

Threat Intelligence & IOC

Traccia:

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.

Analizzate la cattura 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

Svolgimento:

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...
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=...
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:...	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 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	36.774541723	192.168.200.100	192.168.200.150	TCP	74	46132 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface e...						
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						
Command: Host Announcement (0x01)						
Update Count: 1						
Update Periodicity: 2 minutes						
Host Name: METASPLOITABLE						
Windows version:						

Identifico 192.168.200.150 come IP della macchina Metasploitable.

Dall'analisi del traffico deduco che vi è una comunicazione tra due macchine aventi come IP una 192.168.200.150 (macchina Metasploitable) e un'altra 192.168.200.100.

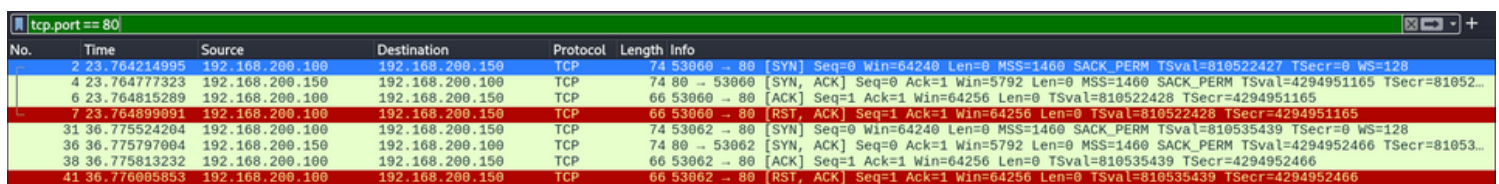
Si evidenzia un'attività di port scanning, un metodo comunemente usato per identificare le porte aperte e i servizi attivi su un computer in una rete. Questo tipo di attività è spesso associato a tentativi di rilevare vulnerabilità o configurazioni non sicure in sistemi di rete. Analizzando il caso specifico, si rileva che le richieste TCP provengono dalla macchina con IP 192.168.200.100 e sono dirette verso diverse porte dell'host con IP 192.168.200.150, noto come Metasploitable, una piattaforma spesso utilizzata per la formazione in ambito di sicurezza informatica a causa delle sue note vulnerabilità.

L'ipotesi che il tool utilizzato per lo scanning sia Nmap si basa sulla sua popolarità e versatilità nell'ambito della sicurezza informatica.

Nmap è un potente strumento open-source utilizzato per la discovery di rete e la sicurezza auditing. Una delle sue funzionalità chiave è proprio la capacità di effettuare scansioni di porte utilizzando vari metodi.

La scansione specifica in questione sembra essere un TCP Connect Scan, indicato dall'opzione -sT in Nmap. Questo tipo di scansione si avvale del completo three-way handshake, un processo fondamentale nel protocollo TCP, per stabilire una connessione. Il three-way handshake consiste in tre fasi: SYN (synchronize), SYN-ACK (synchronize-acknowledge), e ACK (acknowledge). Quando una porta è aperta, il target risponde con un SYN-ACK dopo aver ricevuto un SYN, e la scansione completa il processo inviando un ACK. Questo è diverso dal SYN Scan (opzione -sS in nmap), che non completa il three-way handshake e si limita a inviare un pacchetto RST (reset) dopo aver ricevuto il SYN-ACK, riducendo così la visibilità della scansione.

Prendo in considerazione la porta 80: in una scansione TCP Connect con Nmap (opzione -sT) lo scanner tenta di stabilire una connessione completa tramite il three-way handshake con il server web. Se la porta 80 è aperta il server web è attivo e accessibile. Questo tipo di scansione può fornire informazioni utili sull'esistenza e sulla configurazione del server web.

