S9 L3

Report esercizio “Threat Intelligence & IOC”

Giulia Salani

TRACCIA

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

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:

1. Identificare 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

REPORT

INTRODUZIONE

1. Cos'è Wireshark?

Wireshark è uno **sniffer di rete** e un analizzatore di protocollo **che consente di catturare e analizzare il traffico di rete in tempo reale**. Questo software open-source offre una visualizzazione dettagliata dei pacchetti di dati scambiati su una rete, consentendo agli utenti di esaminare protocolli, identificare problemi di rete, e analizzare comunicazioni. Wireshark supporta un'ampia gamma di protocolli e offre strumenti avanzati per l'analisi dei dati, facilitando la risoluzione dei problemi di rete e la comprensione del traffico.

2. Perché WS può essere utile per individuare IOC nel traffico di rete?

Wireshark è un potente strumento per individuare Indicatori di Compromissione (IOC) nel traffico di rete. Analizzando i pacchetti di dati scambiati, Wireshark **permette di identificare modelli di comportamento anomalo**, individuare attività sospette come attacchi di rete o comunicazioni con server di comando e controllo associati a malware. La sua capacità di esaminare dettagliatamente il traffico aiuta a **rilevare eventuali pattern che indicano compromissioni o attività malevole**. Gli analisti possono utilizzare Wireshark per monitorare e rispondere tempestivamente a minacce, migliorando la sicurezza informatica complessiva dell'ambiente di rete.

