Table of Contents

Introduction

More OSINT options are explored including mind blowing techniques such as searching the internet with a search engine. Email scrapers and webcam creepers abound.

The primary focus of this document however are more everyday elements of network administration and security such as protecting your DNS against unwanted zone transfers, protecting users against themselves undesirably elevating their privileges, and being aware of the different types of obfuscating port scans that could be conducted against your network.

Part 1

Whois

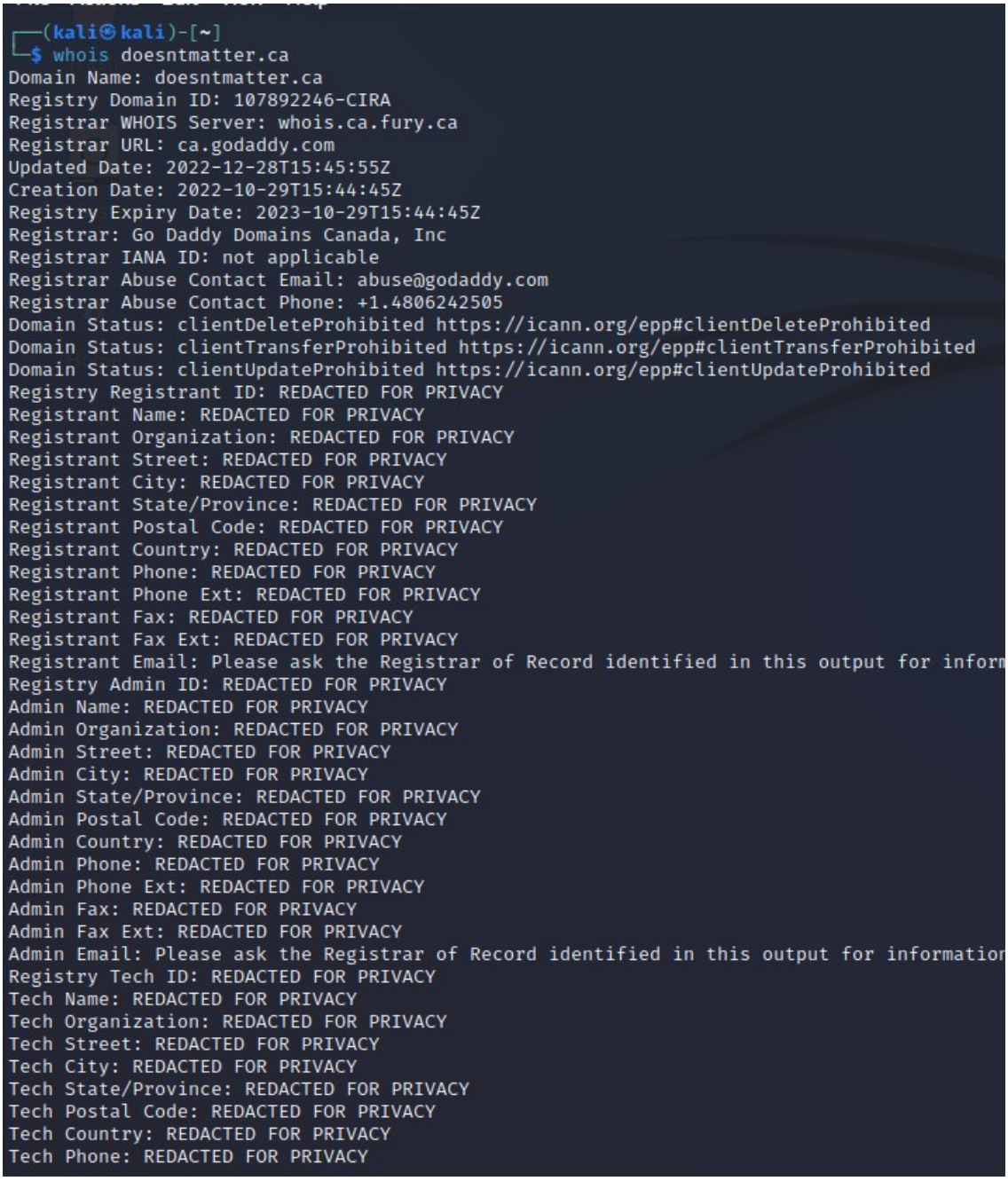

Figure 1: whois Result for doesntmatter.ca

As we can see, godaddy, is the registrar for doesntmatter.ca. Most other details are redacted for "privacy", but if we could actually see who owned the domain then we wouldn't need a broker to help acquire the website now would we?

