

Cattura_U3_W1_L5.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	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	23.764287789	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	192.168.200.150	192.168.200.100	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	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	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	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:1e	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:1e	PCSSystemtec_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:1e
10	28.774852257	PCSSystemtec_39:7d:1e	PCSSystemtec_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775211999	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:1e	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.775141273	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
13	36.775141273	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
14	36.775141273	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 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	36.774405627	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	36.774405627	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	36.775141273	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	36.774685652	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 → 33876 [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	36.775141273	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	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	36.775141273	192.168.200.150	192.168.200.100	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
29	36.775337000	192.168.200.150	192.168.200.100	TCP	74	59174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 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	36.775589806	192.168.200.150	192.168.200.100	TCP	66	56120 → 111 [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	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775796938	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	36.775863786	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

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), 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: 138, 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 08 00

27 fd 87 1e 08 00 45 00

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 a8

0030

c8 96 00 8a 00 e6 00 00

20 45 4e 45 46 46 45 45

0040

42 46 44 46 41 45 4d 45

50 45 4a 46 45 45 42 45

0050

43 45 4d 45 46 43 41 41

41 00 20 46 48 45 50 46

0060

43 45 4c 45 48 46 43 45

50 46 46 46 41 43 41 43

0070

41 43 41 43 41 43 41 43

41 42 4e 00 ff 53 4d 42

0080

25 00 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 11 00 00 4c

00a0

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00b0

00 00 00 4c 00 56 00 03

00 01 00 01 00 02 00 5d

00c0

00 5c 4d 41 49 4c 53 4c

4f 54 5c 42 52 4f 57 53

00d0

45 00 01 01 c0 d4 01 00

4d 45 54 41 52 50 4e 4f

00e0

49 54 41 42 4c 45 00 00

04 09 03 9a 00 00 00 00

00f0

55 aa 00 05 74 61 73 70

6c 6f 69 72 00 00 00 00

0100

20 73 05 72 76 05 72 20

28 53 61 60 00 00 00 00

0110

2e 30 2e 32 30 2d 44 05

62 69 61 6e 29 00 00 00

Made with Gamma

Threat Intelligence & IOC: Analisi di una Cattura di Rete

Nell'esercitazione di oggi analizzeremo una cattura di rete effettuata con Wireshark, concentrandoci sull'identificazione e analisi degli Indicatori di Compromissione (IOC) che evidenziano potenziali attacchi in corso.

Esamineremo attentamente i dati per formulare ipotesi sui vettori di attacco utilizzati e proporremo azioni concrete per mitigare l'impatto dell'attacco attuale e prevenire simili minacce in futuro.

tcp.flags.syn == 1 and tcp.flags.ack == 1									
No.	Time	Source	Destination	Protocol	Length	Info			
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64	
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	36.774685652	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	
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	
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656	[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	
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64	
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64	
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64	

Identificazione degli IOC: Scansione delle Porte



Pattern di Scansione

Numerosi pacchetti TCP con flag [SYN] inviati da 192.168.200.100 verso 192.168.200.150 su varie porte (80, 443, 23, 21, ecc.), seguiti da risposte [SYN, ACK] o [RST, ACK].



Comportamento Tipico

Questo comportamento è caratteristico di una scansione delle porte, dove un potenziale attaccante cerca di identificare servizi attivi sul sistema bersaglio.



IOC Rilevato

Elevato numero di tentativi [SYN] su porte diverse in un breve intervallo di tempo, indicativo di un'attività di reconnaissance.

Analisi delle Risposte del Sistema Target

Risposte [RST, ACK]

Molte porte rispondono con [RST, ACK], indicando che il servizio non è attivo o che la macchina target rifiuta la connessione.

L'alto volume di tali risposte conferma che il sistema è sotto scansione attiva, fornendo all'attaccante informazioni sulle porte chiuse.

Connessioni Riuscite

Alcune porte rispondono con [SYN, ACK] seguite da [ACK], completando il Three-Way Handshake. Queste connessioni riuscite (es. porta 80, 23, 22) indicano servizi attivi.

