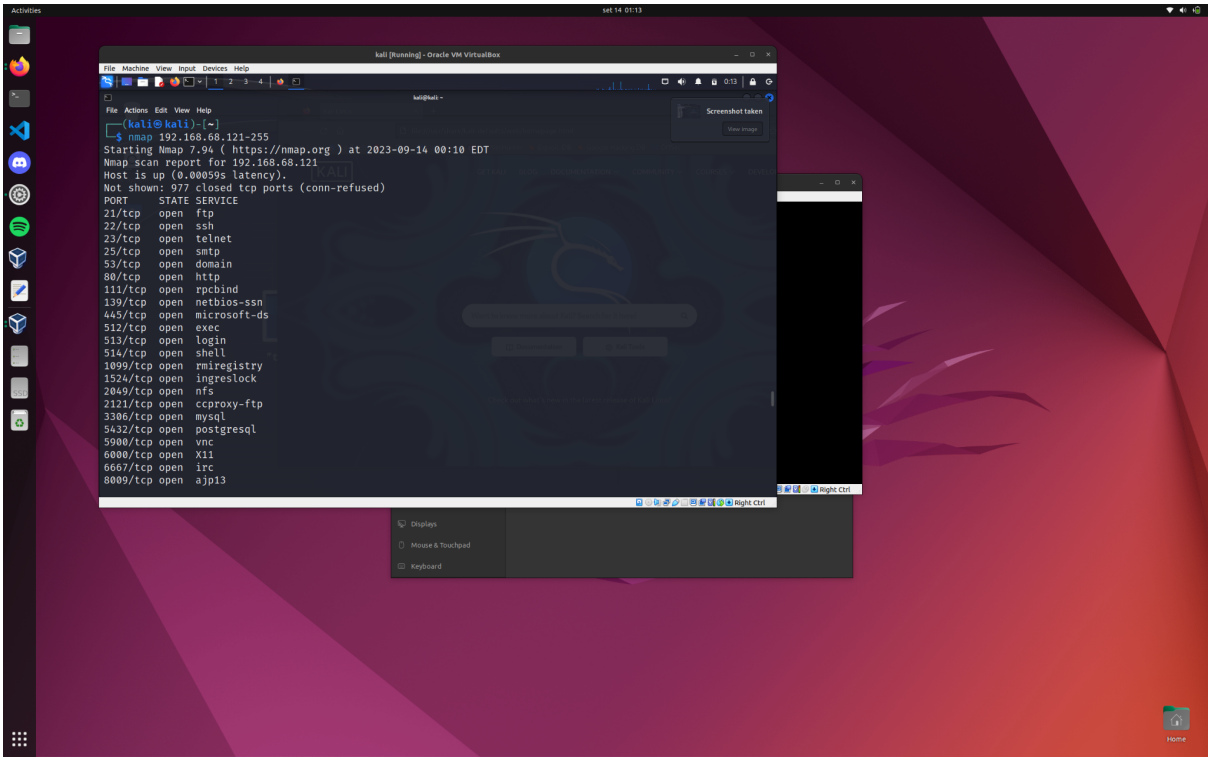
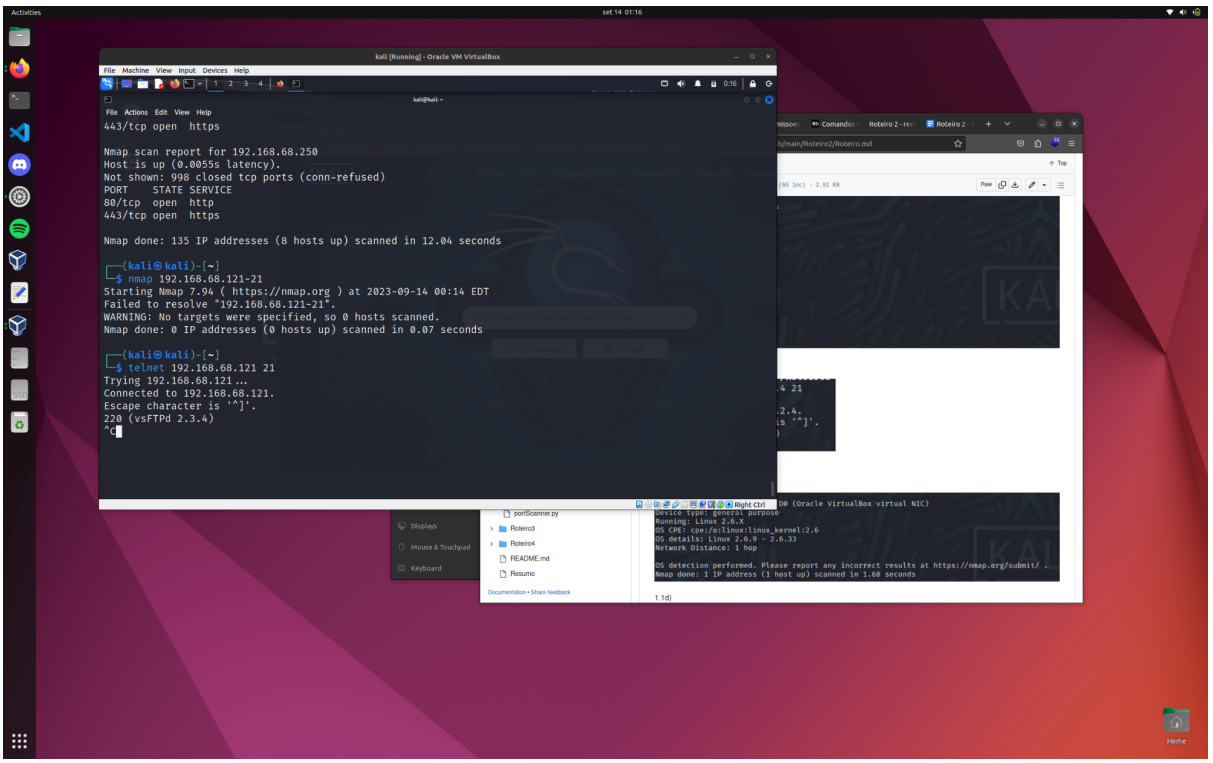
Tecnologias Hacker - Roteiro 2

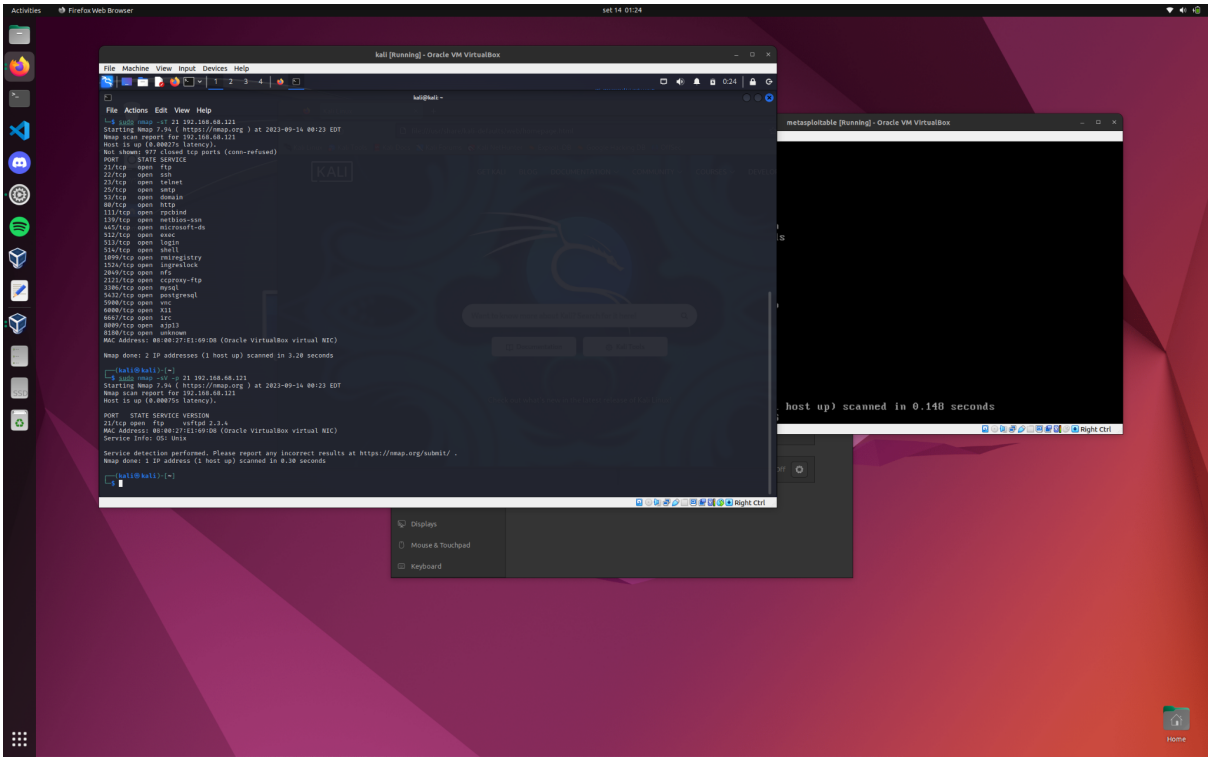
Arthur Carvalho

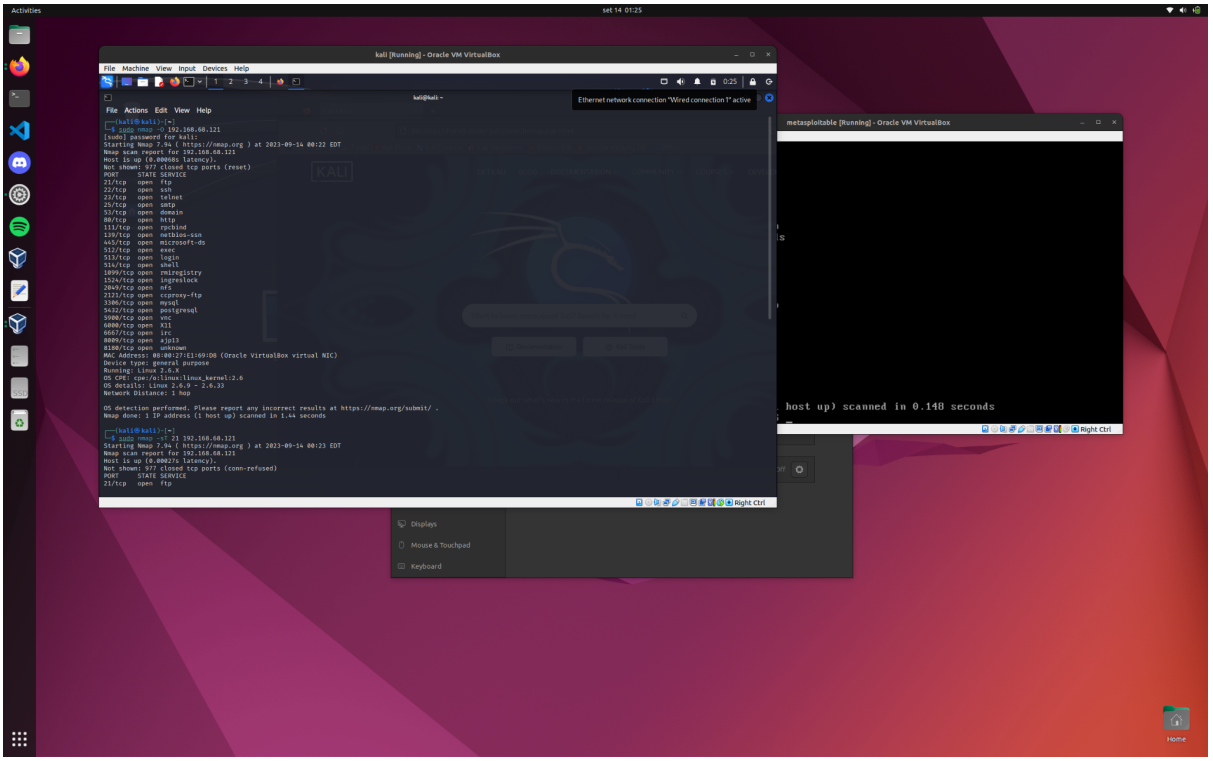
A:

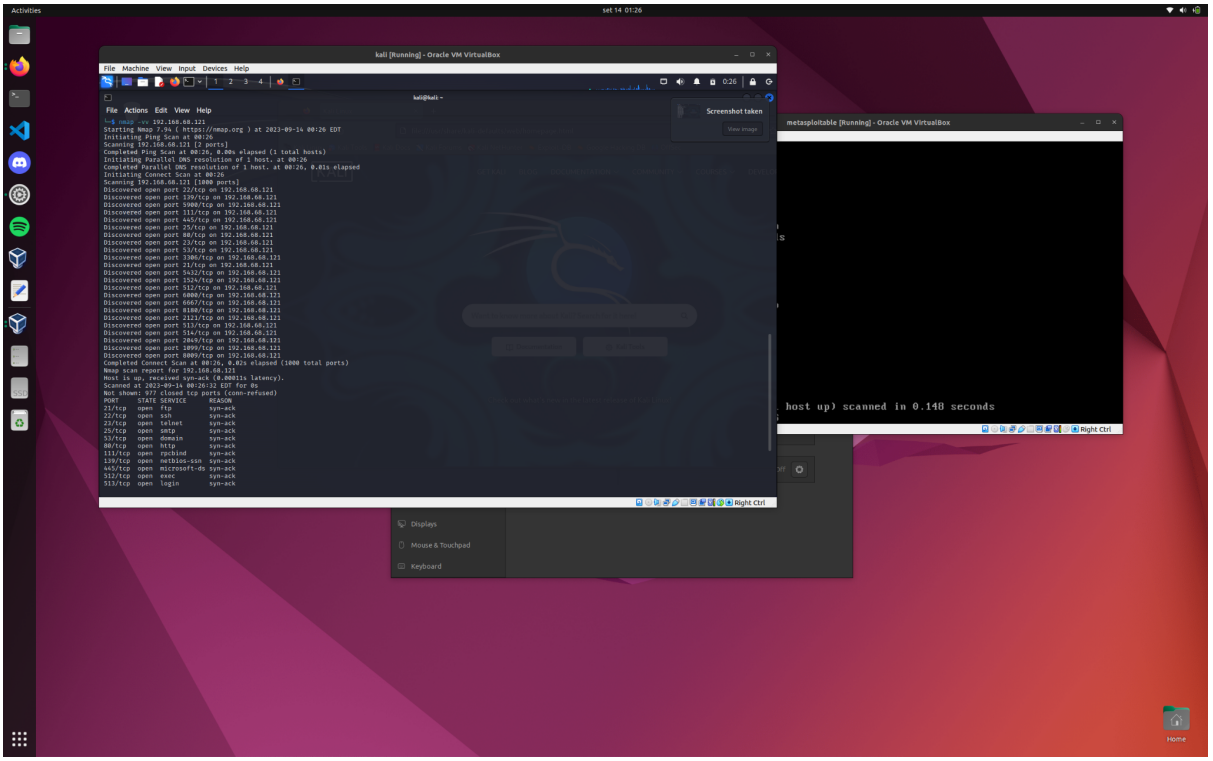




B

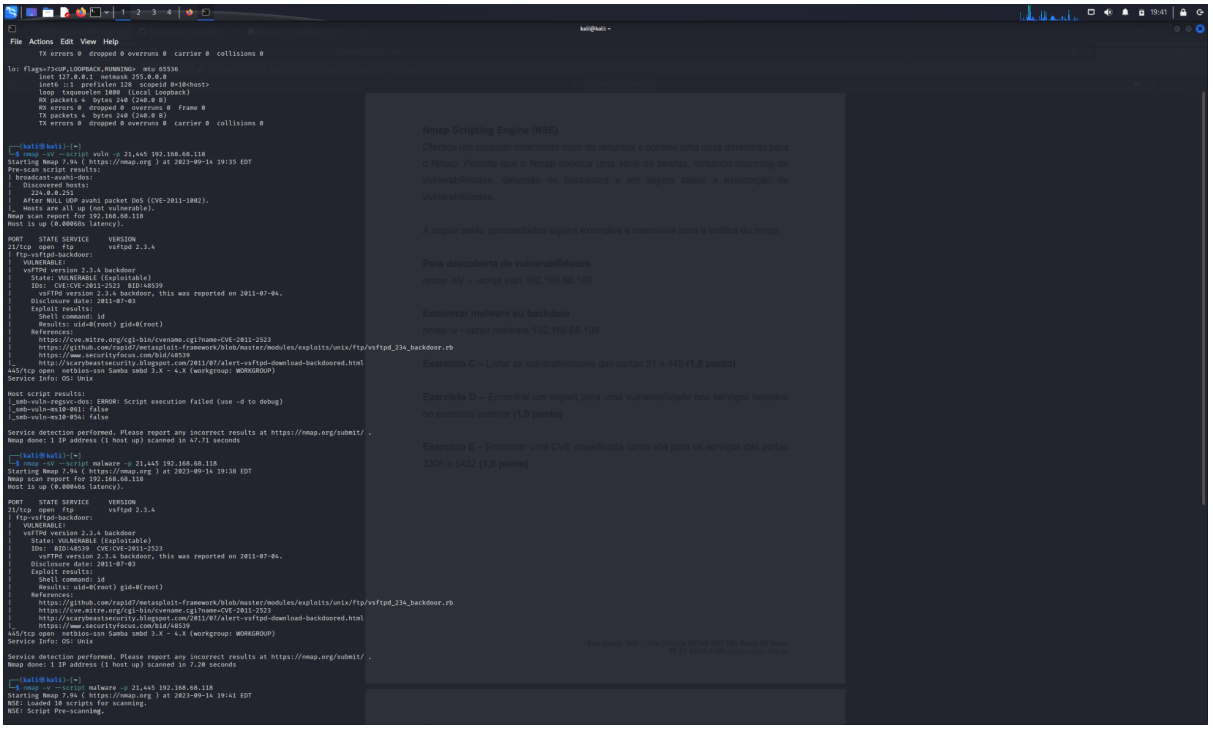

Activities
Firefox Web Browser
set 14 01:24
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
$ sudo nmap -sT 21 192.168.68.121
Starting Nmap 7.94 (https://nmap.org) at 2023-09-14 00:23 EDT
Nmap scan report for 192.168.68.121
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:E1:69:D8 (Oracle VirtualBox virtual NIC)
Nmap done: 2 IP addresses (1 host up) scanned in 3.20 seconds
$ sudo nmap -sV -p 21 192.168.68.121
Starting Nmap 7.94 (https://nmap.org) at 2023-09-14 00:23 EDT
Nmap scan report for 192.168.68.121
Host is up (0.00075s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
MAC Address: 08:00:27:E1:69:D8 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
Right Ctrl
metasploitable [Running] - Oracle VM VirtualBox
host up) scanned in 0.148 seconds
Right Ctrl
Displays
Mouse & Touchpad
Keyboard
Home

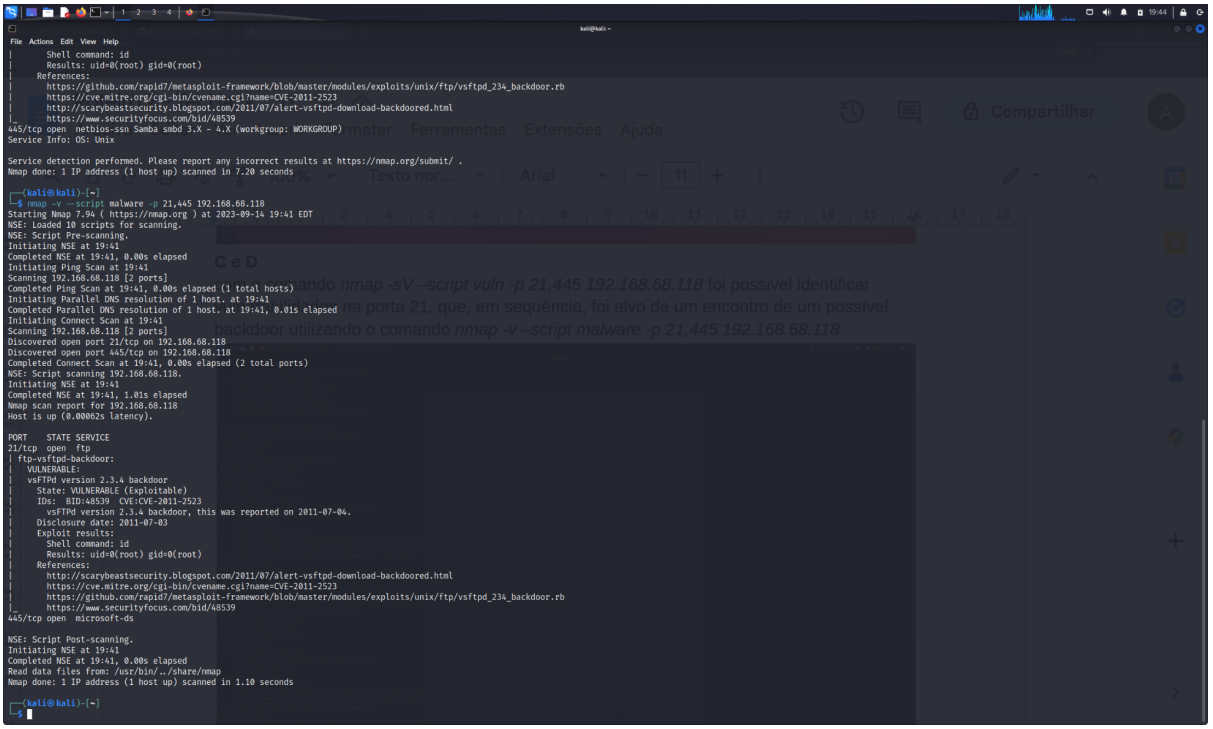

Activities
set 14 01:25
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ethernet network connection "Wired connection 1" active
File Actions Edit View Help
$ sudo nmap -O 192.168.68.121
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2023-09-14 00:22 EDT
Nmap scan report for 192.168.68.121
Host is up (0.000086 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:E1:69:D8 (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 1.44 seconds
$ sudo nmap -sT 21 192.168.68.121
Starting Nmap 7.94 (https://nmap.org) at 2023-09-14 00:23 EDT
Nmap scan report for 192.168.68.121
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
Right Ctrl
metasploitable [Running] - Oracle VM VirtualBox
host up) scanned in 0.148 seconds
Right Ctrl
Displays
Mouse & Touchpad
Keyboard
Home



C e D

com o comando *nmap -sV –script vuln -p 21,445 192.168.68.118* foi possivel 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*



