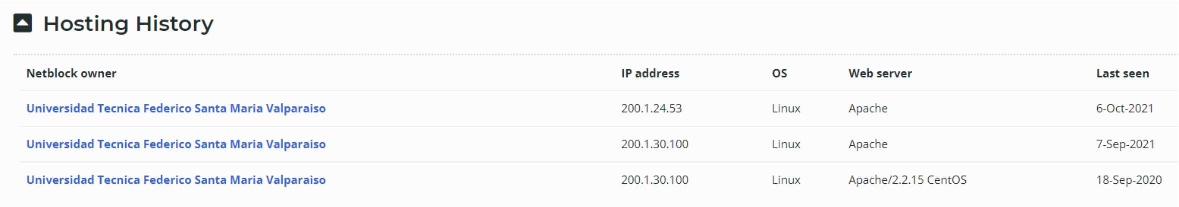
- http://testphp.vulnweb.com



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	nginx/1.19.0	6-Oct-2021
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	unknown	24-Jul-2021
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	nginx/1.19.0	23-Jul-2021
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	unknown	10-Apr-2021
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	nginx/1.19.0	9-Apr-2021
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	unknown	3-Apr-2021
A100 ROW GmbH Marcel-Breuer-Strasse 10 Munchen DE 80807	18.192.172.30	Linux	nginx/1.19.0	2-Apr-2021
Host Europe GmbH	176.28.50.165	Linux	nginx/1.4.1	17-Nov-2020
Host Europe GmbH	176.28.50.165	Linux	unknown	23-Aug-2019
Host Europe GmbH	176.28.50.165	Linux	nginx/1.4.1	22-Aug-2019

- https://www.usm.cl/

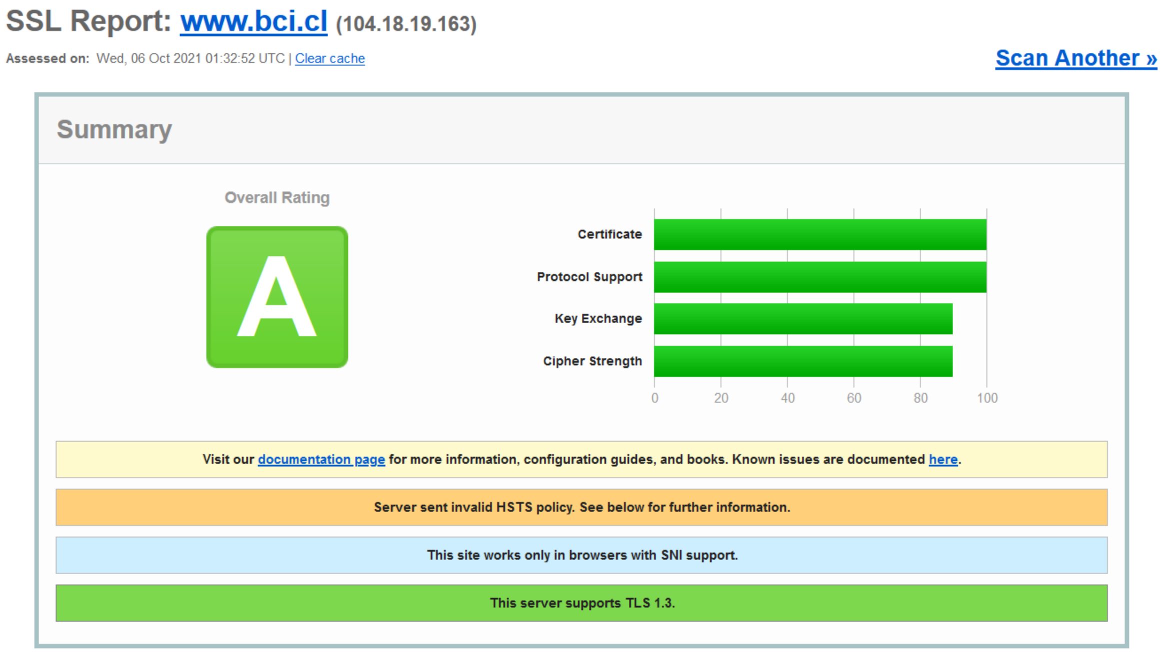


Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Universidad Tecnica Federico Santa Maria Valparaiso	200.1.24.53	Linux	Apache	6-Oct-2021
Universidad Tecnica Federico Santa Maria Valparaiso	200.1.30.100	Linux	Apache	7-Sep-2021
Universidad Tecnica Federico Santa Maria Valparaiso	200.1.30.100	Linux	Apache/2.2.15 CentOS	18-Sep-2020

2) Obtenga la categoría de seguridad SSL/TLS de los siguientes sitios:

- www.bci.cl



SSL Report: www.bci.cl (104.18.19.163)

Assessed on: Wed, 06 Oct 2021 01:32:52 UTC | Clear cache

Scan Another »

Summary

Overall Rating

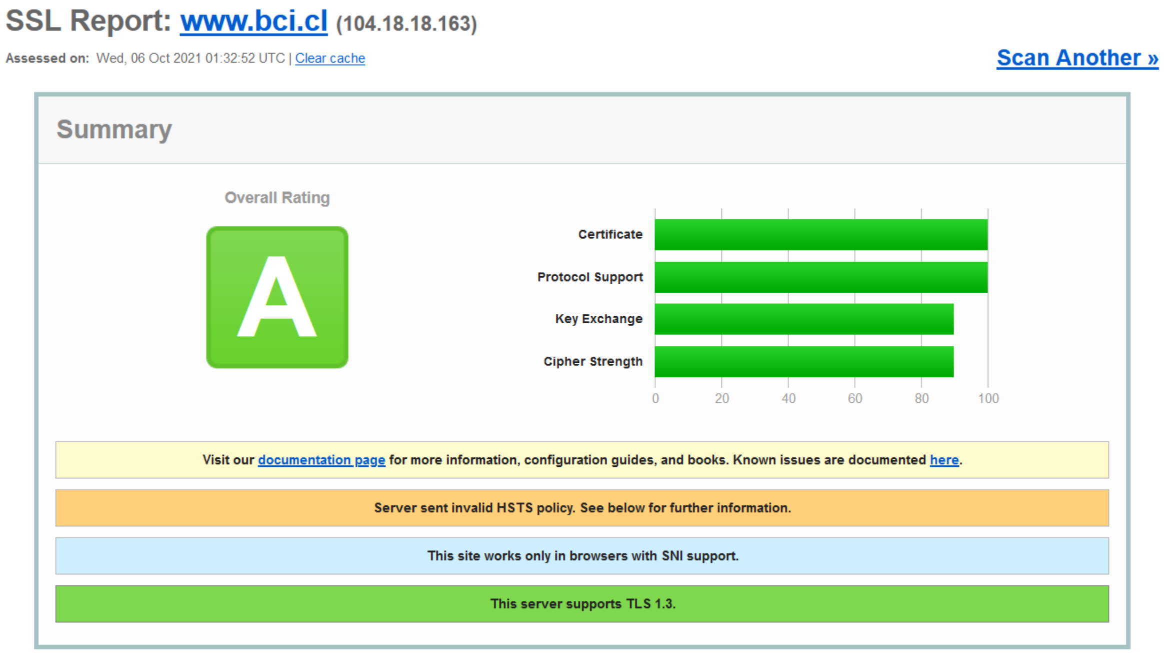
A

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Server sent invalid HSTS policy. See below for further information.

This site works only in browsers with SNI support.

This server supports TLS 1.3.



SSL Report: www.bci.cl (104.18.18.163)

Assessed on: Wed, 06 Oct 2021 01:32:52 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A

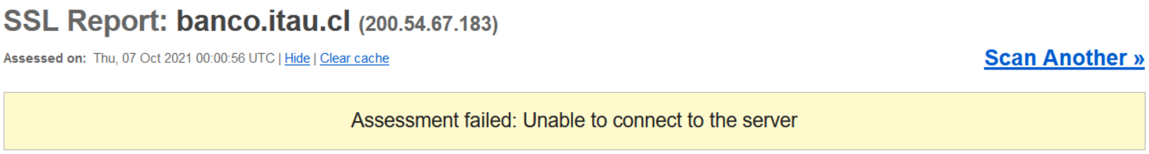
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Server sent invalid HSTS policy. See below for further information.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

- banco.itau.cl



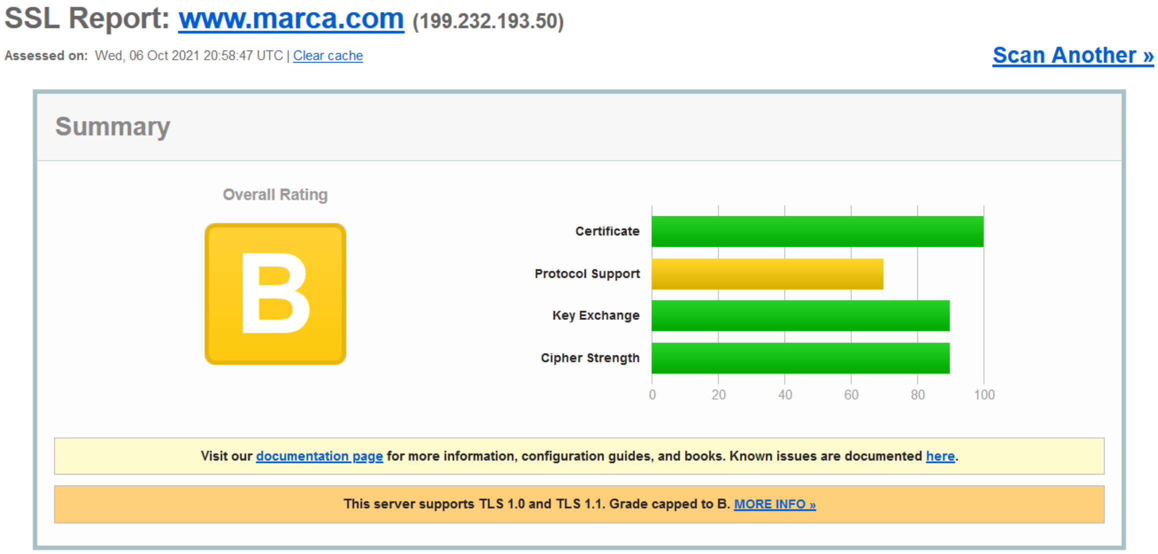
SSL Report: banco.itau.cl (200.54.67.183)

Assessed on: Thu, 07 Oct 2021 00:00:56 UTC | Hide | Clear cache

Scan Another »

Assessment failed: Unable to connect to the server

- www.marca.com



SSL Report: www.marca.com (199.232.193.50)

Assessed on: Wed, 06 Oct 2021 20:58:47 UTC | Clear cache

Scan Another »

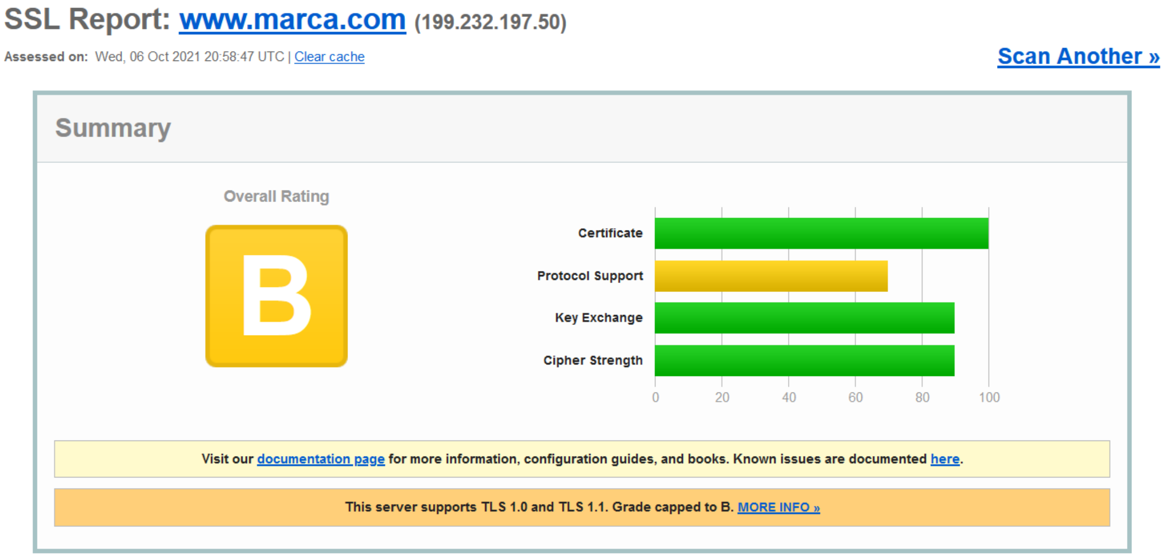
Summary

Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »



SSL Report: www.marca.com (199.232.197.50)

Assessed on: Wed, 06 Oct 2021 20:58:47 UTC | Clear cache

Scan Another »

