

Threat Intelligence & IOC

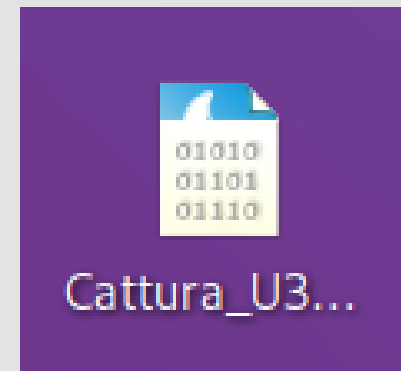
Cyber Security & Ethical Hacking



Traccia:

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

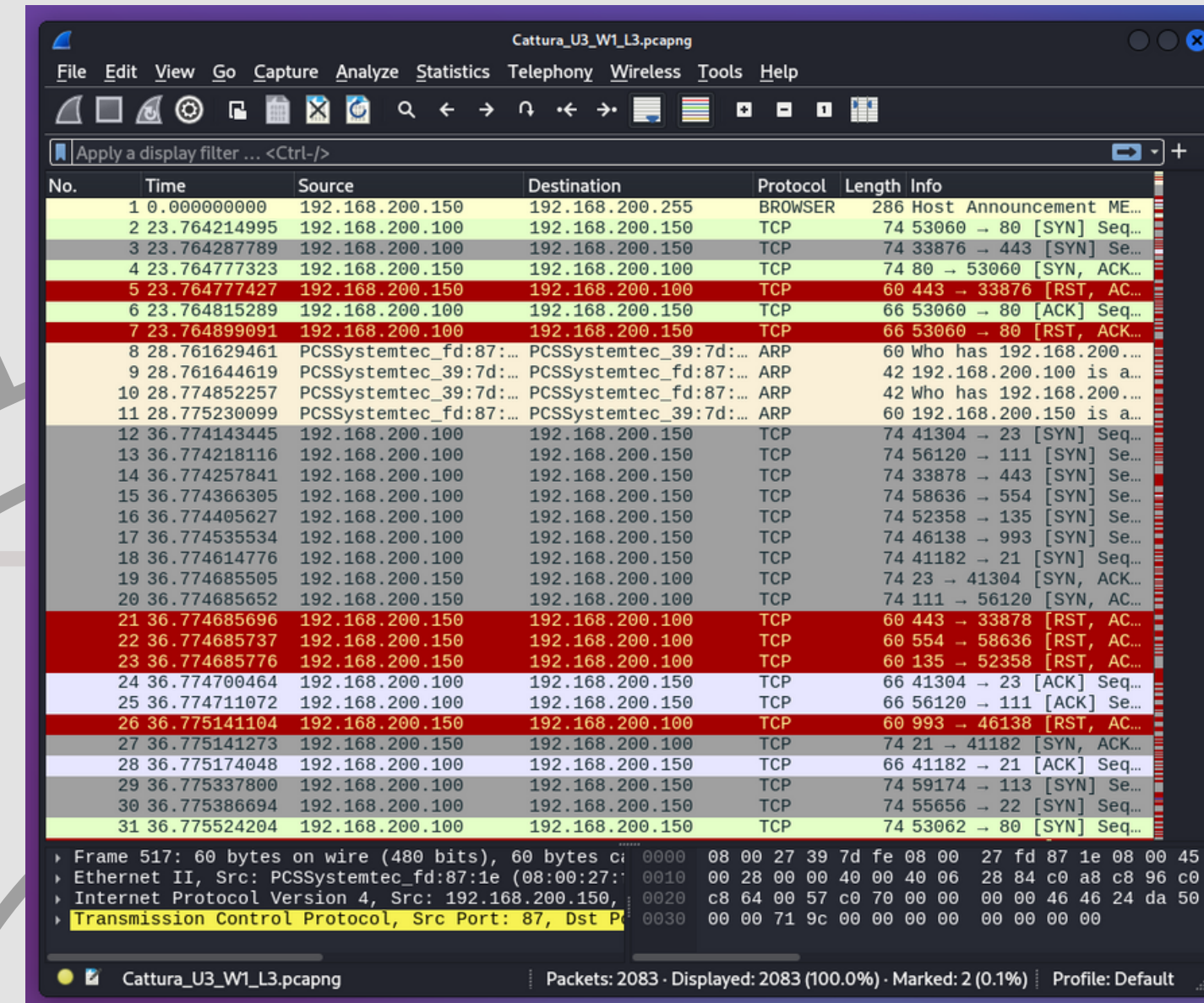


Compito

Analizzando attentamente la cattura, emergono chiaramente numerosi tentativi di connessione TCP (SYN) da parte dell'host 192.168.200.100 verso l'host di destinazione 192.168.200.150, evidenziati da un notevole variare delle porte di destinazione. Questa tendenza suggerisce un'ipotesi di scansione in corso da parte dell'host mittente. La robustezza di tale ipotesi trova fondamento nelle risposte del target: alcuni pacchetti [SYN+ACK] confermano l'apertura delle porte, mentre altri [RST+ACK] indicano chiaramente la chiusura delle stesse. Questo comportamento differenziato denota un approccio selettivo nel testare specifiche porte, potenzialmente finalizzato a individuare vulnerabilità o servizi attivi.

Per comprendere a fondo la situazione, è importante considerare anche la prospettiva del target. Le risposte [RST+ACK] potrebbero rivelare l'applicazione di regole firewall mirate, configurate sul lato del destinatario, allo scopo di respingere le richieste provenienti dall'host 192.168.200.100. Questo suggerisce un tentativo di difendersi contro la scansione in corso, indicando la presenza di misure di sicurezza proattive.

In conclusione, l'analisi della cattura suggerisce fortemente la possibilità di un'attività di scansione da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150. L'osservazione delle risposte del target, insieme alla considerazione delle potenziali regole firewall, fornisce una panoramica chiara di un potenziale confronto tra il mittente e il destinatario, con implicazioni significative per la sicurezza della rete.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement ME...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq...
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Se...
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK...
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, AC...
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq...
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK...
8	28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200....
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is a...
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200....
11	28.775230099	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is a...
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq...
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Se...
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Se...
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq...
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Se...
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Se...
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq...
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK...
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, AC...
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, AC...
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, AC...
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, AC...
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq...
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Se...
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, AC...
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK...
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq...
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Se...
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq...
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq...

Frame 517: 60 bytes on wire (480 bits), 60 bytes captured on interface (480 bits) on 08:00:27:39:7d:fe
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:39:7d:fe), Dst: PCSSystemtec_39:7d:1e (08:00:27:39:7d:1e)
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100
Transmission Control Protocol, Src Port: 87, Dst Port: 80, Seq: 53062, Win: 0, Len: 0