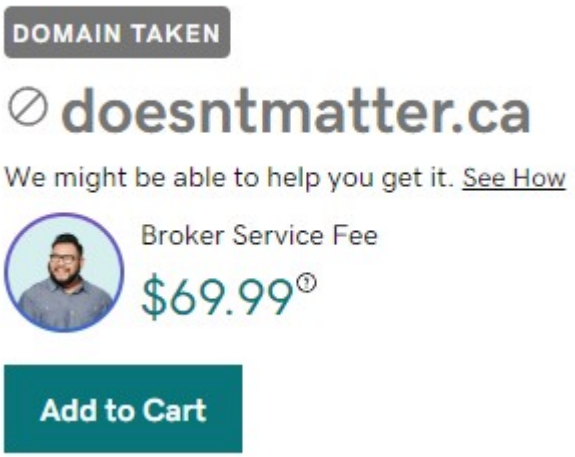

Figure 2: Broker Service Fee

Open Zone Transfers

For some reason ns2 didn't show up but that's ok. This shows that a zone transfer isn't accepted from this IP.

```
┌──(kali㉿kali)-[~]
└─$ dig @10.10.10.2 NS riley.rocky

; <<>> DiG 9.18.8-1-Debian <<>> @10.10.10.2 NS riley.rocky
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20286
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 72152f871983007c013b7cef63d73d26e79066ed1e883d2c (good)
;; QUESTION SECTION:
;riley.rocky.                   IN      NS

;; ANSWER SECTION:
riley.rocky.            1300    IN      NS      ns1.riley.rocky.

;; ADDITIONAL SECTION:
ns1.riley.rocky.        1300    IN      A       10.10.10.2

;; Query time: 0 msec
;; SERVER: 10.10.10.2#53(10.10.10.2) (UDP)
;; WHEN: Sun Jan 29 22:44:37 EST 2023
;; MSG SIZE  rcvd: 102


┌──(kali㉿kali)-[~]
└─$ dig axfr @10.10.10.2 riley.rocky

; <<>> DiG 9.18.8-1-Debian <<>> axfr @10.10.10.2 riley.rocky
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Figure 3: Failed Zone Transfer

```
┌──(kali㉿kali)-[~]
└─$ dig axfr @10.10.10.2 riley.rocky

; <<>> DiG 9.18.8-1-Debian <<>> axfr @10.10.10.2 riley.rocky
; (1 server found)
;; global options: +cmd
riley.rocky.            1300    IN      SOA     ns1.riley.rocky. rockyrockyrocky.riley.rocky. 2022112103
3600 1800 604800 1300
riley.rocky.            1300    IN      MX      10 Mail.riley.rocky.
riley.rocky.            1300    IN      A       10.10.10.13
riley.rocky.            1300    IN      NS      ns1.riley.rocky.
Apache.riley.rocky.     1300    IN      A       10.10.10.200
freeburritos.riley.rocky. 1300  IN      A       10.10.10.67
freeguac.riley.rocky.   1300    IN      A       10.10.10.68
freetacos.riley.rocky.  1300    IN      A       10.10.10.66
Mail.riley.rocky.       1300    IN      A       10.10.10.222
mail1.riley.rocky.      1300    IN      A       10.10.10.100
mail2.riley.rocky.      1300    IN      A       10.10.10.101
Monitor.riley.rocky.    1300    IN      A       10.10.10.150
NGinX.riley.rocky.      1300    IN      A       10.10.10.200
