IOC & THREAT INTELLIGENCE

In data odierna, il Sig. Rossi ci ha chiesto di verificare la sicurezza della rete verificando se sono presenti **Indicatori di compromissione** (IOC).

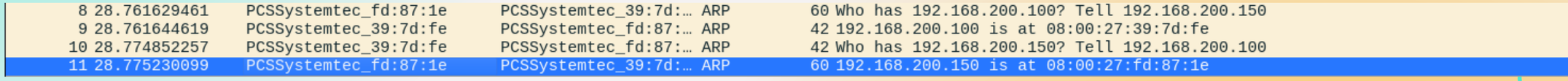
Decidiamo di effettuare subito una scansione di rete ed avviamo “**Wireshark**”.

Notiamo, intanto che tra la riga 1 e 4 abbiamo delle richieste TCP. Ci viene detto che la richiesta viene da una macchina di **Metasploitable**.

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 Workstation, NT Server,
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → http(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 → https(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	http(80) → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64

Sebbene la richiesta sia inusuale, non abbiamo ancora sufficienti informazioni su cosa stia avvenendo, poiché questo protocollo è utilizzato per molti scopi differenti.

Tra la riga 8 e 11 osserviamo la presenza di pacchetti ARP associati al dispositivo "PCSSystemtec" nel traffico di rete. Questi potrebbero indicare un potenziale attacco di tipo **Man-In-The-Middle** (MITM), specialmente se le richieste ARP non sono usuali o sospette. Gli attacchi MITM spesso sfruttano l'ARP spoofing per intercettare e reindirizzare il traffico di rete.



8	28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:…	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:…	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:…	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:…	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Questo tipo di richieste vengono effettuate dall’attaccante per associare all’indirizzo IP della vittima il corrispondente indirizzo MAC del dispositivo.

Nei casi peggiori possiamo sospettare che qualcuno voglia effettuare un **ARP Poisoning**.

arp spoofing

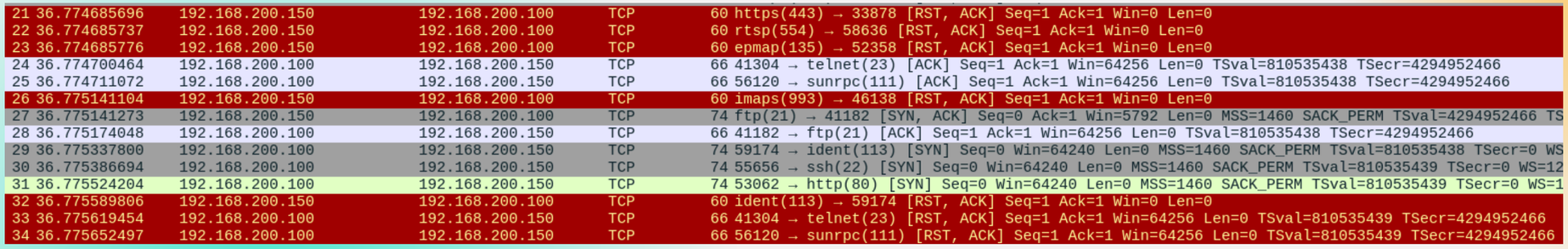
Cos'è?

Gli attacchi MITM che utilizzano ARP spoofing consistono nell'inviare risposte ARP falsificate per associare il proprio indirizzo MAC all'indirizzo IP di un altro dispositivo sulla rete. Questo permette all'attaccante di intercettare e manipolare il traffico tra due dispositivi legittimi.

Come difendersi?

Abilitare funzionalità di sicurezza come ARP inspection sui dispositivi di rete per prevenire l'ARP spoofing. Configurare static ARP entries per dispositivi critici, se possibile.

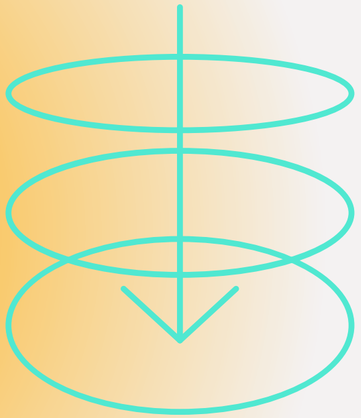
Un fattore molto importante è dato dalla presenza di molteplici richieste (quelle evidenziate in rosso) da parte dello stesso IP su servizi/porte differenti.
Le porte delle richieste evidenziate bloccano subito la richiesta tramite reset(RST).



21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 https(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 rtsp(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 epmap(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 → telnet(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	66 56120 → sunrpc(111) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 imaps(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 ftp(21) → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TS
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → ftp(21) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → ident(113) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → ssh(22) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=12
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=1
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 ident(113) → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → telnet(23) [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → sunrpc(111) [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Si può ipotizzare che qualcuno stia effettuando una scansione di rete con strumenti tipo **nmap**.

Un altro elemento molto interessante è dato dalla presenza di pacchetti **SYN ACK**(riga 27). questi tentano di sfruttare il processo “Three way handshake”, senza tuttavia concluderlo.



```
27 36.775141273    192.168.200.150          192.168.200.100      TCP        74 ftp(21) → 41182 [SYN, ACK]
```

SUGGERIMENTI

Continuare a monitorare l’Host “PCSSystemtec” e l’Host “192.168.200.150” ed eventualmente, bloccarli .

Creare delle sotto-reti divise per area di lavoro, in modo che l’attaccante non possa muoversi agilmente all’interno della rete aziendale.

Installare e configuare un firewall in modo da bloccare richieste sospette.

Cifrare, se non ancora fatto, i dati sensibili