SVOLGIMENTO

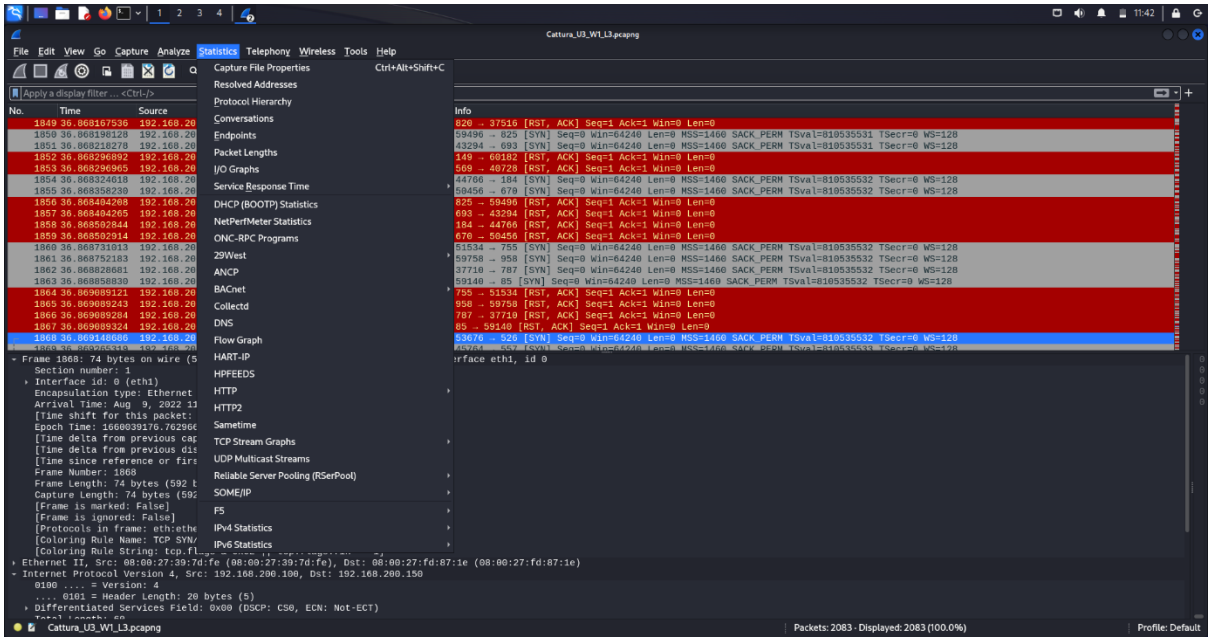
Premessa

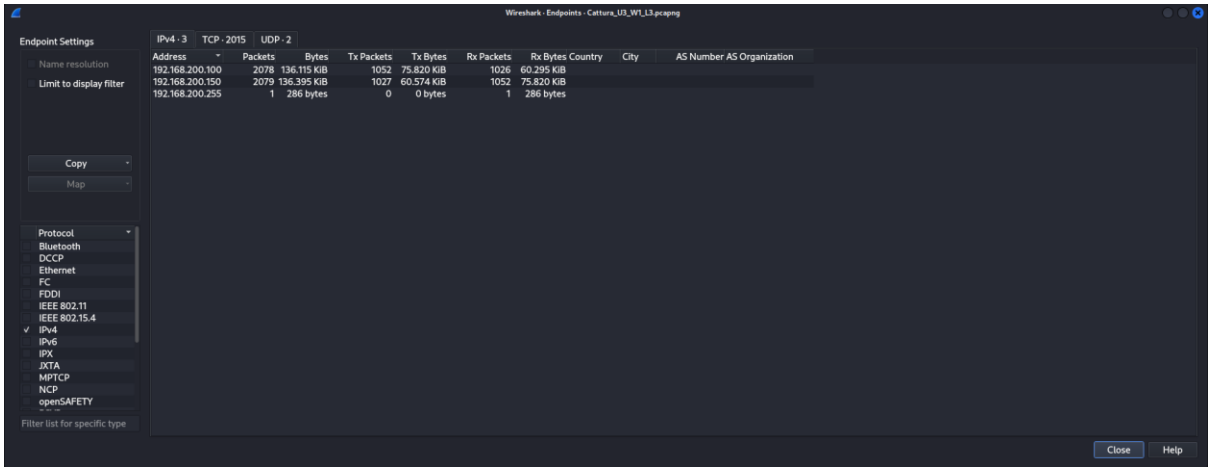
Scarichiamo la cartella zip con il file dell'intercettazione sul nostro host ed estraiamo il file. Lanciamo Kali Linux e, con un semplice drag and drop del file, trasferiamo il file dall'host alla macchina.

Apriamo il file con doppio click; il sistema lo apre in automatico con Wireshark.

Identificare eventuali IOC, ovvero evidenze di attacchi in corso

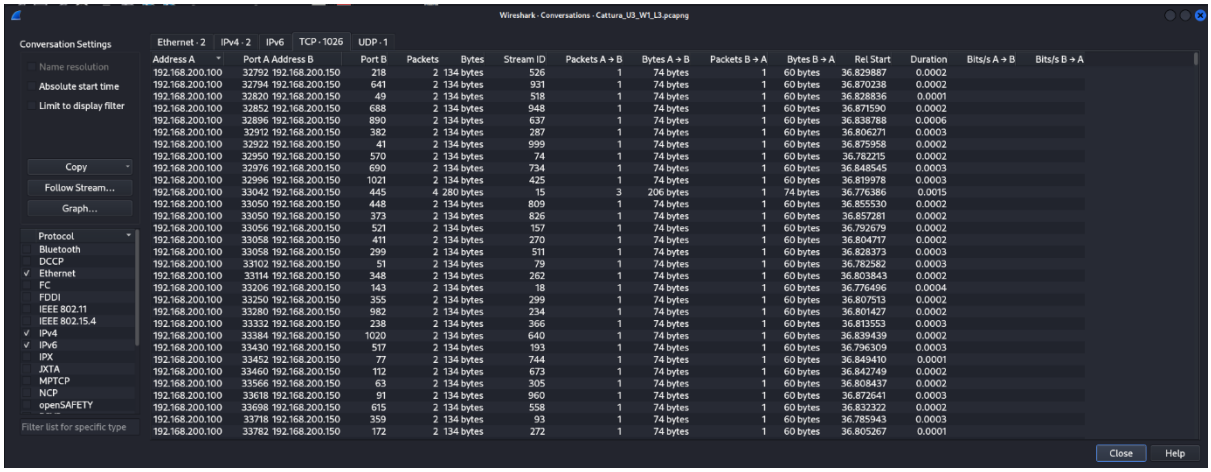
All'interno di Wireshark, nel menù in cima all'applicazione selezioniamo Statistics e Endpoints (5° riga dall'alto):