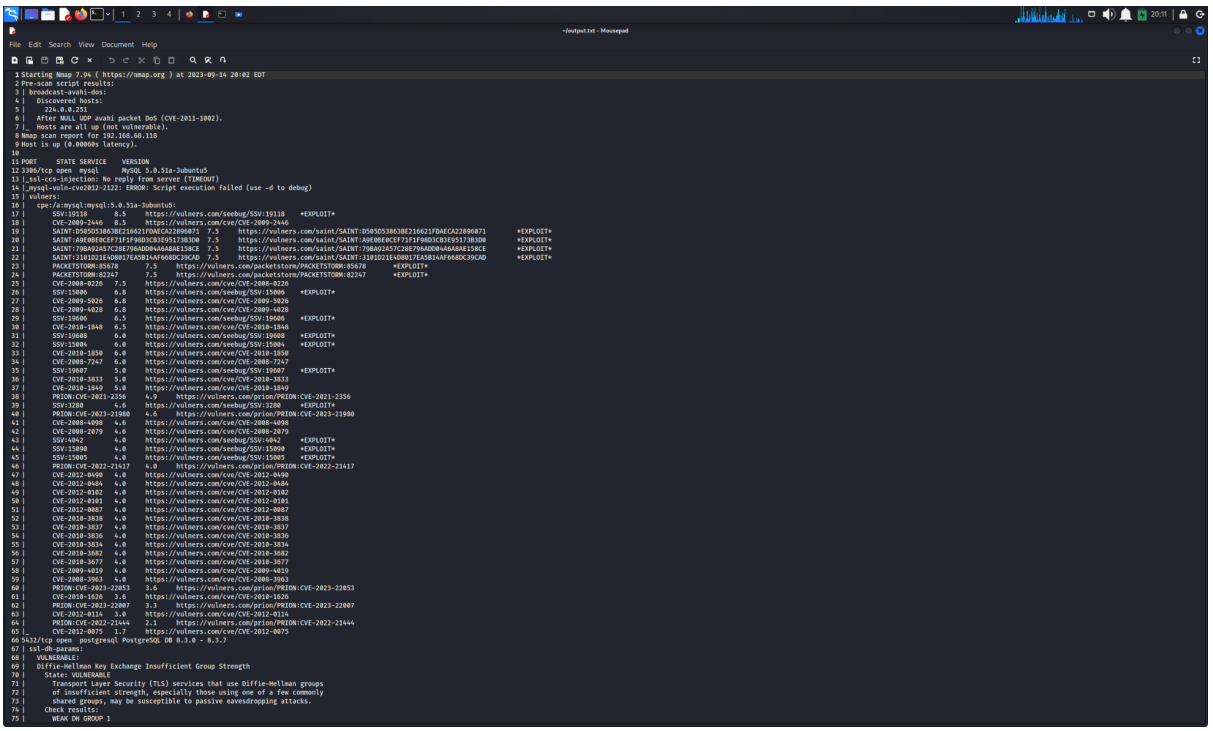


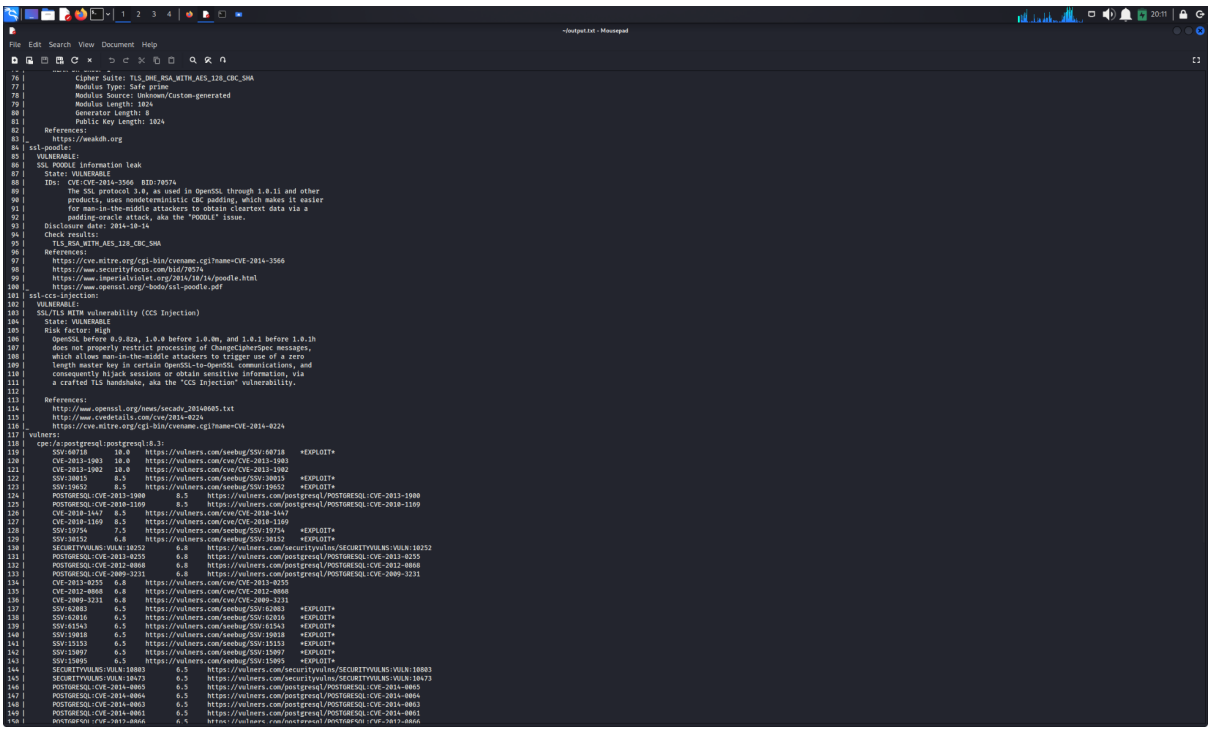
E

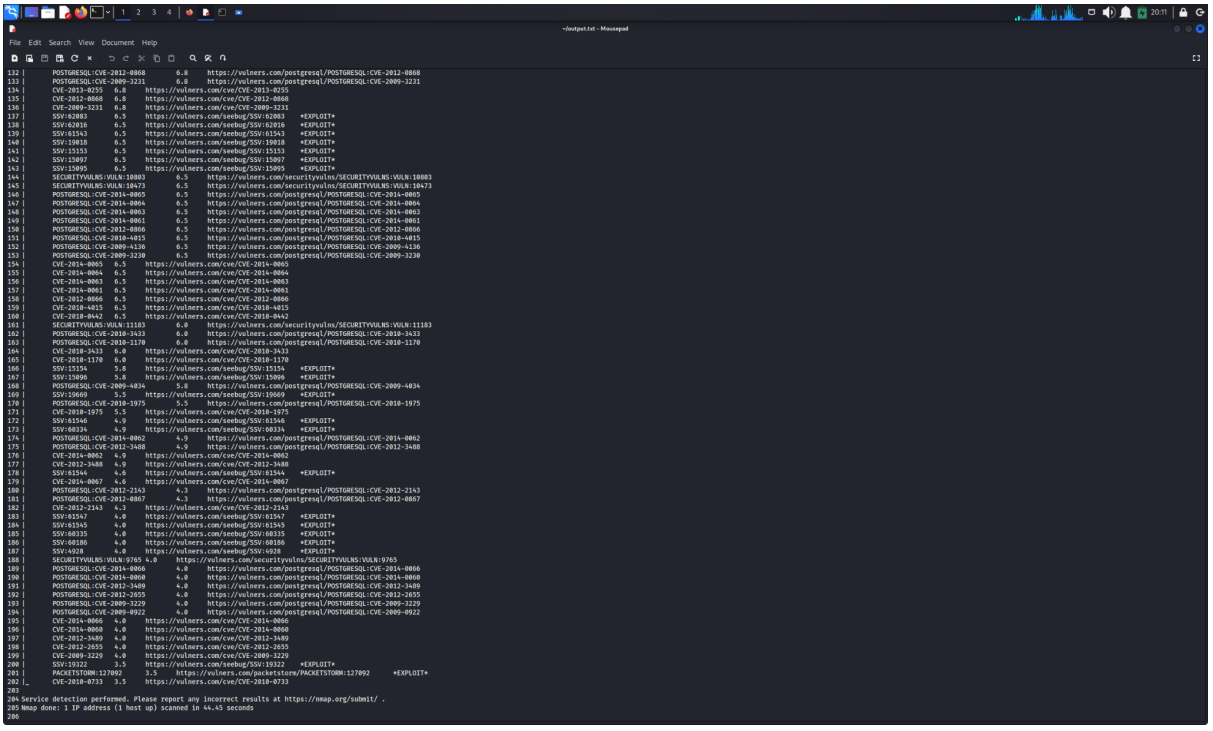
As portas apresentam as seguintes vulnerabilidades de maior criticalidade:

- 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.

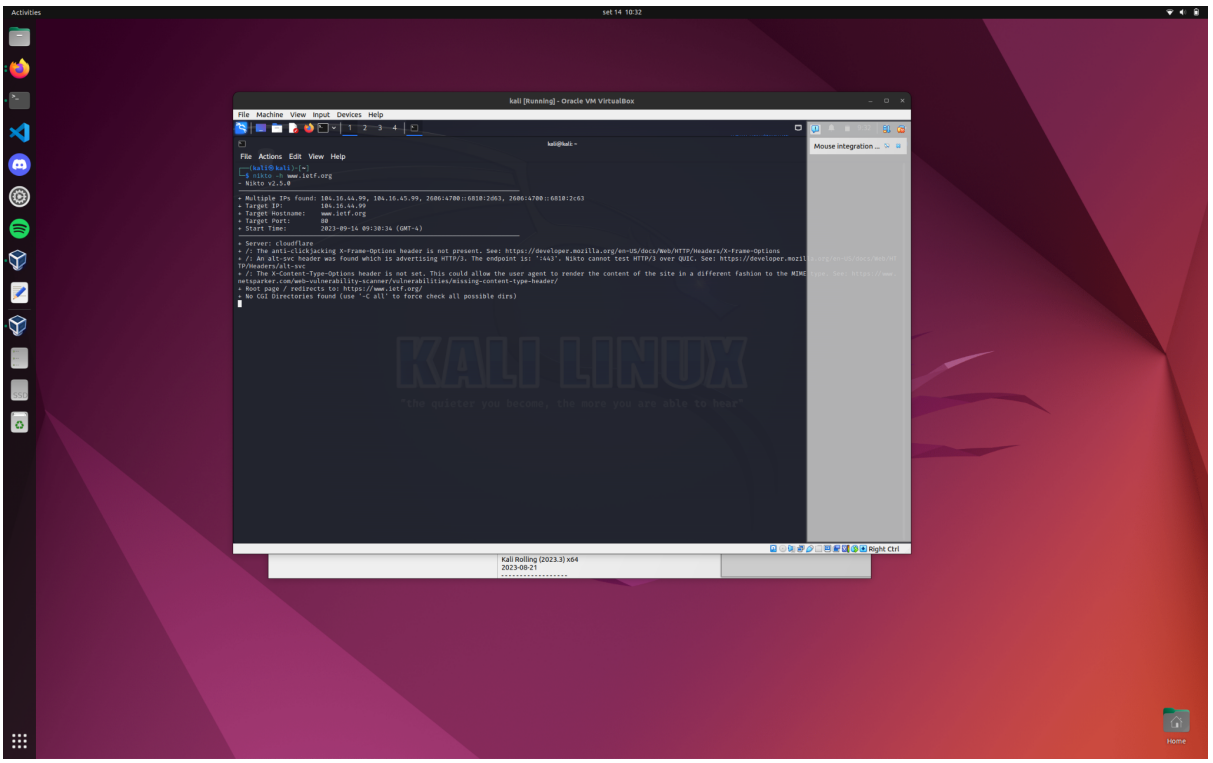



~/output.txt - Mousepad
File Edit Search View Document Help
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
ssl-poodle:
VULNERABLE:
SSL POODLE 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
https://www.securityfocus.com/bid/70574
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
ssl-ccs-injection:
VULNERABLE:
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
http://www.cvedetails.com/cve/2014-0224
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
vulners:
cpe:/a:postgresql:postgresql:8.3:
SSV:60718 10.0 https://vulners.com/seebug/SSV:60718 *EXPLOIT*
CVE-2013-1903 10.0 https://vulners.com/cve/CVE-2013-1903
CVE-2013-1902 10.0 https://vulners.com/cve/CVE-2013-1902
SSV:30015 8.5 https://vulners.com/seebug/SSV:30015 *EXPLOIT*
SSV:19652 8.5 https://vulners.com/seebug/SSV:19652 *EXPLOIT*
POSTGRESQL:CVE-2013-1900 8.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
POSTGRESQL:CVE-2010-1169 8.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
CVE-2010-1447 8.5 https://vulners.com/cve/CVE-2010-1447
CVE-2010-1169 8.5 https://vulners.com/cve/CVE-2010-1169
SSV:19754 7.5 https://vulners.com/seebug/SSV:19754 *EXPLOIT*
SSV:30152 6.8 https://vulners.com/seebug/SSV:30152 *EXPLOIT*
SECURITYVULNS:VULN:10252 6.8 https://vulners.com/securityvulns/SECURITYVULNS:VULN:10252
POSTGRESQL:CVE-2013-0255 6.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2013-0255
POSTGRESQL:CVE-2012-0868 6.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0868
POSTGRESQL:CVE-2009-3231 6.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3231
CVE-2013-0255 6.8 https://vulners.com/cve/CVE-2013-0255
CVE-2012-0868 6.8 https://vulners.com/cve/CVE-2012-0868
CVE-2009-3231 6.8 https://vulners.com/cve/CVE-2009-3231
SSV:62083 6.5 https://vulners.com/seebug/SSV:62083 *EXPLOIT*
SSV:62016 6.5 https://vulners.com/seebug/SSV:62016 *EXPLOIT*
SSV:61543 6.5 https://vulners.com/seebug/SSV:61543 *EXPLOIT*
SSV:19018 6.5 https://vulners.com/seebug/SSV:19018 *EXPLOIT*
SSV:15153 6.5 https://vulners.com/seebug/SSV:15153 *EXPLOIT*
SSV:15097 6.5 https://vulners.com/seebug/SSV:15097 *EXPLOIT*
SSV:15095 6.5 https://vulners.com/seebug/SSV:15095 *EXPLOIT*
SECURITYVULNS:VULN:10803 6.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:10803
SECURITYVULNS:VULN:10473 6.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:10473
POSTGRESQL:CVE-2014-0065 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0065
POSTGRESQL:CVE-2014-0064 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0064
POSTGRESQL:CVE-2014-0063 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0063
POSTGRESQL:CVE-2014-0061 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0061


