

# Threat Intelligence & IOC

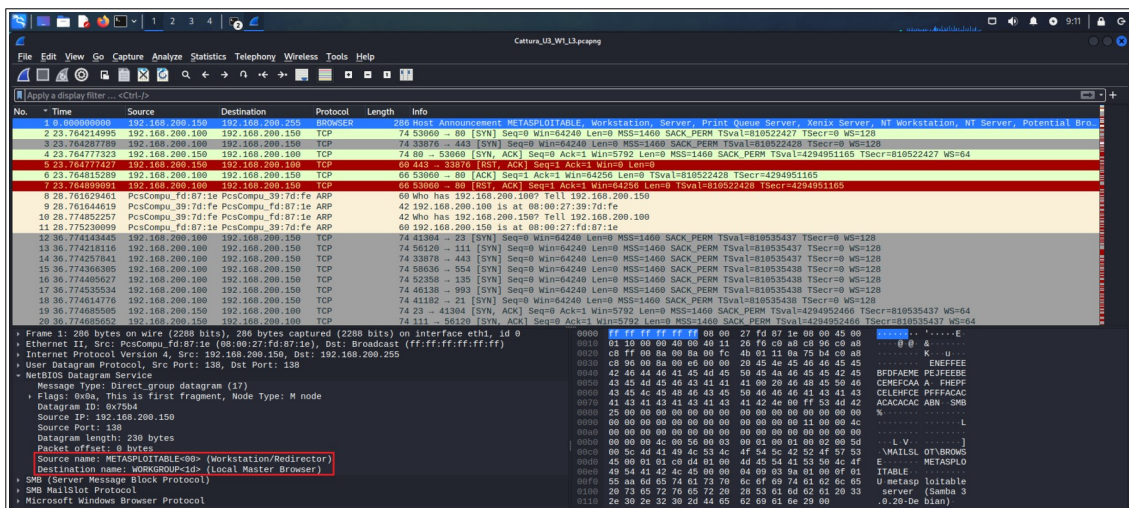
Obiettivo: analizzare una scansione catturata con Wireshark e ricavare più informazioni possibili.

## 1) Prima analisi

Per cominciare ho caricato il file su **Kali** grazie ad una *cartella condivisa* e aprendolo successivamente con **Wireshark**. La schermata mi elencava circa 2000 pacchetti analizzati dal tool.

Si può notare proprio all'inizio il **Protocollo BROWSER**, ovvero viene utilizzato per identificare il traffico di rete per risorse condivise, cioè quando un dispositivo ne vuole trovare altri in condivisione invia messaggi attraverso questo Protocollo.

Infatti setacciando il pacchetto troviamo come destinazione **WORKGROUP**, probabilmente una cartella di lavoro condivisa.



## 2) Analisi dei Pacchetti

Per prima cosa ho cercato di capire chi fosse l'attaccante in questa scansione; o almeno chi ha iniziato a cercare una connessione con l'altra macchina. Le richieste **SYN** partono dal **Source** 192.168.200.100, invece la risposta **SYN ACK** la trasmette 192.168.200.150; perciò posso dedurre che sia il primo indirizzo IP a cercare una connessione.

Il numero di pacchetti è notevole (oltre 2000), ma usando il filtro di **Wireshark**

**tcp.flags**

ho scoperto che quasi tutti i pacchetti sono trasmessi con il protocollo **TCP** ed alcuni terminano la connessione con flag **ACK**. Sulla base di queste considerazioni posso dedurre che non si tratta di un attacco hacker vero e proprio ma piuttosto di una scansione delle porte, probabilmente con il tool **nmap** o simili, avviato ad una scansione **TCP**.