Questo rappresenta un IOC significativo, poiché l'attaccante potrebbe sfruttare questi servizi aperti per ulteriori attacchi.


```
8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 192.168.200.150 is at 08:00:27:fd:87:1e
```

Traffico ARP e Mappatura della Rete

Risoluzione degli Indirizzi

I pacchetti ARP (8-11) mostrano una risoluzione degli indirizzi IP 192.168.200.100 e 192.168.200.150 con i rispettivi MAC address (08:00:27:39:7d:fe e 08:00:27:fd:87:1e).

Comportamento Normale ma Sospetto

Questo è un comportamento normale in una rete locale, ma in combinazione con la scansione delle porte, indica che l'attaccante sta mappando la rete per identificare dispositivi attivi.

Fase di Reconnaissance

La combinazione di traffico ARP e scansione delle porte suggerisce una fase di reconnaissance strutturata, dove l'attaccante sta costruendo una mappa completa della rete target.

Ipotesi sui Vettori di Attacco



Scansione delle Porte

192.168.200.100 sta inviando un elevato numero di pacchetti TCP con flag [SYN] verso 192.168.200.150, su numerose porte in poco tempo.



Mappatura dei Servizi

L'obiettivo è identificare quali porte sono aperte e ospitano servizi in ascolto, come confermato dalle risposte [SYN, ACK] ricevute su porte comuni.



Preparazione all'Attacco

Questa attività di reconnaissance è probabilmente il preludio a un attacco più mirato, dove l'aggressore sfrutterà le vulnerabilità dei servizi identificati.



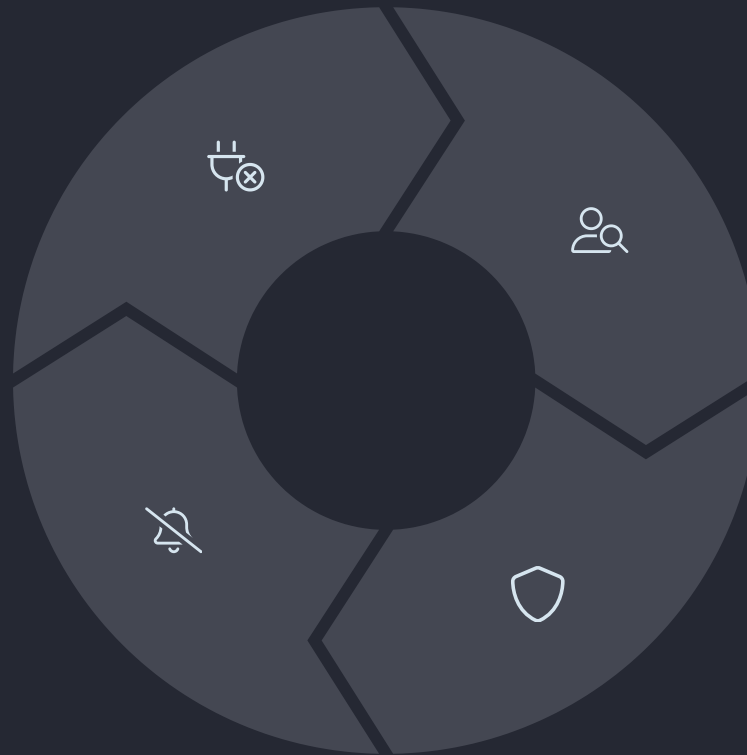
Azioni per Mitigare l'Attacco Attuale

Isolamento del Dispositivo

Scollegare 192.168.200.100 dalla rete per contenere l'attività malevola

Implementazione IDS

Installare un sistema di rilevamento delle intrusioni per monitorare il traffico



Verifica dei Log

Analizzare i log di 192.168.200.150 per identificare tentativi di accesso o anomalie

Modifica Firewall

Configurare il firewall per bloccare tentativi di scansione delle porte

Prevenzione di Attacchi Futuri



Conclusioni



Reconnaissance Identificata

La cattura di rete evidenzia un sistema (192.168.200.150, "METASPLOITABLE") sottoposto a una scansione delle porte



Azioni Immediate

Modificare le regole firewall e isolare il dispositivo sospetto



Misure Preventive

Implementare restrizione delle porte e monitoraggio continuo

L'analisi condotta ha permesso di identificare chiaramente un'attività di reconnaissance attraverso la scansione delle porte. Le azioni immediate e le misure preventive proposte sono fondamentali per mitigare l'attuale minaccia e proteggere la rete da future attività simili, garantendo un ambiente più sicuro e resiliente.