~/output.txt - Mousepad
File Edit Search View Document Help
POSTGRESQL:CVE-2012-0868 6.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0868
POSTGRESQL:CVE-2009-3231 6.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3231
CVE-2013-0255 6.8 https://vulners.com/cve/CVE-2013-0255
CVE-2012-0868 6.8 https://vulners.com/cve/CVE-2012-0868
CVE-2009-3231 6.8 https://vulners.com/cve/CVE-2009-3231
SSV:62083 6.5 https://vulners.com/seebug/SSV:62083 *EXPLOIT*
SSV:62016 6.5 https://vulners.com/seebug/SSV:62016 *EXPLOIT*
SSV:61543 6.5 https://vulners.com/seebug/SSV:61543 *EXPLOIT*
SSV:19018 6.5 https://vulners.com/seebug/SSV:19018 *EXPLOIT*
SSV:15153 6.5 https://vulners.com/seebug/SSV:15153 *EXPLOIT*
SSV:15097 6.5 https://vulners.com/seebug/SSV:15097 *EXPLOIT*
SSV:15095 6.5 https://vulners.com/seebug/SSV:15095 *EXPLOIT*
SECURITYVULNS:VULN:10803 6.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:10803
SECURITYVULNS:VULN:10473 6.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:10473
POSTGRESQL:CVE-2014-0065 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0065
POSTGRESQL:CVE-2014-0066 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0066
POSTGRESQL:CVE-2014-0063 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0063
POSTGRESQL:CVE-2014-0061 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0061
POSTGRESQL:CVE-2012-0866 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0866
POSTGRESQL:CVE-2010-4015 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-4015
POSTGRESQL:CVE-2009-4136 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4136
POSTGRESQL:CVE-2009-3230 6.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3230
CVE-2014-0065 6.5 https://vulners.com/cve/CVE-2014-0065
CVE-2014-0066 6.5 https://vulners.com/cve/CVE-2014-0066
CVE-2014-0063 6.5 https://vulners.com/cve/CVE-2014-0063
CVE-2014-0061 6.5 https://vulners.com/cve/CVE-2014-0061
CVE-2012-0866 6.5 https://vulners.com/cve/CVE-2012-0866
CVE-2010-4015 6.5 https://vulners.com/cve/CVE-2010-4015
CVE-2010-0442 6.5 https://vulners.com/cve/CVE-2010-0442
SECURITYVULNS:VULN:11183 6.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:11183
POSTGRESQL:CVE-2010-3433 6.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-3433
POSTGRESQL:CVE-2010-1170 6.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1170
CVE-2010-3433 6.0 https://vulners.com/cve/CVE-2010-3433
CVE-2010-1170 6.0 https://vulners.com/cve/CVE-2010-1170
SSV:15154 5.8 https://vulners.com/seebug/SSV:15154 *EXPLOIT*
SSV:15090 5.8 https://vulners.com/seebug/SSV:15090 *EXPLOIT*
POSTGRESQL:CVE-2009-4034 5.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4034
SSV:19669 5.5 https://vulners.com/seebug/SSV:19669 *EXPLOIT*
POSTGRESQL:CVE-2010-1975 5.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1975
CVE-2010-1975 5.5 https://vulners.com/cve/CVE-2010-1975
SSV:61546 4.9 https://vulners.com/seebug/SSV:61546 *EXPLOIT*
SSV:60334 4.9 https://vulners.com/seebug/SSV:60334 *EXPLOIT*
POSTGRESQL:CVE-2014-0062 4.9 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0062
POSTGRESQL:CVE-2012-3488 4.9 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3488
CVE-2014-0062 4.9 https://vulners.com/cve/CVE-2014-0062
CVE-2012-3488 4.9 https://vulners.com/cve/CVE-2012-3488
SSV:61544 4.6 https://vulners.com/seebug/SSV:61544 *EXPLOIT*
CVE-2014-0067 4.6 https://vulners.com/cve/CVE-2014-0067
POSTGRESQL:CVE-2012-2143 4.3 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-2143
POSTGRESQL:CVE-2012-0867 4.3 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0867
CVE-2012-2143 4.3 https://vulners.com/cve/CVE-2012-2143
SSV:61547 4.0 https://vulners.com/seebug/SSV:61547 *EXPLOIT*
SSV:61545 4.0 https://vulners.com/seebug/SSV:61545 *EXPLOIT*
SSV:60335 4.0 https://vulners.com/seebug/SSV:60335 *EXPLOIT*
SSV:60186 4.0 https://vulners.com/seebug/SSV:60186 *EXPLOIT*
SSV:4928 4.0 https://vulners.com/seebug/SSV:4928 *EXPLOIT*
SECURITYVULNS:VULN:9765 4.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9765
POSTGRESQL:CVE-2014-0066 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0066
POSTGRESQL:CVE-2014-0060 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0060
POSTGRESQL:CVE-2012-3489 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3489
POSTGRESQL:CVE-2012-2655 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-2655
POSTGRESQL:CVE-2009-3229 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3229
POSTGRESQL:CVE-2009-0922 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-0922
CVE-2014-0066 4.0 https://vulners.com/cve/CVE-2014-0066
CVE-2014-0060 4.0 https://vulners.com/cve/CVE-2014-0060
CVE-2012-3489 4.0 https://vulners.com/cve/CVE-2012-3489
CVE-2012-2655 4.0 https://vulners.com/cve/CVE-2012-2655
CVE-2009-3229 4.0 https://vulners.com/cve/CVE-2009-3229
SSV:19322 3.5 https://vulners.com/seebug/SSV:19322 *EXPLOIT*
PACKETSTORM:127092 3.5 https://vulners.com/packetstorm/PACKETSTORM:127092 *EXPLOIT*
CVE-2010-0733 3.5 https://vulners.com/cve/CVE-2010-0733
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.45 seconds