Summary

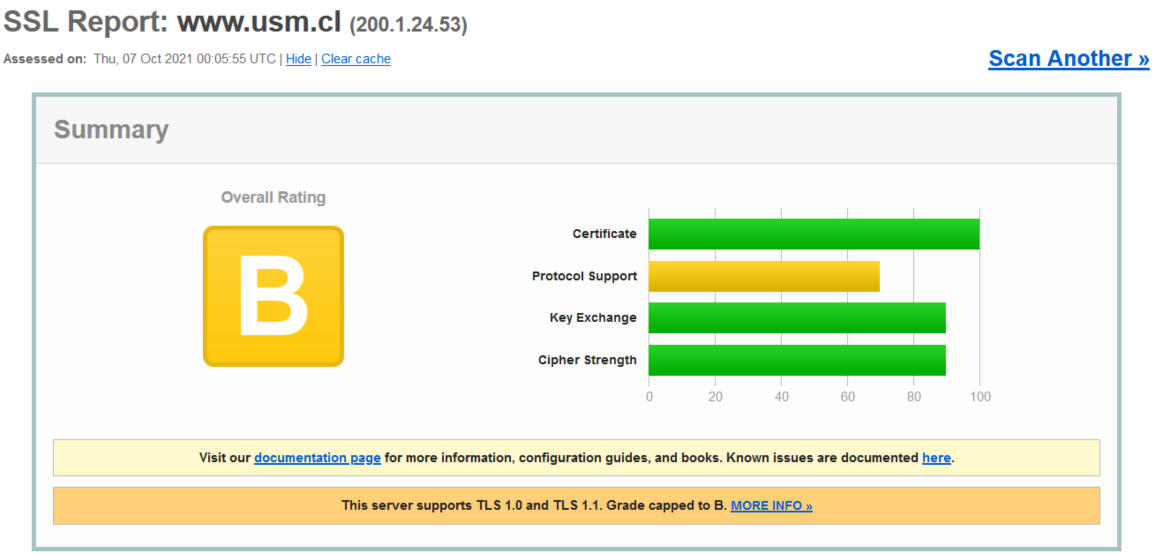
Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

- www.usm.cl



SSL Report: www.usm.cl (200.1.24.53)

Assessed on: Thu, 07 Oct 2021 00:05:55 UTC | Hide | Clear cache

Scan Another »

Summary

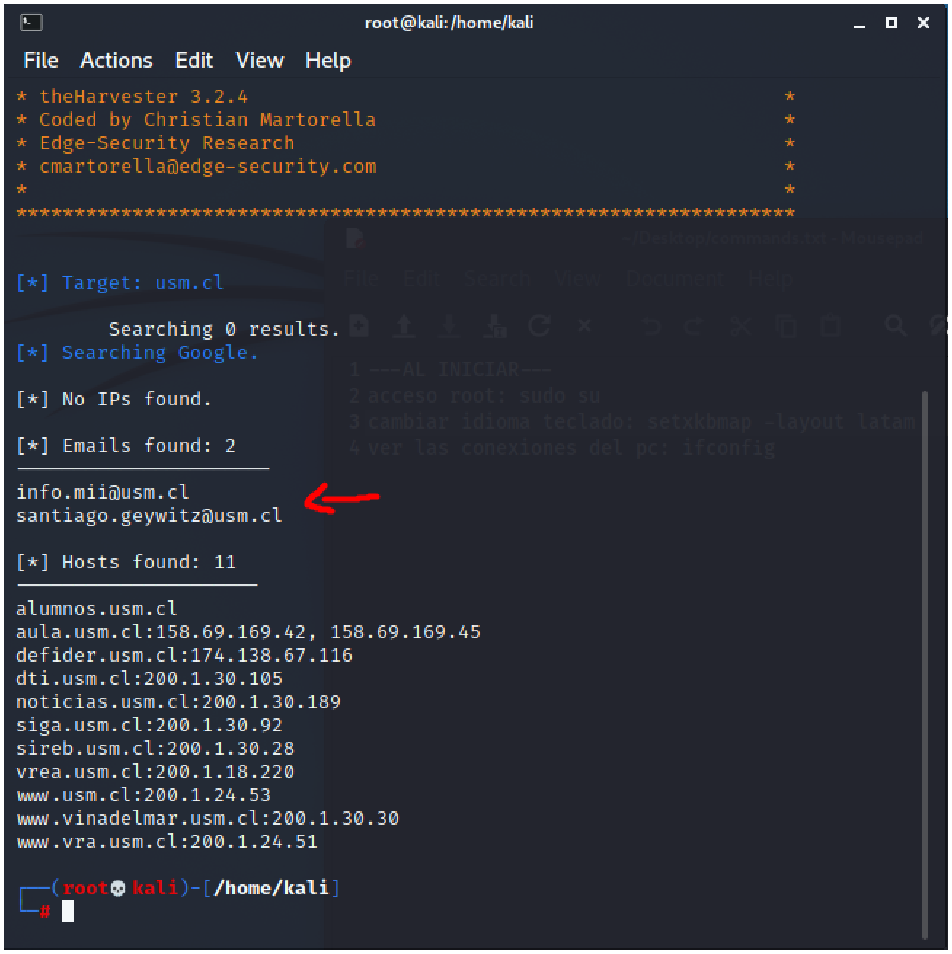
Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

3) Obtenga el lisado de direcciones de correo disponibles desde el dominio “usm.cl”

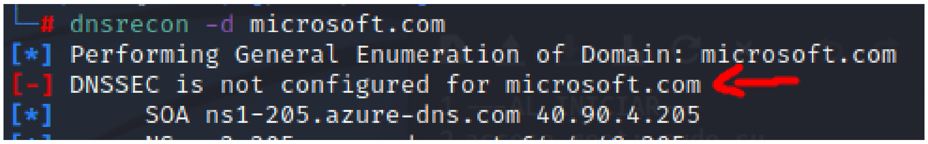

root@kali: /home/kali
File Actions Edit View Help
~/Desktop/commands.txt - Mousepad
File Edit Search View Document Help

```
* theHarvester 3.2.4                                               *
* Coded by Christian Martorella                                    *
* Edge-Security Research                                           *
* cmartorella@edge-security.com                                    *
*                                                                  *
********************************************************************


[*] Target: usm.cl

        Searching 0 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 2
----------------------
info.mii@usm.cl
santiago.geywitz@usm.cl

[*] Hosts found: 11
---------------------
alumnos.usm.cl
aula.usm.cl:158.69.169.42, 158.69.169.45
defider.usm.cl:174.138.67.116
dti.usm.cl:200.1.30.105
noticias.usm.cl:200.1.30.189
siga.usm.cl:200.1.30.92
sireb.usm.cl:200.1.30.28
vrea.usm.cl:200.1.18.220
www.usm.cl:200.1.24.53
www.vinadelmar.usm.cl:200.1.30.30
www.vra.usm.cl:200.1.24.51

┌──(root💀kali)-[/home/kali]
└─#
```

```
---AL INICIAR---
acceso root: sudo su
cambiar idioma teclado: setxkbmap -layout latam
ver las conexiones del pc: ifconfig
```

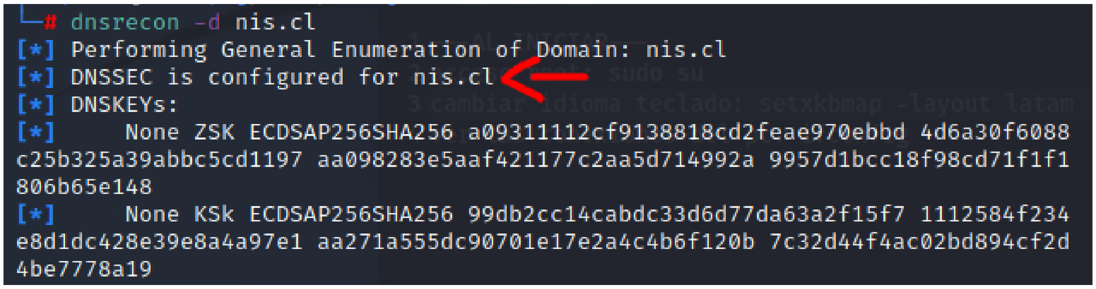
4) Valide si los siguientes dominios tienen habilitado DNSSec en sus servidores DNS

- microsoft.com



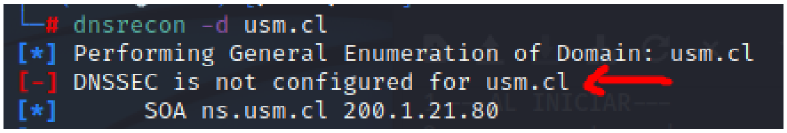
```
└─# dnsrecon -d microsoft.com
[*] Performing General Enumeration of Domain: microsoft.com
[-] DNSSEC is not configured for microsoft.com
[*]      SOA ns1-205.azure-dns.com 40.90.4.205
```

- nis.cl



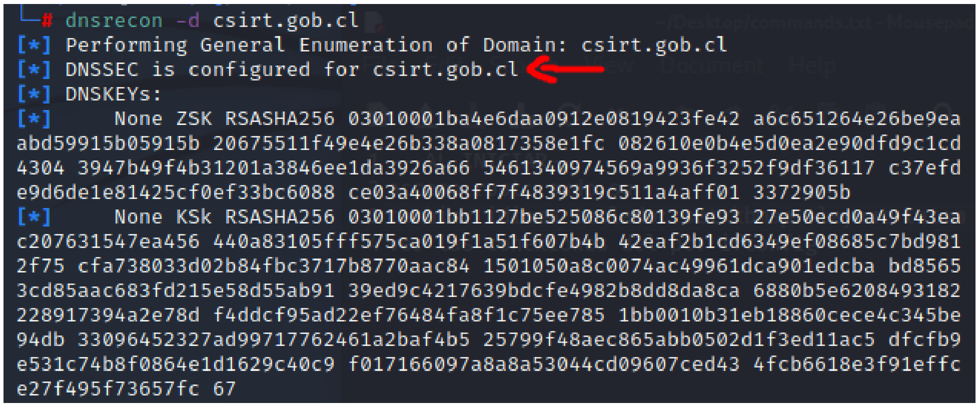
```
└─# dnsrecon -d nis.cl
[*] Performing General Enumeration of Domain: nis.cl
[*] DNSSEC is configured for nis.cl
[*] DNSKEYs:
[*]      None ZSK ECDSAP256SHA256 a09311112cf9138818cd2feae970ebbd 4d6a30f6088
c25b325a39abbc5cd1197 aa098283e5aaf421177c2aa5d714992a 9957d1bcc18f98cd71f1f1
806b65e148
[*]      None KSk ECDSAP256SHA256 99db2cc14cabdc33d6d77da63a2f15f7 1112584f234
e8d1dc428e39e8a4a97e1 aa271a555dc90701e17e2a4c4b6f120b 7c32d44f4ac02bd894cf2d
4be7778a19
```

- usm.cl



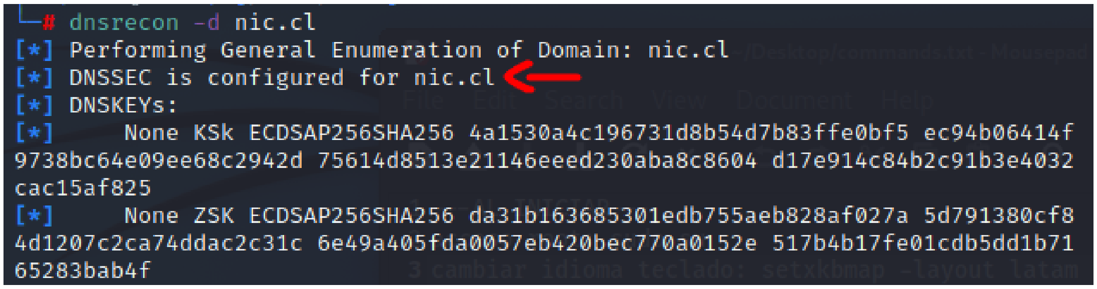
```
└─# dnsrecon -d usm.cl
[*] Performing General Enumeration of Domain: usm.cl
[-] DNSSEC is not configured for usm.cl
[*]      SOA ns.usm.cl 200.1.21.80
```

- csirt.gob.cl



```
└─# dnsrecon -d csirt.gob.cl
[*] Performing General Enumeration of Domain: csirt.gob.cl
[*] DNSSEC is configured for csirt.gob.cl
[*] DNSKEYs:
[*]      None ZSK RSASHA256 03010001ba4e6daa0912e0819423fe42 a6c651264e26be9ea
abd59915b05915b 20675511f49e4e26b338a0817358e1fc 082610e0b4e5d0ea2e90dfd9c1cd
4304 3947b49f4b31201a3846ee1da3926a66 5461340974569a9936f3252f9df36117 c37efd
e9d6de1e81425cf0ef33bc6088 ce03a40068ff7f4839319c511a4aff01 3372905b
[*]      None KSk RSASHA256 03010001bb1127be525086c80139fe93 27e50ecd0a49f43ea
c207631547ea456 440a83105fff575ca019f1a51f607b4b 42eaf2b1cd6349ef08685c7bd981
2f75 cfa738033d02b84fbc3717b8770aac84 1501050a8c0074ac49961dca901edcba bd8565
3cd85aac683fd215e58d55ab91 39ed9c4217639bdcfe4982b8dd8da8ca 6880b5e6208493182
228917394a2e78d f4ddcf95ad22ef76484fa8f1c75ee785 1bb0010b31eb18860cece4c345be
94db 33096452327ad99717762461a2baf4b5 25799f48aec865abb0502d1f3ed11ac5 dfcfb9
e531c74b8f0864e1d1629c40c9 f017166097a8a8a53044cd09607ced43 4fcb6618e3f91effc
e27f495f73657fc 67
```

