

Threat Intelligence & IOC

Profilo studente

data:03/02/2026

studente: Gabriel Giustinelli 15/06/2004

Epicode classe: CS0525

Cyber Security Specialist

Obiettivo

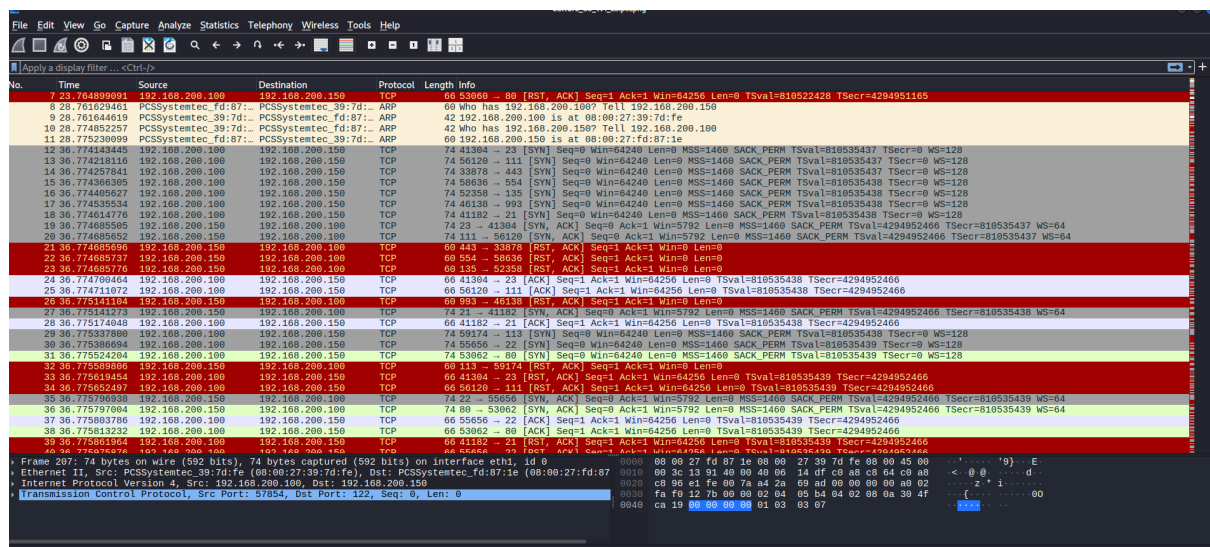
In questo progetto ha l'obiettivo di analizzare il traffico di dati catturato di **Cattura_U3_W1_L3.pcapng** a noi affidato per identificare eventuali o potenziali minacce alla sicurezza del perimetro della macchina sottostante.

Il lavoro quindi si basa sull'analisi di dati grezzi per estrarre informazioni utili per mitigare o prevenire attacchi informatici.

Metodologia di Analisi

Tramite lo strumento di visualizzazione **Wireshark** possiamo condurre l'analisi dei pacchetti, andando a focalizzarsi sulla ricerca di eventuali indicatori di compromissione (**IOC**).

Il nostro compito di analisi comprende l'ispezione dei protocolli, l'analisi comportamentale e la valutazione dell'impatto .



No.	Time	Source	Destination	Protocol	Length	Info
7	23.764899891	192.168.200.100	192.168.200.150	TCP	66	53660 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951105
8	28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	30.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 -> 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	30.774218116	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	30.774257841	192.168.200.100	192.168.200.150	TCP	74	33078 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	30.774306305	192.168.200.100	192.168.200.150	TCP	74	50636 -> 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	30.774405627	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	30.774535534	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
18	30.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 -> 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	30.774655555	192.168.200.100	192.168.200.150	TCP	74	23 -> 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	30.774885652	192.168.200.150	192.168.200.100	TCP	74	111 -> 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	30.774885652	192.168.200.150	192.168.200.100	TCP	60	443 -> 33078 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	30.774885737	192.168.200.150	192.168.200.100	TCP	60	554 -> 50636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	30.774885776	192.168.200.150	192.168.200.100	TCP	60	135 -> 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	30.774908464	192.168.200.100	192.168.200.150	TCP	66	41304 -> 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
25	30.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 -> 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	30.775141104	192.168.200.150	192.168.200.100	TCP	60	993 -> 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	30.775141104	192.168.200.150	192.168.200.100	TCP	74	21 -> 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	30.775174648	192.168.200.100	192.168.200.150	TCP	66	41182 -> 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	30.775378890	192.168.200.100	192.168.200.150	TCP	74	59174 -> 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	30.775398694	192.168.200.100	192.168.200.150	TCP	74	55656 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	30.775524204	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	30.775589860	192.168.200.100	192.168.200.150	TCP	60	113 -> 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	30.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 -> 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	30.77562497	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	30.775790938	192.168.200.100	192.168.200.150	TCP	74	22 -> 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=810535439 WS=64
36	30.775797084	192.168.200.100	192.168.200.150	TCP	74	80 -> 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	30.775803786	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	30.775813232	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	30.775819064	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
40	30.775847074	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

Frame 207: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 57854, Dst Port: 122, Seq: 0, Len: 0

1. Identificazione e analisi degli IOC

Dall'ispezione dei pacchetti sono stati rilevati i seguenti elementi critici:

1.1 Identificazione dell'attaccante e del target:

Nel primo pacchetto l'intercettazione del **protocollo BROWSER** ha rivelato l'**hostname** della vittima "**METASPLOITABLE**" questo è un dato fondamentale poiché identifica la macchina target orientando l'attaccante verso exploit delle vulnerabilità note.