F

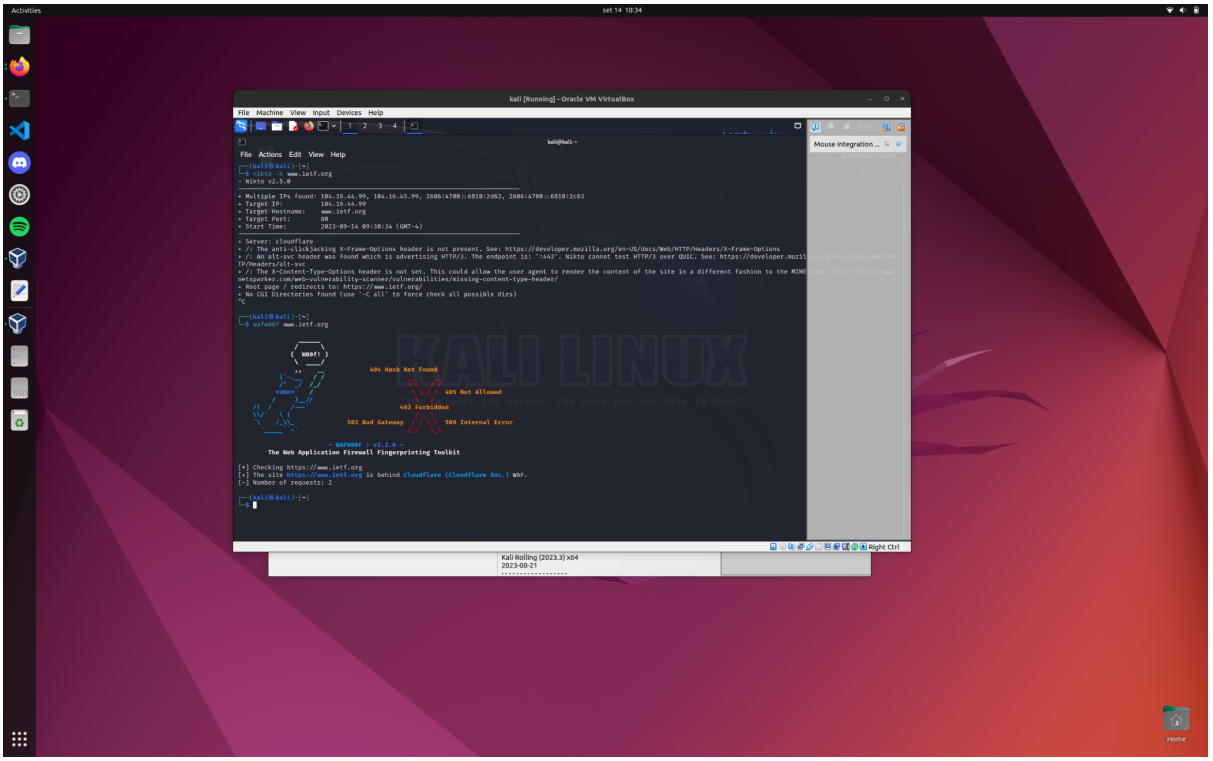
1 -



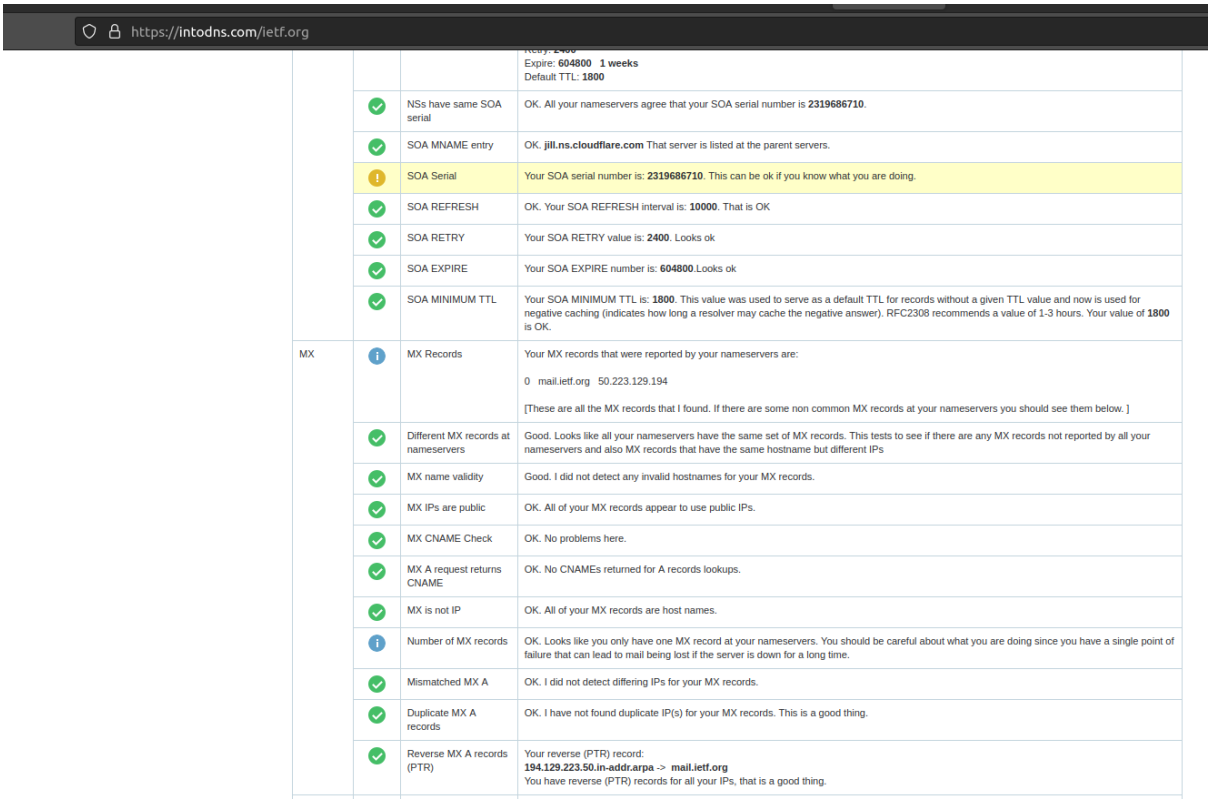
o endereco IP associado e 104.16.44.99

2 -

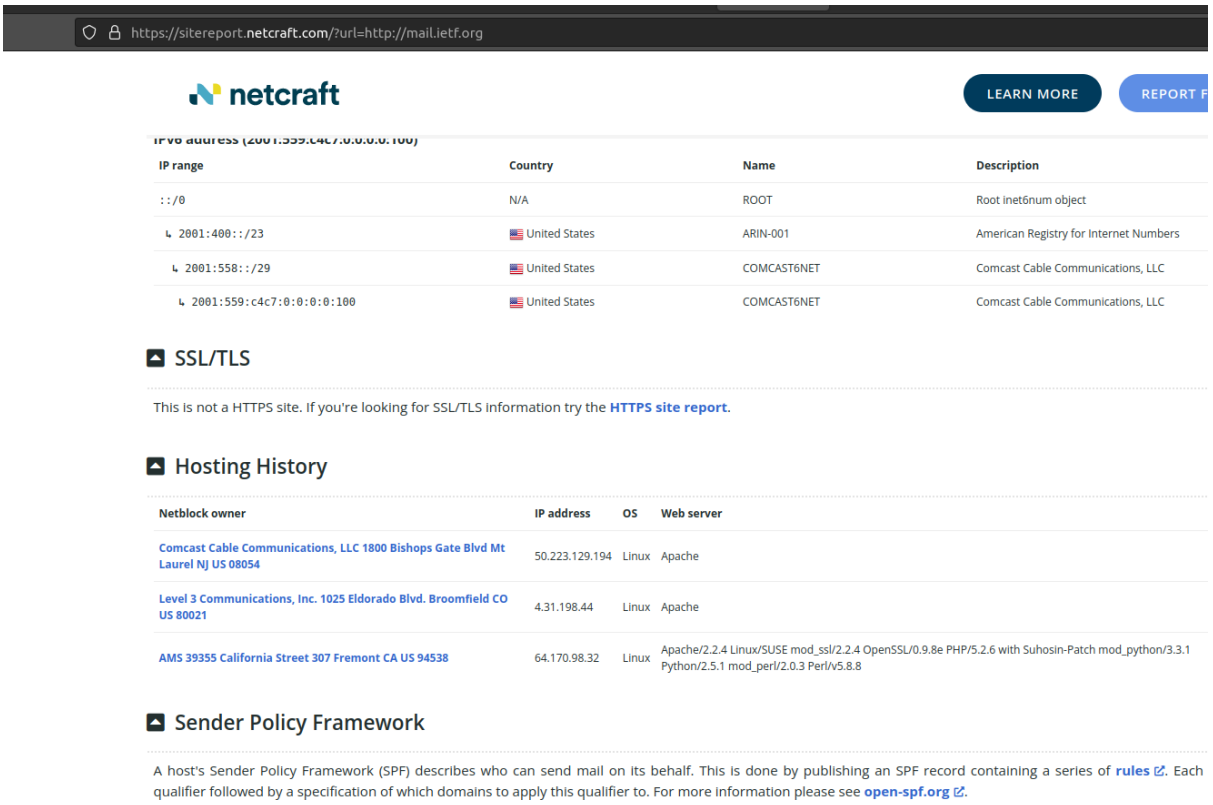
Como evidenciado no output do comando acima e do comando abaixo, o servidor DNS utilizado e o cloudflare



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

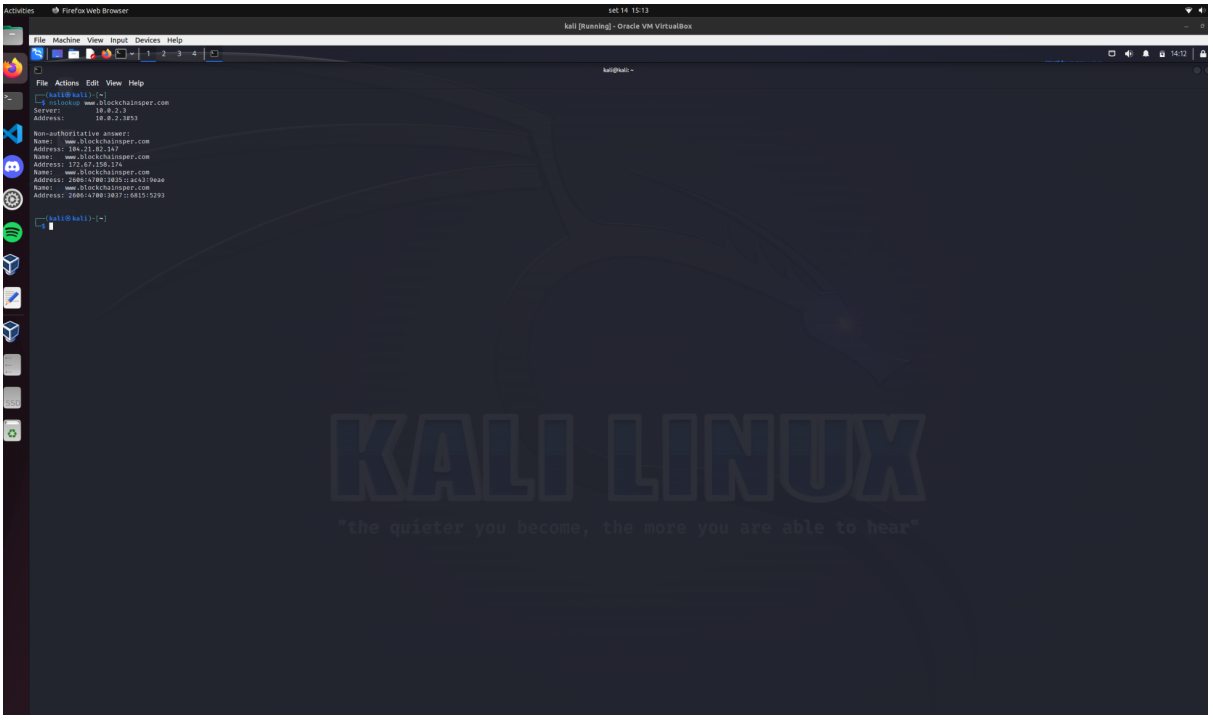


A partir dessa informação, e uma rápida pesquisa no netcraft, foi inserido o link relativo ao serviço mx, mail.ietf.org, e foi encontrado que o servico esta sendo hosteado no IP 50.223.129.194, com sede na Comcast Cable Communications, LLC 1800 Bishops Gate Blvd Mt Laurel NJ US 08054.



