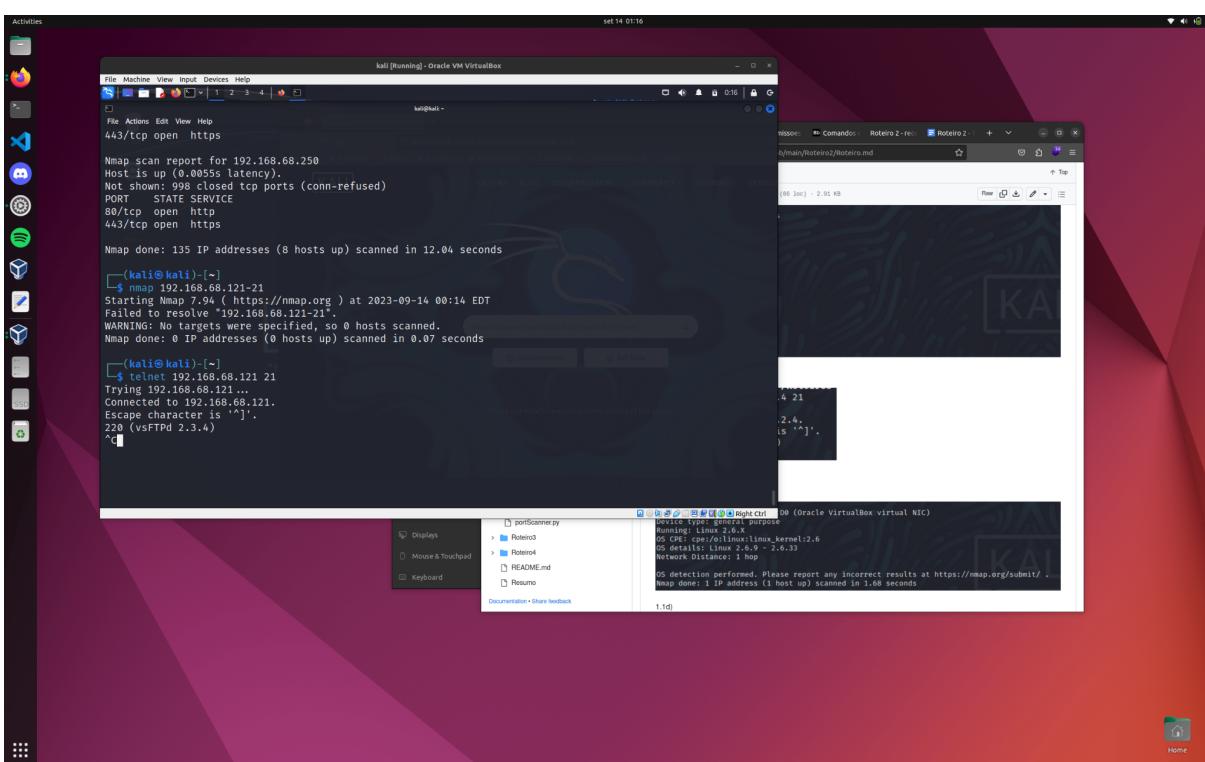
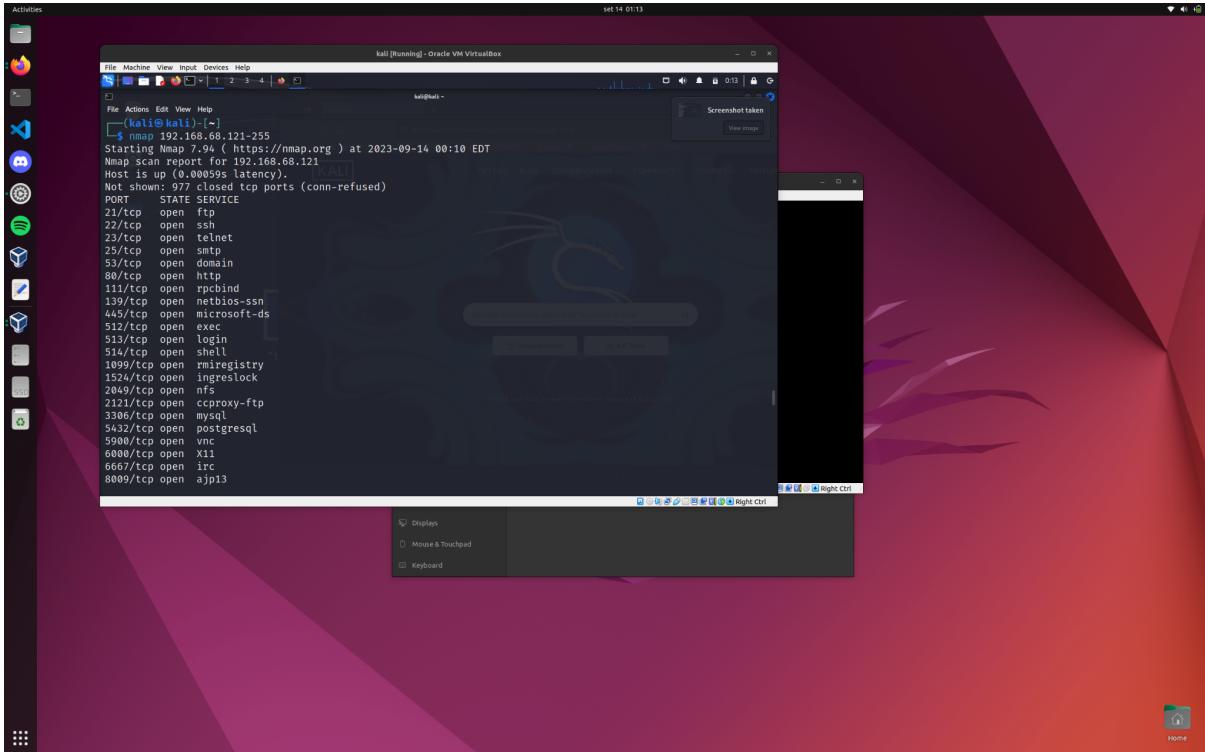