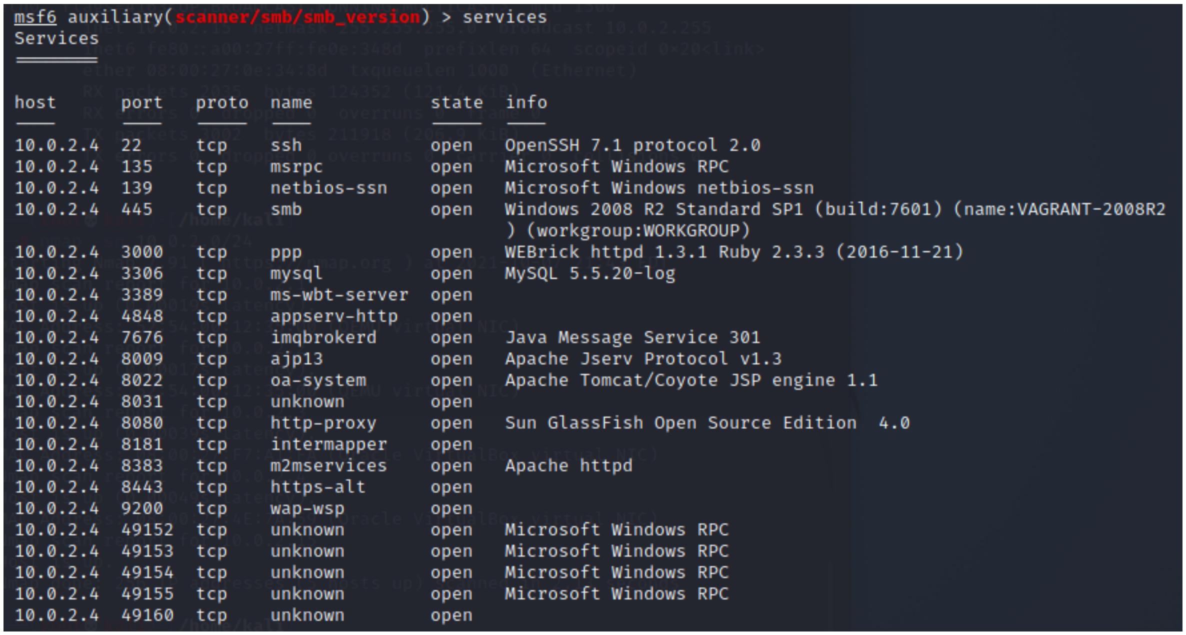
- nic.cl



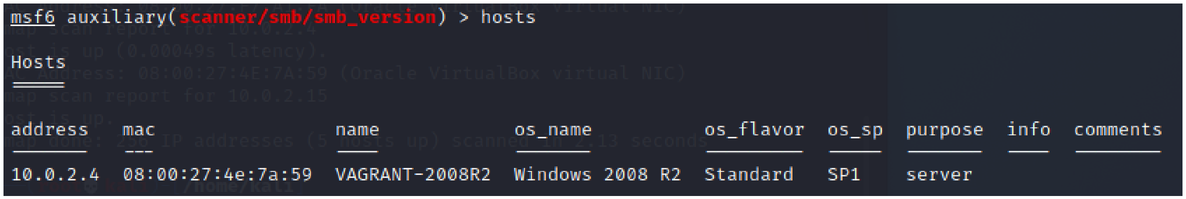
```
└─# dnsrecon -d nic.cl
[*] Performing General Enumeration of Domain: nic.cl
[*] DNSSEC is configured for nic.cl
[*] DNSKEYs:
[*]      None KSk ECDSAP256SHA256 4a1530a4c196731d8b54d7b83ffe0bf5 ec94b06414f
9738bc64e09ee68c2942d 75614d8513e21146eeed230aba8c8604 d17e914c84b2c91b3e4032
cac15af825
[*]      None ZSK ECDSAP256SHA256 da31b163685301edb755aeb828af027a 5d791380cf8
4d1207c2ca74ddac2c31c 6e49a405fda0057eb420bec770a0152e 517b4b17fe01cdb5dd1b71
65283bab4f
```

5) Utilizando workspace con Metasploit obtenga el listado de todos los servicios y sus versiones de las máquinas Metasploitable III y Windows 7, además del sistema operativo.

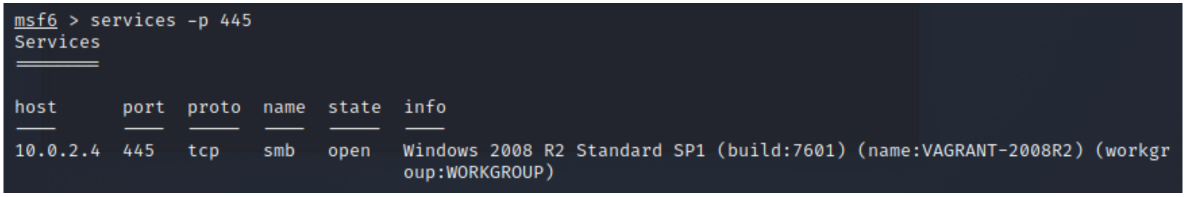
Para Metasploitable III



```
msf6 auxiliary(scanner/smb/smb_version) > services
Services
========

host      port   proto  name           state  info
----      ----   -----  ----           -----  ----
10.0.2.4  22     tcp    ssh            open   OpenSSH 7.1 protocol 2.0
10.0.2.4  135    tcp    msrpc          open   Microsoft Windows RPC
10.0.2.4  139    tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
10.0.2.4  445    tcp    smb            open   Windows 2008 R2 Standard SP1 (build:7601) (name:VAGRANT-2008R2
                                              ) (workgroup:WORKGROUP)
10.0.2.4  3000   tcp    ppp            open   WEBrick httpd 1.3.1 Ruby 2.3.3 (2016-11-21)
10.0.2.4  3306   tcp    mysql          open   MySQL 5.5.20-log
10.0.2.4  3389   tcp    ms-wbt-server  open
10.0.2.4  4848   tcp    appserv-http   open
10.0.2.4  7676   tcp    imqbrokerd     open   Java Message Service 301
10.0.2.4  8009   tcp    ajp13          open   Apache Jserv Protocol v1.3
10.0.2.4  8022   tcp    oa-system      open   Apache Tomcat/Coyote JSP engine 1.1
10.0.2.4  8031   tcp    unknown        open
10.0.2.4  8080   tcp    http-proxy     open   Sun GlassFish Open Source Edition  4.0
10.0.2.4  8181   tcp    intermapper    open
10.0.2.4  8383   tcp    m2mservices    open   Apache httpd
10.0.2.4  8443   tcp    https-alt      open
10.0.2.4  9200   tcp    wap-wsp        open
10.0.2.4  49152  tcp    unknown        open   Microsoft Windows RPC
10.0.2.4  49153  tcp    unknown        open   Microsoft Windows RPC
10.0.2.4  49154  tcp    unknown        open   Microsoft Windows RPC
10.0.2.4  49155  tcp    unknown        open   Microsoft Windows RPC
10.0.2.4  49160  tcp    unknown        open
```

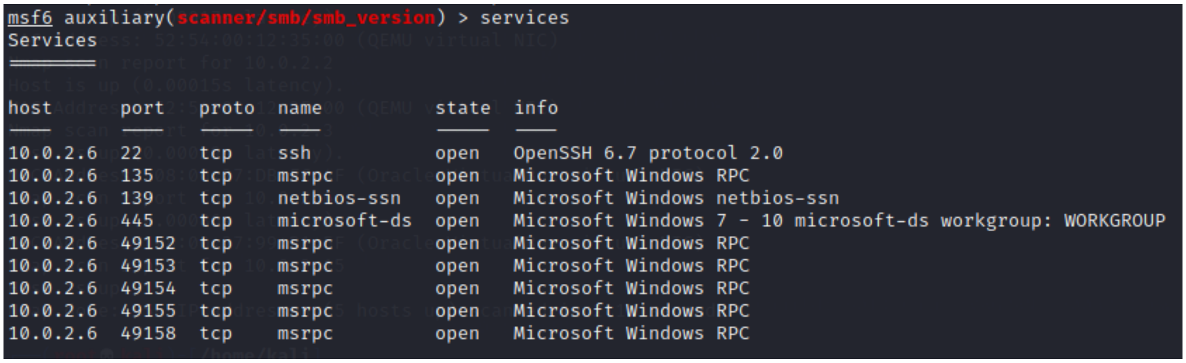


```
msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address   mac                name            os_name           os_flavor  os_sp  purpose  info  comments
-------   ---                ----            -------           ---------  -----  -------  ----  --------
10.0.2.4  08:00:27:4e:7a:59  VAGRANT-2008R2  Windows 2008 R2   Standard   SP1    server
```

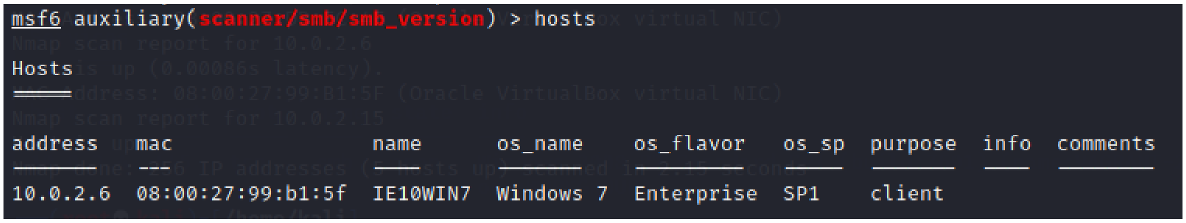


```
msf6 > services -p 445
Services
========

host      port  proto  name  state  info
----      ----  -----  ----  -----  ----
10.0.2.4  445   tcp    smb   open   Windows 2008 R2 Standard SP1 (build:7601) (name:VAGRANT-2008R2) (workgr
                                    oup:WORKGROUP)
```

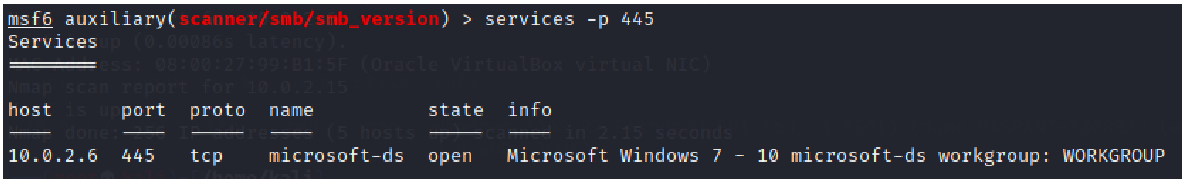
Windows 7



```
msf6 auxiliary(scanner/smb/smb_version) > services
Services
========

host      port   proto  name          state  info
----      ----   -----  ----          -----  ----
10.0.2.6  22     tcp    ssh           open   OpenSSH 6.7 protocol 2.0
10.0.2.6  135    tcp    msrpc         open   Microsoft Windows RPC
10.0.2.6  139    tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
10.0.2.6  445    tcp    microsoft-ds  open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.0.2.6  49152  tcp    msrpc         open   Microsoft Windows RPC
10.0.2.6  49153  tcp    msrpc         open   Microsoft Windows RPC
10.0.2.6  49154  tcp    msrpc         open   Microsoft Windows RPC
10.0.2.6  49155  tcp    msrpc         open   Microsoft Windows RPC
10.0.2.6  49158  tcp    msrpc         open   Microsoft Windows RPC
```



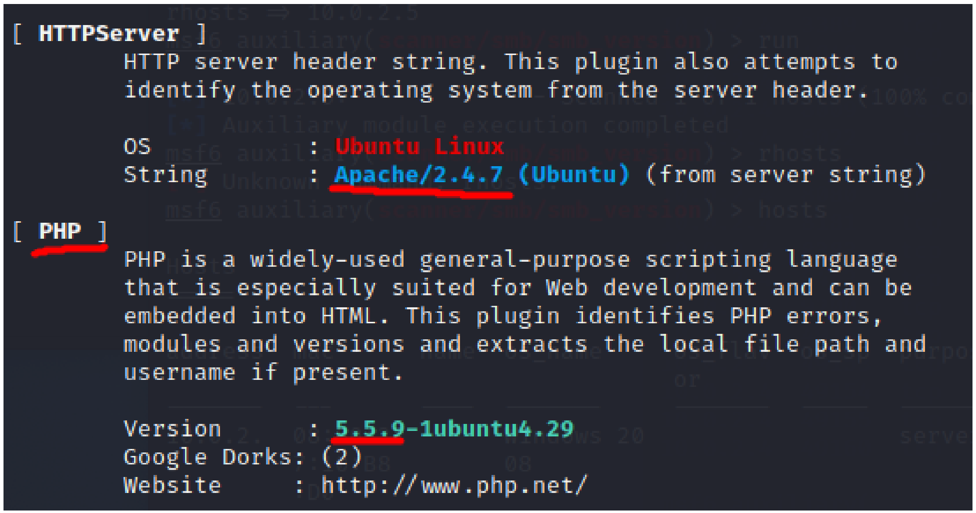
```
msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address   mac                name      os_name    os_flavor   os_sp  purpose  info  comments
-------   ---                ----      -------    ---------   -----  -------  ----  --------
10.0.2.6  08:00:27:99:b1:5f  IE10WIN7  Windows 7  Enterprise  SP1    client
```



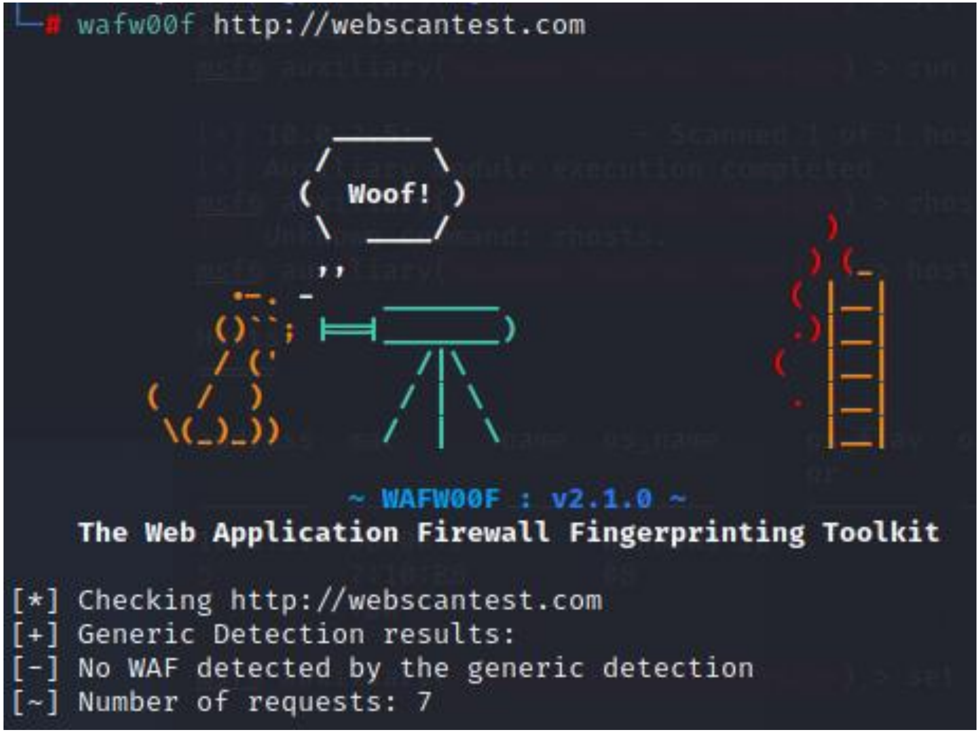
```
msf6 auxiliary(scanner/smb/smb_version) > services -p 445
Services
========

host      port  proto  name          state  info
----      ----  -----  ----          -----  ----
10.0.2.6  445   tcp    microsoft-ds  open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
```