ns1.riley.rocky.        1300    IN      A       10.10.10.2
ns2.riley.rocky.        1300    IN      A       10.10.10.3
rockyrockyrocky.riley.rocky. 1300 IN    A       10.10.10.5
site1.riley.rocky.      1300    IN      A       10.10.10.200
site2.riley.rocky.      1300    IN      A       10.10.10.200
site3.riley.rocky.      1300    IN      A       10.10.10.200
site4.riley.rocky.      1300    IN      A       10.10.10.200
site5.riley.rocky.      1300    IN      A       10.10.10.200
site6.riley.rocky.      1300    IN      A       10.10.10.200
www.riley.rocky.        1300    IN      CNAME   riley.rocky.
riley.rocky.            1300    IN      SOA     ns1.riley.rocky. rockyrockyrocky.riley.rocky. 2022112103
3600 1800 604800 1300
;; Query time: 0 msec
;; SERVER: 10.10.10.2#53(10.10.10.2) (TCP)
;; WHEN: Sun Jan 29 22:46:11 EST 2023
;; XFR size: 24 records (messages 1, bytes 622)
```

Figure 4: Successful Zone Transfer

Once I added Kali's private IP to the allowed transfers this was the output. I double checked and both ns1 and ns2 have NS records yet the zone transfer only shows one of them. The freetacos and freeburritos appear to be of particular interest, but really the MX record is interesting because you could potentially learn some email addresses and skip this whole hacking business and get the people to hand over the keys to the kingdom without needing any more technical knowledge whatsoever.

Part 2

Spoof MAC address

10.10.10.2 is the IP address of my DNS server.

sudo nmap 10.10.10.2 -T2 -p 1-1024 -n -sV -Pn --spoof-mac Apple --send-ip -v5

Flag Explanations:

- T2 – Slows down speed of scan
- p – Restrict port range

- n – No DNS Resolution
- sV – Version scanning
- Pn – No ping
- spoof-mac – Disguises source MAC address
- send-ip – Sends IP packets even over local LAN
- v5 – Enables very verbose output

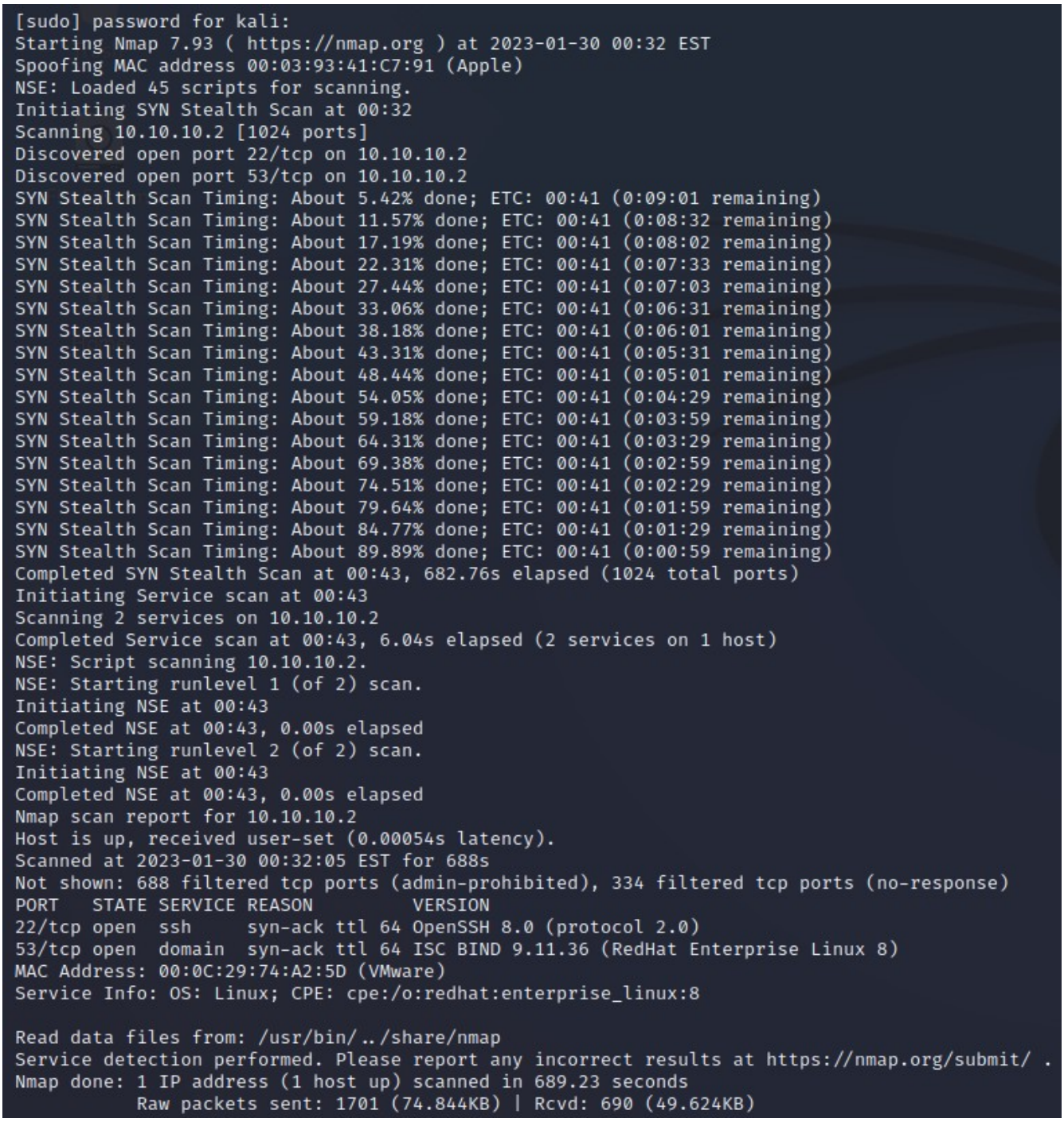

Figure 5: Sneaky Slow nmap Scan

Decoy IP Address

nmap -D 172.16.102.254 172.16.102.0/24 -PR -sn -v5

Flag Explanations:

- D – Decoy lets scan appear to come from multiple IP addresses
- PR – ARP Scan

- sn – ping scan does not include ports