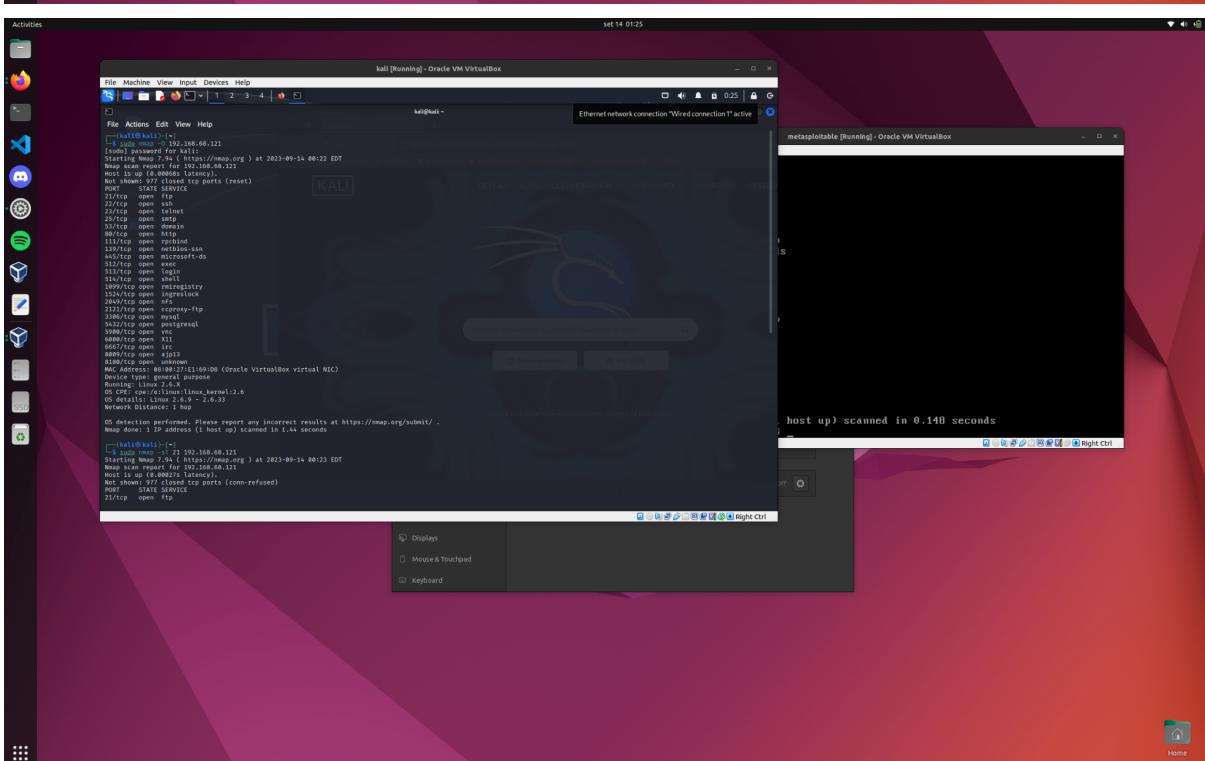
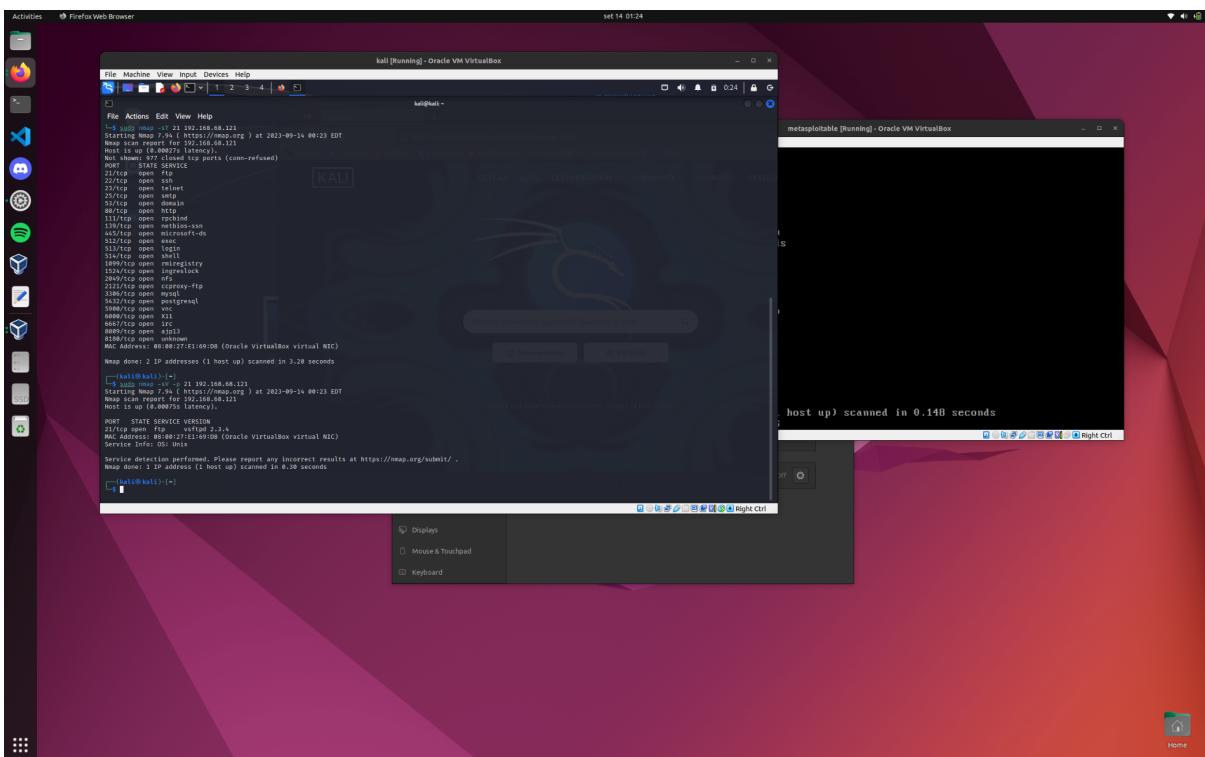
Tecnologias Hacker - Roteiro 2

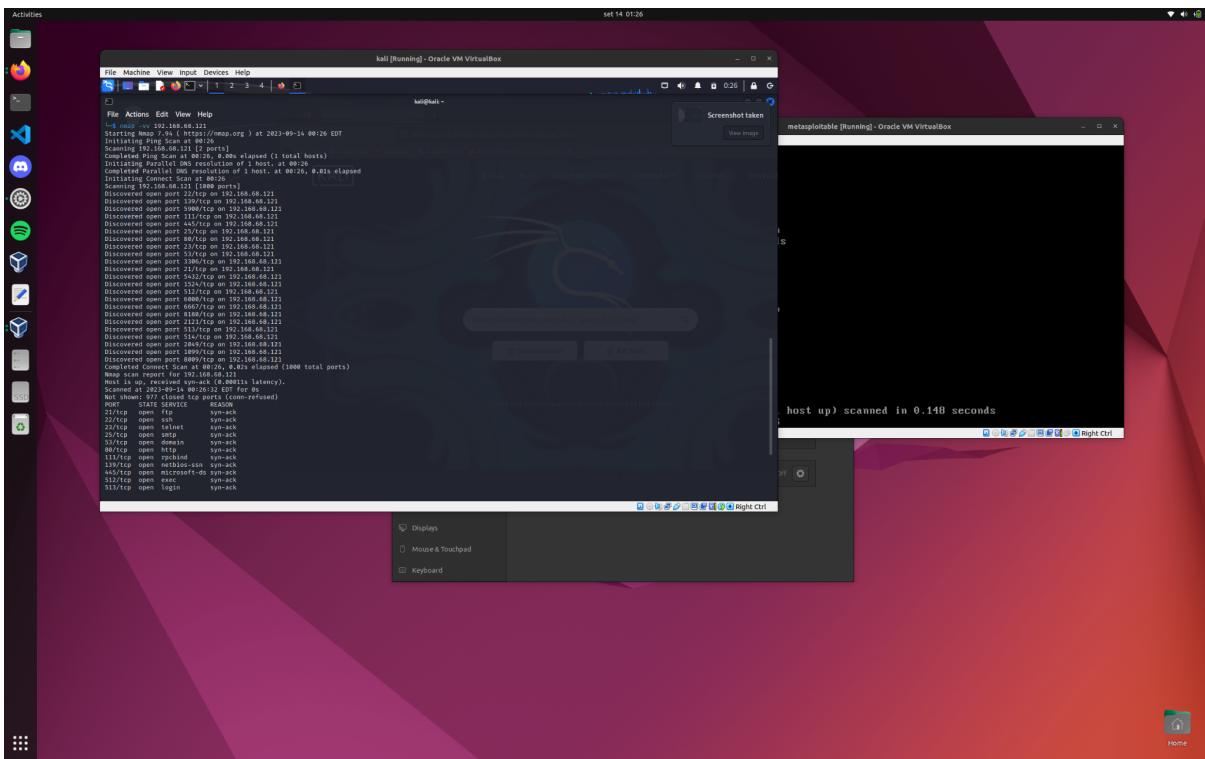
Arthur Carvalho

A:



B





C e D

com o comando `nmap -sV --script vuln -p 21,445 192.168.68.118` foi possível identificar vulnerabilidades na porta 21, que, em sequência, foi alvo de um encontro de um possível backdoor utilizando o comando `nmap -v --script malware -p 21,445 192.168.68.118`

```

File Actions Edit View Help
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
Starting Nmap 7.7.0 ( https://nmap.org ) at 2023-09-14 08:26 EDT
Nmap scan report for 192.168.68.118
Host is up (0.0000s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.148 seconds
[!] vuln[kali]:~ -> nmap -sV -script vuln -p 21,445 192.168.68.118
Starting Nmap 7.7.0 ( https://nmap.org ) at 2023-09-14 09:35 EDT
NSE: loaded 10 scripts for scanning.
NSE: Script pre-scanning.
NSE: Script pre-scanning completed. Please report any incorrect results at https://nmap.org/submit/
Host script results:
|_vsftpd-backdoor: Script execution failed (use -d to debug)
|_vsftpd-backdoor: false
|_vsftpd-backdoor: false
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds
[!] vuln[kali]:~ -> nmap -v --script malware -p 21,445 192.168.68.118
Starting Nmap 7.7.0 ( https://nmap.org ) at 2023-09-14 09:41 EDT
NSE: loaded 10 scripts for scanning.
NSE: Script pre-scanning.
NSE: Script pre-scanning completed. Please report any incorrect results at https://nmap.org/submit/
Host script results:
|_vsftpd-backdoor: Script execution failed (use -d to debug)
|_vsftpd-backdoor: false
|_vsftpd-backdoor: false
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds

```

E

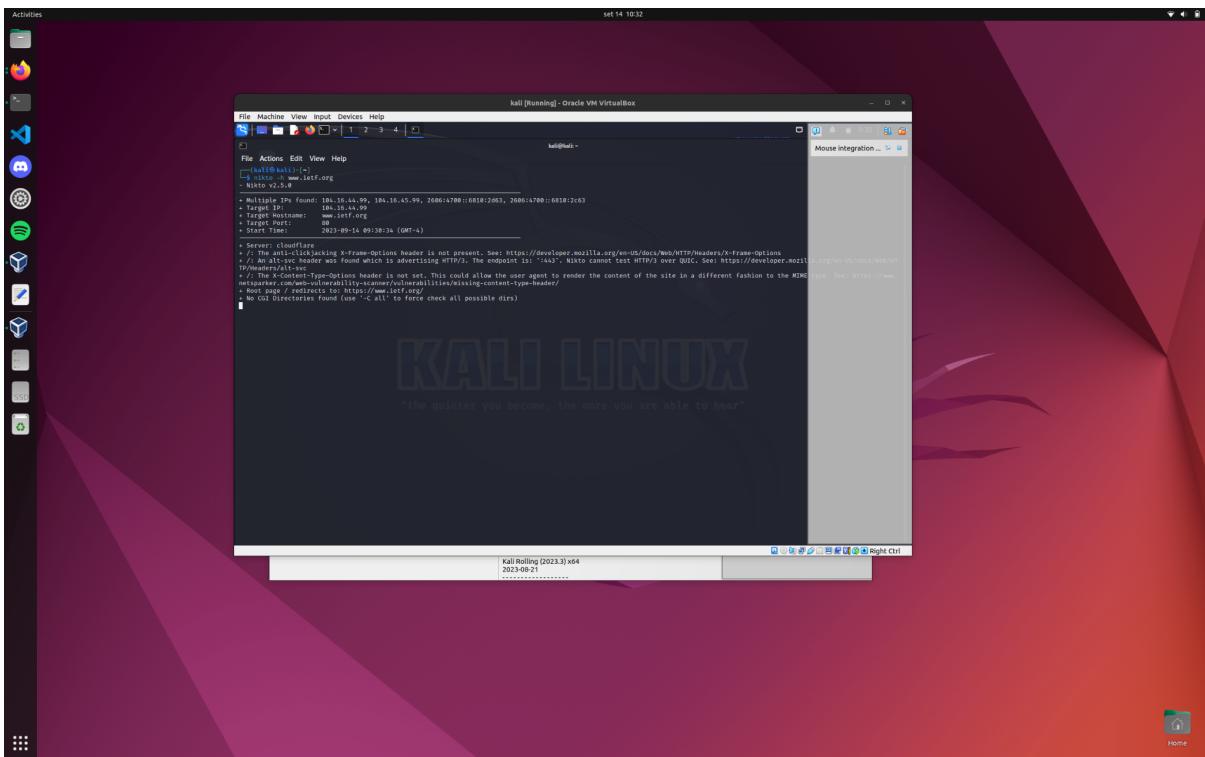
As portas apresentam as seguintes vulnerabilidades de maior criticalidade:

- 3306: [CVE-2009-2446](#), [CVE-2008-0226](#)
 - 5432: [CVE-2013-1902](#), [CVE-2013-1903](#), [POSTGRESQL:CVE-2013-1900](#),
[POSTGRESQL:CVE-2010-1169](#), [CVE-2010-1147](#), [CVE-2010-1169](#)