No.	Time	Source	Destination	Protocol	Length	Info
2	74.3421495	192.168.200.100	192.168.200.150	TCP	74	53960 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
3	74.342151210	192.168.200.100	192.168.200.150	TCP	74	53960 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.74477323	192.168.200.150	192.168.200.100	TCP	74	80 → 53960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=429495246 TSecr=810522427 WS=64
5	6.23.744815209	192.168.200.100	192.168.200.150	TCP	60	53960 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
6	723.744899991	192.168.200.100	192.168.200.150	TCP	60	53960 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810522428 TSecr=4294951165
12	136.77428844	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
13	36.774288116	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	36.774287641	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	36.774304395	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	36.774459534	192.168.200.100	192.168.200.150	TCP	74	45138 → 4390 [SYN, ACK] Seq=0 Ack=1 Win=5792 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 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.100	192.168.200.150	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=429495246 TSecr=810535437 WS=64
20	36.774685652	192.168.200.100	192.168.200.150	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=429495246 TSecr=810535437 WS=64
21	36.774685690	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685707	192.168.200.150	192.168.200.100	TCP	60	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	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	60	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711912	192.168.200.100	192.168.200.150	TCP	60	56120 → 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	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141233	192.168.200.150	192.168.200.100	TCP	74	41384 → 23 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174848	192.168.200.100	192.168.200.150	TCP	60	41182 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775373880	192.168.200.100	192.168.200.150	TCP	74	59174 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386660	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53962 → 60 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775538980	192.168.200.100	192.168.200.150	TCP	60	111 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	60	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775625457	192.168.200.100	192.168.200.150	TCP	60	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775932991	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775977004	192.168.200.150	192.168.200.100	TCP	74	80 → 53960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803706	192.168.200.100	192.168.200.150	TCP	60	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813212	192.168.200.100	192.168.200.150	TCP	60	53962 → 60 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775801804	192.168.200.100	192.168.200.150	TCP	60	41182 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775973816	192.168.200.100	192.168.200.150	TCP	60	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

### 3) Differenze tra le scansioni

Ho affermato che la scansione avvenuta sulla macchina **Metasploit** è una **TCP Scan** anche dal fatto che ci sono differenze che si possono notare nelle catture con **Wireshark**; io ho provato a scansionare una macchina **Metasploitable** con altri tipi di *switch* di **nmap** per sottolineare queste differenze.

#### - TCP Scan

La **TCP Scan** conclude il *3 Way Hand-shake* su una porta, ovvero a una richiesta **SYN**, segue una risposta **SYN ACK** per concludere con un ultimo pacchetto che ha flag **ACK**.

No.	Time	Source	Destination	Protocol	Length	Info
19	13.005755256	192.168.66.100	192.168.66.120	TCP	74	44640 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718621 TSecr=0 WS=128
20	13.005952104	192.168.66.100	192.168.66.120	TCP	74	56136 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718621 TSecr=0 WS=128
21	13.006004271	192.168.66.100	192.168.66.120	TCP	74	53496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718622 TSecr=0 WS=128
22	13.006033841	192.168.66.100	192.168.66.120	TCP	74	52528 → 3380 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718622 TSecr=0 WS=128
23	13.006046471	192.168.66.100	192.168.66.120	TCP	74	50706 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718622 TSecr=0 WS=128
24	13.006059583	192.168.66.120	192.168.66.100	TCP	74	531 → 41390 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=673829 TSecr=3047718623 WS=32
25	13.006059613	192.168.66.120	192.168.66.100	TCP	60	587 → 30130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	13.006073516	192.168.66.100	192.168.66.120	TCP	74	41390 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718623 TSecr=0 WS=128
27	13.006098974	192.168.66.100	192.168.66.120	TCP	74	55536 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718623 TSecr=0 WS=128
28	13.006094919	192.168.66.100	192.168.66.120	TCP	74	55536 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718623 TSecr=0 WS=128
29	13.007145907	192.168.66.100	192.168.66.120	TCP	74	55536 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718623 TSecr=0 WS=128
30	13.007259043	192.168.66.120	192.168.66.100	TCP	60	587 → 30130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	13.007305316	192.168.66.100	192.168.66.120	TCP	74	55536 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718623 TSecr=0 WS=128
32	13.007309055	192.168.66.100	192.168.66.120	TCP	60	41390 → 58 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3047718623 TSecr=673829
33	13.007578891	192.168.66.120	192.168.66.100	TCP	74	80 → 53496 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=673829 TSecr=3047718622 WS=32
34	13.007730831	192.168.66.100	192.168.66.120	TCP	74	53496 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3047718623 TSecr=673829
35	13.008015393	192.168.66.100	192.168.66.120	TCP	60	53496 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3047718624 TSecr=673829
36	13.008325844	192.168.66.120	192.168.66.100	TCP	60	3380 → 52528 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	13.008339504	192.168.66.100	192.168.66.120	TCP	74	41390 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718624 TSecr=0 WS=128
38	13.008323960	192.168.66.120	192.168.66.100	TCP	74	23 → 49204 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=673829 TSecr=3047718622 WS=32
39	13.008327380	192.168.66.120	192.168.66.100	TCP	74	111 → 55536 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=673829 TSecr=3047718623 WS=32
40	13.008327685	192.168.66.120	192.168.66.100	TCP	74	55536 → 111 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 TSval=3047718624 TSecr=673829
41	13.008328040	192.168.66.120	192.168.66.100	TCP	60	1025 → 60814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	13.008332991	192.168.66.100	192.168.66.120	TCP	74	41390 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718624 TSecr=0 WS=128
43	13.008438925	192.168.66.100	192.168.66.120	TCP	60	49204 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3047718624 TSecr=673829
44	13.008503648	192.168.66.100	192.168.66.120	TCP	60	55536 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3047718624 TSecr=673829
45	13.008511111	192.168.66.100	192.168.66.120	TCP	60	60990 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3047718624 TSecr=673829
46	13.008718926	192.168.66.100	192.168.66.120	TCP	74	46484 → 1720 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718624 TSecr=0 WS=128
47	13.008972480	192.168.66.100	192.168.66.120	TCP	74	40528 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718625 TSecr=0 WS=128
48	13.009242709	192.168.66.120	192.168.66.100	TCP	60	159 → 35034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	13.009243170	192.168.66.120	192.168.66.100	TCP	60	1720 → 46484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
50	13.009414060	192.168.66.100	192.168.66.120	TCP	74	55412 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718625 TSecr=0 WS=128
51	13.009621290	192.168.66.100	192.168.66.120	TCP	74	48666 → 3308 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718625 TSecr=0 WS=128
52	13.009894905	192.168.66.100	192.168.66.120	TCP	74	58100 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3047718625 TSecr=0 WS=128
53	13.009950078	192.168.66.120	192.168.66.100	TCP	74	139 → 45098 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=673829 TSecr=3047718625 WS=32

