Lane Maitland

>>> 1: passive information gathering <<<

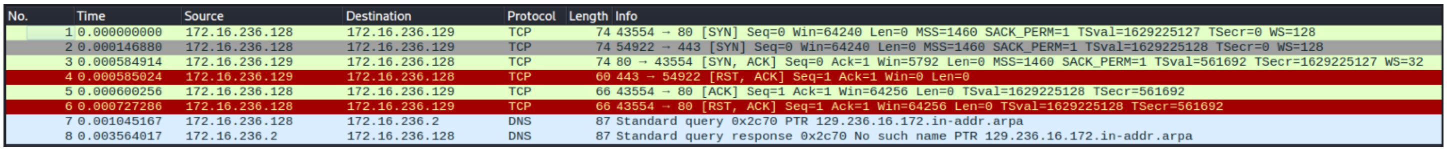
- domain: nationalgeographic.com
- IP address: 172.16.236.2
    - “non-authoritative answer”:
        - 52.22.200.24
        - 3.224.105.17
        - 18.213.238.129
- when registration expires: 2022-10-09T04:00:00Z
- what I learned about people responsible for domain:
    - “Registry Registrant”, “Registry Admin”, “Registry Tech” are the same
    - National Geographic is based in Washington DC
- what happened when I tried searching by IP address instead of by domain name:
    - got nothing about National Geographic
    - nslookup 172.16.236.2 →
        - ** server can't find 2.236.16.172.in-addr.arpa: NXDOMAIN
    - whois 172.16.236.2 →
        - got info about “Internet Assigned Numbers Authority”
    - also tested commands with “non-authoritative answer” IP addresses, but those did not return anything about National Geographic either
- what I do not understand:
    - what a registrar is
    - why Ascio is the registrar (and if there are others)
    - differences among “Registry Registrant”, “Registry Admin”, “Registry Tech” (they all have the same info in my case)
    - why there are 4 “Name Server”
    - why there are 4 IP addresses
    - what a “non-authoritative answer” is
    - why `nslookup` changes 172.16.236.2 to 2.236.16.172
    - implications of “VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability”
    - which domains are protected such that their info is not returned when searching by IP address
    - why registration expires
    - what happens when registration expires

>>> 2: host detection <<<

- kali IP address: 172.16.236.128
- what “-sn” does: disable port scan [https://nmap.org/book/man-briefoptions.html]
- what “/24” does: 24 refers to a number of bits, this scans every IP address for which the first 24 bits are the same as for the given IP address (172.16.236.128) [https://nmap.org/book/man-target-specification.html]
    - confirmed by `nmap` output → “256 IP addresses (4 hosts up) scanned in 2.43 seconds”

nmap -sn 172.16.236.128/24

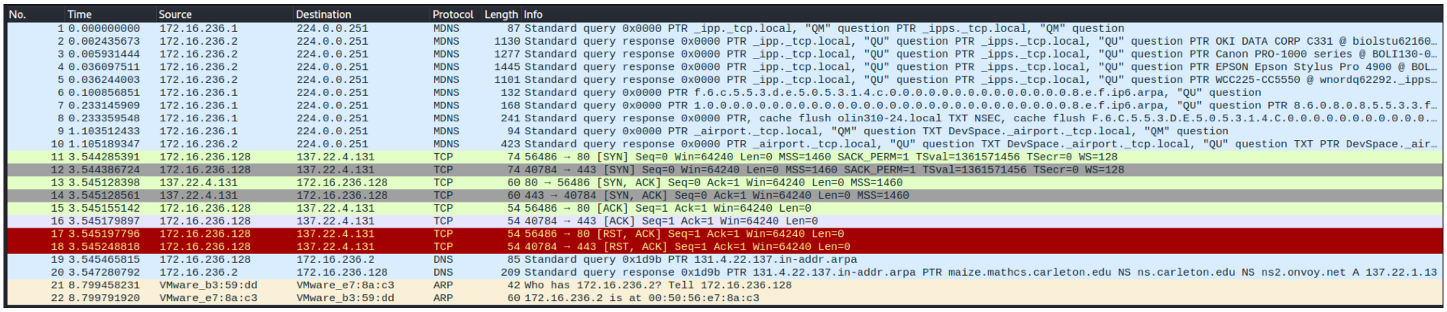
- IP addresses for active hosts (there were 4 out of 256)
    - 172.16.236.1
    - 172.16.236.2
    - 172.16.236.128
    - 172.16.236.129
- entities that IP addresses represent
    - I tried doing `nslookup` for each IP address, but nothing was returned
    - 172.16.236.128 is kali
- time: 2.43 seconds
- steps in wireshark
    - TCP handshake → frames 1,3,5
    - TCP [SYN] from different port of kali → frame 2
    - TCP [RST] → frames 4,6
        - [RST] refers to reset, terminates connection after packet is sent to closed port [https://isc.sans.edu/forums/diary/The+special+case+of+TCP+RST/26824/]
    - DNS query/response → frames 7,8
        - the query/response seems similar to those I sent/received when trying to get info on domain from IP address