- **IP sorgente:** 192.168.200.100
- **IP destinazione:** 192.168.200.150

1.2 Analisi del comportamento:

- **Scan aggressivo:** Dai dati è emersa una massiccia raffica di pacchetti con flag **[SYN]** diretti a porte sequenziali non standard.
- **Analisi risposte:** La costante presenza di risposte con flag **[RST,ACK]** evidenziate in rosso ci dice che l'host di destinazione sta rifiutando le connessioni su porte chiuse.



Lo scambio indica che tra i due host non è presente alcun firewall con politiche di dropping attivo, permettendo così una scansione libera.

- **Enumerazione servizi:** La presenza di traffico NBNS (NetBios Name Service) conferma che l'attaccante non sta solo cercando le porte aperte, ma sta cercando di trovare i nomi dei servizi e dei gruppi di lavoro per mappare la gerarchia della rete locale.

Sintesi dei Risultati

L'analisi ha permesso di rilevare un'attività di **ricognizione** ostile proveniente dall'IP **192.168.200.100**. L'attaccante invia un pacchetto **SYN** a migliaia di porte diverse in sequenza rapidissima senza mai concludere l'handshake a tre vie il che lo rende meno tracciabile, il sistema operativo risponde con un **RST** per chiudere immediatamente il tentativo di richiesta su porte chiuse. La prevalenza di questi pacchetti indica che l'attaccante sta effettuando un **brute-force di porte**, cercando di capire quali sono le porte aperte.

82	36	777758636	192.168.200.150	192.168.200.100	TCP	60	580	-	36138	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0
83	36	777758696	192.168.200.150	192.168.200.100	TCP	60	962	-	52428	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0
84	36	777871245	192.168.200.150	192.168.200.100	TCP	60	764	-	41874	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0
85	36	777871293	192.168.200.150	192.168.200.100	TCP	60	435	-	51506	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0
86	36	777893298	192.168.200.150	192.168.200.100	TCP	66	33842	-	445	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0 TSval=810535441 TSecr=4294952466
87	36	777912717	192.168.200.150	192.168.200.100	TCP	66	46998	-	139	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0 TSval=810535441 TSecr=4294952466
88	36	777986759	192.168.200.150	192.168.200.100	TCP	66	60632	-	25	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0 TSval=810535441 TSecr=4294952466

2. Ipotesi sui Vettori di Attacco e Metodologia

Sulla base dei dati raccolti, l'attacco è classificabile come una fase di **Ricognizione attiva ed aggressiva**:

1. **Vettore Principale:** Sfruttamento di falle nei servizi di rete (Network Service Exploitation).
2. **Automatizzazione:** La velocità dei millisecondi dell'invio dei pacchetti (nella colonna **Time**) e la graduazione numerica delle porte indicano l'uso di tool automatizzati come **Nmap** o il framework **Metasploit**.
3. **Strategia dell'Attaccante:** L'attaccante sta eseguendo un "**OS Fingerprinting**" e una mappatura dei servizi per identificare vettori di ingresso specifici (come backdoor o servizi obsoleti tipici dei sistemi Metasploitable) per una **successiva fase di Exploitation**.

3. Piano di Mitigazione e Azioni Correttive

Per neutralizzare la minaccia e innalzare il livello di sicurezza, si propongono le seguenti misure:

- **Contenimento Immediato:** Implementazione di una regola di filtraggio (**ACL**) sul firewall per il blocco totale del traffico proveniente dall'IP **192.168.200.100**.
- **Rate Limiting:** Configurazione di soglie di rate limiting per le connessioni **SYN** entranti, al fine di mitigare gli effetti di scansioni massive e prevenire potenziali Denial of Service (DoS) sulle tabelle di stato dei servizi.
- **Network Hardening:** Disabilitazione dei protocolli legacy (**NetBIOS/LLMNR**) e configurazione del sistema affinché **non risponda** con pacchetti **RST** alle porte chiuse, adottando una **politica di "Silent Drop"** per rendere l'host invisibile agli scanner automatici.
- **Isolamento degli Asset Critici:** Spostamento di macchine vulnerabili (come Metasploitable) in reti isolate (VLAN dedicata) senza connettività verso gli asset di produzione.

5. Conclusioni

L'analisi dimostra che il monitoraggio tramite Wireshark consente di intercettare le fasi preparatorie di un attacco informatico.

L'identificazione precoce dei pattern di scansione e dell'enumerazione dei servizi è essenziale per implementare contromisure efficaci prima che l'attaccante possa procedere alla fase di infiltrazione vera e propria.