```
Nmap scan report for 172.16.102.11 [host down, received no-response]
Nmap scan report for rockyrockyrocky (172.16.102.12)
Host is up, received arp-response (0.00018s latency).
MAC Address: 00:0C:29:C3:31:D6 (VMware)
Nmap scan report for 172.16.102.13
Host is up, received arp-response (0.0014s latency).
MAC Address: 00:0C:29:9A:2F:14 (VMware)
Nmap scan report for kobikali (172.16.102.14)
Host is up, received arp-response (0.026s latency).
MAC Address: 04:56:E5:AE:25:31 (Intel Corporate)
Nmap scan report for 172.16.102.15 [host down, received no-response]
```

Figure 6: ARP Scan with Decoys

Hiding Apache Version

According to reference [9], having the lines

ServerTokens Prod

ServerSignature Off

in your Apache conf file will turn your banner into only "Apache". This is successful. Having to locate where in the configuration files for each of your open port's daemons takes a lot of time and it would be nice to have a global setting to be able to stop your daemons from giving away so much free information.

Zenmap

Before installing firewall-cmd all ports were in ignored states. After installing and starting firewalld the ssh port becomes available. It is closed in the below screenshot because the ssh service itself is not running.

Using the -sV flag results in NSOCK ERROR which is apparently a bug.

Recommended fixes:

- Run sudo firewall-cmd --zone=public --remove-interface=eth1 to restrict ssh to private IP range only
- sudo firewall-cmd --zone=public --add-source=10.10.10.1 to further restrict ssh to host IP only

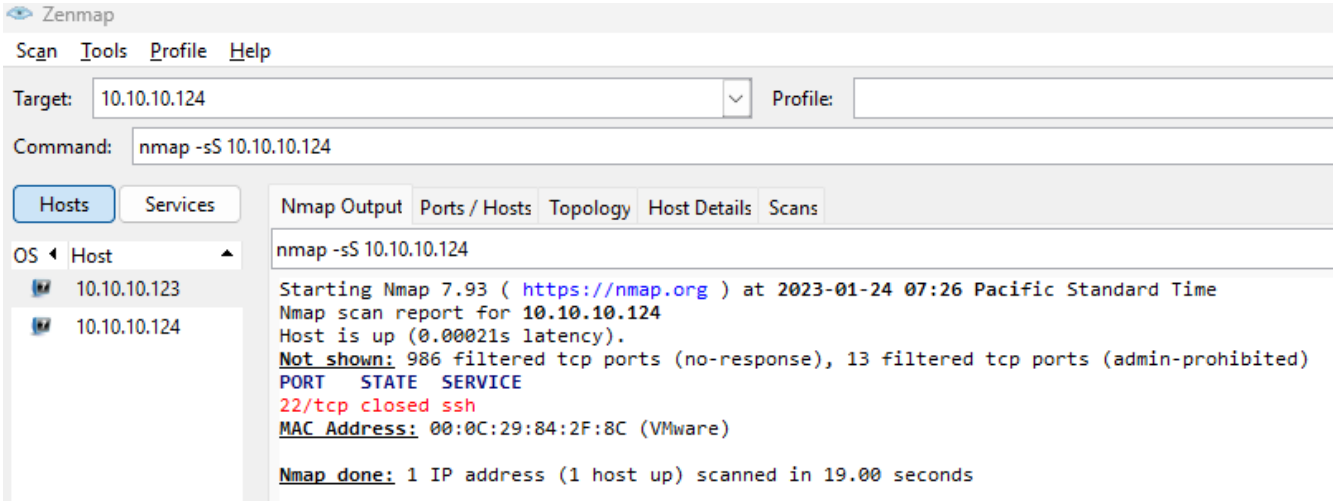

Figure 7: Available TCP Ports for Kali Linux on Private IP

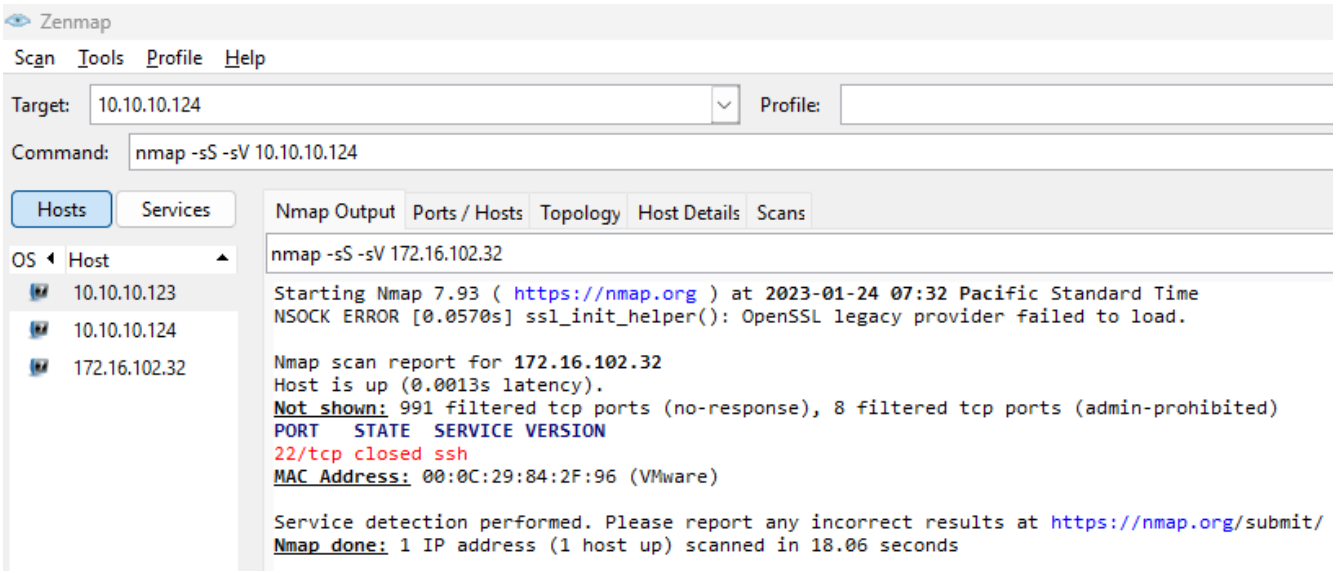

Figure 8: Available TCP Ports for Kali Linux on Public IP

Metasploit Portscan

msfconsole is the command used to start metasploit, then once metasploit has started the command

use auxiliary/scanner/portscan/syn

Like other Metasploit modules RHOSTS and PORTS must be set

set RHOSTS 10.10.10.1

set PORTS 1-1024

To begin the probe simply enter

run