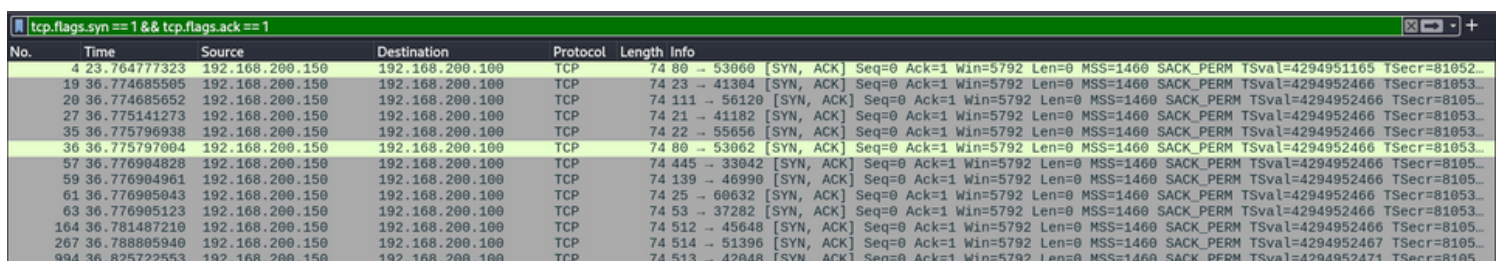


No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427
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	23.764899991	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
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
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
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
41	36.776095853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Procedo utilizzando un filtro su Wireshark per avere contezza delle porte aperte:

tcp.flags.syn == 1 && tcp.flags.ack == 1

Questo filtro seleziona tutti i pacchetti TCP in cui il flag SYN è impostato (cioè tcp.flags.syn == 1, indicando una richiesta di inizio connessione) e il flag ACK è impostato (cioè tcp.flags.ack == 1, indicando un riconoscimento).



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
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=810535439
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=810535439
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=810535439
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
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
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=810535439
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=810535439
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=810535439
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=810535439
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=810535439
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=810535439
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=810535439

In totale ci sono 12 porte aperte.

Consigli per ridurre gli impatti dell'attacco

Alla luce delle vulnerabilità esposte da una scansione delle porte, è fondamentale adottare misure preventive e di mitigazione per ridurre il rischio di attacchi. Ecco alcune raccomandazioni:

1. **Chiudere le Porte Critiche:** le porte come ftp (21), telnet (23), netbios (139), smb (445) e quelle per il remote login, se non sono essenziali, devono essere chiuse. Questo riduce la superficie di attacco disponibile. È importante notare che alcune di queste porte potrebbero essere utilizzate da servizi legittimi all'interno dell'organizzazione; pertanto, una valutazione approfondita è necessaria prima di chiuderle.
2. **Firewall e Accesso Limitato:** configurare policy di sicurezza sui firewall per limitare l'accesso ai servizi esposti è cruciale. Questo può includere l'abilitazione di regole che consentono l'accesso solo a specifici indirizzi IP autorizzati. È anche consigliabile impiegare tecniche come il filtraggio degli indirizzi MAC, quando possibile, per un ulteriore livello di sicurezza.
3. **Autenticazione Forte e Controllo Accessi:** dove i servizi sono necessari e devono rimanere aperti, assicurarsi che vi siano misure di autenticazione forte e controllo degli accessi. L'uso di password complesse, l'autenticazione a più fattori (MFA) e certificati digitali può notevolmente aumentare la sicurezza.
4. **Aggiornamenti e Patch di Sicurezza:** mantenere aggiornati i sistemi e le applicazioni è fondamentale. Gli aggiornamenti spesso includono patch per vulnerabilità di sicurezza note che potrebbero essere sfruttate da un attaccante.
5. **Monitoraggio e Analisi del Traffico di Rete:** implementare soluzioni di monitoraggio del traffico di rete per identificare modelli di traffico insoliti o sospetti. Gli strumenti di rilevamento delle intrusioni (IDS) e i sistemi di prevenzione delle intrusioni (IPS) possono aiutare a identificare e bloccare attività potenzialmente dannose.
6. **Sicurezza a Livelli Multipli (Defense in Depth):** applicare un approccio di sicurezza a più livelli, dove diversi strati di sicurezza lavorano insieme per proteggere gli asset. Questo può includere, oltre ai firewall e al controllo degli accessi, la segregazione della rete, la cifratura dei dati e la formazione degli utenti sulla sicurezza informatica.
7. **Valutazioni Periodiche di Sicurezza:** effettuare regolari valutazioni di sicurezza e penetration test per identificare e mitigare le vulnerabilità prima che possano essere sfruttate.