

Epicode
CS-0124
Pratica S9/L3
Francesco Ficetti

Traccia.....	3
Svolgimento.....	4

Traccia

Analizzare una cattura Wireshark e rispondere ai seguenti quesiti:

- Identificare gli IOC.
- In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliare un'azione per ridurre gli impatti dell'attacco.

Svolgimento

Analizzando questa cattura si nota subito che i soggetti della stessa sono due macchine:

1. 192.168.200.100 → la macchina che esegue le richieste;
2. 192.168.200.150 → la macchina che riceve le richieste.

Si presume che la macchina 1 stia eseguendo una scansione *nmap* sulla macchina 2. Lo si può notare dal fatto che ci sono moltissime richieste di connessione tramite protocollo TCP, tutte su porte diverse.

```
192.168.200.100 192.168.200.150 TCP 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
192.168.200.100 192.168.200.150 TCP 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
192.168.200.100 192.168.200.150 TCP 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
192.168.200.100 192.168.200.150 TCP 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.100 192.168.200.150 TCP 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.100 192.168.200.150 TCP 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.100 192.168.200.150 TCP 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
```

Molte di queste richieste vengono rifiutate subito.

```
192.168.200.150 192.168.200.100 TCP 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.150 192.168.200.100 TCP 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.150 192.168.200.100 TCP 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Alcune porte, invece, accettano la connessione in entrata. Essa però, viene interrotta subito dopo. Questo dimostra che non c'è un reale interesse ad effettuare una comunicazione, ma queste richieste vengono eseguite solo per verificare che le porte siano aperte.

Di seguito un esempio di quanto appena detto, filtro applicato sulla porta 21, tramite il comando *tcp.port == 21*.

```
192.168.200.100 192.168.200.150 TCP 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.150 192.168.200.100 TCP 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
192.168.200.100 192.168.200.150 TCP 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
192.168.200.100 192.168.200.150 TCP 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
```

Per ridurre gli impatti dell'attacco, si consiglia di bloccare, tramite un firewall, tutte le richieste provenienti dall'indirizzo IP della macchina 1.