6) Obtenga la versión del servidor web y del lenguaje de los siguientes sitios web

- http://webscantest.com/

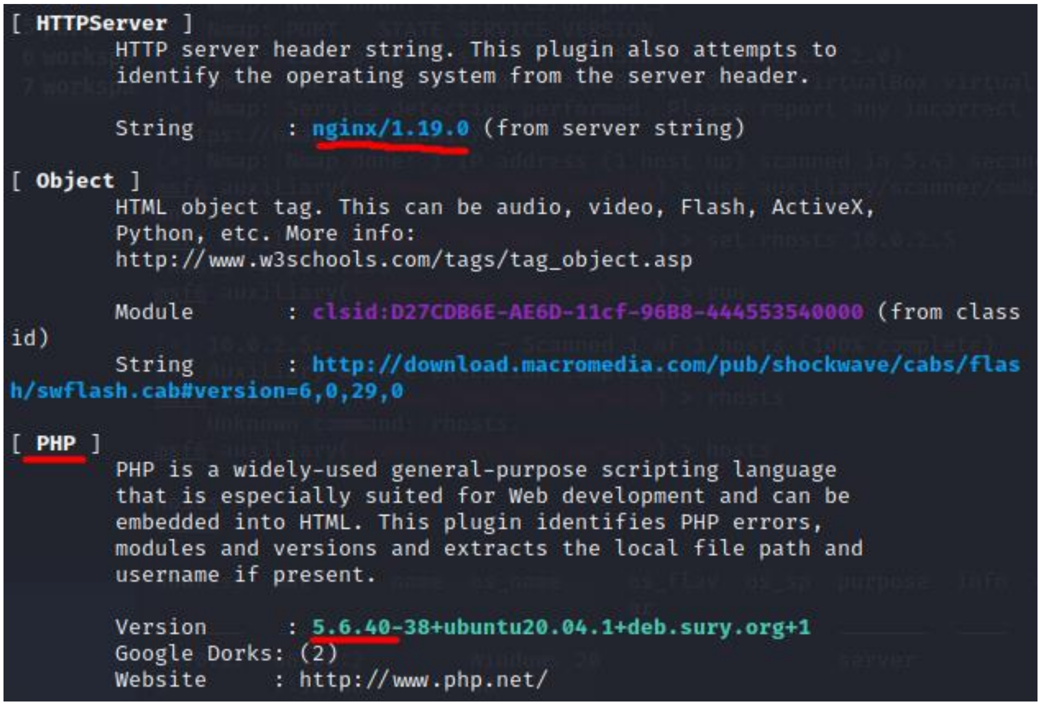


```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS          : Ubuntu Linux
        String      : Apache/2.4.7 (Ubuntu) (from server string)

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version     : 5.5.9-1ubuntu4.29
        Google Dorks: (2)
        Website     : http://www.php.net/
```

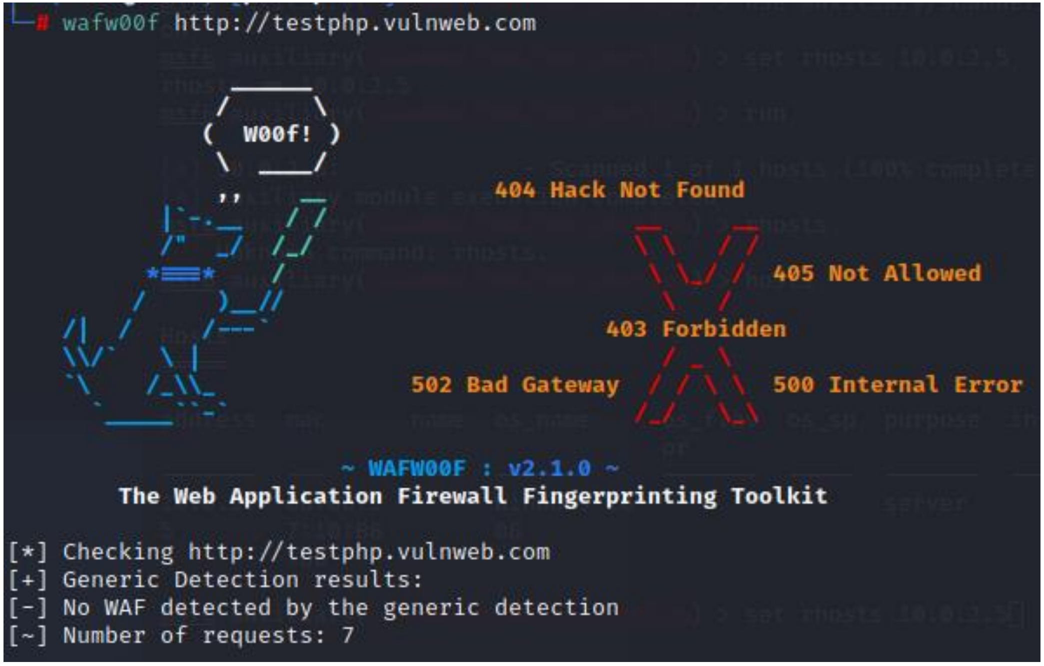


```
└─# wafw00f http://webscantest.com

                ~ WAFW00F : v2.1.0 ~
 The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://webscantest.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- http://testphp.vulnweb.com/

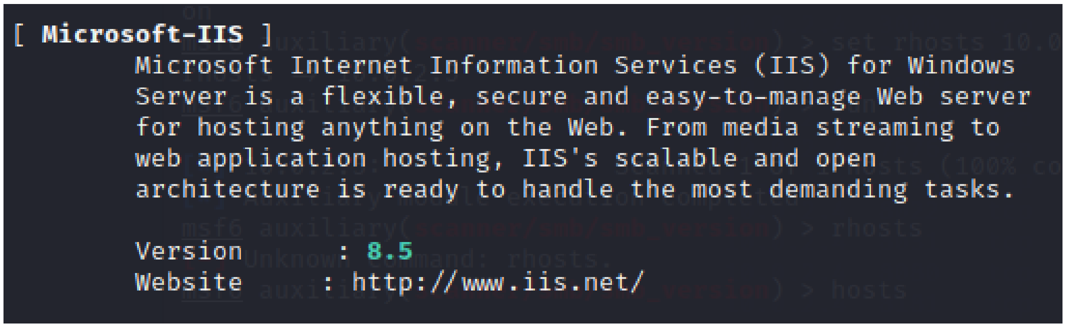


```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : nginx/1.19.0 (from server string)

[ Object ]
        HTML object tag. This can be audio, video, Flash, ActiveX,
        Python, etc. More info:
        http://www.w3schools.com/tags/tag_object.asp

        Module       : clsid:D27CDB6E-AE6D-11cf-96B8-444553540000 (from class
id)
        String       : http://download.macromedia.com/pub/shockwave/cabs/flas
h/swflash.cab#version=6,0,29,0

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
        Google Dorks: (2)
        Website      : http://www.php.net/
```

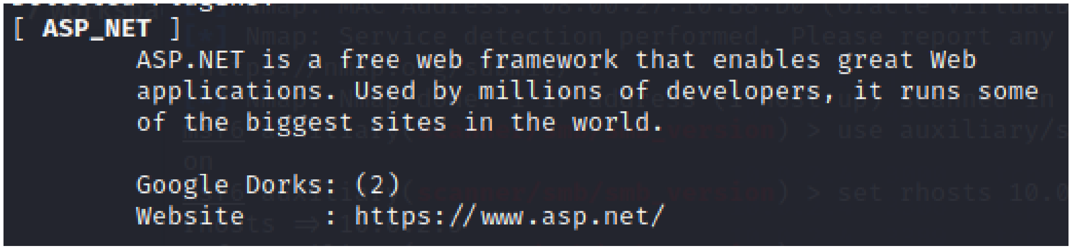


```
└─# wafw00f http://testphp.vulnweb.com

                ( W00f! )

                                404 Hack Not Found
                                                    405 Not Allowed
                                        403 Forbidden
                            502 Bad Gateway          500 Internal Error

                        ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://testphp.vulnweb.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

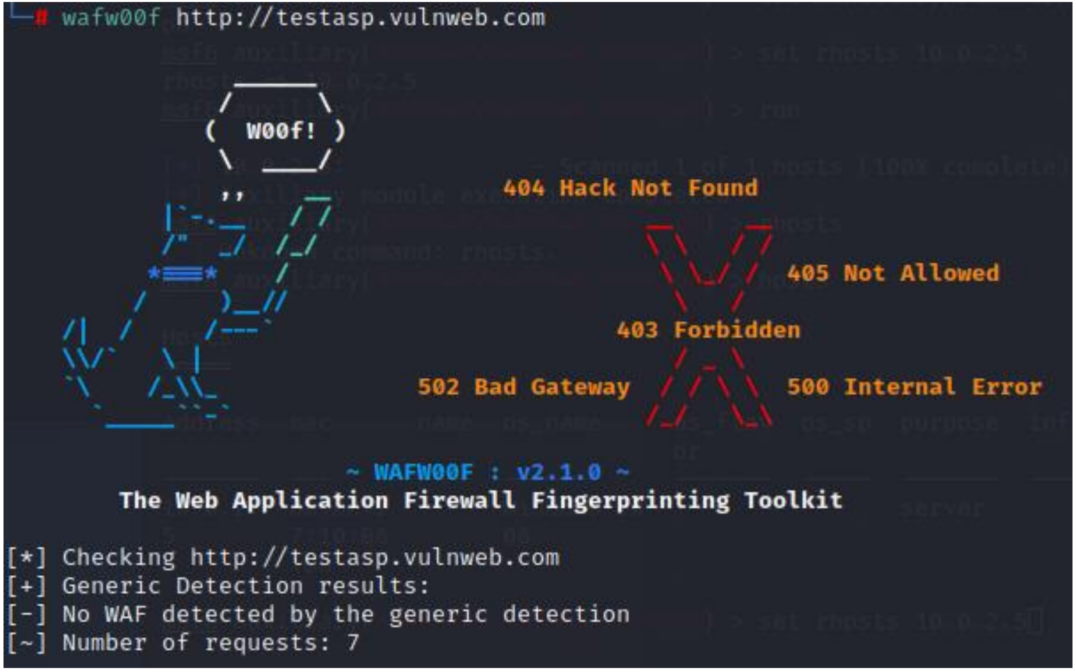
- http://testasp.vulnweb.com/



```
[ Microsoft-IIS ]
        Microsoft Internet Information Services (IIS) for Windows
        Server is a flexible, secure and easy-to-manage Web server
        for hosting anything on the Web. From media streaming to
        web application hosting, IIS's scalable and open
        architecture is ready to handle the most demanding tasks.

        Version      : 8.5
        Website     : http://www.iis.net/
```

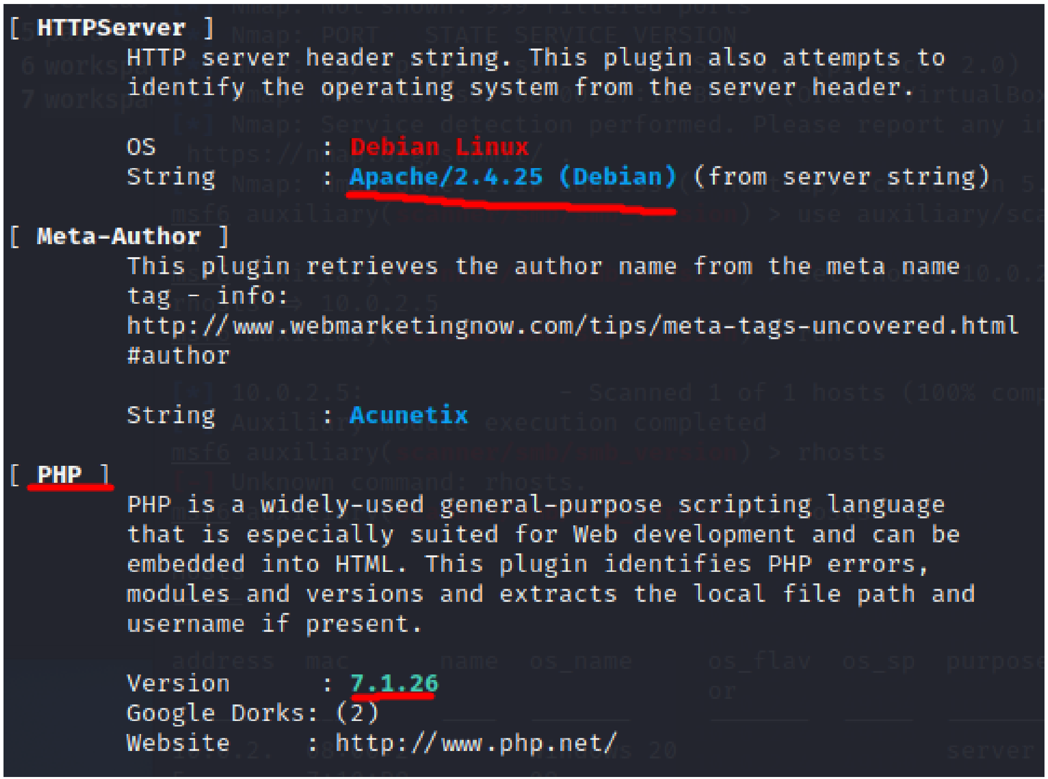


```
[ ASP_NET ]
        ASP.NET is a free web framework that enables great Web
        applications. Used by millions of developers, it runs some
        of the biggest sites in the world.

        Google Dorks: (2)
        Website     : https://www.asp.net/
```