```
msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.10.1
RHOSTS ⇒ 10.10.10.1
msf6 auxiliary(scanner/portscan/syn) > set PORTS 1-1024
PORTS ⇒ 1-1024
msf6 auxiliary(scanner/portscan/syn) > run


[+]  TCP OPEN 10.10.10.1:135
[+]  TCP OPEN 10.10.10.1:139
[+]  TCP OPEN 10.10.10.1:445
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 9: SYN Scan Successfully Completed

Filtering on syn flags is possible using tcp.flags.syn==1 in the filter

If you're going to be trying this in a real scenario please randomize the port order to prevent appearing like a complete amateur.

ip.src == 10.10.10.124 && tcp.flags.syn==1

No.	Time	Source	TCP Segment Len	Sequence Number	Next Sequence Number	Acknowledgment Number	Destination	Protocol	Info
61	25.632475	10.10.10.124	0	0	1	0	10.10.10.1	TCP	27622 → 927 [SYN] Seq=0 Win=3072 Len=0
62	26.134407	10.10.10.124	0	0	1	0	10.10.10.1	TCP	29803 → 928 [SYN] Seq=0 Win=3072 Len=0
63	26.637051	10.10.10.124	0	0	1	0	10.10.10.1	TCP	52921 → 929 [SYN] Seq=0 Win=3072 Len=0
64	27.139673	10.10.10.124	0	0	1	0	10.10.10.1	TCP	52287 → 930 [SYN] Seq=0 Win=3072 Len=0
65	27.643111	10.10.10.124	0	0	1	0	10.10.10.1	TCP	2794 → 931 [SYN] Seq=0 Win=3072 Len=0
66	28.145660	10.10.10.124	0	0	1	0	10.10.10.1	TCP	54003 → 932 [SYN] Seq=0 Win=3072 Len=0
67	28.648539	10.10.10.124	0	0	1	0	10.10.10.1	TCP	57883 → 933 [SYN] Seq=0 Win=3072 Len=0
68	29.151478	10.10.10.124	0	0	1	0	10.10.10.1	TCP	45753 → 934 [SYN] Seq=0 Win=3072 Len=0
69	29.654124	10.10.10.124	0	0	1	0	10.10.10.1	TCP	2467 → 935 [SYN] Seq=0 Win=3072 Len=0
70	30.157496	10.10.10.124	0	0	1	0	10.10.10.1	TCP	55079 → 936 [SYN] Seq=0 Win=3072 Len=0
71	30.659940	10.10.10.124	0	0	1	0	10.10.10.1	TCP	46250 → 937 [SYN] Seq=0 Win=3072 Len=0
72	31.162765	10.10.10.124	0	0	1	0	10.10.10.1	TCP	5231 → 938 [SYN] Seq=0 Win=3072 Len=0
73	31.665500	10.10.10.124	0	0	1	0	10.10.10.1	TCP	37057 → 939 [SYN] Seq=0 Win=3072 Len=0
74	32.167435	10.10.10.124	0	0	1	0	10.10.10.1	TCP	33564 → 940 [SYN] Seq=0 Win=3072 Len=0
75	32.669451	10.10.10.124	0	0	1	0	10.10.10.1	TCP	2601 → 941 [SYN] Seq=0 Win=3072 Len=0
76	33.172260	10.10.10.124	0	0	1	0	10.10.10.1	TCP	8106 → 942 [SYN] Seq=0 Win=3072 Len=0
77	33.674483	10.10.10.124	0	0	1	0	10.10.10.1	TCP	34066 → 943 [SYN] Seq=0 Win=3072 Len=0

Figure 10: Syn Scan Detection in Wireshark

Part 3

Hunter.io

This tool was very questionable. The web sources don't even contain anything about John Gaetz. Before clicking the Verify email below the name it was showing at a 90% confidence interval. Since this pdf document is hosted and publicly accessible can a bot scrape the emails in these pictures?

