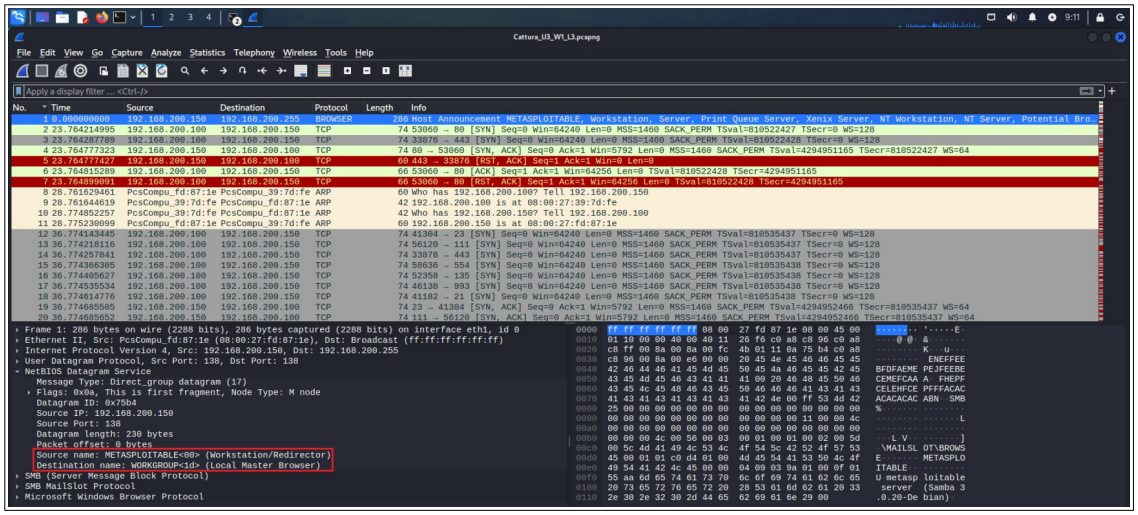
Threat Intelligence & IOC

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.

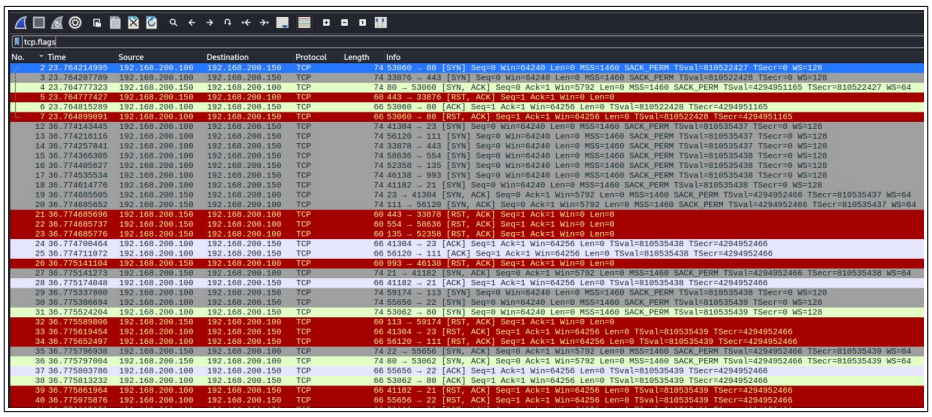


2) Analisi dei Pacchetti

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**.

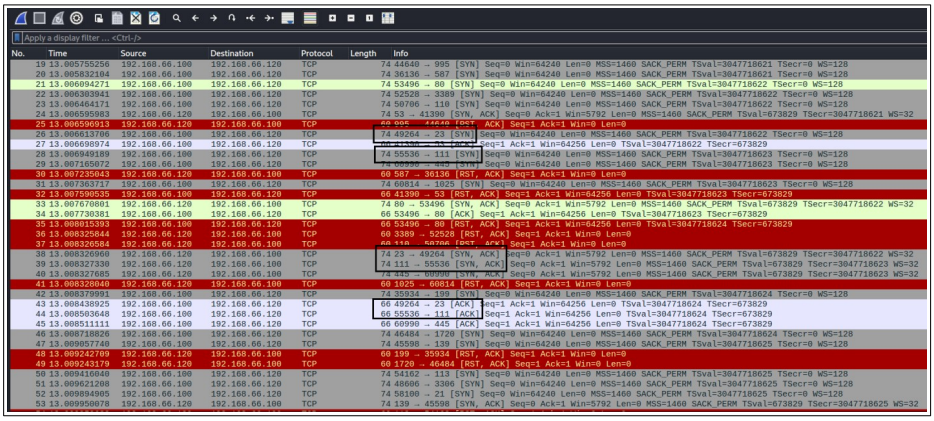


3) Differenze tra le scansioni

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.