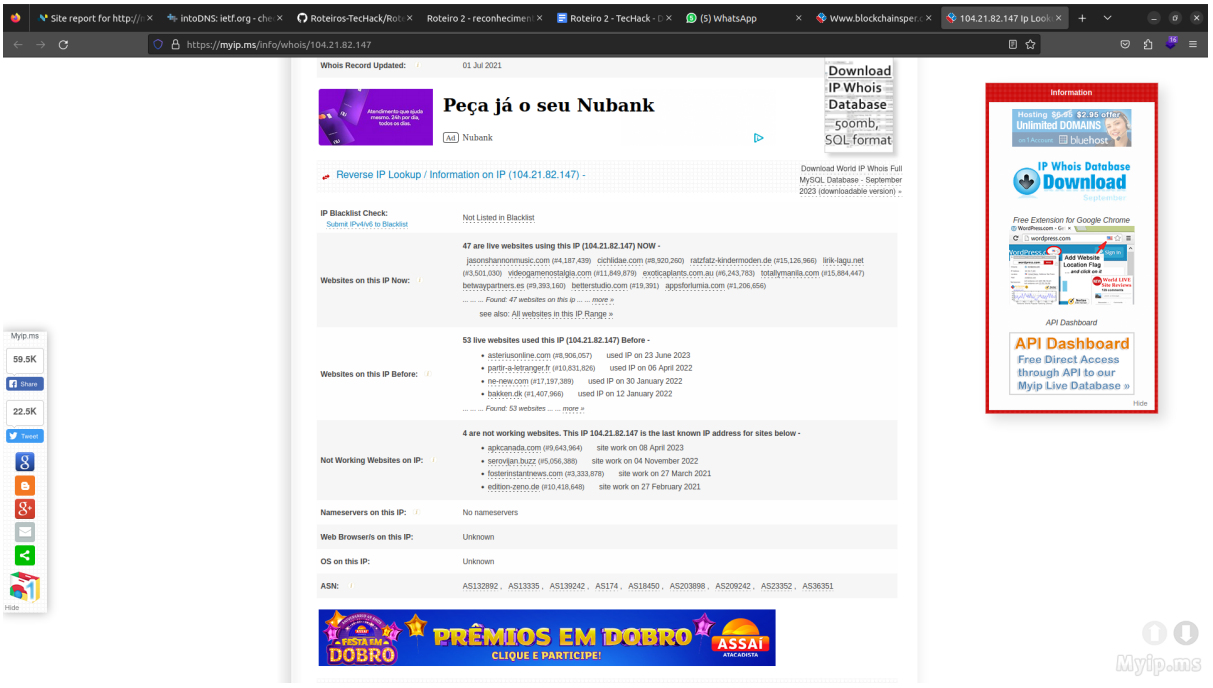
G - Site escolhido: blockchainsper.com

1



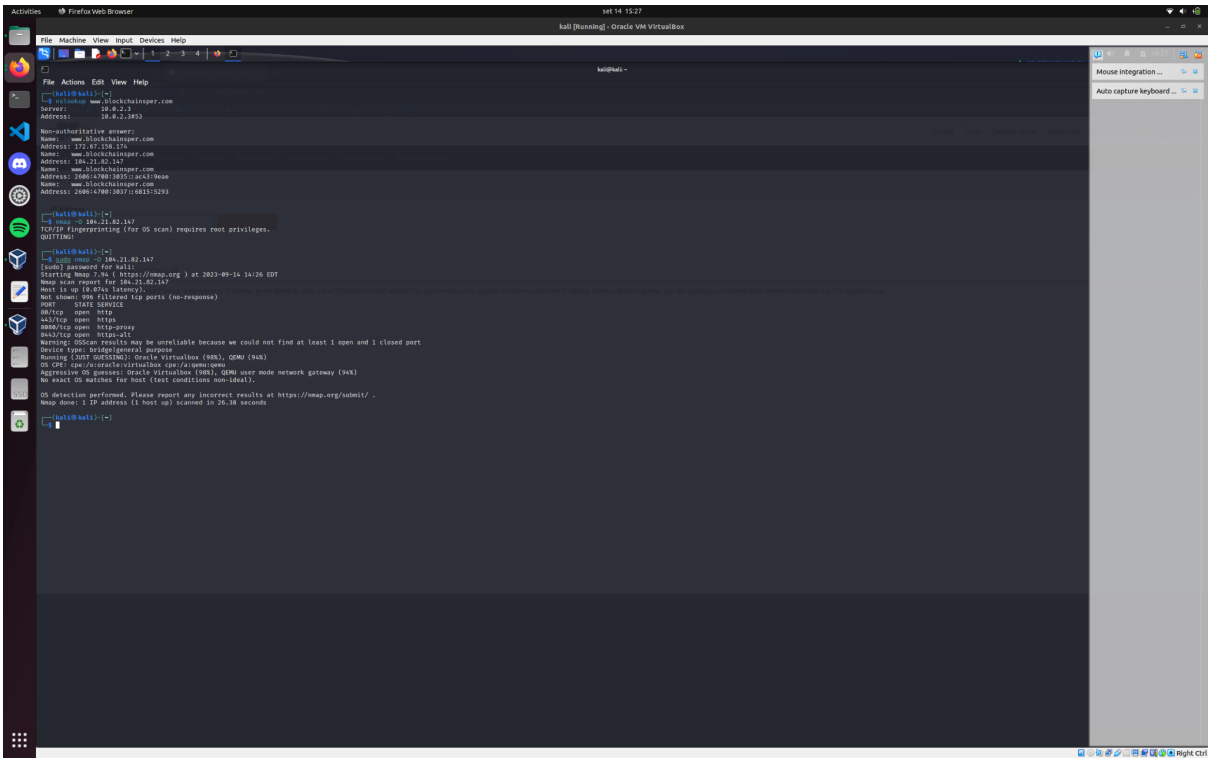
2

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

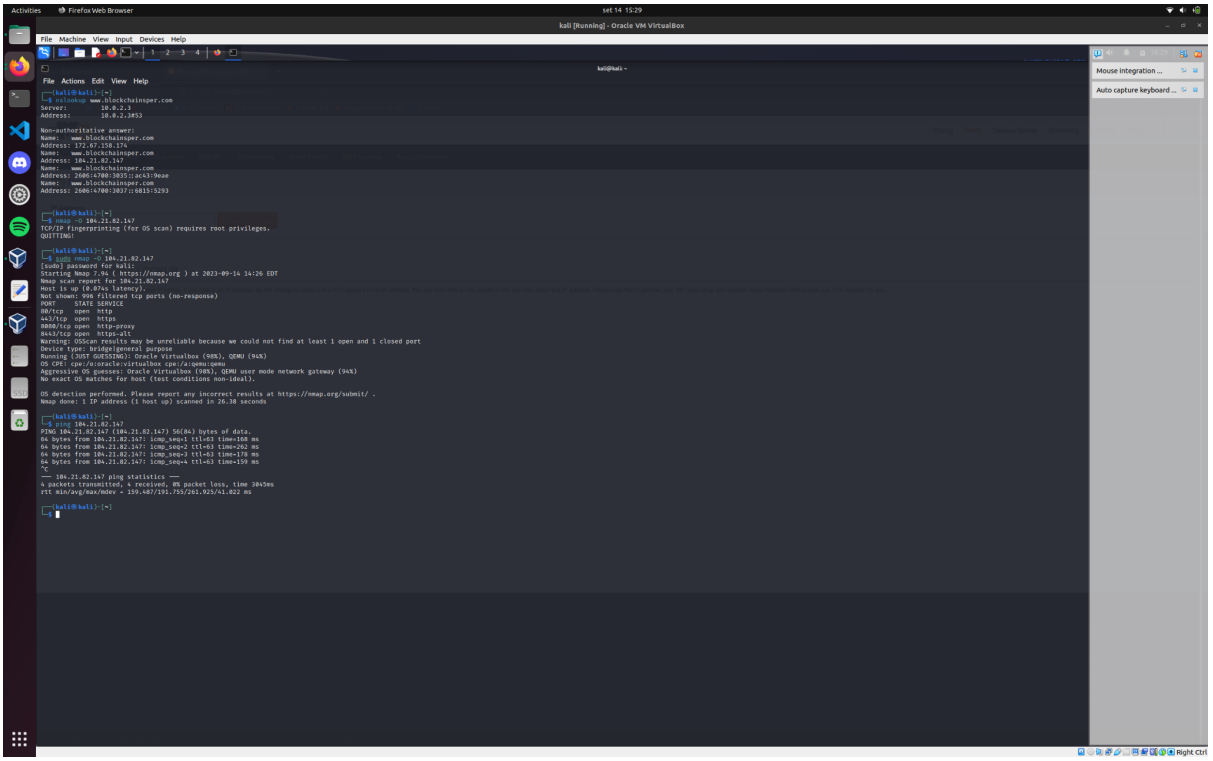


3

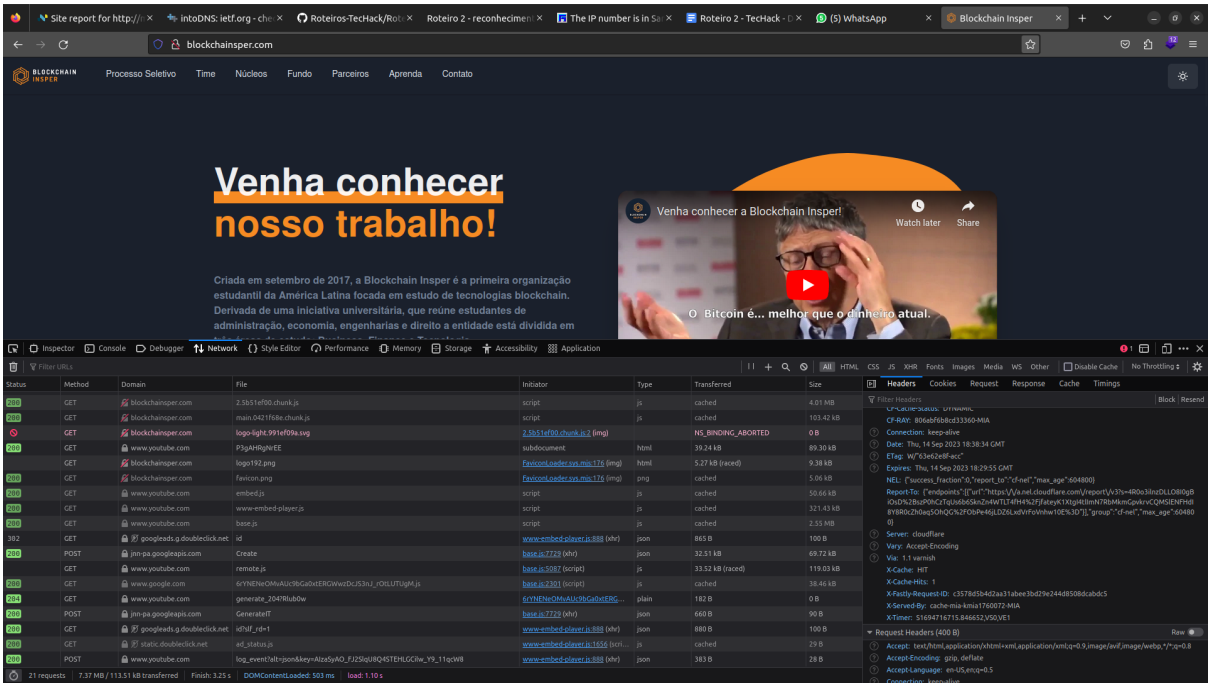
utilizando o comando de nmap, é possível dizer, com 98% de certeza, que o OS do IP e o Oracle Virtualbox.



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

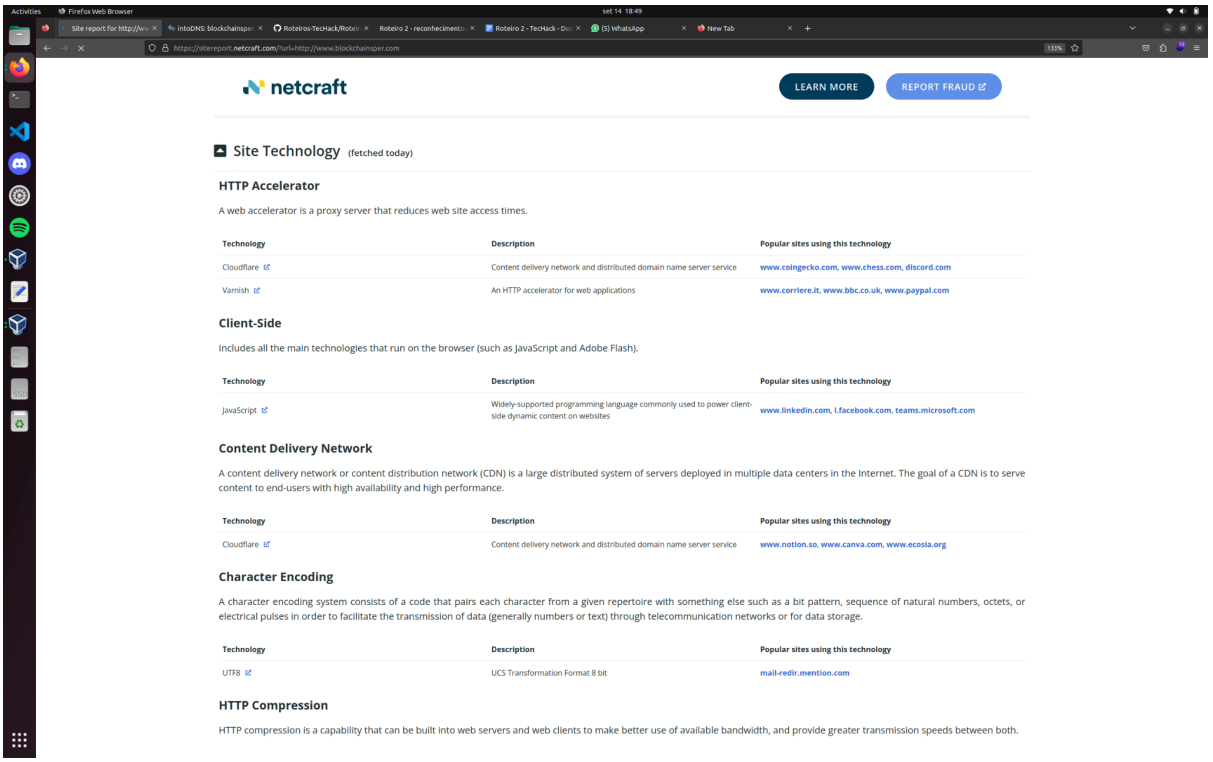


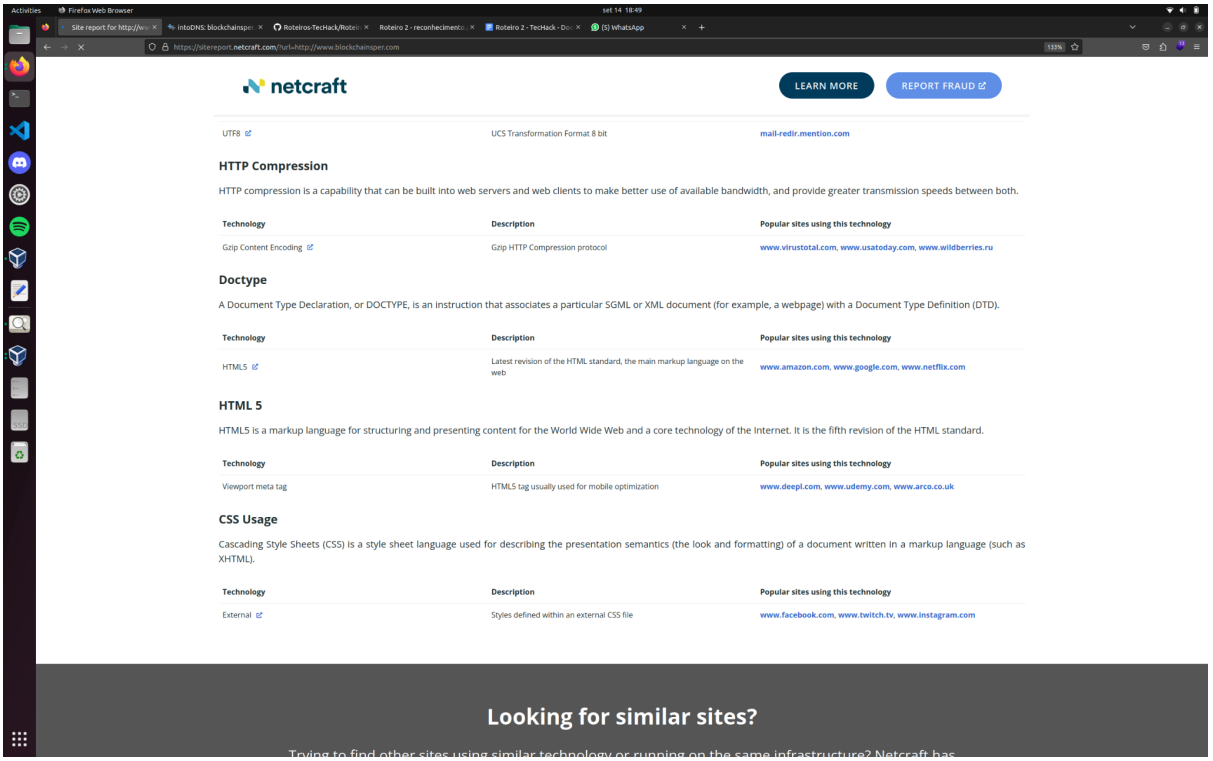
Ao consultar o site https://www.robtex.com/ip-lookup/104.21.82.147 e ao ver o header do site pelo browser, é possível concluir que o webserver de host do IP e o cloudflare.