Além dessas, outras vulnerabilidades menores foram expostas, as quais estão sendo mostradas no output abaixo.

```
-root.txt - Msfvenom  
File Edit Search View Document Help  
132 POSTGRESQL-CVE-2012-8668 6.8 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-8668  
133 POSTGRESQL-CVE-2009-3231 6.8 https://vulners.com/postgresql/POSTGRESQL-CVE-2009-3231  
134 CVE-2012-8668 6.8 https://vulners.com/cve/CVE-2012-8668  
135 CVE-2012-8668 6.8 https://vulners.com/cve/CVE-2012-8668  
136 CVE-2009-3231 6.4 https://vulners.com/cve/CVE-2009-3231  
137 SSV-62018 6.5 https://vulners.com/sebug/SSV-62018 +EXPLOIT+  
138 SSV-62016 6.5 https://vulners.com/sebug/SSV-62016 +EXPLOIT+  
139 SSV-61543 6.5 https://vulners.com/sebug/SSV-61543 +EXPLOIT+  
140 SSV-61542 6.5 https://vulners.com/sebug/SSV-61542 +EXPLOIT+  
141 SSV-15151 6.5 https://vulners.com/sebug/SSV-15151 +EXPLOIT+  
142 SSV-15095 6.5 https://vulners.com/sebug/SSV-15095 +EXPLOIT+  
143 SSV-15095 6.5 https://vulners.com/sebug/SSV-15095 +EXPLOIT+  
144 SECURITYVULNSJULY18003 6.5 https://vulners.com/securityvulnsjuly18003/SECURITYVULN-VULN:48803  
145 SECURITYVULNSJULY18003 6.5 https://vulners.com/securityvulnsjuly18003/SECURITYVULN-VULN:19673  
146 POSTGRESQL-CVE-2011-0065 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2011-0065  
147 POSTGRESQL-CVE-2011-0064 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2011-0064  
148 POSTGRESQL-CVE-2011-0063 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2011-0063  
149 POSTGRESQL-CVE-2014-0061 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2014-0061  
150 POSTGRESQL-CVE-2014-0060 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2014-0060  
151 POSTGRESQL-CVE-2010-4415 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2010-4415  
152 POSTGRESQL-CVE-2009-4136 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2009-4136  
153 POSTGRESQL-CVE-2009-5230 6.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2009-5230  
154 CVE-2013-0065 6.5 https://vulners.com/cve/CVE-2013-0065  
155 CVE-2014-0063 6.5 https://vulners.com/cve/CVE-2014-0063  
156 CVE-2013-0063 6.5 https://vulners.com/cve/CVE-2013-0063  
157 CVE-2014-0063 6.5 https://vulners.com/cve/CVE-2014-0063  
158 CVE-2013-4415 6.5 https://vulners.com/cve/CVE-2013-4415  
159 CVE-2013-4415 6.5 https://vulners.com/cve/CVE-2013-4415  
160 CVE-2013-0442 6.5 https://vulners.com/cve/CVE-2013-0442  
161 CVE-2013-0442 6.5 https://vulners.com/cve/CVE-2013-0442  
162 CVE-2018-3433 6.4 https://vulners.com/cve/CVE-2018-3433  
163 POSTGRESQL-CVE-2018-3433 6.8 https://vulners.com/postgresql/POSTGRESQL-CVE-2018-3433  
164 CVE-2018-3433 6.8 https://vulners.com/cve/CVE-2018-3433  
165 CVE-2018-1170 6.8 https://vulners.com/cve/CVE-2018-1170  
166 SSV-15095 6.8 https://vulners.com/sebug/SSV-15095 +EXPLOIT+  
167 SSV-15095 6.8 https://vulners.com/sebug/SSV-15095 +EXPLOIT+  
168 POSTGRESQL-CVE-2009-4434 5.8 https://vulners.com/postgresql/POSTGRESQL-CVE-2009-4434  
169 SSV-15095 5.8 https://vulners.com/sebug/SSV-15095 +EXPLOIT+  
170 POSTGRESQL-CVE-2018-1975 5.5 https://vulners.com/postgresql/POSTGRESQL-CVE-2018-1975  
171 CVE-2018-1975 5.5 https://vulners.com/cve/CVE-2018-1975  
172 SSV-61544 4.9 https://vulners.com/sebug/SSV-61544 +EXPLOIT+  
173 SSV-60334 4.9 https://vulners.com/sebug/SSV-60334 +EXPLOIT+  
174 POSTGRESQL-CVE-2012-3488 4.9 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-3488  
175 CVE-2012-3488 4.9 https://vulners.com/cve/CVE-2012-3488  
176 CVE-2014-0062 4.9 https://vulners.com/cve/CVE-2014-0062  
177 CVE-2014-0062 4.9 https://vulners.com/cve/CVE-2014-0062  
178 SSV-61544 4.8 https://vulners.com/sebug/SSV-61544 +EXPLOIT+  
179 CVE-2012-2143 4.8 https://vulners.com/cve/CVE-2012-2143  
180 POSTGRESQL-CVE-2012-2143 4.8 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-2143  
181 POSTGRESQL-CVE-2012-0067 4.8 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-0067  
182 CVE-2012-0067 4.8 https://vulners.com/cve/CVE-2012-0067  
183 SSV-61547 4.0 https://vulners.com/sebug/SSV-61547 +EXPLOIT+  
184 SSV-61545 4.0 https://vulners.com/sebug/SSV-61545 +EXPLOIT+  
185 SSV-60333 4.0 https://vulners.com/sebug/SSV-60333 +EXPLOIT+  
186 SSV-60336 4.0 https://vulners.com/sebug/SSV-60336 +EXPLOIT+  
187 SSV-15095 4.0 https://vulners.com/sebug/SSV-15095 +EXPLOIT+  
188 SECURITYVULNSJULY9765 4.0 https://vulners.com/securityvulnsjuly9765/SECURITYVULN-VULN:9765  
189 POSTGRESQL-CVE-2014-0066 4.0 https://vulners.com/postgresql/POSTGRESQL-CVE-2014-0066  
190 POSTGRESQL-CVE-2012-3489 4.0 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-3489  
191 POSTGRESQL-CVE-2012-3489 4.0 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-3489  
192 POSTGRESQL-CVE-2012-2655 4.0 https://vulners.com/postgresql/POSTGRESQL-CVE-2012-2655  
193 POSTGRESQL-CVE-2009-4922 4.0 https://vulners.com/postgresql/POSTGRESQL-CVE-2009-4922  
194 CVE-2013-0060 4.0 https://vulners.com/cve/CVE-2013-0060  
195 CVE-2013-0060 4.0 https://vulners.com/cve/CVE-2013-0060  
196 CVE-2013-0060 4.0 https://vulners.com/cve/CVE-2013-0060  
197 CVE-2012-3449 4.0 https://vulners.com/cve/CVE-2012-3449  
198 CVE-2012-3449 4.0 https://vulners.com/cve/CVE-2012-3449  
199 CVE-2009-3229 4.0 https://vulners.com/cve/CVE-2009-3229  
200 SSV-19322 3.5 https://vulners.com/sebug/SSV-19322 +EXPLOIT+  
201 CVE-report-0708173 3.5 https://vulners.com/cve/CVE-2017-08173  
202 CVE-report-0708173 3.5 https://vulners.com/cve/CVE-2017-08173  
203 CVE-report-0708173 3.5 https://vulners.com/cve/CVE-2017-08173  
204 Service detection performed. Please report any incorrect results at https://map.org/submit/ .  
205 Map done : 1 IP address ( 1 host up ) scanned in 44.6 seconds
```

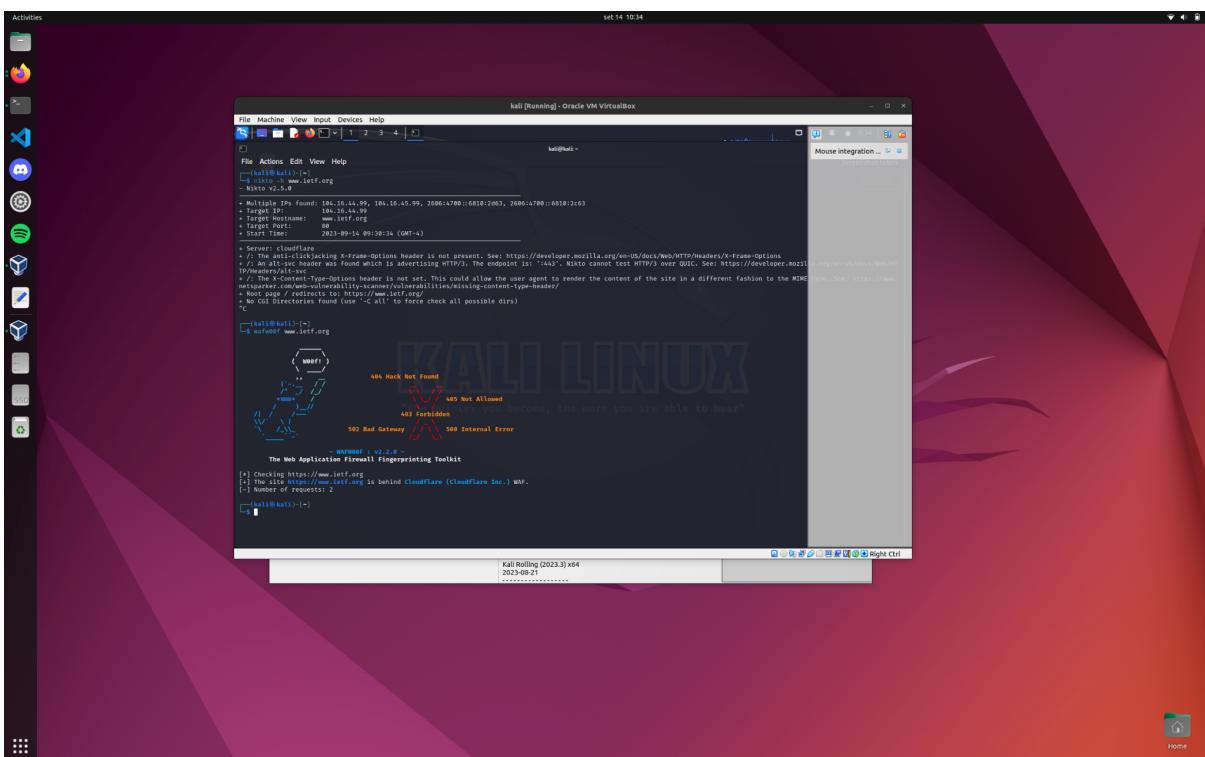
F
1 -



o endereço IP associado é 104.16.44.99

2 -

Como evidenciado no output do comando acima e do comando abaixo, o servidor DNS utilizado e o cloudflare