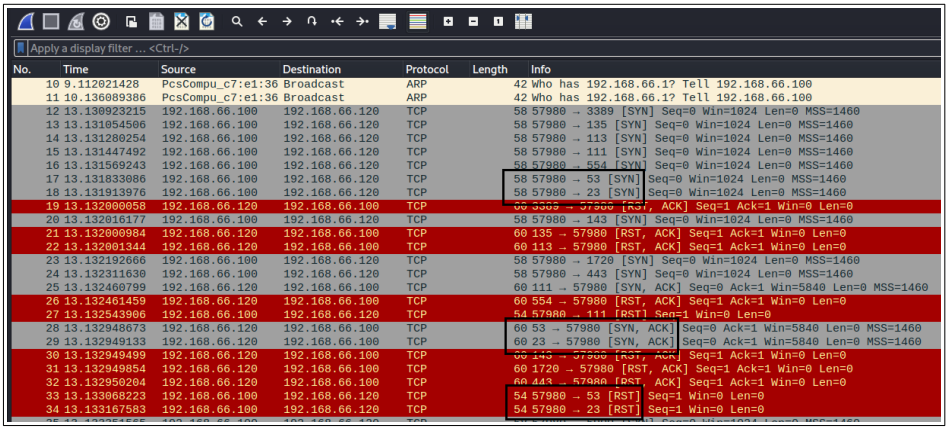
- **TCP Scan**

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**.



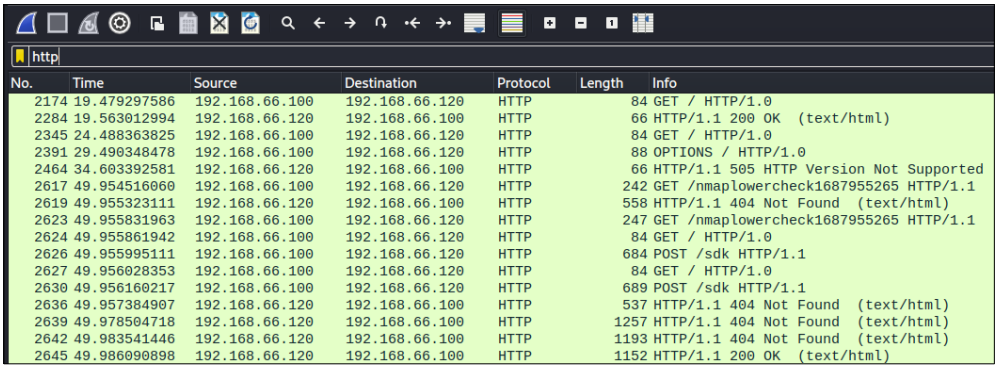
-**SYN Scan**

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.



-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.

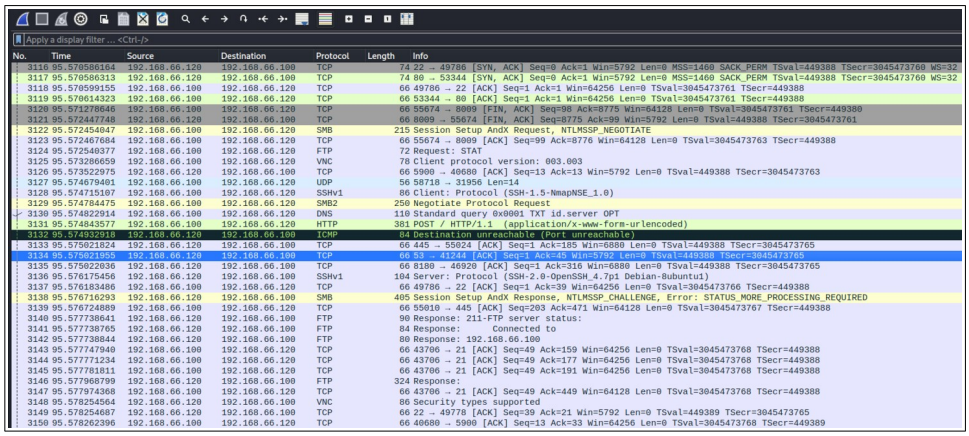


http

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.