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.236.128	172.16.236.129	TCP	74	43554 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1629225127 TSecr=0 WS=128
2	0.000146880	172.16.236.128	172.16.236.129	TCP	74	54922 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1629225128 TSecr=0 WS=128
3	0.000584914	172.16.236.129	172.16.236.128	TCP	74	80 → 43554 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=561692 TSecr=1629225127 WS=32
4	0.000585024	172.16.236.129	172.16.236.128	TCP	60	443 → 54922 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000600256	172.16.236.128	172.16.236.129	TCP	66	43554 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1629225128 TSecr=561692
6	0.000727286	172.16.236.128	172.16.236.129	TCP	66	43554 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1629225128 TSecr=561692
7	0.001045167	172.16.236.128	172.16.236.2	DNS	87	Standard query 0x2c70 PTR 129.236.16.172.in-addr.arpa
8	0.003564017	172.16.236.2	172.16.236.128	DNS	87	Standard query response 0x2c70 No such name PTR 129.236.16.172.in-addr.arpa

nmap -sn 137.22.4.0/24

- IP addresses for active hosts (there were 6 out of 256), with entities that they represent (if found)
    - 137.22.4.5 (elegit.mathcs.carleton.edu)
    - 137.22.4.17 (perlman.mathcs.carleton.edu)
    - 137.22.4.20
    - 137.22.4.22
    - 137.22.4.56 (olin310-24.mathcs.carleton.edu)
    - 137.22.4.131 (maize.mathcs.carleton.edu)
- time: 3.16 seconds
- steps in wireshark
    - MDNS queries/responses → frames 1-10
    - 2 TCP handshakes → frames 11-16
    - TCP [RST] → frames 17,18
    - DNS query/response → frames 19,20
    - ARP → frames 21,22
        - this looks like communication between two locations of the virtual machine
        - one location requests the domain of the IP address and informs the other location about where this information should be delivered, the other location responds



