Rapporto

● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

Indirizzo IP dell'attaccante: 192.168.200.100

IP di destinazione: 192.168.200.150

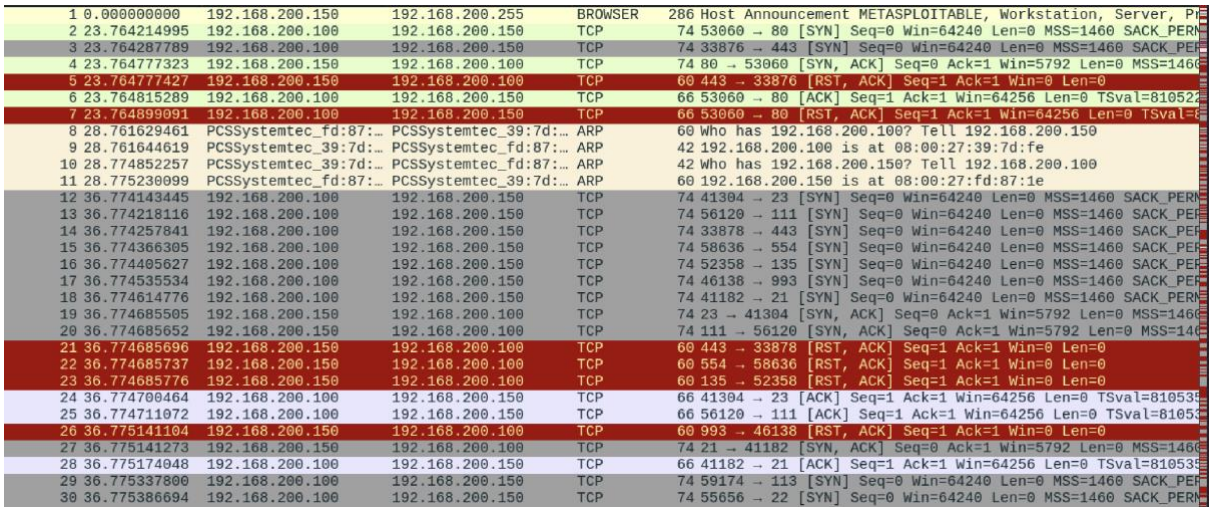
Porte di interesse: 1-1024

Flag osservati: SYN, ACK, RST

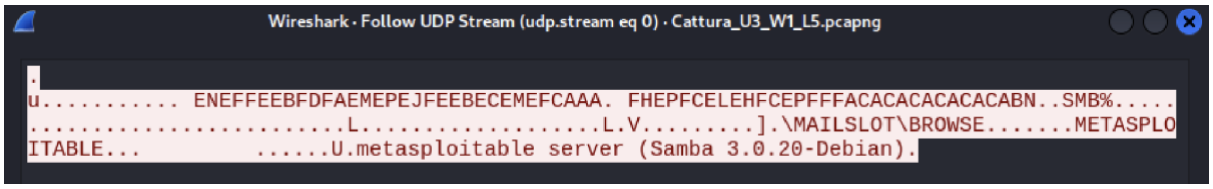
Protocolli utilizzati: TCP, ARP, UDP

Strumenti possibili: Nmap, Masscan o script personalizzati.

● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati



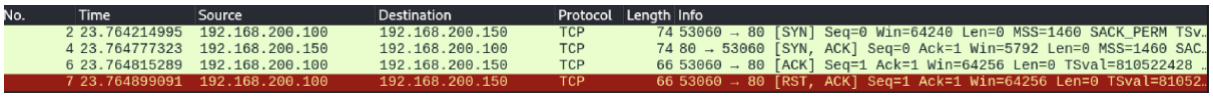
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPLOITABLE, Workstation, Server, Pr
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
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=146
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=810522
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=8
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
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
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_PER
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_PER
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_PER
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_PER
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_PER
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
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=146
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=146
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=810535
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=81053
26	36.775141104	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=146
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=810535
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_PER
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



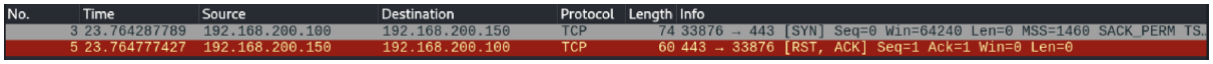
Quando osserviamo le prime catture, possiamo vedere che la prima è UDP. Dopo essere entrati nel flusso UDP, possiamo vedere che questa

sessione è aperta sul server Metasploitable ed esegue il NetBios Name Service. Invia il traffico all'indirizzo di broadcast per scoprire le risorse sulla stessa subnet.

