Threat Intelligence & IOC

Attraverso il pacchetto n. 1 veniamo a conoscenza che l'indirizzo IP 192.168.200.150 identifica un server presente in rete. [1]

1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPLOITABLE,

```
▾ NetBIOS Datagram Service
    Message Type: Direct_group datagram (17)
  › Flags: 0x0a, This is first fragment, Node Type: M node
    Datagram ID: 0x75b4
    Source IP: 192.168.200.150
    Source Port: 138
    Datagram length: 230 bytes
    Packet offset: 0 bytes
    Source name: METASPLOITABLE<00> (Workstation/Redirector)
    Destination name: WORKGROUP<1d> (Local Master Browser)
```

Dai pacchetti nn. 2, 4 e 6 notiamo che è avvenuto un three-way handshake tra il client 192.168.200.100 e il server 192.168.200.150 sulla porta 80 ma con il pacchetto n. 7 la connessione termina.

2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=
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 TS
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len

Fin qui la cattura non evidenzia nulla di anomalo ma analizzando i successivi pacchetti notiamo molteplici richieste di connessione dal client 192.168.200.100 al server 192.168.200.150 sul range di porte 0 - 1024.
Tale comportamento potrebbe essere riconducibile a una scansione delle porte sul server 192.168.200.150 utilizzando ad esempio il tool *nmap*.
Il passaggio successivo è quello di individuare il soggetto che sta mettendo in atto tale attività. Dallo sniffing notiamo che le richieste provengono da un client presente nella stessa rete pertanto ci assicuriamo quale macchina stia producendo il traffico analizzato. Una volta individuata, possiamo capire se si tratta di un client che si è introdotto senza autorizzazione in rete oppure se l'attaccante sta sfruttando una macchina legittimamente presente in rete.
Al fine di risolvere quanto scoperto dobbiamo prima capire a quale casistica ci troviamo davanti, per esempio nel caso in cui dovessimo trovarci davanti ad una macchina compromessa dovremmo mettere in pratica tutte le procedure per comprendere attraverso quale vulnerabilità l'attaccante è riuscito a sfruttare un client locale per poter eseguire una scansione sul server così da poter conseguentemente sanare tale vulnerabilità.

[1] "A server […] sends a HostAnnouncement browser frame to advertise its presence and to specify the types of resources and services it supports" - https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-brws/10536677-8a14-4726-bc52-c0ef39cb7130