#### -SYN Scan

La **SYN Scan** invia pacchetti con flag **SYN** con risposta **SYN ACK** però interrompendo la connessione (**RST**) non appena capisce che la porta scansionata è attiva o no.

No.	Time	Source	Destination	Protocol	Length	Info
10	9.112021428	PcsCompu.c7:e1:36	Broadcast	ARP	42	Who has 192.168.66.17 Tell 192.168.66.100
11	10.136089386	PcsCompu.c7:e1:36	Broadcast	ARP	42	Who has 192.168.66.17 Tell 192.168.66.100
12	13.130923215	192.168.66.100	192.168.66.120	TCP	58	57980 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	13.131054566	192.168.66.100	192.168.66.120	TCP	58	57980 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	13.131202254	192.168.66.100	192.168.66.120	TCP	58	57980 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	13.131447492	192.168.66.100	192.168.66.120	TCP	58	57980 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13.131569243	192.168.66.100	192.168.66.120	TCP	58	57980 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	13.131833086	192.168.66.100	192.168.66.120	TCP	58	57980 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	13.131913976	192.168.66.100	192.168.66.120	TCP	58	57980 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	13.132000058	192.168.66.120	192.168.66.100	TCP	60	3305 → 3389 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	13.132016177	192.168.66.100	192.168.66.120	TCP	58	57980 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	13.132000058	192.168.66.120	192.168.66.100	TCP	60	135 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	13.132001344	192.168.66.120	192.168.66.100	TCP	60	113 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.132126666	192.168.66.100	192.168.66.120	TCP	58	57980 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	13.132311630	192.168.66.100	192.168.66.120	TCP	58	57980 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	13.132460799	192.168.66.100	192.168.66.120	TCP	60	111 → 57980 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26	13.132614559	192.168.66.120	192.168.66.100	TCP	60	554 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	13.132654396	192.168.66.100	192.168.66.120	TCP	54	57980 → 411 [RST] Seq=1 Win=0 Len=0
28	13.132948073	192.168.66.120	192.168.66.100	TCP	60	53 → 57980 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
29	13.132949133	192.168.66.120	192.168.66.100	TCP	60	173 → 57980 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
30	13.132949499	192.168.66.120	192.168.66.100	TCP	60	443 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	13.132949854	192.168.66.120	192.168.66.100	TCP	60	1720 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	13.132950264	192.168.66.120	192.168.66.100	TCP	60	443 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	13.133068223	192.168.66.100	192.168.66.120	TCP	54	57980 → 53 [RST] Seq=1 Win=0 Len=0
34	13.133167583	192.168.66.100	192.168.66.120	TCP	54	57980 → 23 [RST] Seq=1 Win=0 Len=0

## -Service Scan

Questo tipo di scansione è utile a scoprire la versione dei servizi attivi sulla macchina analizzata. Troviamo protocolli di tipo HTTP che nella scansione dell'esercizio sono assenti.

