Fiori Stefano

THREAT INTELLIGENCE

IOC

INTRODUZIONE

Grazie ad una cattura di Wireshark si è potuto evidenziare un elevato scambio di pacchetti tra due utenti, si è ritenuta necessaria un’analisi approfondita svolgendo tecniche di threat intelligence per evidenziare eventuali attacchi e prendere provvedimenti se necessario.

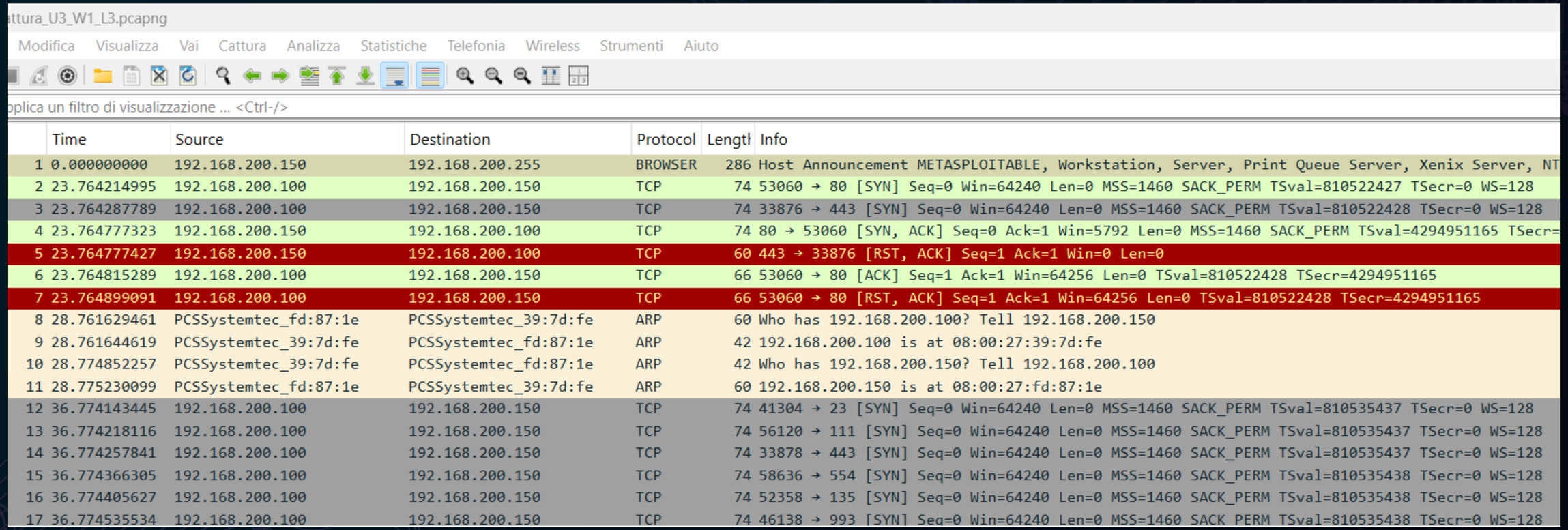
WIRESHARK

Wireshark è uno strumento di analisi del traffico di rete. È in grado di catturare e visualizzare: dati, pacchetti e protocolli che transitano su una rete in tempo reale.

THREAT INTELLIGENCE

Si tratta di un processo di raccolta, analisi e condivisione di informazioni relative a potenziali minacce informatiche. Ha l'obiettivo di prevenire, identificare e mitigare gli attacchi informatici.

CATTURA DI WIRESHARK



	Time	Source	Destination	Protocol	Lengtl	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:87:1e	PCSSystemtec_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	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

ANALISI DELLA CATTURA

Si può analizzare nella foto precedente l’inizio della cattura effettuata con Wireshark.
Questo divide ogni dettaglio dei pacchetti trasmessi in righe diverse.
Possiamo vedere nella prima riga una richiesta in broadcast da parte di un server che annuncia la propria presenza sulla rete tramite il protocollo “browser”.
In wireshark il protocollo “browser” si riferisce al “NetBIOS” utilizzato nei sistemi Windows per condividere informazioni sui dispositivi e le risorse disponibili su una rete locale (LAN).
Notiamo poi un tentativo di connessione HTTP/HTTPS e uno scambio di protocollo ARP(Address resolution protocol). Con il protocollo ARP, due dispositivi sulla stessa LAN si scambiano gli indirizzi MAC (indirizzo fisico della macchina), in modo da consentire la comunicazione diretta tramite i rispettivi indirizzi IP. Successivamente si evidenzia il problema notato in precedenza: un elevato scambio di pacchetti tra due utenti:

- IP Mittente: 192.168.200.100
- IP Destinatario: 192.168.200.150

ANALISI DELLA CATTURA

Si tratta di uno scambio SYN, SYN/ACK, ACK tra i due indirizzi IP con il protocollo TCP.
Uno scambio così elevato in poco tempo (2000+ richieste in meno di 1 secondo) può essere un chiaro IOC (indicatore di compromissione).

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 36.775589806	192.168.200.150	192.168.200.100	TCP	60 113 → 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 → 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 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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
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
37 36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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
39 36.775861964	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Oltre lo scambio elevato di pacchetti sipossono notare le richieste dal mittente al destinatario su varie porte. Grazie all’analisi della scansione ho potuto dedurre che ci fosse in atto un scansione delle porte attive indirizzata sulla macchina 192.168.200.150.

ANALISI DELLA CATTURA

La scansione delle porte attive è la prima metodologia solitamente utilizzata da un attaccante. Ci sono vari software che permettono una scansione, ad esempio nmap. Questo ci permette di impostare destinatario dello scan e tramite vari comandi scegliere se effettuare scansioni più o meno aggressive personalizzando la ricerca in modo specifico.
In questo caso l'attaccante prova a trovare le porte aperte tramite il protocollo TCP. Questo agisce con una stretta di mano a 3 vie tramite lo scambio di pacchetti SYN, SYN/ACK, ACK. Viene prima inviato il SYN verso la vittima, se questa risponderà con il SYN/ACK, la connessione si stabilirà con l'ultimo pacchetto ACK inviato alla vittima.
Se quindi si chiude la stretta di mano a 3 vie, nmap rileva e mostra all'utente la porta aperta. Personalizzando la scansione si possono vedere anche i servizi attivi sulle porte aperte e relative versioni, rendendo più semplice un'azione offensiva in caso di versioni dei protocolli non aggiornate.

CONSIGLI DIFENSIVI

La tecnica del port scanning è, di solito, il primo passo di un attaccante. Si ritiene necessaria un’azione difensiva per interrompere proattivamente l’attacco.
Si possono attuare più soluzioni:

- Limitare l’IP del mittente (tramite regole firewall)
- Individuare il dispositivo (essendo in rete LAN)
- Rivedere la segmentazione della rete
- Limitare il numero di connessioni simultanee dallo stesso IP
- Disabilitare servizi superflui
- Chiudere porte non necessarie

THANK YOU