Quindi vediamo che ci sono diversi protocolli TCP utilizzati specificamente per la porta 80 e 443. Possiamo vedere che la porta 80 risponde con una connessione http riuscita, tuttavia il servizio https sulla porta 443 viene immediatamente terminato, il che significa che la porta 443 è chiusa o impedita da un firewall o IDS/IPS:



No.	Time	Source	Destination	Protocol	Length	Info
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 TSv…
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 SAC…
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 …
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=81052…



No.	Time	Source	Destination	Protocol	Length	Info
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 TS…
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

Quindi possiamo vedere che sono utilizzati protocolli ARP. Se questo non fa parte della comunicazione di routine, potrebbe significare che è un segno di spoofing ARP.

Nel resto delle catture, osserviamo che c'è traffico catturato con handshake TCP. Ci sono principalmente due condizioni:

1) L'attaccante tenta di avviare una connessione al server utilizzando porte diverse con un SYN. Il server vittima risponde con un SYN, ACK che riconosce la richiesta. Quindi l'attaccante invia un ACK, completando l'handshake e aprendo la connessione. Alla fine la vittima invia un RST, ACK per ripristinare o chiudere la connessione.

2) L'attaccante tenta di avviare una connessione al server utilizzando porte diverse con un SYN. La vittima invia un RST, ACK per ripristinare o chiudere la connessione.

Il primo caso significa che è stato utilizzato un handshake completo da TCP e la porta è aperta. D'altro canto, il secondo caso significa che la connessione viene terminata direttamente perché la porta è chiusa o perché il firewall di IDS/IPS e così via.

In base a ciò, quando guardiamo le catture, possiamo notare che diverse connessioni hanno utilizzato l'handshake completo, il che significa che le porte sono aperte. Sono le porte 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.

Tutte le altre catture si riferiscono al secondo caso - le porte sono chiuse.

In sintesi, l'attaccante (192.168.200.100) ha molto probabilmente eseguito una scansione nmap sulla macchina Metasploitable utilizzando uno dei seguenti comandi:

nmap -p 1-1024 192.168.200.150

nmap -sT -p 1-1024 192.168.200.150

● Consigliate un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un simile attacco future

1) **Chiudere porte inutilizzate**: Bloccare i porti non necessari tramite firewall e segmentare la rete.
2) **Rafforzare i servizi**: Configurare correttamente i servizi aperti (FTP, SSH, SMB, ecc.), disabilitare i protocolli non sicuri e usare connessioni criptate.
3) **Mitigare l'ARP Spoofing**: Utilizzare voci ARP statiche, IDS/IPS e **Dynamic ARP Inspection (DAI)** su switch gestiti.

4) **Rafforzare firewall e IDS/IPS**: Configurare il firewall per bloccare traffico non autorizzato e il sistema IDS/IPS per rilevare attività anomale.
5) **Monitoraggio continuo**: Implementare un sistema di monitoraggio per rilevare scansioni di porte e traffico sospetto.
6) **Autenticazione forte**: Utilizzare autenticazione basata su chiave per SSH e altre misure di autenticazione sicura per i servizi.
7) **Prevenire la scansione della rete**: Implementare tecniche come il **port knocking** e configurare il firewall per nascondere alcune porte.
8) **Applicare patch di sicurezza**: Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza.
9) **Mitigare attacchi DDoS**: Usare servizi di mitigazione DDoS o configurare meccanismi di limitazione del traffico.
10) **Audit di sicurezza regolari**: Condurre regolarmente valutazioni delle vulnerabilità e penetration test.