No.	Time	Source	Destination	Protocol	Length	Info
2174	19.479297586	192.168.66.100	192.168.66.120	HTTP	84	GET / HTTP/1.0
2284	19.563012994	192.168.66.120	192.168.66.100	HTTP	66	HTTP/1.1 200 OK (text/html)
2345	24.488363825	192.168.66.100	192.168.66.120	HTTP	84	GET / HTTP/1.0
2391	29.490348478	192.168.66.100	192.168.66.120	HTTP	88	OPTIONS / HTTP/1.0
2464	34.603392581	192.168.66.120	192.168.66.100	HTTP	66	HTTP/1.1 505 HTTP Version Not Supported
2617	49.954516060	192.168.66.100	192.168.66.120	HTTP	242	GET /nmaplowercheck1687955265 HTTP/1.1
2619	49.955323111	192.168.66.120	192.168.66.100	HTTP	558	HTTP/1.1 404 Not Found (text/html)
2623	49.955831963	192.168.66.100	192.168.66.120	HTTP	247	GET /nmaplowercheck1687955265 HTTP/1.1
2624	49.955861942	192.168.66.100	192.168.66.120	HTTP	84	GET / HTTP/1.0
2626	49.955995111	192.168.66.100	192.168.66.120	HTTP	684	POST /sdk HTTP/1.1
2627	49.956028353	192.168.66.100	192.168.66.120	HTTP	84	GET / HTTP/1.0
2630	49.956160217	192.168.66.100	192.168.66.120	HTTP	689	POST /sdk HTTP/1.1
2636	49.957384907	192.168.66.120	192.168.66.100	HTTP	537	HTTP/1.1 404 Not Found (text/html)
2639	49.978504718	192.168.66.120	192.168.66.100	HTTP	1257	HTTP/1.1 404 Not Found (text/html)
2642	49.983541446	192.168.66.120	192.168.66.100	HTTP	1193	HTTP/1.1 404 Not Found (text/html)
2645	49.986090898	192.168.66.120	192.168.66.100	HTTP	1152	HTTP/1.1 200 OK (text/html)

## -Aggressive Scan

Questo tipo di scansione invia una moltitudine di pacchetti al bersaglio per ottenere più informazioni possibili e di ogni tipo (ad esempio possiamo ottenere informazioni sul sistema operativo) non in maniera “silenziosa” purtroppo.