4

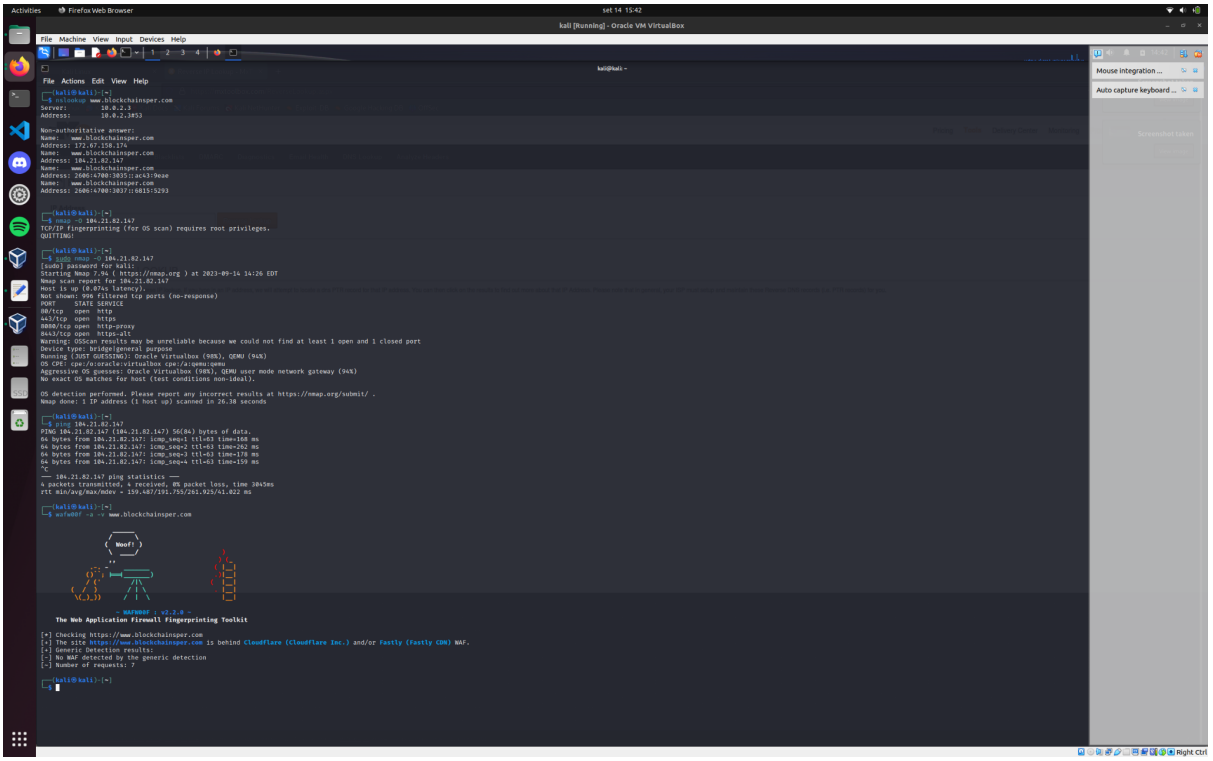
As tecnologias utilizadas pelo site, como demonstrado pelo relatório do netstat, são as abaixo:





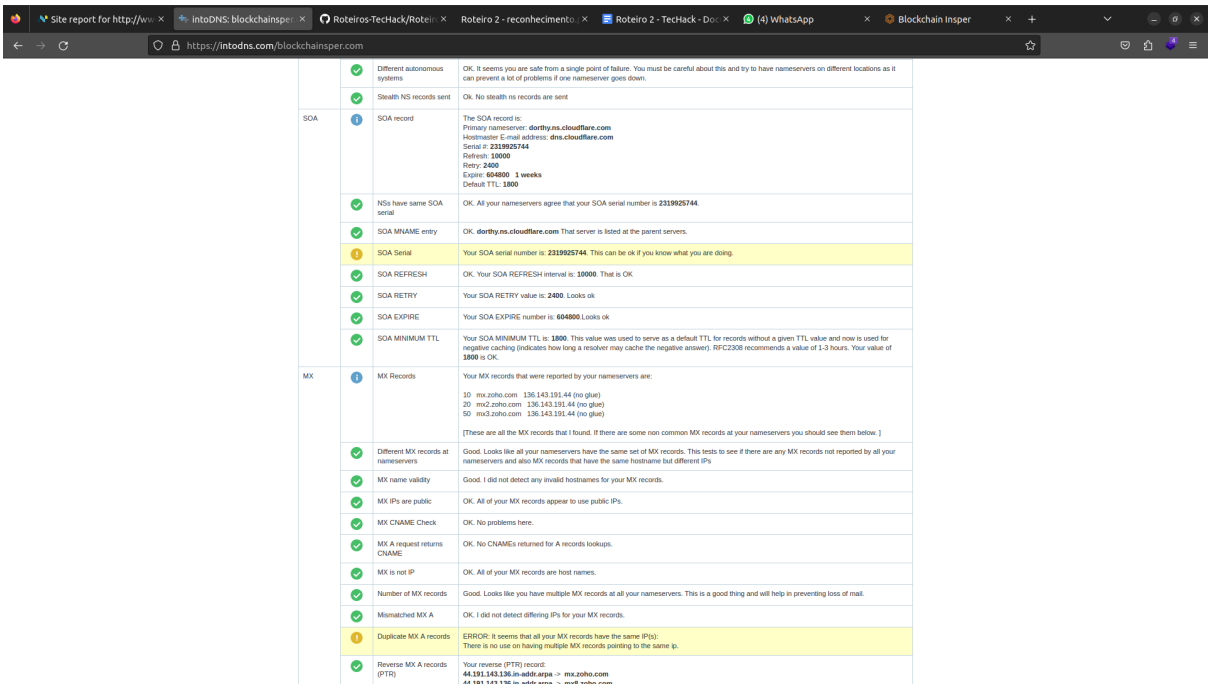
5

Pela busca realizada o site não é protegido por WAF



6

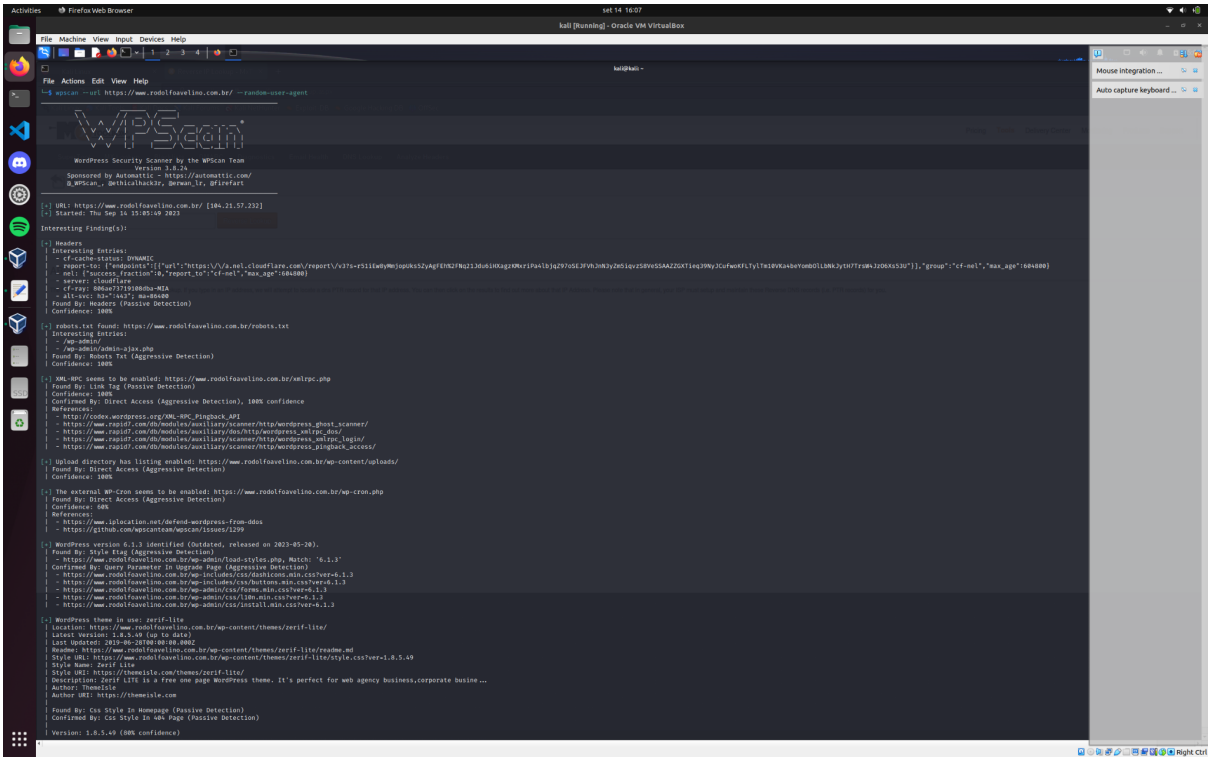
Realizando a busca pelo site intodns, são reconhecidos 3 serviços de email, todos hosteados pela zoho. O IP atrelado pelo servico e o 136.143.191.44

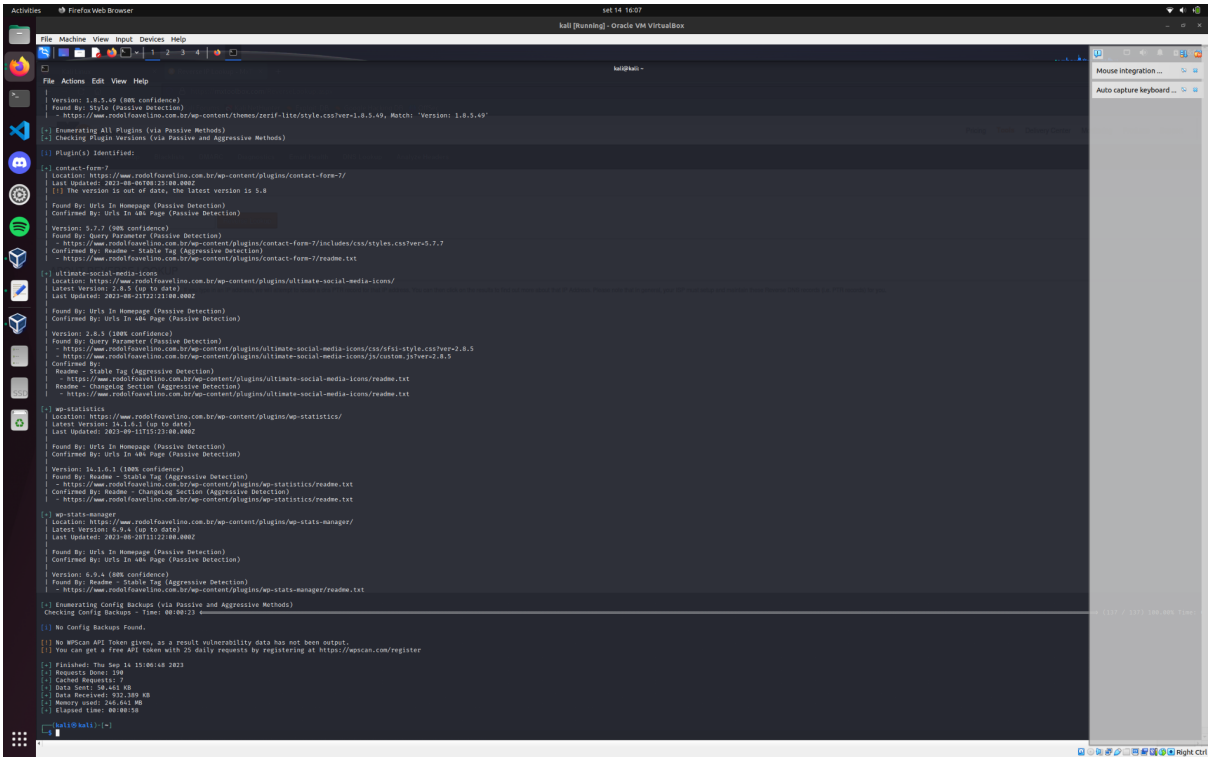


	✓	Different autonomous systems	OK. It seems you are safe from a single point of failure. You must be careful about this and try to have nameservers on different locations as it can prevent a lot of problems if one nameserver goes down.
	✓	Stealth NS records sent	Ok. No stealth ns records are sent
SOA	i	SOA record	The SOA record is: Primary nameserver: **dorthy.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. **dorthy.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	i	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 of 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: **44.191.143.136.in-addr.arpa** -> **mx.zoho.com**