3 - Utilizando o relatório realizado pelo site intodns, que detalha quais serviços estão sendo utilizados em cada porta do dns, foi descoberto que o serviço de mx, o serviço de email, existe. <https://intodns.com/ietf.org>

			Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800
		NSs have same SOA serial	OK. All your nameservers agree that your SOA serial number is 2319686710.
		SOA MNAME entry	OK. jill.ns.cloudflare.com That server is listed at the parent servers.
		! SOA Serial	Your SOA serial number is: 2319686710. This can be ok if you know what you are doing.
		SOA REFRESH	OK. Your SOA REFRESH interval is: 10000. That is OK
		SOA RETRY	Your SOA RETRY value is: 2400. Looks ok
		SOA EXPIRE	Your SOA EXPIRE number is: 604800. Looks ok
		SOA MINIMUM TTL	Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.
MX		MX Records	Your MX records that were reported by your nameservers are: 0 mail.ietf.org 50.223.129.194 [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]
		Different MX records at nameservers	Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs
		MX name validity	Good. I did not detect any invalid hostnames for your MX records.
		MX IPs are public	OK. All of your MX records appear to use public IPs.
		MX CNAME Check	OK. No problems here.
		MX A request returns CNAME	OK. No CNAMEs returned for A records lookups.
		MX is not IP	OK. All of your MX records are host names.
		Number of MX records	OK. Looks like you only have one MX record at your nameservers. You should be careful about what you are doing since you have a single point of failure that can lead to mail being lost if the server is down for a long time.
		Mismatched MX A	OK. I did not detect differing IPs for your MX records.
		Duplicate MX A records	OK. I have not found duplicate IP(s) for your MX records. This is a good thing.
		Reverse MX A records (PTR)	Your reverse (PTR) record: mail.ietf.org">194.129.223.50.in-addr.arpa->mail.ietf.org You have reverse (PTR) records for all your IPs, that is a good thing.

A partir dessa informação, e uma rápida pesquisa no netcraft, foi inserido o link relativo ao serviço mx, mail.ietf.org, e foi encontrado que o serviço esta sendo hosteado no IP 50.223.129.194, com sede na [Comcast Cable Communications, LLC 1800 Bishops Gate Blvd Mt Laurel NJ US 08054](#).

https://sitereport.netcraft.com/?url=http://mail.ietf.org

IPV6 address (2001:559:c4c7::0:0:0:100)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2001:400::/23	United States	ARIN-001	American Registry for Internet Numbers
↳ 2001:558::/29	United States	COMCAST6NET	Comcast Cable Communications, LLC
↳ 2001:559:c4c7::/100	United States	COMCAST6NET	Comcast Cable Communications, LLC

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the [HTTPS site report](#).

Hosting History

Netblock owner	IP address	OS	Web server
Comcast Cable Communications, LLC 1800 Bishops Gate Blvd Mt Laurel NJ US 08054	50.223.129.194	Linux	Apache
Level 3 Communications, Inc. 1025 Eldorado Blvd. Broomfield CO US 80021	4.31.198.44	Linux	Apache
AMS 39355 California Street 307 Fremont CA US 94538	64.170.98.32	Linux	Apache/2.2.4 Linux/SUSE mod_ssl/2.2.4 OpenSSL/0.9.8e PHP/5.2.6 with Suhosin-Patch mod_python/3.3.1 Python/2.5.1 mod_perl/2.0.3 Perl/v5.8.8

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

G - Site escolhido: blockchainsper.com

1



2

Sendo um IP do cloudflare, é possível checar, utilizando o site myip.ms, que 47 outros hosts estão utilizando desse IP agora.

Site report for http://x intoDNS: letf.org - che x Roteiro-TechHack/Rot x Roteiro 2 - reconhecimen x Roteiro 2 - TechHack - x (5) WhatsApp x www.blockchainsper x 104.21.82.147 ip Look x + -

https://myip.ms/info/whois/104.21.82.147

Whois Record Updated: 01 Jul 2021

Peça já o seu Nubank

[Ad] Nubank

Reverse IP Lookup / Information on IP (104.21.82.147) ·

Download IP Whois Database 500mb, SQL format

Download Whois IP Virus Full MySQL Database - September 2023 (downloadable version) ·

IP Blacklist Check: Submit IPv4/v6 to Blacklist

Not Listed in Blacklist

4 are live websites using this IP (104.21.82.147) Now ·

jasonshannomusic.com (#14,187,439) cichlidbase.com (#8,920,260) ratzatz-kindermedien.de (#15,126,966) link-lagu.net (#3,501,030) videogrammognostics.com (#11,849,879) expatcalifornia.com.au (#6,243,783) totallymanila.com (#15,884,447) beawaypartners.es (#9,363,140) betterstudio.com (#19,391) appsfornutia.com (#1,206,656)

..... Found 47 websites on this IP ... move » see also: All websites in this IP Range »

53 live websites used this IP (104.21.82.147) Before ·

asteriskonline.com (#6,905,057) used IP on 23 June 2023
parfit-a-freitanger.de (#10,831,826) used IP on 06 April 2022
ne-new.com (#17,197,389) used IP on 30 January 2022
baikom.de (#1,407,966) used IP on 12 January 2022

..... Found 53 websites ... more »

4 are not working websites. This IP 104.21.82.147 is the last known IP address for sites below ·

specularmedia.com (#6,905,057) site work on 04 November 2022
serviziabuzz.it (#6,905,368) site work on 04 November 2022
hostressurfaces.com (#3,333,878) site work on 27 March 2021
edition-zeno.de (#10,418,646) site work on 27 February 2021

Nameservers on this IP: No nameservers

Web Browser(s) on this IP: Unknown

OS on this IP: Unknown

ASN: AS132892, AS13335, AS139242, AS174, AS18450, AS203898, AS209242, AS23352, AS363651

Information

Hosting \$6.95 \$2.95 offers Unlimited DOMAINS GoDaddy bluehost

IP Whois Database Download September

Free Extension for Google Chrome Add Website Location Flag

API Dashboard

API Direct Access through API to our MyIP Live Database »

Hide

Myip.ms

59.5K

22.5K

Twitter

Facebook

Instagram

LinkedIn

YouTube

Reddit

Link

Image

File

Print

Help

Hide

PRÊMIOS EM DOBRO CLIQUE E PARTICIPE! ASSAÍ ATacadista

Mvip.ms

3

utilizando o comando de nmap, é possível dizer, com 98% de certeza, que o OS do IP é o Oracle Virtualbox.