No.	Time	Source	Destination	Protocol	Length	Info
3116	95.570561654	192.168.66.120	192.168.66.100	TCP	74	80 → 53344 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=449388 TSecr=3045473760 WS=32
3117	95.570586313	192.168.66.120	192.168.66.100	TCP	74	80 → 53344 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=449388 TSecr=3045473760 WS=32
3118	95.570599155	192.168.66.100	192.168.66.120	TCP	66	49786 → 22 [ACK] Seq=1 Ack=1 Min=64256 Len=0 TSval=3045473761 TSecr=449388
3119	95.570614323	192.168.66.100	192.168.66.120	TCP	66	53344 → 80 [ACK] Seq=1 Ack=1 Min=64256 Len=0 TSval=3045473761 TSecr=449388
3120	95.571278646	192.168.66.100	192.168.66.120	TCP	66	53674 → 8089 [FIN, ACK] Seq=98 Ack=8775 Win=64128 Len=0 TSval=3045473761 TSecr=449388
3121	95.572447748	192.168.66.120	192.168.66.100	TCP	66	8089 → 53674 [FIN, ACK] Seq=8775 Ack=99 Win=5792 Len=0 TSval=449388 TSecr=3045473761
3122	95.572454047	192.168.66.100	192.168.66.120	SMB	215	Session Setup AndX Request, NTLMSSP_NEGOTIATE
3123	95.572467684	192.168.66.100	192.168.66.120	TCP	66	53674 → 8089 [ACK] Seq=99 Ack=8776 Win=64128 Len=0 TSval=3045473763 TSecr=449388
3124	95.572540377	192.168.66.100	192.168.66.120	FTP	72	Request: STAT
3125	95.573206059	192.168.66.100	192.168.66.120	VNC	78	Client protocol version: 003.003
3126	95.573522975	192.168.66.100	192.168.66.120	TCP	66	5900 → 40680 [ACK] Seq=13 Ack=13 Win=5792 Len=0 TSval=449388 TSecr=3045473763
3127	95.574679461	192.168.66.100	192.168.66.120	UDP	56	58718 → 31956 Len=1
3128	95.574715107	192.168.66.100	192.168.66.120	SSHv1	86	Client: Protocol (SSH-1.5-NmapNSE-1.0)
3129	95.574784475	192.168.66.100	192.168.66.120	SMTP	250	Negotiate Protocol Request
3130	95.574822514	192.168.66.100	192.168.66.120	DNS	119	Standard query 0x0001 TXT id.server.opf
3131	95.574843877	192.168.66.100	192.168.66.120	HTTP	381	POST / HTTP/1.1 (application/x-www-form-urlencoded)
3132	95.574932918	192.168.66.120	192.168.66.100	ICMP	84	Destination unreachable (Port unreachable)
3133	95.575021824	192.168.66.120	192.168.66.100	TCP	66	445 → 55024 [ACK] Seq=1 Ack=185 Win=6880 Len=0 TSval=449388 TSecr=3045473765
3134	95.575027159	192.168.66.120	192.168.66.100	TCP	66	11728 → 40680 [ACK] Seq=2 Ack=13 Win=5792 Len=0 TSval=449388 TSecr=3045473765
3135	95.575022036	192.168.66.120	192.168.66.100	TCP	66	8180 → 40920 [ACK] Seq=1 Ack=310 Win=6880 Len=0 TSval=449388 TSecr=3045473765
3136	95.576175456	192.168.66.120	192.168.66.100	SSHv1	184	Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-Rubuntu1)
3137	95.576183486	192.168.66.100	192.168.66.120	TCP	66	49786 → 22 [ACK] Seq=1 Ack=39 Win=64256 Len=0 TSval=3045473766 TSecr=449388
3138	95.576710293	192.168.66.120	192.168.66.100	SMB	405	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
3139	95.576724804	192.168.66.100	192.168.66.120	TCP	66	55016 → 445 [ACK] Seq=203 Ack=471 Win=64128 Len=0 TSval=3045473767 TSecr=449388
3140	95.577738641	192.168.66.120	192.168.66.100	FTP	90	Response: 211-FTP server status:
3141	95.577738765	192.168.66.120	192.168.66.100	FTP	84	Response: Connected to
3142	95.577738844	192.168.66.100	192.168.66.120	FTP	80	Response: 192.168.66.100
3143	95.577747948	192.168.66.100	192.168.66.120	TCP	66	43706 → 21 [ACK] Seq=49 Ack=159 Win=64256 Len=0 TSval=3045473768 TSecr=449388
3144	95.577771234	192.168.66.100	192.168.66.120	TCP	66	43706 → 21 [ACK] Seq=49 Ack=177 Win=64256 Len=0 TSval=3045473768 TSecr=449388
3145	95.577781011	192.168.66.100	192.168.66.120	TCP	66	43706 → 21 [ACK] Seq=49 Ack=191 Win=64256 Len=0 TSval=3045473768 TSecr=449388
3146	95.577968799	192.168.66.120	192.168.66.100	FTP	324	Response:
3147	95.577974368	192.168.66.100	192.168.66.120	TCP	66	43706 → 21 [ACK] Seq=49 Ack=249 Win=64128 Len=0 TSval=3045473768 TSecr=449388
3148	95.578254064	192.168.66.120	192.168.66.100	VNC	86	Security types supported
3149	95.578254067	192.168.66.120	192.168.66.100	TCP	66	22 → 49770 [ACK] Seq=39 Ack=21 Win=5792 Len=0 TSval=449389 TSecr=3045473765
3150	95.578262396	192.168.66.100	192.168.66.120	TCP	66	40680 → 5900 [ACK] Seq=13 Ack=33 Win=64256 Len=0 TSval=3045473768 TSecr=449388

## -XMAS Scan

La *Scan ad “Albero di Natale”* è un tipo di tecnica utilizzata per evadere alcuni tipi di firewall poco potenti. Utilizza nelle sue richieste flag di tipo FIN, URG, PUSH non presenti nella scansione analizzata.

