

Esercitazione W19D4

Threat intelligence & IOC

Fabio Benevento - 15/03/2024

Traccia

Analizzate la cattura fornita attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Implementazione


Analizzando la cattura con Wireshark è possibile individuare una serie di richieste TCP a distanza ravvicinata provenienti dalla macchina 192.168.200.100 verso la macchina 192.168.200.150 con porta di destinazione sempre diversa.

The image shows a Wireshark packet capture titled "Cattura_U3_W1_L3.pcapng". The packet list on the left shows a series of TCP packets. The packet details pane on the right shows the structure of a TCP packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane at the bottom shows the raw data of the selected packet, which is a TCP RST packet with a sequence number of 665566 and a window size of 0.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	288	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764277789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.100	192.168.200.150	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777323	192.168.200.150	192.168.200.100	TCP	60	443 → 80 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
6	23.764815189	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_39:7d:7e	PcsCompu_39:7d:7e	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644819	PcsCompu_39:7d:7e	PcsCompu_39:7d:7e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:7e
10	28.774852257	PcsCompu_39:7d:7e	PcsCompu_39:7d:7e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230899	PcsCompu_39:7d:7e	PcsCompu_39:7d:7e	ARP	60	192.168.200.150 is at 08:00:27:39:7d:7e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685505	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775111104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775360294	192.168.200.100	192.168.200.150	TCP	74	59596 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796338	192.168.200.150	192.168.200.100	TCP	74	22 → 59596 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861064	192.168.200.150	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
> Ethernet II, Src: PcsCompu_39:7d:7e (08:00:27:39:7d:7e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255
> User Datagram Protocol, Src Port: 135, Dst Port: 138
> NetBIOS Datagram Service
> SMB (Server Message Block Protocol)
> SMB Mailslot Protocol
> Microsoft Windows Browser Protocol

0000 ff ff ff ff ff ff 00 00 27 fd 87 1e 00 00 45 00E
0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8@&.....
0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8K-u....
0030 c8 96 00 8a 00 e0 00 20 45 4e 45 46 46 45 45EHEEEE
0040 42 46 44 46 41 45 6d 45 50 45 4a 46 45 42 45BFDAENE PEJEEB
0050 43 45 4d 46 43 41 41 41 00 20 46 48 45 50 46CEMEFCAA A-FHEP
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43CELEHCFCE PFFACAC
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42ACACACAC ABN-SMB
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00%.....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00L



Ciò fa supporre che siamo in presenza di una scansione di tipo TCP da parte di un attaccante con strumenti tipo nmap volta ad individuare le porte aperte sulla macchina target.

In caso di porta aperta il target risponde con SYN+ACK (righe 35, 36 ad es.) mentre nel caso di porta chiusa la risposta è di tipo RST+ACK (righe 21, 22 e 23 ad es.).

Per ridurre gli impatti di un possibile attacco è consigliabile l'utilizzo di un firewall opportunamente configurato al fine di limitare l'accesso alla macchina solo a determinati IP sulla rete interna e/o a determinate porte.