A screenshot of a Linux desktop environment. On the left, there's a dock with icons for various applications like a file manager, terminal, and system monitor. The main window is a terminal window titled 'kali@kali: ~'. It contains several commands and their outputs:

```
set root
kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help
File kali@kali: ~
└─ netcat -n www.blockchaingrapher.com
      Address: 18.6.2.3853
      Non-authoritative answer:
      www.blockchaingrapher.com
      Address: 172.0.7.150.174
      Name: www.blockchaingrapher.com
      Address: 18.6.2.3853
      Name: www.blockchaingrapher.com
      Address: 172.0.7.150.174
      Name: www.blockchaingrapher.com
      Address: 2000:4000:5007::d415:5293

kali@kali: ~ [~]
└─ nmap -sT -O 184.21.82.147
    TCP/IP fingerprinting (for OS scan) requires root privileges.
    QUITTING!
[+] Nmap scan report for 184.21.82.147
[+] Host is up.
[+] OS: Linux 4.14 - 4.19 [Ubuntu 18.04 LTS]
[+] Not shown: 996 filtered port(s) (no-response)
[+] Ports: 80/tcp open http
[+] 80/tcp open http-proxy
[+] 80/tcp open https
[+] 80/tcp open https-proxy
[+] 80/tcp open http
[+] 80/tcp open https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device: eth0 (Intel PRO/100 MT Desktop)
  Status: DOWN (not connected)
  HWaddr 56:84:7a:4f:00:00
  Device: eth1 (VirtualBox Host-Only Network)
  Status: UP (host up)
  HWaddr 00:0c:29:4f:00:00
  MTU: 1500 qdisc mq
  RX: 0 B/s (0.0 Kbytes/s)
  TX: 0 B/s (0.0 Kbytes/s)
  Errors: 0 Rx errors 0 Tx errors 0 dropped 0 overruns
  Queueing discipline: pfifo_fast
  IP: 192.168.56.1/24 brd 192.168.56.255
  MAC: 00:0c:29:4f:00:00
  Device: virbr0 (VirtualBox Internal Network)
  Status: UP (host up)
  HWaddr 00:0c:29:4f:00:01
  MTU: 1500 qdisc pfifo_fast
  RX: 0 B/s (0.0 Kbytes/s)
  TX: 0 B/s (0.0 Kbytes/s)
  Errors: 0 Rx errors 0 Tx errors 0 dropped 0 overruns
  Queueing discipline: pfifo_fast
  IP: 192.168.1.100/24 brd 192.168.1.255
  MAC: 00:0c:29:4f:00:01
OS: CPE: cpe:/o:oracle:virtualbox:cpu:/aliosm:genx
  No exact OS matches for host (test conditions non-ideal)
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.38 seconds
[~]
```

The terminal window has a dark background with light-colored text. In the top right corner of the desktop, there's a floating window titled 'kali [Running] - Oracle VM VirtualBox' which shows settings for a virtual machine named 'kali'. The window includes tabs for 'Policy', 'Traces', 'Delivery Control', and 'Monitoring'. The overall interface is typical of a Kali Linux desktop setup.

Agora, ao pingar o site, o ttl indicado é 63, confirmando que o OS é um linux.

Ao consultar o site <https://www.robtex.com/ip-lookup/104.21.82.147> e ao ver o header do site pelo browser, é possível concluir que o webserver de host do IP e o cloudflare.

4

As tecnologias utilizadas pelo site, como demonstrado pelo relatório do netstat, são as abaixo:

The screenshot shows a Firefox browser window with multiple tabs open. The main content is the netcraft.com analysis page for the website www.blockchainsper.com. The page provides detailed information about the site's technology stack, including:

- HTTP Compression:** Describes the capability to make better use of available bandwidth.
- Doctype:** A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).
- HTML 5:** A markup language for structuring and presenting content for the World Wide Web and a core technology of the internet. It is the fifth revision of the HTML standard.
- CSS Usage:** Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Below the analysis, there is a section titled "Looking for similar sites?" which encourages users to find other sites using similar technology or running on the same infrastructure.

5

Pela busca realizada o site não é protegido por WAF

The screenshot shows a terminal window on a Kali Linux VM (running in Oracle VM VirtualBox). The user has run a Nmap scan against the IP address 10.21.82.147. The output shows the following results:

```

[*] Nmap 7.94 | https://nmap.org/ | at 2023-01-18 14:26 EDT
[*] Host is up (0.074s latency).
[*] PORT      STATE SERVICE          VERSION
[*] 22/tcp    open  ssh
[*] 23/tcp    open  telnet
[*] 25/tcp    open  smtp
[*] 443/tcp   open  https
[*] 80/tcp    open  http
Warning: OS guess may be unreliable because we could not find at least 1 open and 1 closed port
[*] Aggressive OS guesses: Oracle VirtualBox (98%), QEMU (94%)
[*] No OS detected.
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Map done: 1 IP address (1 host up) scanned in 26.38 seconds

```

Below the Nmap output, the user runs the `wafme` tool against the target website www.blockchainsper.com. The tool reports that Cloudflare (Cloudflare Inc.) and/or Fastly (Fastly CDN) WAF is present.

6

Realizando a busca pelo site intodns, são reconhecidos 3 serviços de email, todos hosteados pela zoho. O IP atrelado pelo serviço e o 136.143.191.44