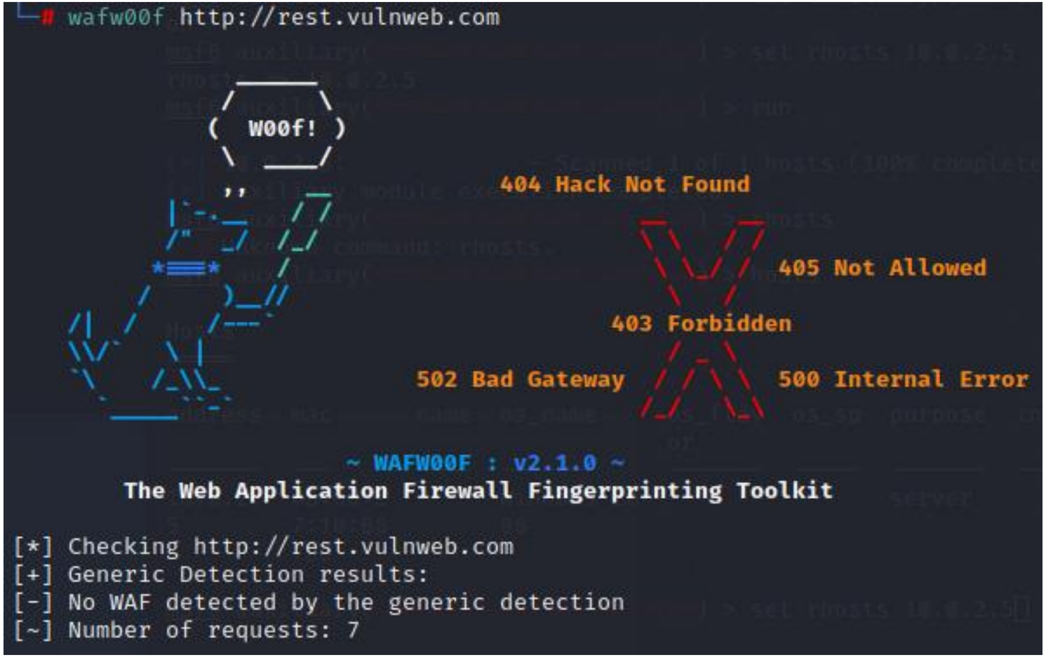


```
└─# wafw00f http://testasp.vulnweb.com

                    ______
                   /      \
                  (  W00f! )
                   \  ____/
                   ,,                    404 Hack Not Found

                                                                405 Not Allowed

                                                  403 Forbidden

                                         502 Bad Gateway             500 Internal Error

                             ~ WAFW00F : v2.1.0 ~
              The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://testasp.vulnweb.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- http://rest.vulnweb.com/

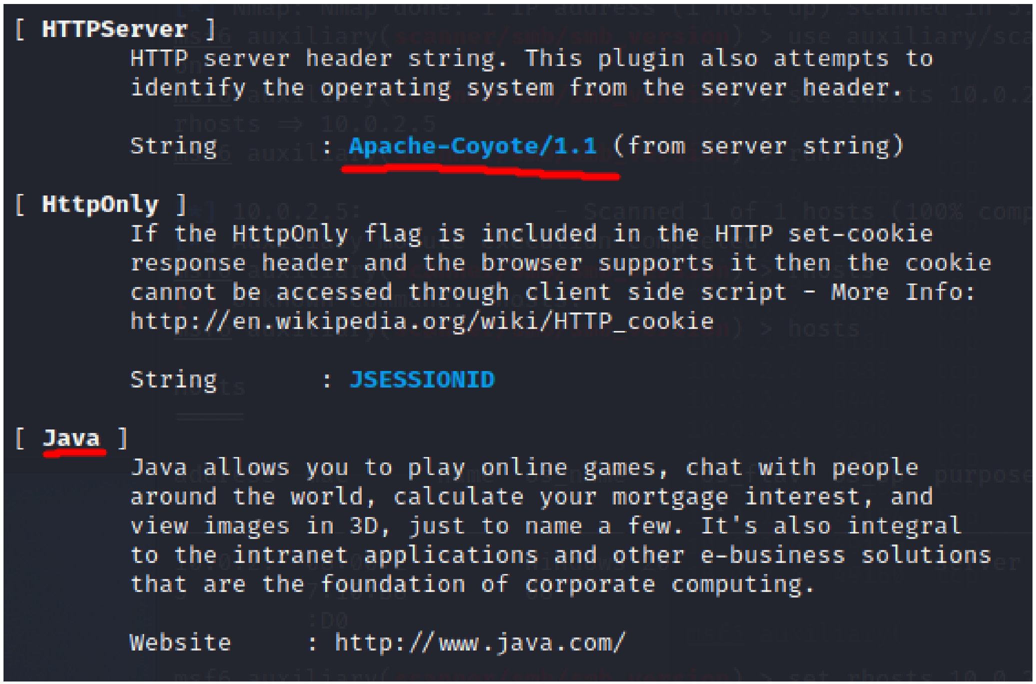


```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Debian Linux
        String       : Apache/2.4.25 (Debian) (from server string)

[ Meta-Author ]
        This plugin retrieves the author name from the meta name
        tag - info:
        http://www.webmarketingnow.com/tips/meta-tags-uncovered.html
        #author

        String       : Acunetix

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 7.1.26
        Google Dorks: (2)
        Website     : http://www.php.net/
```

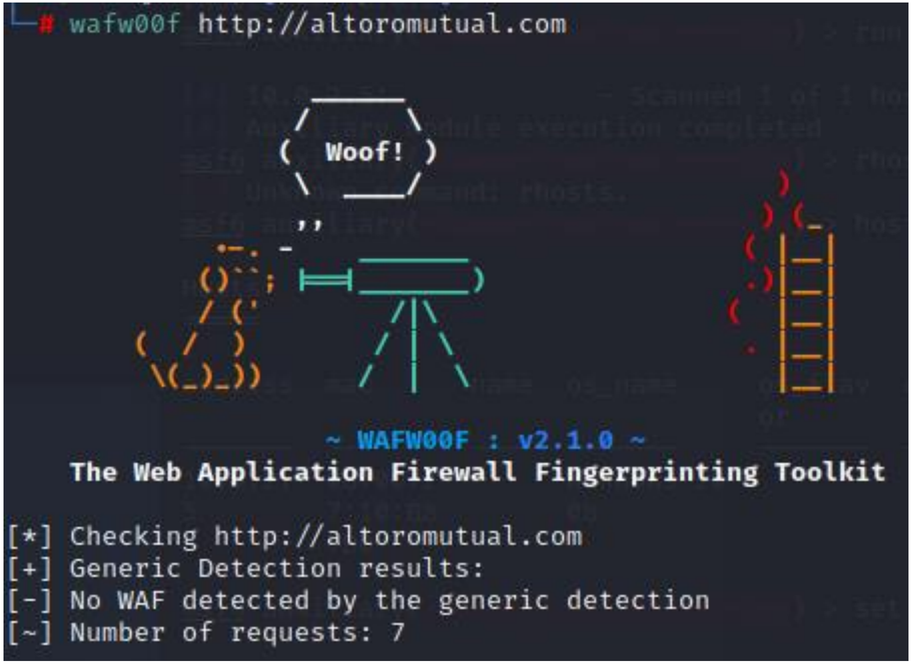


```
└─# wafw00f http://rest.vulnweb.com

                ( Woof! )
                                  404 Hack Not Found
                                                      405 Not Allowed
                                          403 Forbidden
                          502 Bad Gateway             500 Internal Error

                       ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://rest.vulnweb.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- https://altoromutual.com/



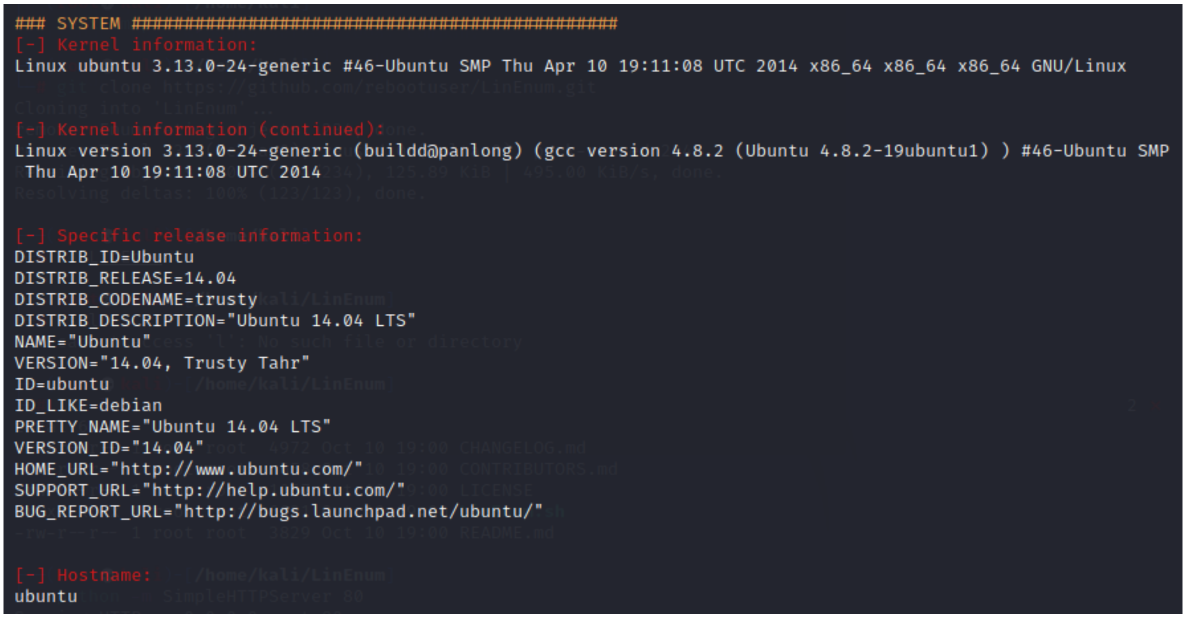
```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Apache-Coyote/1.1 (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

        String       : JSESSIONID

[ Java ]
        Java allows you to play online games, chat with people
        around the world, calculate your mortgage interest, and
        view images in 3D, just to name a few. It's also integral
        to the intranet applications and other e-business solutions
        that are the foundation of corporate computing.

        Website     : http://www.java.com/
```



```
└─# wafw00f http://altoromutual.com

                ( Woof! )

                ~ WAFW00F : v2.1.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://altoromutual.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

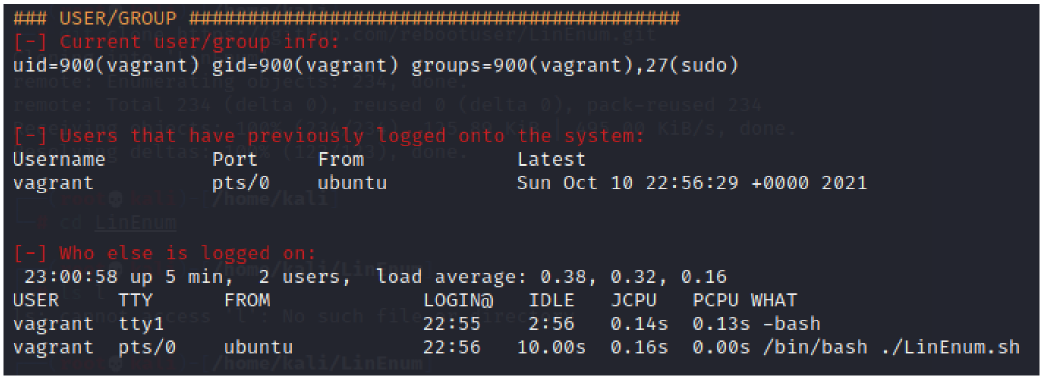
7) Realice la enumeración interna de la máquina Metasploitable III (Linux) utilizando la herramienta Linenum y obtenga lo siguiente:

- Versión del Sistema Operativo

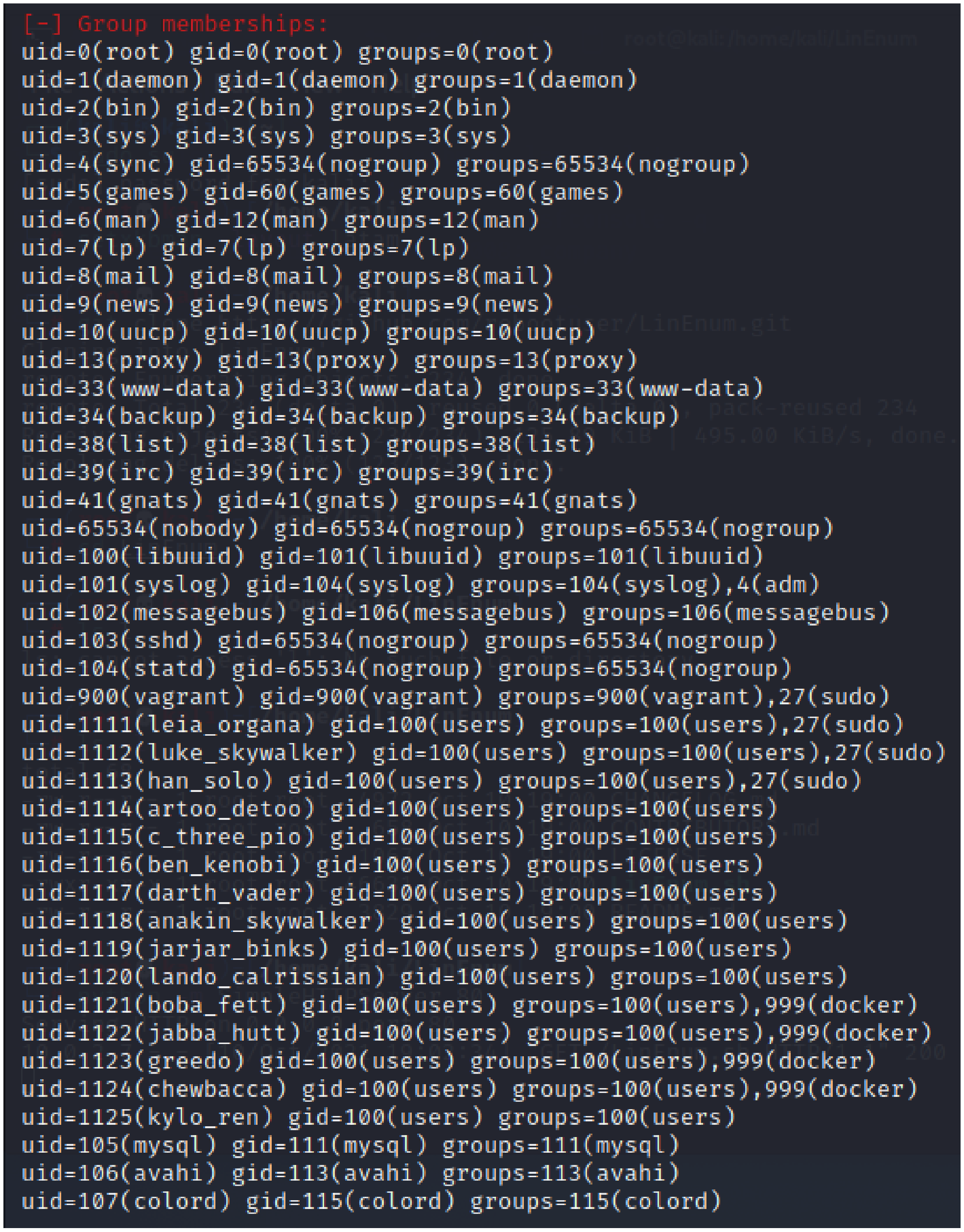


