Opdracht Sniffing

Ik analyseer teamviewer verkeer. Ik doe dit met wireshark.

Mijn IP adres op blechly: 10.150.220.250

Als ik naar de dump kijk zie ik veel communicatie met het ip adres 34.218.151.131.

- DNS-verkeer:

Het DNS-verkeer in de sniff toont DNS-query's voor het domein "sync-v2.brave.com". De pc probeert het ip adres van de deomein op te lossen om verbinding te maken met servers. Maar meer interssant is misschien de DNS dievan teamviewer is.

56	19.765323	10.150.187.95	10.150.220.250	DNS	82	Standard query 0xd3f7 A account.teamviewer.com
57	19.765498	10.150.187.95	10.150.220.250	DNS	82	Standard query 0xafb5 HTTPS account.teamviewer.com

En wanneer ik met mijn google account wou inloggen

104	20.014500	10.150.187.95	40.69.1.232	TCP	54	27932 → 443 [ACK] Seq=1930 Ack=6809 Win=130304 Len=0
105	20.097463	10.150.187.95	10.150.220.250	DNS	79	Standard query 0xb130 A accounts.google.com
106	20.097670	10.150.187.95	10.150.220.250	DNS	79	Standard query 0xed08 HTTPS accounts.google.com
107	20.105957	10.150.220.250	10.150.187.95	DNS	95	Standard query response 0xb130 A accounts.google.com A 142.250.27.84
108	20.106328	10.150.220.250	10.150.187.95	DNS	129	Standard query response 0xed08 HTTPS accounts.google.com SOA ns1.google.com

TLSv1.2 Verkeer:

Er is TLSv1.2-verkeer tussen de computer (10.150.187.95) en een externe server (34.218.151.131) op poort 443. Dit betekent een versleutelde connectie, hoog waarschijnlijk HTTPS. Dit is vermoedelijk de teamviewer server.

1	0.000000	10.150.187.95	52.111.243.13	TLSv1.2	82	Application Data
2	0.030045	52.111.243.13	10.150.187.95	TCP	60	443 → 27005 [ACK] Seq=1 Ack=29 Win=16385 Len=0
3	0.093750	10.150.187.95	52.111.243.13	TLSv1.2	82	Application Data
4	0.129905	52.111.243.13	10.150.187.95	TCP	60	443 → 27007 [ACK] Seq=1 Ack=29 Win=16386 Len=0

TCP-verkeer:

Er zijn verschillend TCP verbindingen met servers op poort 433. Dit betekent activiteiten zoals verbinden met HTTPS websites

12	0.823930	34.218.151.131	10.150.187.95	TCP	60	443 → 24567 [ACK] Seq=1 Ack=113 Win=771 Len=0
13	0.824508	34.218.151.131	10.150.187.95	TCP	60	443 → 24567 [ACK] Seq=1 Ack=159 Win=771 Len=0
14	0.824508	34.218.151.131	10.150.187.95	TCP	60	443 → 24567 [ACK] Seq=1 Ack=551 Win=771 Len=0

ARP-verkeer:

Er is ARP verkeer waar de pc vraagt naar het mac adres van het ip adres 10.150.220.250 en het ontvangt van eergens anders. Dit is normaal voor ARP om het krijgen van een hardware adres van een bepaalde ip adres in het local network

32	5.265589	ae:93:f3:31:38:e7	VMware_88:de:03	ARP	42	Who has 10.150.220.250? Tell 10.150.187.95
33	5.287353	VMware_88:de:03	ae:93:f3:31:38:e7	ARP	60	10.150.220.250 is at 00:50:56:88:de:03

Overige Activiteiten:

Er zijn een paar TCP SYN packets, met externe ip address. Dat geeft aan dat de pc probeert verbinding te maken met andere servers op spefieke poorten. Er zijn ook een maar retransmissies wat kan aanduiden dat er problemen zijn met connectivieit op latentie

Opdracht NMAP

Geen SSL: https://10.150.0.1:3000/lua/login.lua?referer=10.150.0.1%3A3000%2F Pharaos service

Geen SSL: https://10.150.0.1:4443/ Pfsense firewall

Host 1: 10.150.0.1

Status: Actief.

Open Poorten:

22/tcp (OpenSSH 9.3)

53/tcp (tcpwrapped)

3000/tcp (Mongoose httpd)

4443/tcp (nginx)

Service Details:

Poort 3000/tcp: Mongoose httpd, ntopng 5.6.230701 (amd64)

Poort 4443/tcp: nginx, pfSense - Aanmelden

SSL-certificaatinformatie:

Algemene naam: newfw.bletchley.cloud

Uitgever: Let's Encrypt Geldigheid:

Van 15-11-2023 tot 13-02-2024 geldig

Host 2: 10.150.0.253

Status: Actief

Gefilterde Poorten: Alle 1000 gescande poorten bevinden zich in ignore toestand, 987 g efilterde tcp-poorten (no respons), en 13 gefilterde tcp-poorten (host-connected).

Algemene Informatie MAC-adressen:

Beide hosts hebben Hewlett Packard (HP) MAC-adressen.

Apparaattype: General purpose

Besturingssysteem (Guessed): FreeBSD 11.2

Aanvullende Informatie:

Traceroute: Beide hosts zijn 1 hop afstand van de scan machine.

Netwerkafstand: 1 hop.

Moeilijkheid van TCP Sequencing: 262

Analyse:

Host 1 lijkt een server te zijn die verschillende services draait, SSH, DNS, een HTTP-server met ntopng, en een HTTPS-server met pfSense.

Host 2 heeft alle 1000 poorten in ingnore toestand, wat tooont dat ze mogelijk gefilterd of verboden zijn.