		https://intodns.com/blockchainsper.com																																																																						
		<table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different autonomous systems</td><td>OK. It seems you are safe from a single point of failure. You must be careful about this and try to have nameservers on different locations as it can prevent a lot of problems if one nameserver goes down.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Stealth NS records sent</td><td>Ok. No stealth ns records are sent</td></tr> <tr> <td colspan="2" style="text-align: center;">SOA</td><td> <table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>SOA record</td><td>The SOA record is: Primary nameserver: dorothy.ns.cloudflare.com Hostmaster E-mail address: dns.cloudflare.com Serial #: 2319925744 Refresh: 10000 Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>NSs have same SOA serial</td><td>OK. All your nameservers agree that your SOA serial number is 2319925744.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA MNAME entry</td><td>OK. dorothy.ns.cloudflare.com That server is listed at the parent servers.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>SOA Serial</td><td>Your SOA serial number is: 2319925744. This can be ok if you know what you are doing.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA REFRESH</td><td>OK. Your SOA REFRESH interval is: 10000. That is OK</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA RETRY</td><td>Your SOA RETRY value is: 2400 Looks ok</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA EXPIRE</td><td>Your SOA EXPIRE number is: 604800 Looks ok</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA MINIMUM TTL</td><td>Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.</td></tr> <tr> <td colspan="2" style="text-align: center;">MX</td><td colspan="2"> <table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>MX Records</td><td>Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different MX records at nameservers</td><td>Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX name validity</td><td>Good. I did not detect any invalid hostnames for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX IPs are public</td><td>OK. All of your MX records appear to use public IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX CNAME Check</td><td>OK. No problems here.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX A request returns CNAME</td><td>OK. No CNAMEs returned for A records lookups.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX is not IP</td><td>OK. All your MX records are host names.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Number of MX records</td><td>Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Mismatched MX A</td><td>OK. I did not detect differing IPs for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>Duplicate MX A records</td><td>ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Reverse MX A records (PTR)</td><td>Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com</td></tr> </table> </td></tr> </table></td></tr></table>		Different autonomous systems	OK. It seems you are safe from a single point of failure. You must be careful about this and try to have nameservers on different locations as it can prevent a lot of problems if one nameserver goes down.		Stealth NS records sent	Ok. No stealth ns records are sent	SOA		<table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>SOA record</td><td>The SOA record is: Primary nameserver: dorothy.ns.cloudflare.com Hostmaster E-mail address: dns.cloudflare.com Serial #: 2319925744 Refresh: 10000 Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>NSs have same SOA serial</td><td>OK. All your nameservers agree that your SOA serial number is 2319925744.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA MNAME entry</td><td>OK. dorothy.ns.cloudflare.com That server is listed at the parent servers.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>SOA Serial</td><td>Your SOA serial number is: 2319925744. This can be ok if you know what you are doing.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA REFRESH</td><td>OK. Your SOA REFRESH interval is: 10000. That is OK</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA RETRY</td><td>Your SOA RETRY value is: 2400 Looks ok</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA EXPIRE</td><td>Your SOA EXPIRE number is: 604800 Looks ok</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA MINIMUM TTL</td><td>Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.</td></tr> <tr> <td colspan="2" style="text-align: center;">MX</td><td colspan="2"> <table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>MX Records</td><td>Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different MX records at nameservers</td><td>Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX name validity</td><td>Good. I did not detect any invalid hostnames for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX IPs are public</td><td>OK. All of your MX records appear to use public IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX CNAME Check</td><td>OK. No problems here.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX A request returns CNAME</td><td>OK. No CNAMEs returned for A records lookups.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX is not IP</td><td>OK. All your MX records are host names.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Number of MX records</td><td>Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Mismatched MX A</td><td>OK. I did not detect differing IPs for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>Duplicate MX A records</td><td>ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Reverse MX A records (PTR)</td><td>Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com</td></tr> </table> </td></tr> </table>		SOA record	The SOA record is: Primary nameserver: dorothy.ns.cloudflare.com Hostmaster E-mail address: dns.cloudflare.com Serial #: 2319925744 Refresh: 10000 Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800		NSs have same SOA serial	OK. All your nameservers agree that your SOA serial number is 2319925744.		SOA MNAME entry	OK. dorothy.ns.cloudflare.com That server is listed at the parent servers.		SOA Serial	Your SOA serial number is: 2319925744. This can be ok if you know what you are doing.		SOA REFRESH	OK. Your SOA REFRESH interval is: 10000. That is OK		SOA RETRY	Your SOA RETRY value is: 2400 Looks ok		SOA EXPIRE	Your SOA EXPIRE number is: 604800 Looks ok		SOA MINIMUM TTL	Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.	MX		<table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>MX Records</td><td>Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different MX records at nameservers</td><td>Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX name validity</td><td>Good. I did not detect any invalid hostnames for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX IPs are public</td><td>OK. All of your MX records appear to use public IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX CNAME Check</td><td>OK. No problems here.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX A request returns CNAME</td><td>OK. No CNAMEs returned for A records lookups.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX is not IP</td><td>OK. All your MX records are host names.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Number of MX records</td><td>Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Mismatched MX A</td><td>OK. I did not detect differing IPs for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>Duplicate MX A records</td><td>ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Reverse MX A records (PTR)</td><td>Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com</td></tr> </table>			MX Records	Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]		Different MX records at nameservers	Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.		MX name validity	Good. I did not detect any invalid hostnames for your MX records.		MX IPs are public	OK. All of your MX records appear to use public IPs.		MX CNAME Check	OK. No problems here.		MX A request returns CNAME	OK. No CNAMEs returned for A records lookups.		MX is not IP	OK. All your MX records are host names.		Number of MX records	Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.		Mismatched MX A	OK. I did not detect differing IPs for your MX records.		Duplicate MX A records	ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.		Reverse MX A records (PTR)	Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com
	Different autonomous systems	OK. It seems you are safe from a single point of failure. You must be careful about this and try to have nameservers on different locations as it can prevent a lot of problems if one nameserver goes down.																																																																						
	Stealth NS records sent	Ok. No stealth ns records are sent																																																																						
SOA		<table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>SOA record</td><td>The SOA record is: Primary nameserver: dorothy.ns.cloudflare.com Hostmaster E-mail address: dns.cloudflare.com Serial #: 2319925744 Refresh: 10000 Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>NSs have same SOA serial</td><td>OK. All your nameservers agree that your SOA serial number is 2319925744.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA MNAME entry</td><td>OK. dorothy.ns.cloudflare.com That server is listed at the parent servers.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>SOA Serial</td><td>Your SOA serial number is: 2319925744. This can be ok if you know what you are doing.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA REFRESH</td><td>OK. Your SOA REFRESH interval is: 10000. That is OK</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA RETRY</td><td>Your SOA RETRY value is: 2400 Looks ok</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA EXPIRE</td><td>Your SOA EXPIRE number is: 604800 Looks ok</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>SOA MINIMUM TTL</td><td>Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.</td></tr> <tr> <td colspan="2" style="text-align: center;">MX</td><td colspan="2"> <table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>MX Records</td><td>Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different MX records at nameservers</td><td>Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX name validity</td><td>Good. I did not detect any invalid hostnames for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX IPs are public</td><td>OK. All of your MX records appear to use public IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX CNAME Check</td><td>OK. No problems here.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX A request returns CNAME</td><td>OK. No CNAMEs returned for A records lookups.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX is not IP</td><td>OK. All your MX records are host names.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Number of MX records</td><td>Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Mismatched MX A</td><td>OK. I did not detect differing IPs for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>Duplicate MX A records</td><td>ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Reverse MX A records (PTR)</td><td>Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com</td></tr> </table> </td></tr> </table>		SOA record	The SOA record is: Primary nameserver: dorothy.ns.cloudflare.com Hostmaster E-mail address: dns.cloudflare.com Serial #: 2319925744 Refresh: 10000 Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800		NSs have same SOA serial	OK. All your nameservers agree that your SOA serial number is 2319925744.		SOA MNAME entry	OK. dorothy.ns.cloudflare.com That server is listed at the parent servers.		SOA Serial	Your SOA serial number is: 2319925744. This can be ok if you know what you are doing.		SOA REFRESH	OK. Your SOA REFRESH interval is: 10000. That is OK		SOA RETRY	Your SOA RETRY value is: 2400 Looks ok		SOA EXPIRE	Your SOA EXPIRE number is: 604800 Looks ok		SOA MINIMUM TTL	Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.	MX		<table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>MX Records</td><td>Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different MX records at nameservers</td><td>Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX name validity</td><td>Good. I did not detect any invalid hostnames for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX IPs are public</td><td>OK. All of your MX records appear to use public IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX CNAME Check</td><td>OK. No problems here.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX A request returns CNAME</td><td>OK. No CNAMEs returned for A records lookups.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX is not IP</td><td>OK. All your MX records are host names.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Number of MX records</td><td>Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Mismatched MX A</td><td>OK. I did not detect differing IPs for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>Duplicate MX A records</td><td>ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Reverse MX A records (PTR)</td><td>Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com</td></tr> </table>			MX Records	Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]		Different MX records at nameservers	Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.		MX name validity	Good. I did not detect any invalid hostnames for your MX records.		MX IPs are public	OK. All of your MX records appear to use public IPs.		MX CNAME Check	OK. No problems here.		MX A request returns CNAME	OK. No CNAMEs returned for A records lookups.		MX is not IP	OK. All your MX records are host names.		Number of MX records	Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.		Mismatched MX A	OK. I did not detect differing IPs for your MX records.		Duplicate MX A records	ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.		Reverse MX A records (PTR)	Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com									
	SOA record	The SOA record is: Primary nameserver: dorothy.ns.cloudflare.com Hostmaster E-mail address: dns.cloudflare.com Serial #: 2319925744 Refresh: 10000 Retry: 2400 Expire: 604800 1 weeks Default TTL: 1800																																																																						
	NSs have same SOA serial	OK. All your nameservers agree that your SOA serial number is 2319925744.																																																																						
	SOA MNAME entry	OK. dorothy.ns.cloudflare.com That server is listed at the parent servers.																																																																						
	SOA Serial	Your SOA serial number is: 2319925744. This can be ok if you know what you are doing.																																																																						
	SOA REFRESH	OK. Your SOA REFRESH interval is: 10000. That is OK																																																																						
	SOA RETRY	Your SOA RETRY value is: 2400 Looks ok																																																																						
	SOA EXPIRE	Your SOA EXPIRE number is: 604800 Looks ok																																																																						
	SOA MINIMUM TTL	Your SOA MINIMUM TTL is: 1800. This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 1800 is OK.																																																																						
MX		<table border="1"> <tr> <td style="width: 15px; height: 15px; background-color: blue;"></td><td>MX Records</td><td>Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Different MX records at nameservers</td><td>Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX name validity</td><td>Good. I did not detect any invalid hostnames for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX IPs are public</td><td>OK. All of your MX records appear to use public IPs.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX CNAME Check</td><td>OK. No problems here.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX A request returns CNAME</td><td>OK. No CNAMEs returned for A records lookups.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>MX is not IP</td><td>OK. All your MX records are host names.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Number of MX records</td><td>Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Mismatched MX A</td><td>OK. I did not detect differing IPs for your MX records.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: yellow;"></td><td>Duplicate MX A records</td><td>ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.</td></tr> <tr> <td style="width: 15px; height: 15px; background-color: green;"></td><td>Reverse MX A records (PTR)</td><td>Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com</td></tr> </table>			MX Records	Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]		Different MX records at nameservers	Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.		MX name validity	Good. I did not detect any invalid hostnames for your MX records.		MX IPs are public	OK. All of your MX records appear to use public IPs.		MX CNAME Check	OK. No problems here.		MX A request returns CNAME	OK. No CNAMEs returned for A records lookups.		MX is not IP	OK. All your MX records are host names.		Number of MX records	Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.		Mismatched MX A	OK. I did not detect differing IPs for your MX records.		Duplicate MX A records	ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.		Reverse MX A records (PTR)	Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com																																				
	MX Records	Your MX records that were reported by your nameservers are: 10 mx.zoho.com 136.143.191.44 (no glue) 20 mx2.zoho.com 136.143.191.44 (no glue) 50 mx3.zoho.com 136.143.191.44 (no glue) [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]																																																																						
	Different MX records at nameservers	Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs.																																																																						
	MX name validity	Good. I did not detect any invalid hostnames for your MX records.																																																																						
	MX IPs are public	OK. All of your MX records appear to use public IPs.																																																																						
	MX CNAME Check	OK. No problems here.																																																																						
	MX A request returns CNAME	OK. No CNAMEs returned for A records lookups.																																																																						
	MX is not IP	OK. All your MX records are host names.																																																																						
	Number of MX records	Good. Looks like you have multiple MX records at all your nameservers. This is a good thing and will help in preventing loss of mail.																																																																						
	Mismatched MX A	OK. I did not detect differing IPs for your MX records.																																																																						
	Duplicate MX A records	ERROR: It seems that all your MX records have the same IP(s). There is no use on having multiple MX records pointing to the same ip.																																																																						
	Reverse MX A records (PTR)	Your reverse (PTR) record: 44.191.143.191.in-addr.arpa. > mx.zoho.com 44.191.143.191.in-addr.arpa. > mx2.zoho.com 44.191.143.191.in-addr.arpa. > mx3.zoho.com																																																																						