H

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



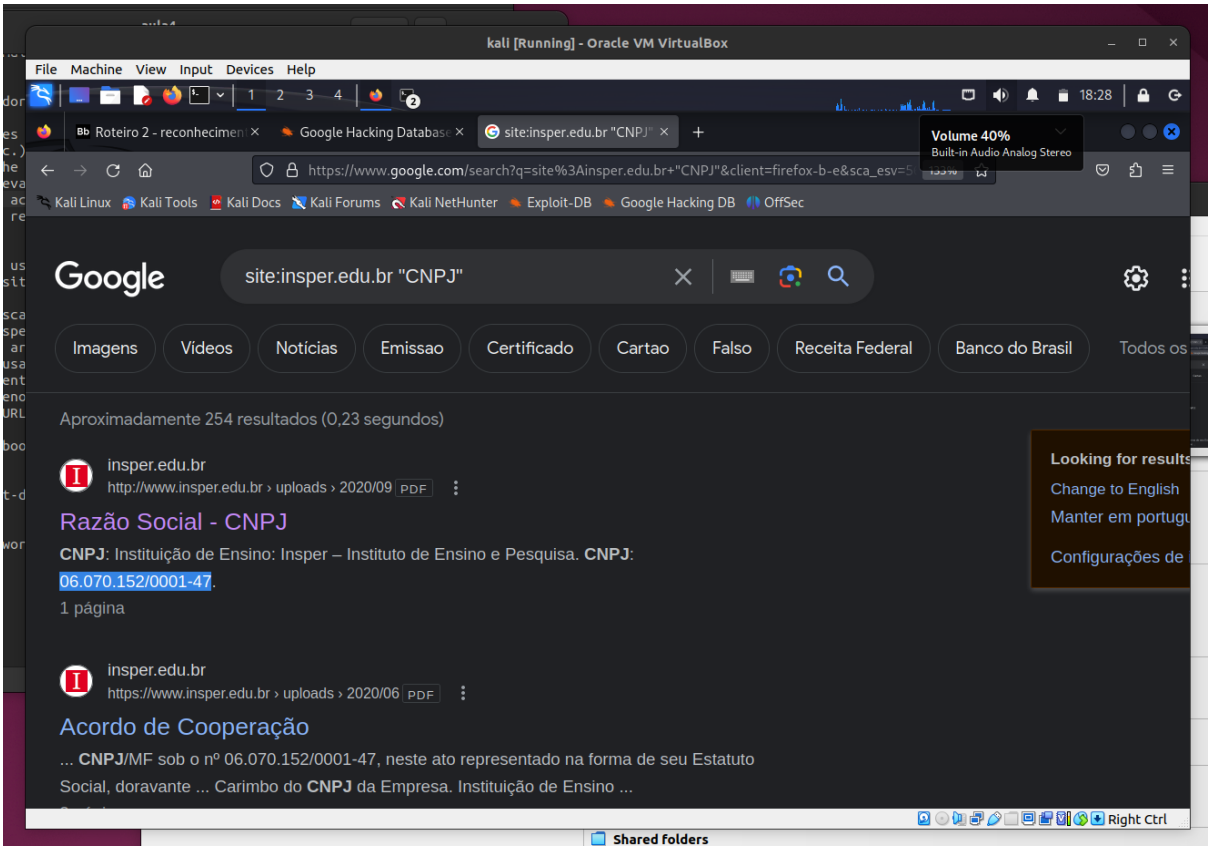


A partir destes resultados,é possível identificar 7 plugins no site, alguns arquivos php que podem conter informações sensíveis e uma identificação de cloudflare como servidor host. O arquivo de maior interesse é um chamado admin-ajax.php, onde seria plausível encontrar informações sensíveis sobre o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

I

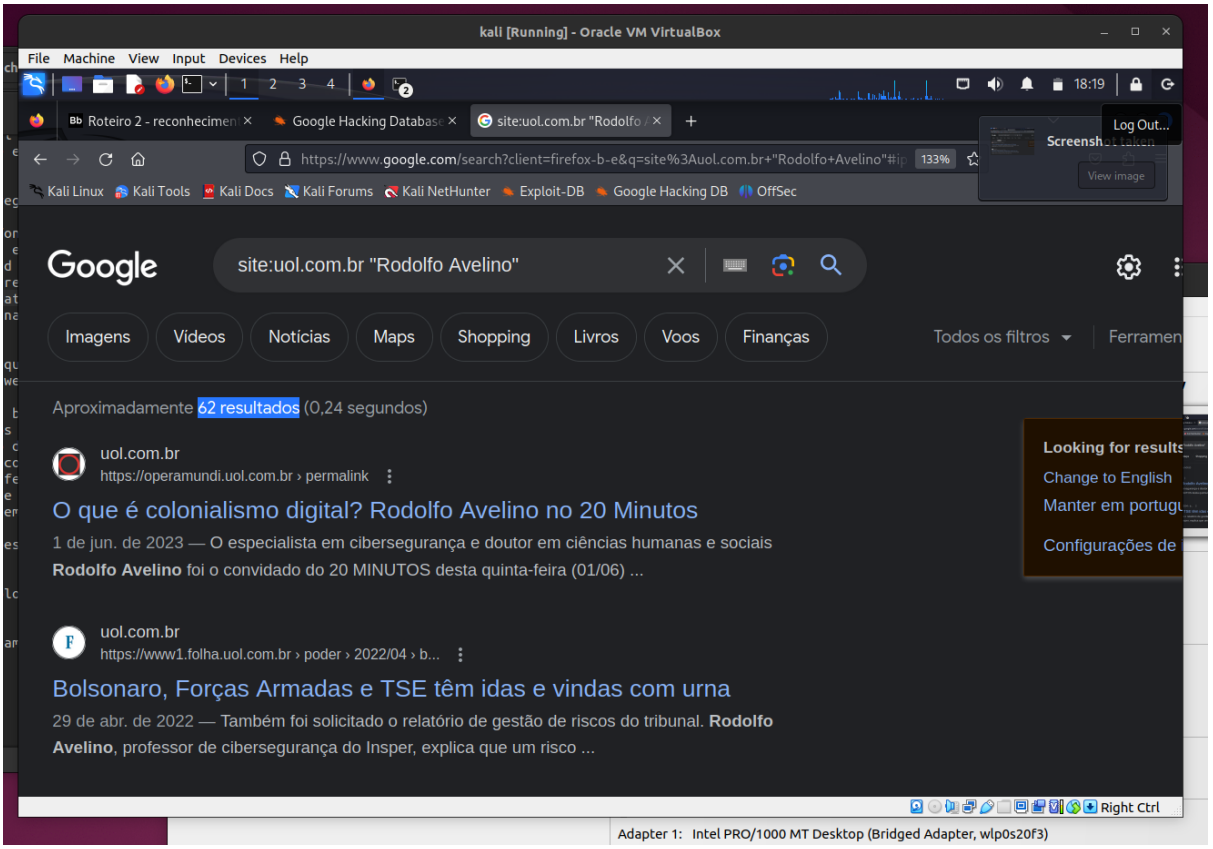
1

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



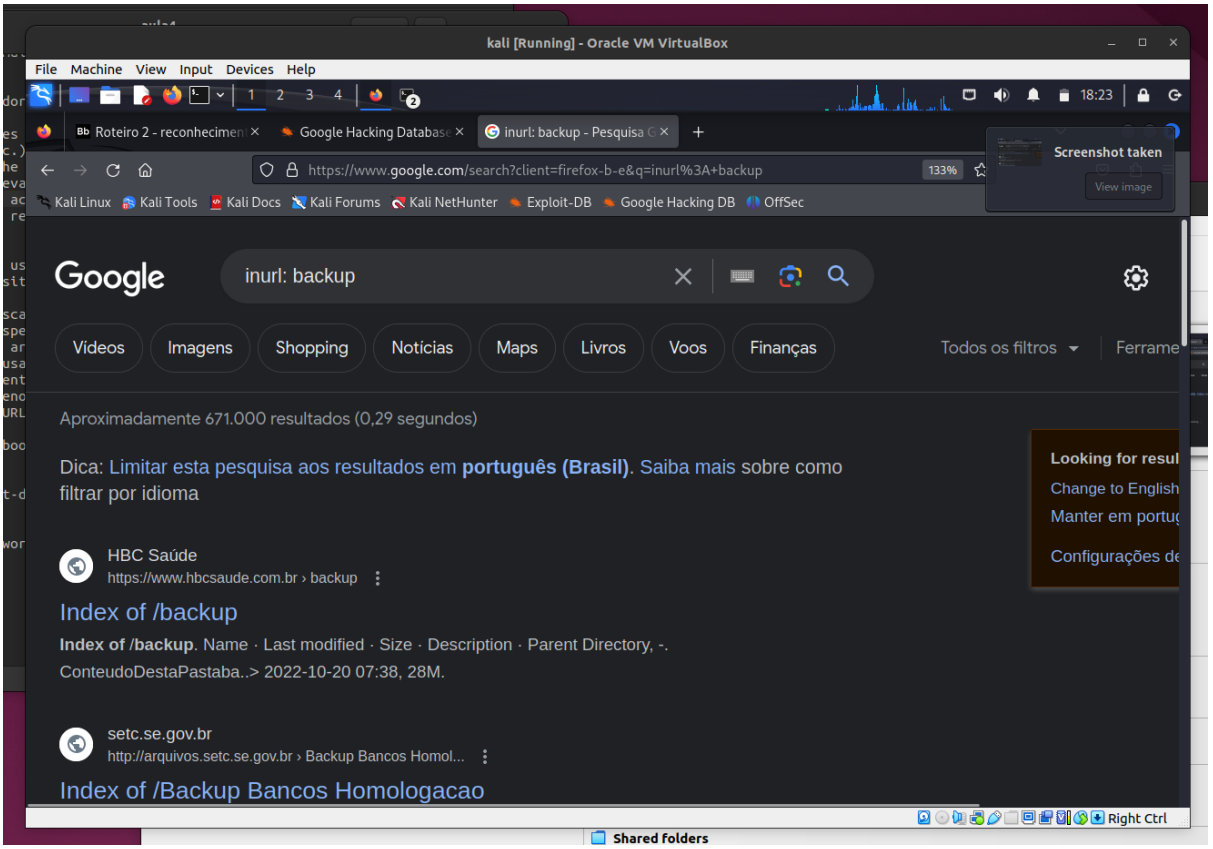
2

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=2ahUKEwi47InwkauBAxWuGbkGHTLACxoQFnoECA8QAQ&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.


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Roteiro 2 - reconhecimen
Google Hacking Databas
inurl: backup - Pesquisa G
https://www.google.com/search?client=firefox-b-e&q=inurl%3A+backup
133%
Screenshot taken
View image
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Google
inurl: backup
Vídeos Imagens Shopping Notícias Maps Livros Voos Finanças
Todos os filtros
Ferrame
Aproximadamente 671.000 resultados (0,29 segundos)
Dica: Limitar esta pesquisa aos resultados em português (Brasil). Saiba mais sobre como filtrar por idioma
Looking for resul
Change to English
Manter em portu
Configurações de
HBC Saúde
https://www.hbcsaude.com.br › backup
Index of /backup
Index of /backup. Name · Last modified · Size · Description · Parent Directory, -.
ConteudoDestaPastaba..> 2022-10-20 07:38, 28M.
setc.se.gov.br
http://arquivos.setc.se.gov.br › Backup Bancos Homol...
Index of /Backup Bancos Homologacao
Right Ctrl
Shared folders