

Threat Intelligence e Indicatori di Compromissione

In questo esercizio ho analizzato un file con estensione **.pcapng** utilizzando il programma **Wireshark**, con l'obiettivo di individuare eventuali **attività sospette nella rete** che possano indicare un attacco informatico in corso o già avvenuto. L'attività prevedeva i seguenti passaggi:

- **identificare gli Indicatori di Compromissione (IOC),**
- **ipotizzare il tipo di attacco**
- **proporre possibili soluzioni per proteggere la rete in futuro.**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	208	Host Announcement 'METASPLOITABLE', Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential
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	23.764217000	192.168.200.100	192.168.200.150	TCP	74	53076 -> 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	23.764815200	192.168.200.150	192.168.200.100	TCP	60	53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899093	192.168.200.100	192.168.200.150	TCP	60	53060 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629403	PCSSystemtec.f0:87::	PCSSystemtec.39:7d::	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644613	PCSSystemtec.39:7d::	PCSSystemtec.f0:87::	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec.39:7d::	PCSSystemtec.f0:87::	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec.f0:87::	PCSSystemtec.39:7d::	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774434446	192.168.200.100	192.168.200.150	TCP	74	43084 -> 22 [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	33876 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774360305	192.168.200.100	192.168.200.150	TCP	74	50636 -> 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 -> 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685502	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	36.774685500	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 -> 50636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685770	192.168.200.150	192.168.200.100	TCP	60	135 -> 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700454	192.168.200.100	192.168.200.150	TCP	60	41384 -> 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	60	56120 -> 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775411104	192.168.200.150	192.168.200.100	TCP	60	993 -> 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775415123	192.168.200.100	192.168.200.150	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	60	41182 -> 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775378080	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	36.775386934	192.168.200.100	192.168.200.150	TCP	74	55056 -> 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	36.775688806	192.168.200.150	192.168.200.100	TCP	60	113 -> 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775918454	192.168.200.100	192.168.200.150	TCP	60	41384 -> 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775952497	192.168.200.100	192.168.200.150	TCP	60	56120 -> 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775969536	192.168.200.150	192.168.200.100	TCP	74	22 -> 55056 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=4294952466
36	36.775979804	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	60	55056 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775613232	192.168.200.100	192.168.200.150	TCP	60	53062 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775983104	192.168.200.100	192.168.200.150	TCP	60	113 -> 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	60	55056 -> 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776065952	192.168.200.100	192.168.200.150	TCP	60	53062 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Indicatori di Compromissione (IOC)

Dall'analisi del traffico di rete ho notato un comportamento anomalo da parte dell'indirizzo IP **192.168.200.100**, che tenta di stabilire connessioni con l'host target **192.168.200.150**. Le connessioni avvengono su numerose porte diverse, tra cui per esempio:

- **22 (SSH)**
- **80 (HTTP)**
- **443 (HTTPS)**
- **445 (SMB)**

La maggior parte di queste connessioni viene **rifiutata**, come si può osservare dalla presenza di pacchetti TCP con flag **RST, ACK**, che indicano una chiusura forzata della comunicazione. Questo comportamento mi fa pensare ad una **scansione delle porte**.

Un altro elemento che ho notato si trova all'inizio della cattura, dove appare un pacchetto **BROWSER** contenente il termine **"Metasploitable"**. In questo caso, però, penso si tratti

semplicemente di un **messaggio di annuncio sulla rete** del protocollo NETBIOS, che serve per comunicare la presenza di un host.

Ipotesi sul tipo di attacco

Le informazioni raccolte indicano che l'indirizzo IP **192.168.200.100** sta probabilmente effettuando una **ricognizione della rete**, cioè uno **scanning**, che corrisponde alla fase iniziale di molti attacchi informatici, durante la quale l'attaccante cerca di identificare i dispositivi attivi e i servizi in ascolto, per poi sfruttare eventuali vulnerabilità.

È possibile che sia stato utilizzato **Nmap**, oppure il framework **Metasploit**.

Qualora l'attaccante riesca a sfruttare una vulnerabilità presente su una delle porte aperte, è possibile che tenti di **ottenere accesso remoto alla macchina** attraverso una **shell** (ad esempio una reverse shell). Successivamente, potrebbe anche **installare una backdoor** per garantirsi un accesso stabile e continuativo nel tempo.

Come difendersi e ridurre il rischio

Per prevenire o bloccare attacchi di questo tipo è importante adottare le seguenti misure:

- **Bloccare l'indirizzo IP sospetto** (192.168.200.100) tramite le regole del firewall.
- **Segnalare l'attività sospetta** agli amministratori di sistema o al team responsabile della sicurezza informatica.
- **Isolare il dispositivo** per evitare la diffusione dell'attacco.
- **Chiudere tutte le porte non necessarie** nei dispositivi della rete, riducendo i punti di accesso.
- **Segmentare la rete**, creando zone separate (ad esempio con VLAN).
- **Aggiornare regolarmente i software e i sistemi operativi**, così da correggere eventuali vulnerabilità note.
- **Utilizzare sistemi IDS/IPS (Intrusion Detection/Prevention Systems)**, in grado di riconoscere automaticamente comportamenti sospetti e intervenire in tempo reale.