 |

H

O mapeamento do link <https://www.rodolfoavelino.com.br/> pelo wpscan retornou os seguintes resultados:

The screenshot shows a Kali Linux desktop environment with two terminal windows open. The top terminal window is titled 'File Actions Edit View Help' and contains the output of a WPScan scan. It lists various findings such as interesting entries, XML-RPC detection, cron jobs, and specific theme and plugin details for the website www.rodolfoavelino.com.br. The bottom terminal window is also titled 'File Actions Edit View Help' and contains the output of a WPScan scan. This window provides similar information about the website's configuration, including plugin versions and statistics. Both terminals show the results of their respective scans against the target website.

A partir destes resultados, é possível identificar 7 plugins no site, alguns arquivos php que podem conter informações sensíveis e uma identificação de cloudflare como servidor host. O arquivo de maior interesse é um chamado admin-ajax.php, onde seria plausível encontrar informações sensíveis sobre o painel de administração do WordPress, que faria com que fosse possível explorar uma vulnerabilidade de bancos de dados sql que são hospedados no site.

1

O CNPJ relacionado ao insper.edu.br é 06.070.152.0001-47.

site:insper.edu.br "CNPJ"

Aproximadamente 254 resultados (0,23 segundos)

insper.edu.br
http://www.insper.edu.br > uploads > 2020/09 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 > uploads > 2020/06 PDF

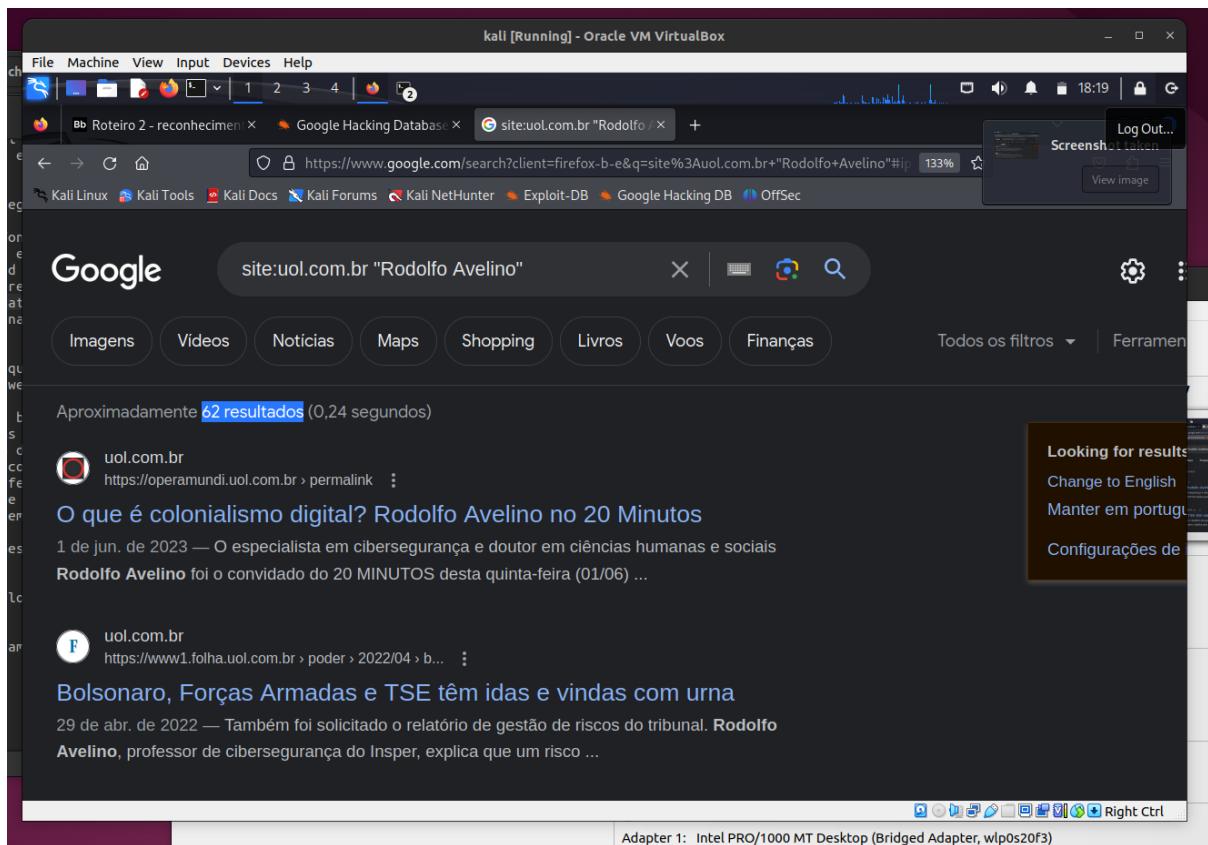
Acordo de Cooperação

... CNPJ/MF sob o nº 06.070.152/0001-47, neste ato representado na forma de seu Estatuto Social, doravante ... Carimbo do **CNPJ** da Empresa. Instituição de Ensino ...

Shared Folders Right Ctrl

2

De acordo com a pesquisa, o Rodolfo Avelino tem 62 matérias no grupo uol.



3

De acordo com minha pesquisa, 670 000 resultados foram encontrados com arquivos de backup expostos de forma insegura (em 0.29 segundos). Um URL encontrado nessa pesquisa foi

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi47lnwkauBAxWuGbkGHTLACxoQFnoECA8QAQ&url=https%3A%2F%2Fwww.hbcsaude.com.br%2Fbackup%2F&usg=AOvVaw361hXAW05eDY-ooBPITC-4&opi=89978449> que direciona para a HBC saúde, uma seguradora de planos de saúde.