```
### SYSTEM ##############################################
[-] Kernel information:
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 3.13.0-24-generic (buildd@panlong) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) ) #46-Ubuntu SMP
 Thu Apr 10 19:11:08 UTC 2014


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04 LTS"
NAME="Ubuntu"
VERSION="14.04, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"


[-] Hostname:
ubuntu
```

- Listado de usuarios

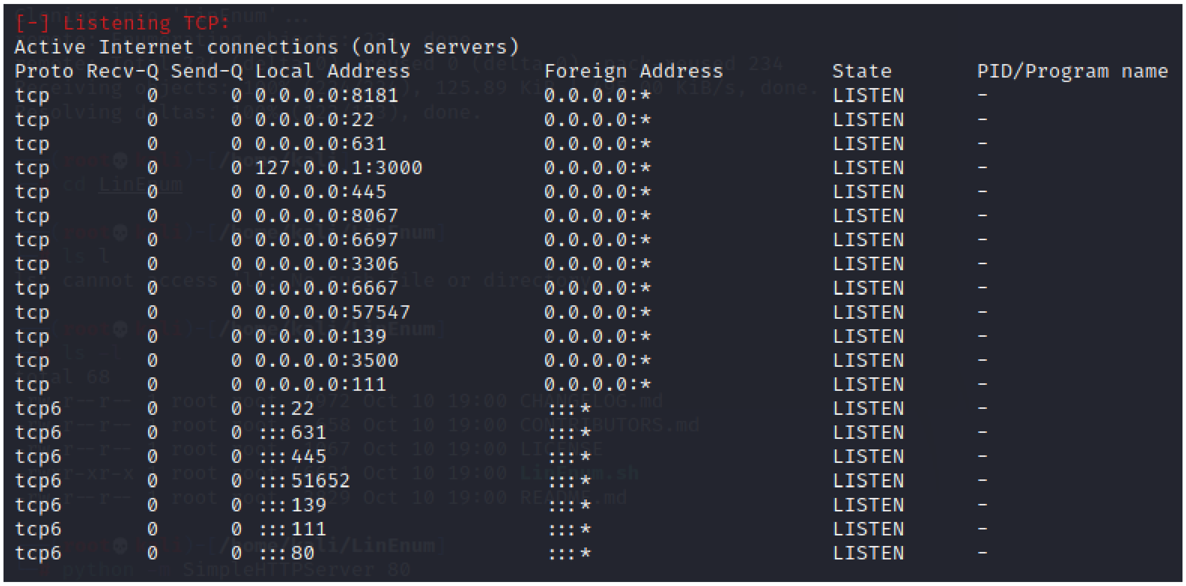


```
### USER/GROUP ##########################################
[-] Current user/group info:
uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo)


[-] Users that have previously logged onto the system:
Username         Port     From             Latest
vagrant          pts/0    ubuntu           Sun Oct 10 22:56:29 +0000 2021


[-] Who else is logged on:
 23:00:58 up 5 min,  2 users,  load average: 0.38, 0.32, 0.16
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
vagrant  tty1                      22:55    2:56   0.14s  0.13s -bash
vagrant  pts/0    ubuntu           22:56   10.00s  0.16s  0.00s /bin/bash ./LinEnum.sh
```



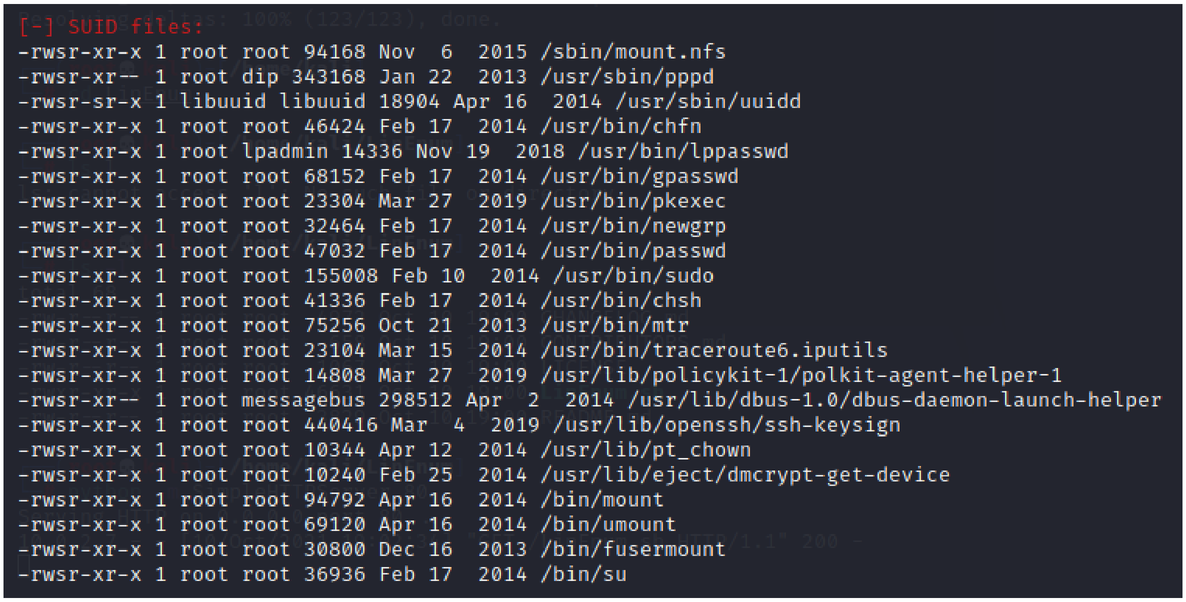
```
[-] Group memberships:
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
uid=101(syslog) gid=104(syslog) groups=104(syslog),4(adm)
uid=102(messagebus) gid=106(messagebus) groups=106(messagebus)
uid=103(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=104(statd) gid=65534(nogroup) groups=65534(nogroup)
uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo)
uid=1111(leia_organa) gid=100(users) groups=100(users),27(sudo)
uid=1112(luke_skywalker) gid=100(users) groups=100(users),27(sudo)
uid=1113(han_solo) gid=100(users) groups=100(users),27(sudo)
uid=1114(artoo_detoo) gid=100(users) groups=100(users)
uid=1115(c_three_pio) gid=100(users) groups=100(users)
uid=1116(ben_kenobi) gid=100(users) groups=100(users)
uid=1117(darth_vader) gid=100(users) groups=100(users)
uid=1118(anakin_skywalker) gid=100(users) groups=100(users)
uid=1119(jarjar_binks) gid=100(users) groups=100(users)
uid=1120(lando_calrissian) gid=100(users) groups=100(users)
uid=1121(boba_fett) gid=100(users) groups=100(users),999(docker)
uid=1122(jabba_hutt) gid=100(users) groups=100(users),999(docker)
uid=1123(greedo) gid=100(users) groups=100(users),999(docker)
uid=1124(chewbacca) gid=100(users) groups=100(users),999(docker)
uid=1125(kylo_ren) gid=100(users) groups=100(users)
uid=105(mysql) gid=111(mysql) groups=111(mysql)
uid=106(avahi) gid=113(avahi) groups=113(avahi)
uid=107(colord) gid=115(colord) groups=115(colord)
```

- Listado de servicios TCP



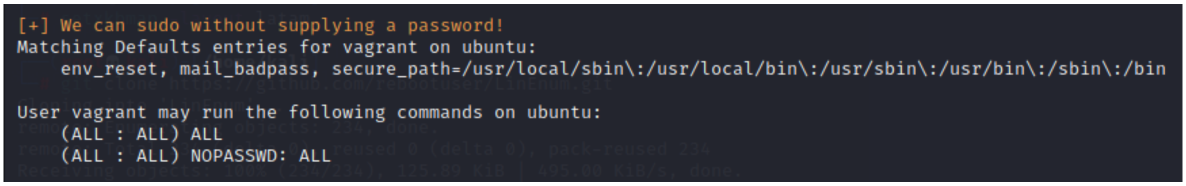
```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:8181            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8067            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:57547           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3500            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::631                  :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
tcp6       0      0 :::51652                :::*                    LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
```

- Listado de archivos con suid habilitado



```
[-] SUID files:
-rwsr-xr-x 1 root root 94168 Nov  6  2015 /sbin/mount.nfs
-rwsr-xr-- 1 root dip 343168 Jan 22  2013 /usr/sbin/pppd
-rwsr-sr-x 1 libuuid libuuid 18904 Apr 16  2014 /usr/sbin/uuidd
-rwsr-xr-x 1 root root 46424 Feb 17  2014 /usr/bin/chfn
-rwsr-xr-x 1 root lpadmin 14336 Nov 19  2018 /usr/bin/lppasswd
-rwsr-xr-x 1 root root 68152 Feb 17  2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 23304 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 32464 Feb 17  2014 /usr/bin/newgrp
-rwsr-xr-x 1 root root 47032 Feb 17  2014 /usr/bin/passwd
-rwsr-xr-x 1 root root 155008 Feb 10  2014 /usr/bin/sudo
-rwsr-xr-x 1 root root 41336 Feb 17  2014 /usr/bin/chsh
-rwsr-xr-x 1 root root 75256 Oct 21  2013 /usr/bin/mtr
-rwsr-xr-x 1 root root 23104 Mar 15  2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 14808 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 298512 Apr  2  2014 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 440416 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10344 Apr 12  2014 /usr/lib/pt_chown
-rwsr-xr-x 1 root root 10240 Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 94792 Apr 16  2014 /bin/mount
-rwsr-xr-x 1 root root 69120 Apr 16  2014 /bin/umount
-rwsr-xr-x 1 root root 30800 Dec 16  2013 /bin/fusermount
-rwsr-xr-x 1 root root 36936 Feb 17  2014 /bin/su
```

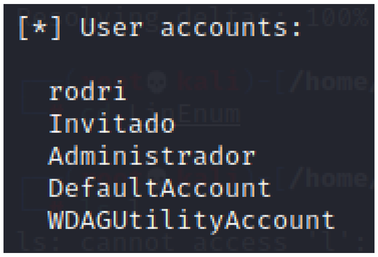
- Comandos que puede ejecutar el usuario vagrant utilizando sudo