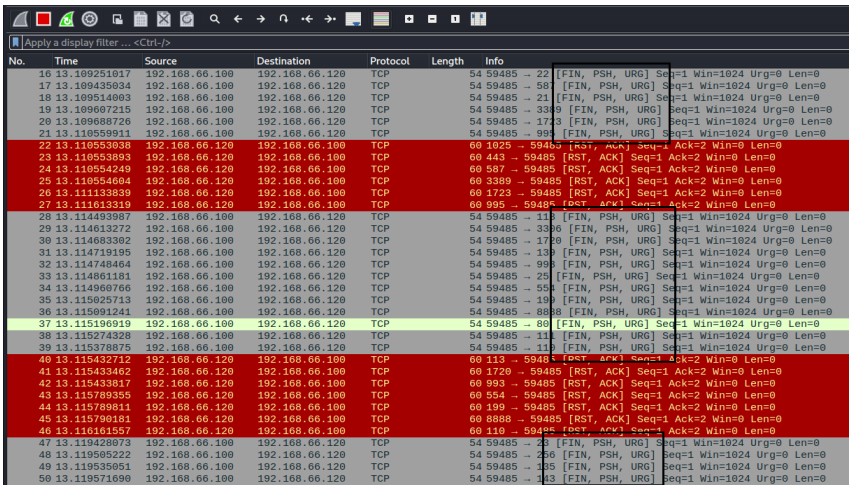


Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3116	59.570586164	192.168.66.120	192.168.66.100	TCP	74	22 → 49786 [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 Win=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 Win=64256 Len=0 TSval=3045473761 TSecr=449388
3120	95.571270646	192.168.66.100	192.168.66.120	TCP	66	55674 → 8009 [FIN, ACK] Seq=98 Ack=8775 Win=64128 Len=0 TSval=3045473761 TSecr=449380
3121	95.572447748	192.168.66.120	192.168.66.100	TCP	66	8009 → 55674 [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	55674 → 8009 [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	95.573286659	192.168.66.100	192.168.66.120	VNC	78	Client protocol version: 003.003
3126	95.573522975	192.168.66.120	192.168.66.100	TCP	66	5900 → 40680 [ACK] Seq=13 Ack=13 Win=5792 Len=0 TSval=449388 TSecr=3045473763
3127	95.574679401	192.168.66.100	192.168.66.120	UDP	56	58718 → 31956 Len=14
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	SMB2	250	Negotiate Protocol Request
3130	95.574822914	192.168.66.100	192.168.66.120	DNS	110	Standard query 0x0001 TXT id.server OPT
3131	95.574843577	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	95.575021955	192.168.66.120	192.168.66.100	TCP	66	53 → 41244 [ACK] Seq=1 Ack=45 Win=5792 Len=0 TSval=449388 TSecr=3045473765
3135	95.575022036	192.168.66.120	192.168.66.100	TCP	66	8180 → 46920 [ACK] Seq=1 Ack=316 Win=6880 Len=0 TSval=449388 TSecr=3045473765
3136	95.576175456	192.168.66.120	192.168.66.100	SSHv1	104	Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1)
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	95.576716293	192.168.66.120	192.168.66.100	SMB	405	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
3139	95.576724889	192.168.66.100	192.168.66.120	TCP	66	55010 → 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	192.168.66.120	192.168.66.100	FTP	80	Response: 192.168.66.100
3143	95.577747940	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	95.577781811	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=449 Win=64128 Len=0 TSval=3045473768 TSecr=449388
3148	95.578254564	192.168.66.120	192.168.66.100	VNC	86	Security types supported
3149	95.578254687	192.168.66.120	192.168.66.100	TCP	66	22 → 49778 [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=449389

-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.



Apply a display filter ... <Ctrl-/>

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	13.109435034	192.168.66.100	192.168.66.120	TCP	54	59485 → 587 [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	13.109607215	192.168.66.100	192.168.66.120	TCP	54	59485 → 3389 [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	13.110559911	192.168.66.100	192.168.66.120	TCP	54	59485 → 995 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
22	13.110553038	192.168.66.120	192.168.66.100	TCP	60	1025 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
23	13.110553893	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	13.110554604	192.168.66.120	192.168.66.100	TCP	60	3389 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
26	13.111133839	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 → 113 [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 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
30	13.114683302	192.168.66.100	192.168.66.120	TCP	54	59485 → 1720 [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 → 139 [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 → 993 [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 → 554 [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 → 199 [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 → 8888 [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 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
39	13.115378075	192.168.66.100	192.168.66.120	TCP	54	59485 → 110 [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	1720 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
42	13.115433817	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	13.115789811	192.168.66.120	192.168.66.100	TCP	60	199 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
45	13.115790181	192.168.66.120	192.168.66.100	TCP	60	8888 → 59485 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
46	13.116161557	192.168.66.120	192.168.66.100	TCP	60	110 → 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 → 23 [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 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
49	13.119535051	192.168.66.100	192.168.66.120	TCP	54	59485 → 135 [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 → 143 [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.