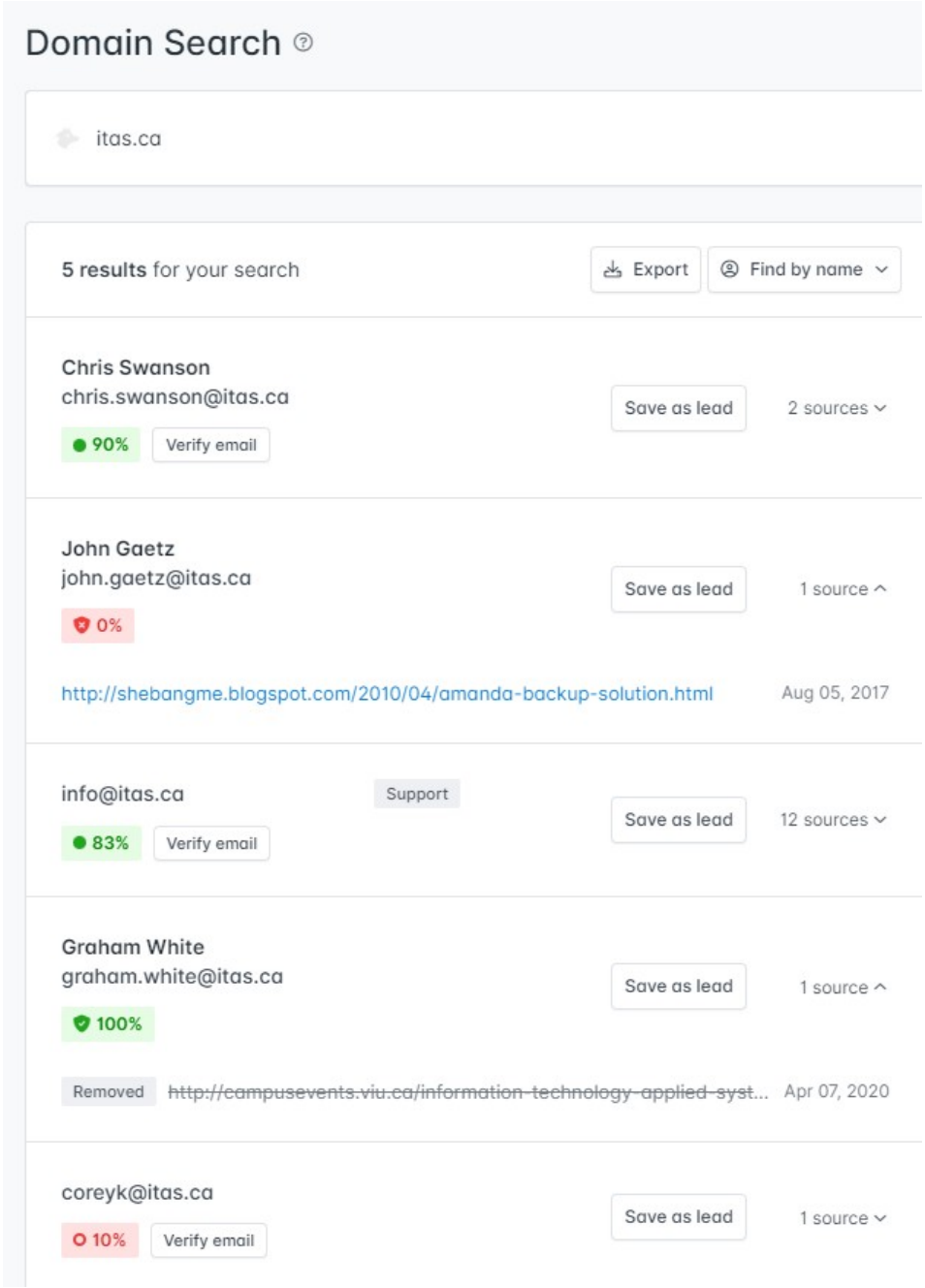

Figure 11: Hunter.io emails for the Domain itas.ca

Shodan.io

It would be interesting to pay $1099/month and hook this up with theHarvester to run a script and probe absolutely everything.

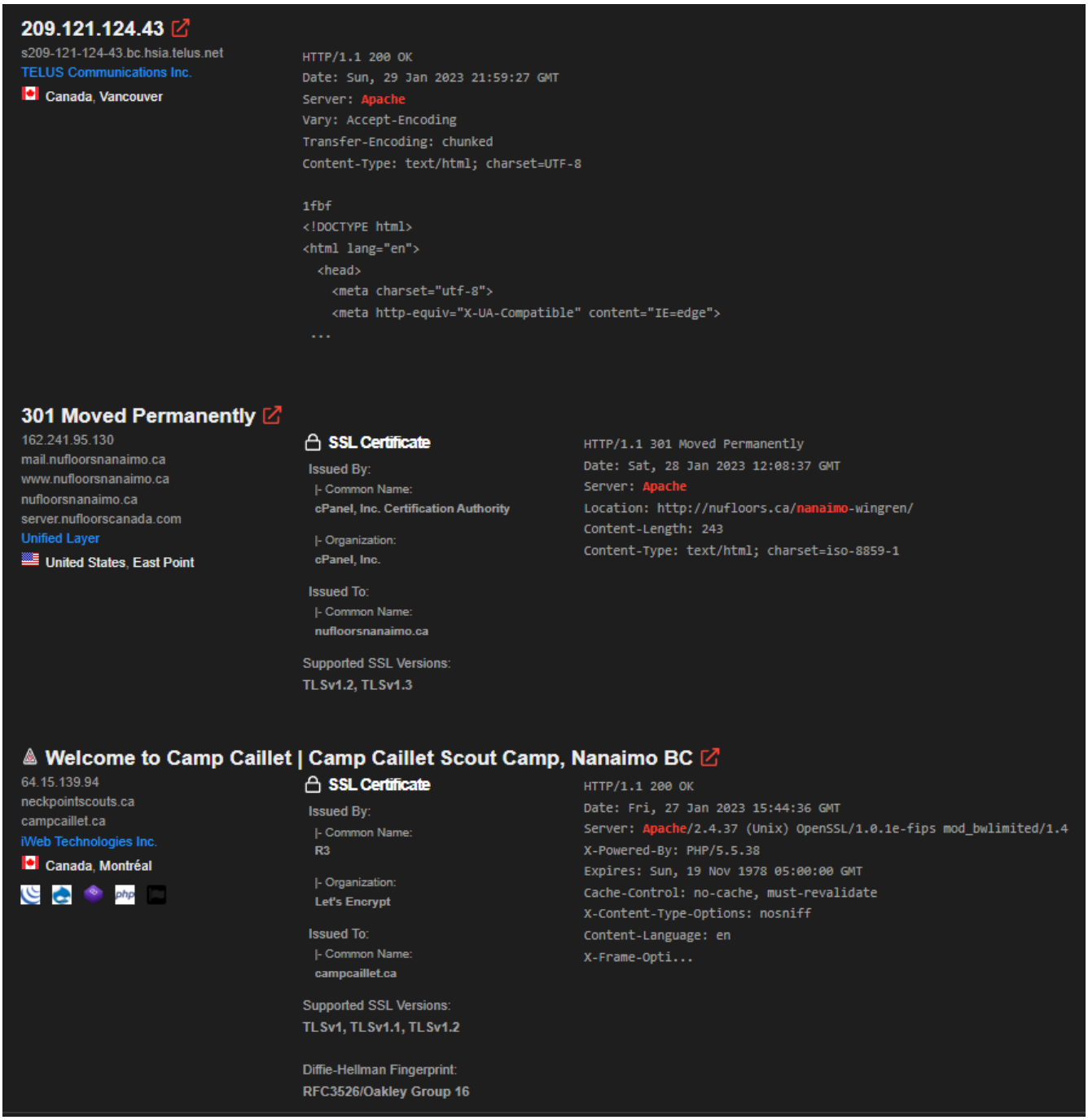

Figure 12: Apache in Nanaimo Shodan Search Result

Camp Caillet Scout Camp's SSL cert expired over 600 days ago and defaults to http anyways. Unless this website is a cover for undercover agents to submit reports it's not a very interesting target.