```
[+] We can sudo without supplying a password!
Matching Defaults entries for vagrant on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User vagrant may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (ALL : ALL) NOPASSWD: ALL
```

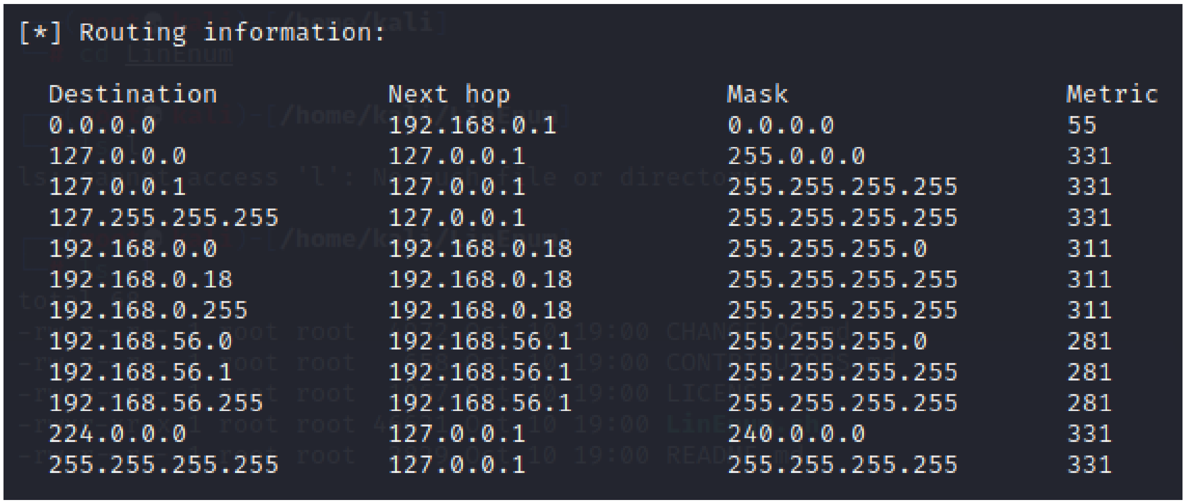
8) Habilite la configuración SNMP en su máquina Windows 10, realice la enumeración de dicho protocolo y obtenga los siguientes datos:

- Listado de usuarios



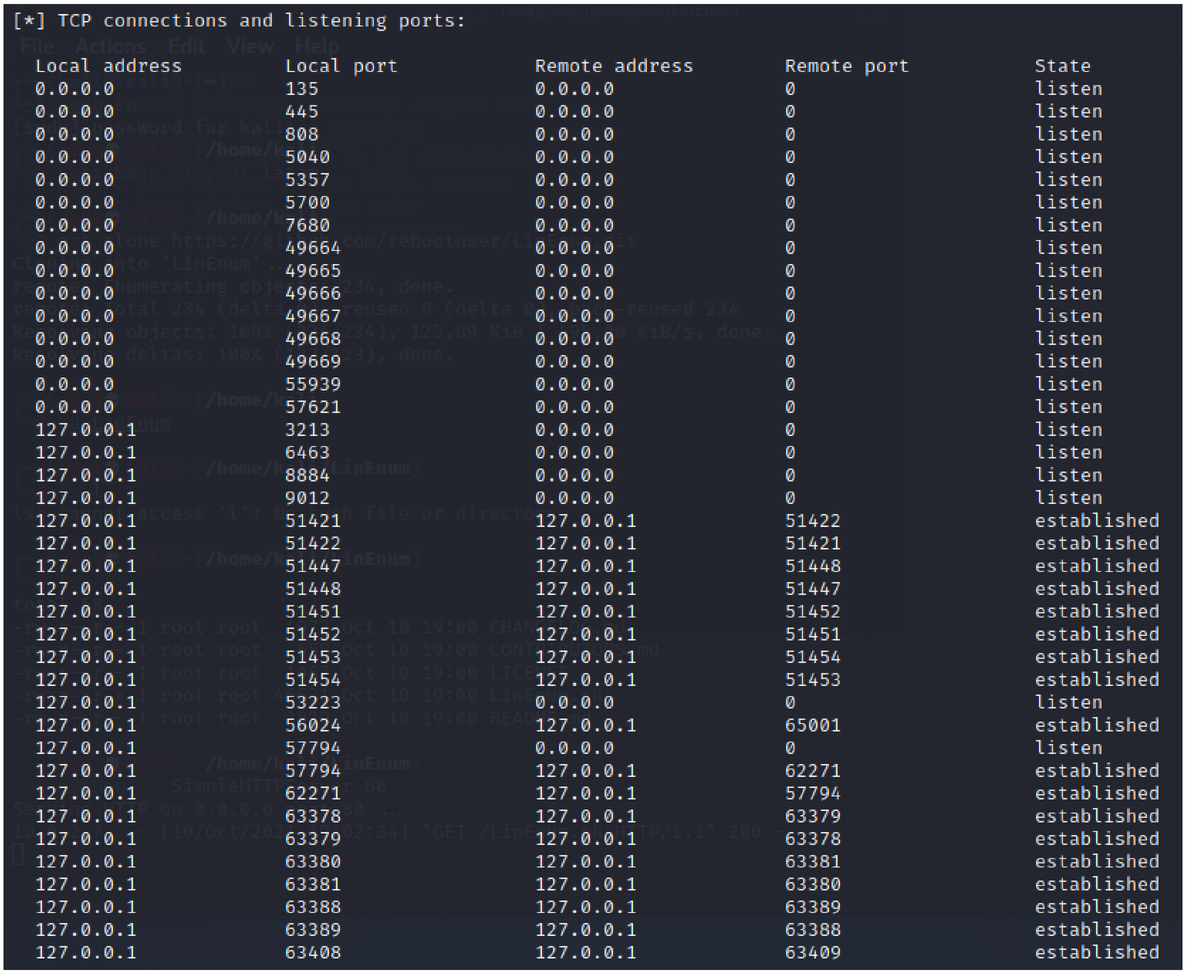
```
[*] User accounts:

  rodri
  Invitado
  Administrador
  DefaultAccount
  WDAGUtilityAccount
```

- Listado de rutas

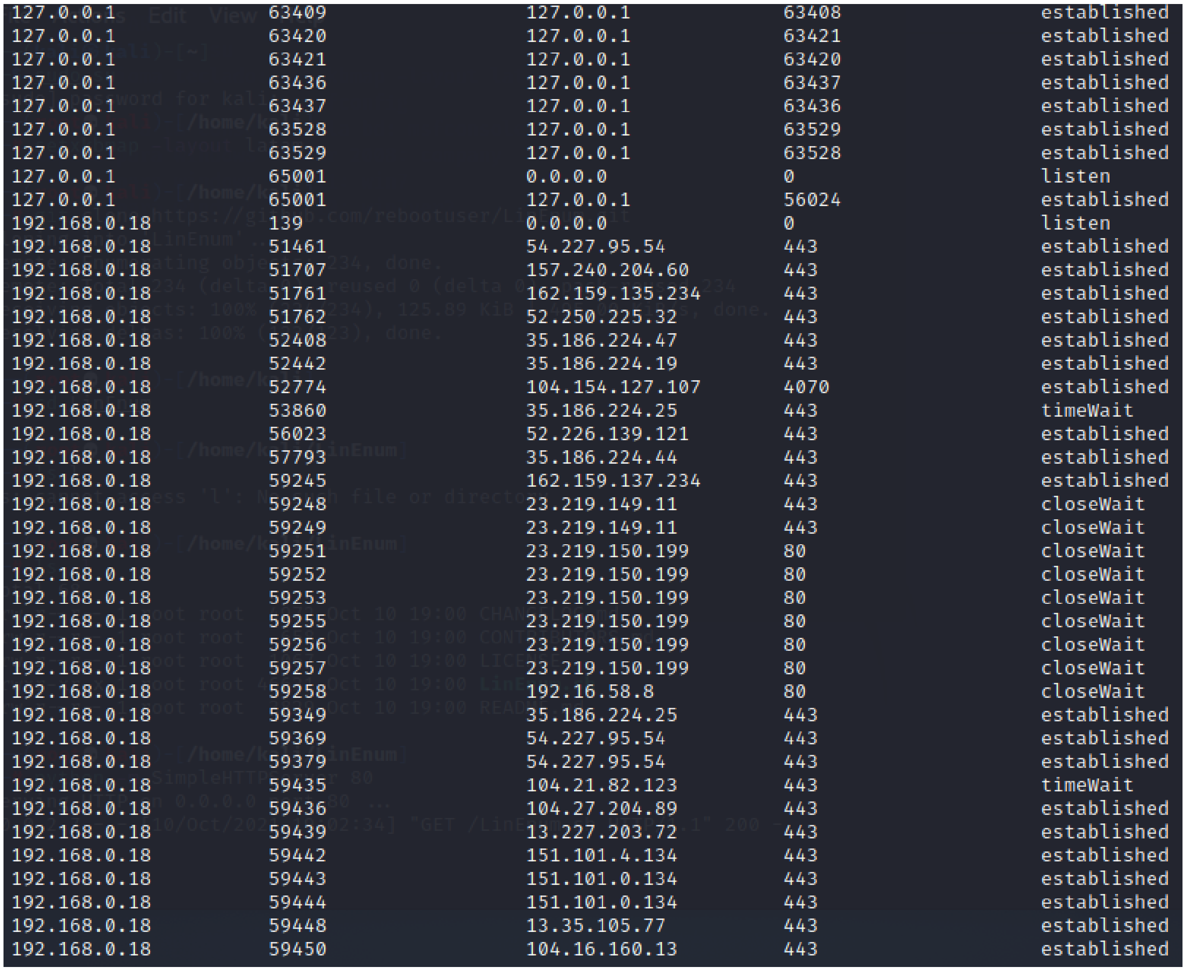


```
[*] Routing information:

  Destination          Next hop             Mask                 Metric
  0.0.0.0              192.168.0.1          0.0.0.0              55
  127.0.0.0            127.0.0.1            255.0.0.0            331
  127.0.0.1            127.0.0.1            255.255.255.255      331
  127.255.255.255      127.0.0.1            255.255.255.255      331
  192.168.0.0          192.168.0.18         255.255.255.0        311
  192.168.0.18         192.168.0.18         255.255.255.255      311
  192.168.0.255        192.168.0.18         255.255.255.255      311
  192.168.56.0         192.168.56.1         255.255.255.0        281
  192.168.56.1         192.168.56.1         255.255.255.255      281
  192.168.56.255       192.168.56.1         255.255.255.255      281
  224.0.0.0            127.0.0.1            240.0.0.0            331
  255.255.255.255      127.0.0.1            255.255.255.255      331
```

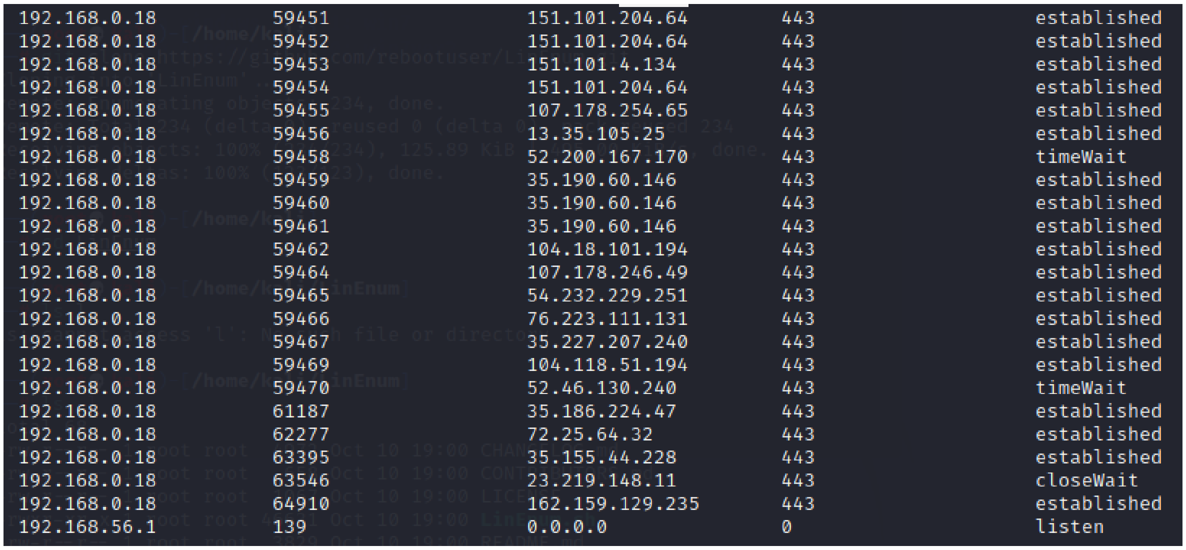
- Listado de servicios TCP



```
[*] TCP connections and listening ports:

   Local address          Local port             Remote address         Remote port            State
   0.0.0.0                135                    0.0.0.0                0                      listen
   0.0.0.0                445                    0.0.0.0                0                      listen
   0.0.0.0                808                    0.0.0.0                0                      listen
   0.0.0.0                5040                   0.0.0.0                0                      listen
   0.0.0.0                5357                   0.0.0.0                0                      listen
   0.0.0.0                5700                   0.0.0.0                0                      listen
   0.0.0.0                7680                   0.0.0.0                0                      listen
   0.0.0.0                49664                  0.0.0.0                0                      listen
   0.0.0.0                49665                  0.0.0.0                0                      listen
   0.0.0.0                49666                  0.0.0.0                0                      listen
   0.0.0.0                49667                  0.0.0.0                0                      listen
   0.0.0.0                49668                  0.0.0.0                0                      listen
   0.0.0.0                49669                  0.0.0.0                0                      listen
   0.0.0.0                55939                  0.0.0.0                0                      listen
   0.0.0.0                57621                  0.0.0.0                0                      listen
   127.0.0.1              3213                   0.0.0.0                0                      listen
   127.0.0.1              6463                   0.0.0.0                0                      listen
   127.0.0.1              8884                   0.0.0.0                0                      listen
   127.0.0.1              9012                   0.0.0.0                0                      listen
   127.0.0.1              51421                  127.0.0.1              51422                  established
   127.0.0.1              51422                  127.0.0.1              51421                  established
   127.0.0.1              51447                  127.0.0.1              51448                  established
   127.0.0.1              51448                  127.0.0.1              51447                  established
   127.0.0.1              51451                  127.0.0.1              51452                  established
   127.0.0.1              51452                  127.0.0.1              51451                  established
   127.0.0.1              51453                  127.0.0.1              51454                  established
   127.0.0.1              51454                  127.0.0.1              51453                  established
   127.0.0.1              53223                  0.0.0.0                0                      listen
   127.0.0.1              56024                  127.0.0.1              65001                  established
   127.0.0.1              57794                  0.0.0.0                0                      listen
   127.0.0.1              57794                  127.0.0.1              62271                  established
   127.0.0.1              62271                  127.0.0.1              57794                  established
   127.0.0.1              63378                  127.0.0.1              63379                  established
   127.0.0.1              63379                  127.0.0.1              63378                  established
   127.0.0.1              63380                  127.0.0.1              63381                  established
   127.0.0.1              63381                  127.0.0.1              63380                  established
   127.0.0.1              63388                  127.0.0.1              63389                  established
   127.0.0.1              63389                  127.0.0.1              63388                  established
   127.0.0.1              63408                  127.0.0.1              63409                  established
```

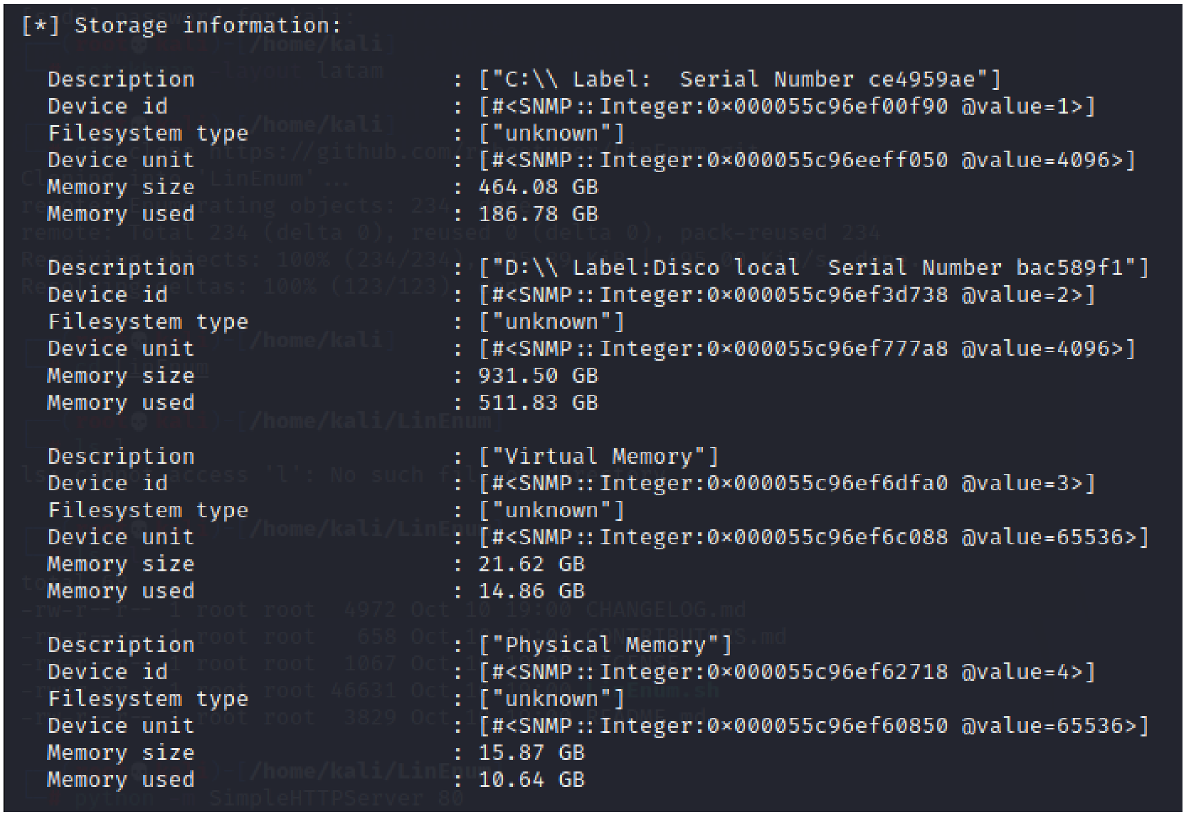