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.236.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipp._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question
2	0.002435673	172.16.236.2	224.0.0.251	MDNS	1130	Standard query response 0x0000 PTR _ipp._tcp.local, "QU" question PTR _ipps._tcp.local, "QU" question PTR OKI DATA CORP C331 @ biolstu62160…
3	0.005931444	172.16.236.2	224.0.0.251	MDNS	1277	Standard query response 0x0000 PTR _ipp._tcp.local, "QU" question PTR _ipps._tcp.local, "QU" question PTR Canon PRO-1000 series @ BOLI130-0…
4	0.036097511	172.16.236.2	224.0.0.251	MDNS	1445	Standard query response 0x0000 PTR _ipp._tcp.local, "QU" question PTR _ipps._tcp.local, "QU" question PTR EPSON Epson Stylus Pro 4900 @ BOL…
5	0.036244003	172.16.236.2	224.0.0.251	MDNS	1101	Standard query response 0x0000 PTR _ipp._tcp.local, "QU" question PTR _ipps._tcp.local, "QU" question PTR WCC225-CC5550 @ wnordq62292._ipps…
6	0.100856851	172.16.236.1	224.0.0.251	MDNS	132	Standard query 0x0000 PTR f.6.c.5.5.3.d.e.5.0.5.3.1.4.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "QU" question
7	0.233145909	172.16.236.1	224.0.0.251	MDNS	168	Standard query 0x0000 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "QU" question PTR 8.6.0.8.0.8.5.5.3.3.f…
8	0.233359548	172.16.236.1	224.0.0.251	MDNS	241	Standard query response 0x0000 PTR, cache flush olin310-24.local TXT NSEC, cache flush F.6.C.5.5.3.D.E.5.0.5.3.1.4.C.0.0.0.0.0.0.0.0.0.0.0.…
9	1.103512433	172.16.236.1	224.0.0.251	MDNS	94	Standard query 0x0000 PTR _airport._tcp.local, "QM" question TXT DevSpace._airport._tcp.local, "QM" question
10	1.105189347	172.16.236.2	224.0.0.251	MDNS	423	Standard query response 0x0000 PTR _airport._tcp.local, "QU" question TXT DevSpace._airport._tcp.local, "QU" question TXT PTR DevSpace._air…
11	3.544285391	172.16.236.128	137.22.4.131	TCP	74	56486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1361571456 TSecr=0 WS=128
12	3.544386724	172.16.236.128	137.22.4.131	TCP	74	40784 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1361571456 TSecr=0 WS=128
13	3.545128398	137.22.4.131	172.16.236.128	TCP	60	80 → 56486 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
14	3.545128561	137.22.4.131	172.16.236.128	TCP	60	443 → 40784 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	3.545155142	172.16.236.128	137.22.4.131	TCP	54	56486 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	3.545179897	172.16.236.128	137.22.4.131	TCP	54	40784 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	3.545197796	172.16.236.128	137.22.4.131	TCP	54	56486 → 80 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
18	3.545248818	172.16.236.128	137.22.4.131	TCP	54	40784 → 443 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
19	3.545465815	172.16.236.128	172.16.236.2	DNS	85	Standard query 0x1d9b PTR 131.4.22.137.in-addr.arpa
20	3.547280792	172.16.236.2	172.16.236.128	DNS	209	Standard query response 0x1d9b PTR 131.4.22.137.in-addr.arpa PTR maize.mathcs.carleton.edu NS ns.carleton.edu NS ns2.onvoy.net A 137.22.1.13
21	8.799458231	VMware_b3:59:dd	VMware_e7:8a:c3	ARP	42	Who has 172.16.236.2? Tell 172.16.236.128
22	8.799791920	VMware_e7:8a:c3	VMware_b3:59:dd	ARP	60	172.16.236.2 is at 00:50:56:e7:8a:c3

comparing wireshark output:

- each shows output from executing `nmap -sn [single IP address]`
- trial 1 IP address did not have associated domain name, trial 2 IP address did
- trial 2 had more steps/frames
- trial 2 included protocols not in trial 1 (MDNS, ARP), and one additional TCP handshake

what do not understand:

- MDNS: source/destination IP addresses, purpose
- ARP: source/destination (do not look like IP addresses)
- how info in ARP protocol gets to kali IP address

>>> 3: port scanning <<<

when I was working on this part of the assignment, I was on a different computer, and the kali IP address differed from that in part 2, so that is why the active hosts do not match those in part 2

- nmap 172.16.127.1 → 1 host, 1 open port

PORT	STATE	SERVICE
22/tcp	filtered	ssh

- nmap 172.16.127.2 → 1 host, 0 open ports
- nmap 172.16.127.128 → 1 host, 0 open ports
- nmap 172.16.127.129 → 1 host, 22 open ports

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
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

    - I confirmed that this was the metasploitable IP address

nmap -A 172.16.127.129

- databases: mysql, postgresql
- RSA SSH host key: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
    - purpose: authenticate computers [https://www.ssh.com/academy/ssh/host-key#:~:text=A%20host%20key%20is%20a,are%20stored%20on%20SSH%20servers]
- exploring: port 25 (smtp)
    - simple mail transfer protocol
    - purpose: send/receive email through network (but primarily send, can be paired with other protocols that receive) [https://www.extrahop.com/resources/protocols/smtp/]