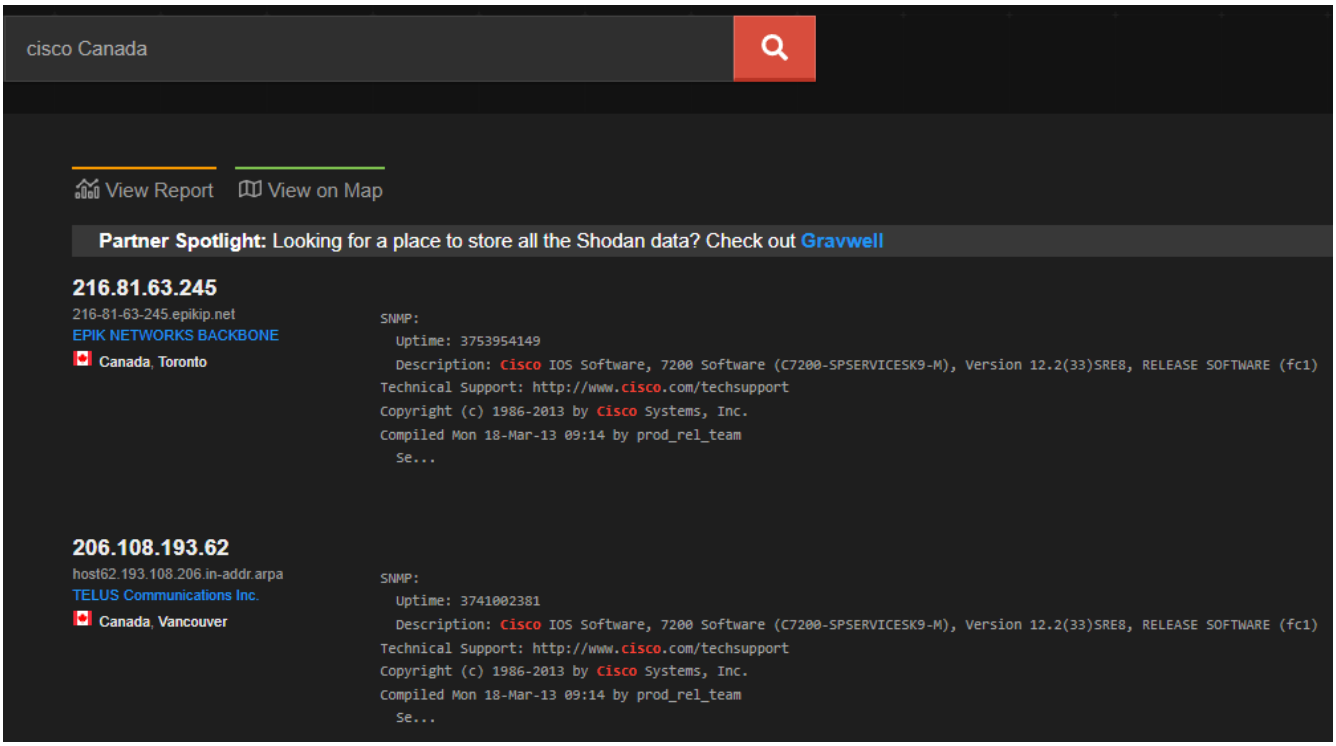

Figure 13: Cisco Canada Shodan Search Result

Epik Networks' website is beanfield.com for some reason.

https://www.cisco.com/c/en/us/td/docs/ios/12_2sr/release/notes/122SRcavs1.html#73700

lists the vulnerabilities associated with version 12.2(33)SRE8 but I'm not sure what to do with any of it.

Dork Scripts

Jackpot. Spearphish these cancer doctors to get the patient data and sell it on the black market. People are much more aware of not putting their email on web pages than they are of having their files exposed.

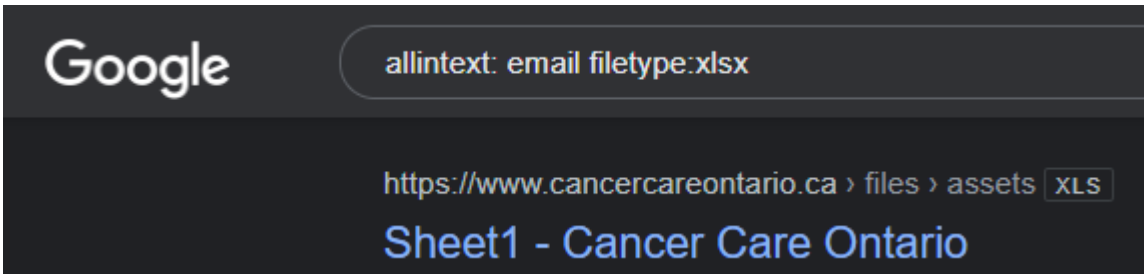

Figure 14: Search for Spreadsheets with the Content "Email"

theHarvester

Leaking emails is a thing of the past. A tool that can parse email at gmail dot com would be the bare minimum to get anything useful out of these types of queries anymore.

Figure 15: theHarvester

Part 4 - sudoers

As root, run the command visudo to edit the sudoers file.

Members of the sudo group by default have access to run any command as any user, including root.

%user1 ALL=(root:root) /usr/bin/ls,/usr/bin/apt-get

will restrict the users in the group user1 to only being able to run the ls and apt-get commands and only as the root user. This can prevent sneaky individuals trying to blame their bad behaviour on other users.