```
127.0.0.1       63409       127.0.0.1         63408      established
127.0.0.1       63420       127.0.0.1         63421      established
127.0.0.1       63421       127.0.0.1         63420      established
127.0.0.1       63436       127.0.0.1         63437      established
127.0.0.1       63437       127.0.0.1         63436      established
127.0.0.1       63528       127.0.0.1         63529      established
127.0.0.1       63529       127.0.0.1         63528      established
127.0.0.1       65001       0.0.0.0           0          listen
127.0.0.1       65001       127.0.0.1         56024      established
192.168.0.18    139         0.0.0.0           0          listen
192.168.0.18    51461       54.227.95.54      443        established
192.168.0.18    51707       157.240.204.60    443        established
192.168.0.18    51761       162.159.135.234   443        established
192.168.0.18    51762       52.250.225.32     443        established
192.168.0.18    52408       35.186.224.47     443        established
192.168.0.18    52442       35.186.224.19     443        established
192.168.0.18    52774       104.154.127.107   4070       established
192.168.0.18    53860       35.186.224.25     443        timeWait
192.168.0.18    56023       52.226.139.121    443        established
192.168.0.18    57793       35.186.224.44     443        established
192.168.0.18    59245       162.159.137.234   443        established
192.168.0.18    59248       23.219.149.11     443        closeWait
192.168.0.18    59249       23.219.149.11     443        closeWait
192.168.0.18    59251       23.219.150.199    80         closeWait
192.168.0.18    59252       23.219.150.199    80         closeWait
192.168.0.18    59253       23.219.150.199    80         closeWait
192.168.0.18    59255       23.219.150.199    80         closeWait
192.168.0.18    59256       23.219.150.199    80         closeWait
192.168.0.18    59257       23.219.150.199    80         closeWait
192.168.0.18    59258       192.16.58.8       80         closeWait
192.168.0.18    59349       35.186.224.25     443        established
192.168.0.18    59369       54.227.95.54      443        established
192.168.0.18    59379       54.227.95.54      443        established
192.168.0.18    59435       104.21.82.123     443        timeWait
192.168.0.18    59436       104.27.204.89     443        established
192.168.0.18    59439       13.227.203.72     443        established
192.168.0.18    59442       151.101.4.134     443        established
192.168.0.18    59443       151.101.0.134     443        established
192.168.0.18    59444       151.101.0.134     443        established
192.168.0.18    59448       13.35.105.77      443        established
192.168.0.18    59450       104.16.160.13     443        established
```



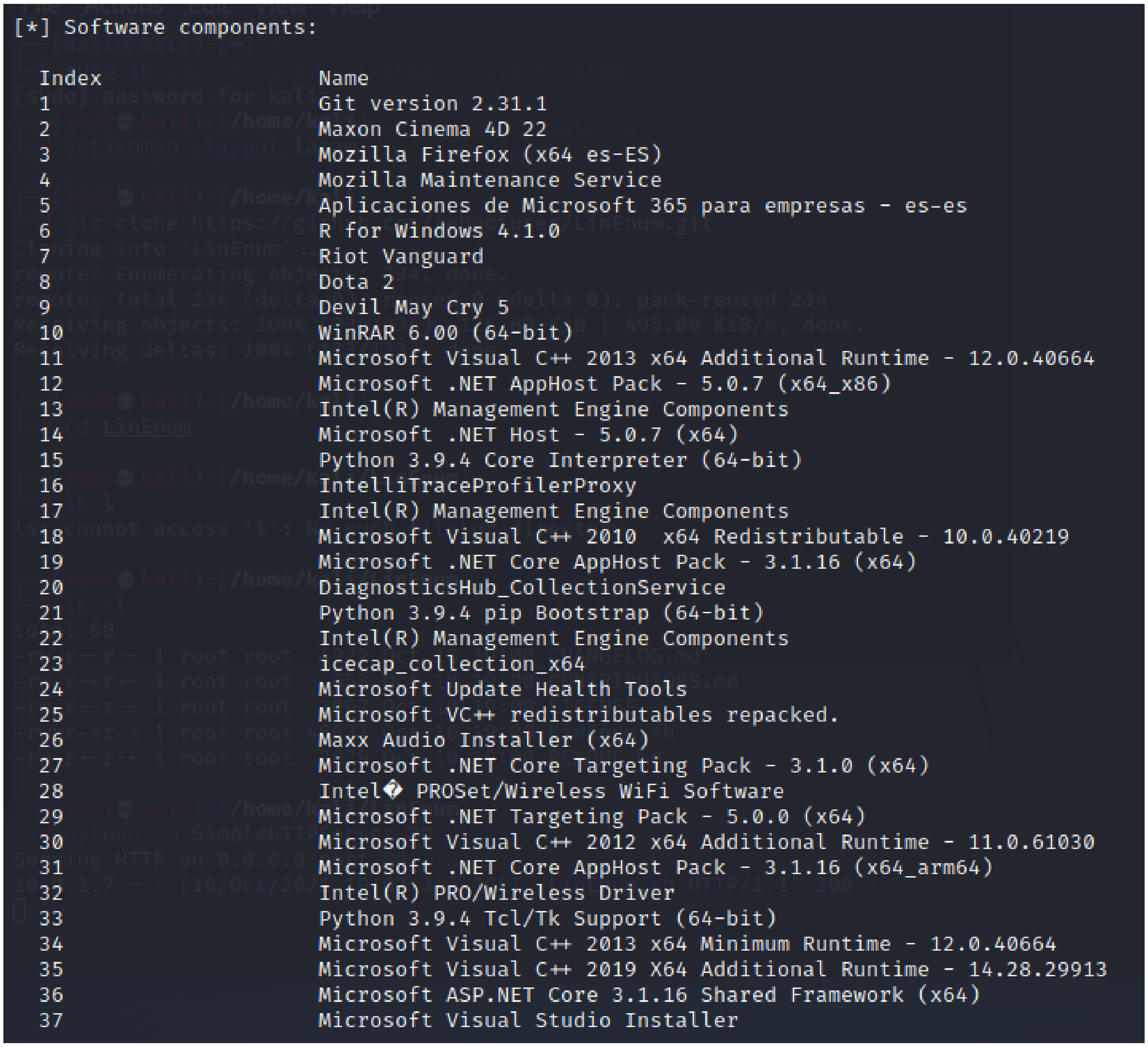
```
192.168.0.18    59451       151.101.204.64    443        established
192.168.0.18    59452       151.101.204.64    443        established
192.168.0.18    59453       151.101.4.134     443        established
192.168.0.18    59454       151.101.204.64    443        established
192.168.0.18    59455       107.178.254.65    443        established
192.168.0.18    59456       13.35.105.25      443        established
192.168.0.18    59458       52.200.167.170    443        timeWait
192.168.0.18    59459       35.190.60.146     443        established
192.168.0.18    59460       35.190.60.146     443        established
192.168.0.18    59461       35.190.60.146     443        established
192.168.0.18    59462       104.18.101.194    443        established
192.168.0.18    59464       107.178.246.49    443        established
192.168.0.18    59465       54.232.229.251    443        established
192.168.0.18    59466       76.223.111.131    443        established
192.168.0.18    59467       35.227.207.240    443        established
192.168.0.18    59469       104.118.51.194    443        established
192.168.0.18    59470       52.46.130.240     443        timeWait
192.168.0.18    61187       35.186.224.47     443        established
192.168.0.18    62277       72.25.64.32       443        established
192.168.0.18    63395       35.155.44.228     443        established
192.168.0.18    63546       23.219.148.11     443        closeWait
192.168.0.18    64910       162.159.129.235   443        established
192.168.56.1    139         0.0.0.0           0          listen
```

- Configuración del disco duro



```
[*] Storage information:

  Description                 : ["C:\\ Label:  Serial Number ce4959ae"]
  Device id                   : [#<SNMP::Integer:0x000055c96ef00f90 @value=1>]
  Filesystem type             : ["unknown"]
  Device unit                 : [#<SNMP::Integer:0x000055c96eeff050 @value=4096>]
  Memory size                 : 464.08 GB
  Memory used                 : 186.78 GB

  Description                 : ["D:\\ Label:Disco local  Serial Number bac589f1"]
  Device id                   : [#<SNMP::Integer:0x000055c96ef3d738 @value=2>]
  Filesystem type             : ["unknown"]
  Device unit                 : [#<SNMP::Integer:0x000055c96ef777a8 @value=4096>]
  Memory size                 : 931.50 GB
  Memory used                 : 511.83 GB

  Description                 : ["Virtual Memory"]
  Device id                   : [#<SNMP::Integer:0x000055c96ef6dfa0 @value=3>]
  Filesystem type             : ["unknown"]
  Device unit                 : [#<SNMP::Integer:0x000055c96ef6c088 @value=65536>]
  Memory size                 : 21.62 GB
  Memory used                 : 14.86 GB

  Description                 : ["Physical Memory"]
  Device id                   : [#<SNMP::Integer:0x000055c96ef62718 @value=4>]
  Filesystem type             : ["unknown"]
  Device unit                 : [#<SNMP::Integer:0x000055c96ef60850 @value=65536>]
  Memory size                 : 15.87 GB
  Memory used                 : 10.64 GB
```

- Listado de aplicaciones instaladas



```
[*] Software components:

  Index                 Name
  1                     Git version 2.31.1
  2                     Maxon Cinema 4D 22
  3                     Mozilla Firefox (x64 es-ES)
  4                     Mozilla Maintenance Service
  5                     Aplicaciones de Microsoft 365 para empresas - es-es
  6                     R for Windows 4.1.0
  7                     Riot Vanguard
  8                     Dota 2
  9                     Devil May Cry 5
  10                    WinRAR 6.00 (64-bit)
  11                    Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664
  12                    Microsoft .NET AppHost Pack - 5.0.7 (x64_x86)
  13                    Intel(R) Management Engine Components
  14                    Microsoft .NET Host - 5.0.7 (x64)
  15                    Python 3.9.4 Core Interpreter (64-bit)
  16                    IntelliTraceProfilerProxy
  17                    Intel(R) Management Engine Components
  18                    Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219
  19                    Microsoft .NET Core AppHost Pack - 3.1.16 (x64)
  20                    DiagnosticsHub_CollectionService
  21                    Python 3.9.4 pip Bootstrap (64-bit)
  22                    Intel(R) Management Engine Components
  23                    icecap_collection_x64
  24                    Microsoft Update Health Tools
  25                    Microsoft VC++ redistributables repacked.
  26                    Maxx Audio Installer (x64)
  27                    Microsoft .NET Core Targeting Pack - 3.1.0 (x64)
  28                    Intel� PROSet/Wireless WiFi Software
  29                    Microsoft .NET Targeting Pack - 5.0.0 (x64)
  30                    Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030
  31                    Microsoft .NET Core AppHost Pack - 3.1.16 (x64_arm64)
  32                    Intel(R) PRO/Wireless Driver
  33                    Python 3.9.4 Tcl/Tk Support (64-bit)
  34                    Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40664
  35                    Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29913
  36                    Microsoft ASP.NET Core 3.1.16 Shared Framework (x64)
  37                    Microsoft Visual Studio Installer
```