No.	Time	Source	Destination	Protocol	Length	Info
16	13.109251017	192.168.66.100	192.168.66.120	TCP	54	59485 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
17	13.109435934	192.168.66.100	192.168.66.120	TCP	54	59485 → 58 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
18	13.109514003	192.168.66.100	192.168.66.120	TCP	54	59485 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
19	13.109507215	192.168.66.100	192.168.66.120	TCP	54	59485 → 338 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
20	13.109688726	192.168.66.100	192.168.66.120	TCP	54	59485 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
21	13.110599911	192.168.66.100	192.168.66.120	TCP	54	59485 → 99 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
22	13.110550030	192.168.66.120	192.168.66.100	TCP	60	1023 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
23	13.110593993	192.168.66.120	192.168.66.100	TCP	60	443 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
24	13.110554249	192.168.66.120	192.168.66.100	TCP	60	587 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
25	13.110554004	192.168.66.120	192.168.66.100	TCP	60	3389 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
26	13.111130830	192.168.66.120	192.168.66.100	TCP	60	1723 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
27	13.111613319	192.168.66.120	192.168.66.100	TCP	60	995 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
28	13.114493987	192.168.66.100	192.168.66.120	TCP	54	59485 → 11 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
29	13.114613272	192.168.66.100	192.168.66.120	TCP	54	59485 → 330 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
30	13.114683062	192.168.66.100	192.168.66.120	TCP	54	59485 → 179 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
31	13.114719195	192.168.66.100	192.168.66.120	TCP	54	59485 → 13 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
32	13.114748464	192.168.66.100	192.168.66.120	TCP	54	59485 → 99 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
33	13.114861181	192.168.66.100	192.168.66.120	TCP	54	59485 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
34	13.114960766	192.168.66.100	192.168.66.120	TCP	54	59485 → 11 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
35	13.115025713	192.168.66.100	192.168.66.120	TCP	54	59485 → 19 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
36	13.115091241	192.168.66.100	192.168.66.120	TCP	54	59485 → 888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
37	13.115196919	192.168.66.100	192.168.66.120	TCP	54	59485 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
38	13.115274328	192.168.66.100	192.168.66.120	TCP	54	59485 → 11 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
39	13.115378875	192.168.66.100	192.168.66.120	TCP	54	59485 → 11 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
40	13.115432712	192.168.66.120	192.168.66.100	TCP	60	113 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
41	13.115433462	192.168.66.120	192.168.66.100	TCP	60	1729 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
42	13.115433917	192.168.66.120	192.168.66.100	TCP	60	993 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
43	13.115789355	192.168.66.120	192.168.66.100	TCP	60	554 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
44	13.115799811	192.168.66.120	192.168.66.100	TCP	60	199 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
45	13.115799181	192.168.66.120	192.168.66.100	TCP	60	888 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
46	13.116161557	192.168.66.120	192.168.66.100	TCP	60	119 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
47	13.119428073	192.168.66.100	192.168.66.120	TCP	54	59485 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
48	13.119505222	192.168.66.100	192.168.66.120	TCP	54	59485 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
49	13.119539051	192.168.66.100	192.168.66.120	TCP	54	59485 → 85 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
50	13.119571690	192.168.66.100	192.168.66.120	TCP	54	59485 → 13 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

#### 4) Conclusioni

Possiamo concludere dicendo che non c'è stato un vero e proprio attacco informatico in questo caso ma piuttosto una scansione esterna delle porte.

Nonostante questo però non è detto che un indirizzo esterno che sta eseguendo una scansione sia una cosa da sottostimare; potrebbe essere un eventuale hacker che prepara l'enumerazione dei servizi di una ipotetica azienda (in questo caso la **Metasploitable**), quindi alcuni suggerimenti che si possono dare sono:

- Attivare un firewall con policy mirate a non permettere il traffico indesiderato.
- Eseguire ogni tot dei Pentest sulle macchine dell'azienda in modo tale da proteggerle da eventuali bug e vulnerabilità patchandole di conseguenza.
- Controllare il traffico costantemente in modo tale da poter anticipare un eventuale attacco esterno.