

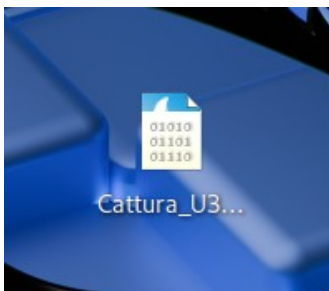
Threat Intelligence & IOC

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

1 Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

2 In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

3 Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro



Apriamo il file sulla nostra macchina virtuale Kali con **Wireshark** per poterlo analizzare. Vediamo come ci sia un intenso traffico di pacchetti TCP tra due IP: **192.168.200.150** e **192.168.200.100** (possibile target)

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, Potential B...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53860 → 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 → 53860 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
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	53860 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764839571	192.168.200.100	192.168.200.150	TCP	66	53860 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	23.761629461	PCSSystemtec.fid:87:...	PCSSystemtec.39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	23.761644619	PCSSystemtec.39:7d:...	PCSSystemtec.fid:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	23.774852257	PCSSystemtec.39:7d:...	PCSSystemtec.fid:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	23.775230999	PCSSystemtec.fid:87:...	PCSSystemtec.39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:39:7d:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41384 → 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	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774306395	192.168.200.100	192.168.200.150	TCP	74	56120 → 22 [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
18	36.774614776	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	36.774685595	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	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	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 86836 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774704644	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711972	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	36.775111104	192.168.200.150	192.168.200.100	TCP	60	103 → 41182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	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	36.775174048	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	36.775378608	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	36.775386634	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	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53862 → 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	41384 → 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=810535439 WS=64
36	36.775797964	192.168.200.150	192.168.200.100	TCP	74	80 → 53862 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775833125	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	36.775833232	192.168.200.100	192.168.200.150	TCP	66	53862 → 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
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776095853	192.168.200.100	192.168.200.150	TCP	66	53862 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	56884 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233888	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128

No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 -- 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53862 -- 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776119318	192.168.200.100	192.168.200.150	TCP	74	50601 -- 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 -- 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 -- 597 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
45	36.776385684	192.168.200.100	192.168.200.150	TCP	74	33842 -- 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776492580	192.168.200.100	192.168.200.150	TCP	74	49814 -- 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 -- 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 -- 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 -- 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 -- 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	68632 -- 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
52	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 -- 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 -- 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 -- 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776831233	192.168.200.150	192.168.200.100	TCP	60	507 -- 31043 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 -- 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 -- 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 -- 43814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904951	192.168.200.150	192.168.200.100	TCP	74	119 -- 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 -- 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 -- 66632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=810535440 WS=64
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 -- 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 -- 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=810535440 WS=64
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 -- 44980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	60	33842 -- 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 -- 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	69032 -- 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 -- 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 -- 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56990 -- 797 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35630 -- 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 -- 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
73	36.777378704	192.168.200.100	192.168.200.150	TCP	74	45780 -- 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	787 -- 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777439741	192.168.200.150	192.168.200.100	TCP	60	436 -- 35630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473818	192.168.200.100	192.168.200.150	TCP	74	36138 -- 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77	36.777522484	192.168.200.100	192.168.200.150	TCP	74	53428 -- 982 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623882	192.168.200.150	192.168.200.100	TCP	60	98 -- 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 -- 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

1. Analisi IOC

Da una prima analisi si nota un elevato numero di connessioni **TCP**. Le porte colpite sono oltre la numero 60000, inoltre le connessioni terminano bruscamente con il flag **“RST, ACK”**. Queste informazioni potrebbero segnalarci un **Port scanning**, con tentativi continui di connessione falliti.

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

Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0

Ethernet II, Src: PCSSystemtec_Fd:87:1e (08:00:27:fd:87:1e), Dst: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe)

Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100

Transmission Control Protocol, Src Port: 443, Dst Port: 33876, Seq: 1, Ack: 1, Len: 0

Source Port: 443
Destination Port: 33876
[Stream index: 1]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (37)]

[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 296487187
0101 = Header Length: 20 bytes (5)

Flags: 0x014 [RST, ACK]
000 = Reserved: Not set
...0 = Accurate ECN: Not set
....0 = Congestion Window Reduced: Not set
....0 = ECN-Echo: Not set
....0 = Urgent: Not set
....1 = Acknowledgment: Set
....0 = Push: Not set
....1 = Reset: Set
....0 = Syn: Not set
....0 = Fin: Not set
[TCP Flags:A.R.]

Window: 0
[Calculated window size: 0]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xfcb5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]

Tutto ci viene ancor di più confermato dal fatto che non sono presenti le risposte **SYN-ACK**, quindi l'**handshake** non viene concluso.

Transmission Control Protocol, Src Port: 443, Dst Port: 33876

Source Port: 443
Destination Port: 33876
[Stream index: 4]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (37)]

...1. = RST: Present
...0. = FIN: Absent
....0... = Data: Absent
....1.. = ACK: Present
....0.. = SYN-ACK: Absent
....1.. = SYN: Present
[Completeness Flags: R..A.S]

2. Ipotesi sui vettori utilizzati

1 Port Scanning: l'host invia vari pacchetti di dati a diverse porte dell'IP del target per determinare quali servizi sono accessibili e in esecuzione. Tra i vari vettori che possono essere utilizzati abbiamo: **nmap**, **netcat** **metasploitable**

2 DoS (Denial of Service): l'host tenta di sovraccaricare la rete del target tramite un traffico eccessivo di dati in entrata. Questo può rendere il sistema lento e malfunzionante. Qui un potenziale vettore che può essere utilizzato è **Nping**

3 Brute Force: l'host tenta sistematicamente di forzare credenziali sui servizi esposti (come ad esempio SSH o Telnet) Tra i vari vettori che possono essere utilizzati abbiamo **Hydra** o **Medusa**

L'ipotesi, in teoria, più corretta dovrebbe essere il **port scanner**, questo perché:

1 Ogni volta che non avviene la risposta **SYN-ACK** l'invio di pacchetti si indirizza verso una porta diversa

2 Le porte attaccate arrivano, e addirittura, superano la 60000

3 I pacchetti sono inviati in ordine e le tempistiche indicano un possibile **nmap**

3. Azioni consigliate

Le precauzioni che si possono prendere per evitare questo tipo attacco possono essere:

1 Bloccare il traffico da 192.168.200.150 tramite firewall

2 Isolare 192.168.200.100 per verificarne l'integrità

3 Implementare un **IDS/IPS**

4 Limitare l'accesso ai servizi essenziali

5 Applicare regole di **firewall interne** per ridurre l'esposizione dei sistemi

6 Mantenere i sistemi aggiornati e chiudere porte non necessarie

4 Conclusione

L'analisi della cattura, evidenzia un comportamento di **ricognizione di rete ostile**, finalizzato all'identificazione dei servizi attivi su una possibile macchina vulnerabile. E' cruciale in questi casi intervenire, isolando il servizio attaccato e attuare delle misure di sicurezza preventive per evitare ulteriori prove di intrusioni da parte di utenti malevoli.