Restricting sudo privileges to certain commands will prevent sneaky things like running the passwd command as root as well.

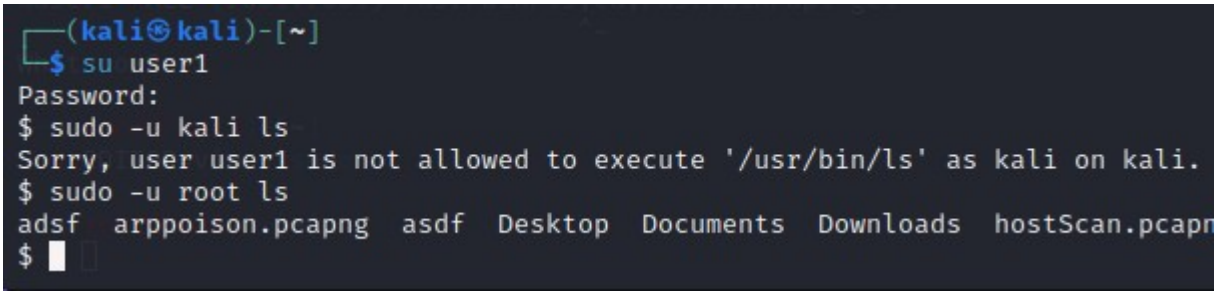

Figure 16: user1 Being Restricted from Using Accounts Other than Root

Inserting the line

Defaults timestamp_timeout=0

into the sudoers file will force you to enter your password every time you use the sudo command. This will prevent social engineering tactics like someone distracting you by getting you to come fix the coffee maker while an accomplice can run some nefarious commands while you are away.

Part 5 - fping

The below command will list all responses from the 172.16.102.0/24 subnet

fping -4qag 172.16.102.1 172.16.102.254

Flag explanations:

- 4 – Only IPv4 addresses
- q – Suppresses annoying Host Unreachable output
- a – Shows alive systems
- g – Scan a range of IPs

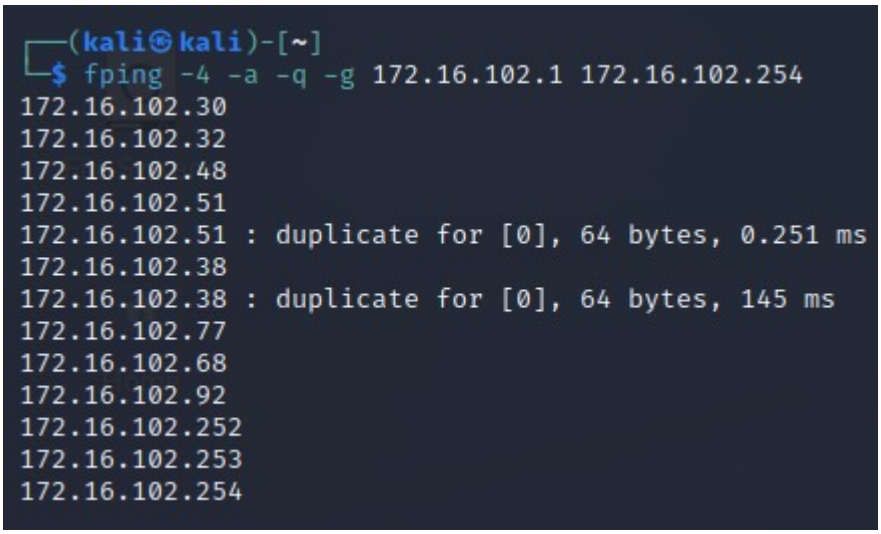

Figure 17: fping Results of Showing All Alive Hosts on Subnet

fping -4qag 172.16.102.1 172.16.102.100 will only ping the first 100 hosts in the subnet

fping -4qug 172.16.102.1 172.16.102.254 will list all of the unreachable hosts in the subnet

References

[1] “Command-line Flags”, Website. https://Nmap.org/book/port-scanning-options.html (accessed January 23, 2023).

[2] “Firewall/IDS Evasion and Spoofing”, Website. https://nmap.org/book/man-bypass-firewalls-ids.html (accessed January 23, 2023).

[3] “DNS Resolution”, Website. https://nmap.org/book/host-discovery-dns.html (accessed January 23, 2023).

[4] U.Y. “Nmap -Pn (No Ping) Option Analysis”, Website. https://informationsecurity.medium.com/nmap-pn-no-ping-option-analysis-d9aaa95be5b0 (accessed January 23, 2023).

[5] Dave McKay, "How to Control sudo Access on Linux", Website. https://www.howtogeek.com/447906/how-to-control-sudo-access-on-linux/ (accessed January 26, 2023).

[6] Sk, "How To Change Sudo Password Timeout In Linux", Website. https://ostechnix.com/how-to-change-sudo-password-timeout-in-linux/ (accessed January 26, 2023).

[7] “FPING”, Website. https://fping.org/fping.1.html (accessed January 24, 2023).

[8] "TCP SYN Port Scanner - Metasploit", Website. https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/scanner/portscan/syn (accessed January 26, 2023).

[9] "How to Hide Your Apache Version and Linux OS From HTTP Headers", Website. https://www.inmotionhosting.com/support/server/apache/hide-apache-version-and-linux-os/ (accessed January 29, 2023).

[10] "Theharvester", Website. https://www.kali.org/tools/theharvester/ (accessed January 29, 2023).