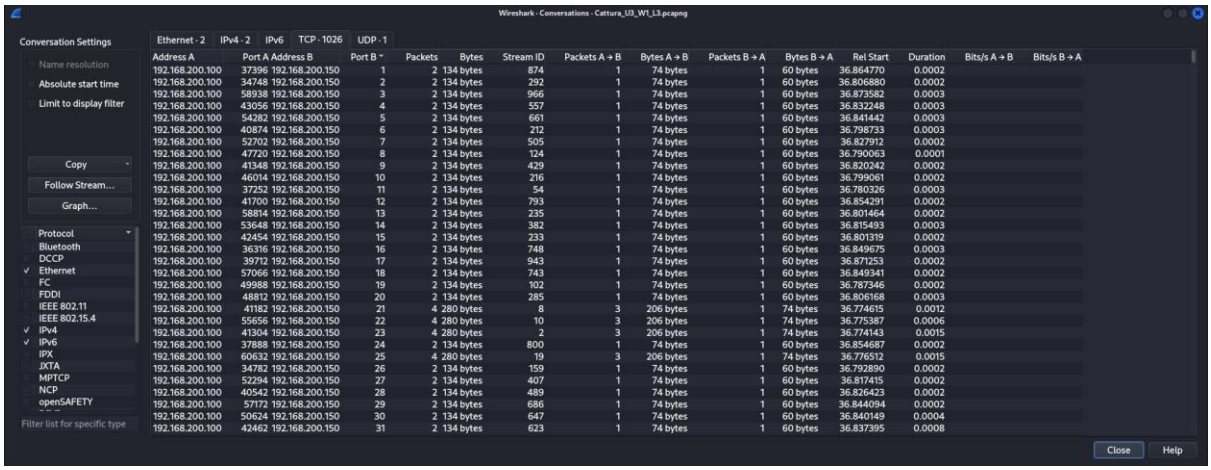
Nella prima tab, che si apre per prima di default, notiamo che vi sono tre endpoint. Studiando gli IP, ci accorgiamo subito che sono sulla stessa rete. C'è un indirizzo che termina in 255 e dunque è l'indirizzo di broadcast. Gli altri terminano rispettivamente in 100 e 150, quindi possiamo supporre appartengano a due macchine che comunicano fra loro.

Chiudiamo ora la finestra e torniamo su Statistics, questa volta però selezioniamo Conversations dove, notando che la tab TCP è quella con più entries, ci spostiamo lì:



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.200.100	32792	192.168.200.150	218	2	134 bytes	526	1	74 bytes	1	60 bytes	36.829887	0.0002		
192.168.200.100	32794	192.168.200.150	641	2	134 bytes	931	1	74 bytes	1	60 bytes	36.870238	0.0002		
192.168.200.100	32820	192.168.200.150	49	2	134 bytes	518	1	74 bytes	1	60 bytes	36.828836	0.0001		
192.168.200.100	32852	192.168.200.150	688	2	134 bytes	948	1	74 bytes	1	60 bytes	36.871590	0.0002		
192.168.200.100	32896	192.168.200.150	890	2	134 bytes	637	1	74 bytes	1	60 bytes	36.838788	0.0006		
192.168.200.100	32912	192.168.200.150	382	2	134 bytes	287	1	74 bytes	1	60 bytes	36.806271	0.0003		
192.168.200.100	32922	192.168.200.150	41	2	134 bytes	999	1	74 bytes	1	60 bytes	36.875958	0.0002		
192.168.200.100	32950	192.168.200.150	570	2	134 bytes	74	1	74 bytes	1	60 bytes	36.782215	0.0002		
192.168.200.100	32976	192.168.200.150	690	2	134 bytes	734	1	74 bytes	1	60 bytes	36.848545	0.0003		
192.168.200.100	32996	192.168.200.150	1021	2	134 bytes	425	1	74 bytes	1	60 bytes	36.819978	0.0003		
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes	1	74 bytes	36.776386	0.0015		
192.168.200.100	33050	192.168.200.150	448	2	134 bytes	809	1	74 bytes	1	60 bytes	36.855530	0.0002		
192.168.200.100	33050	192.168.200.150	373	2	134 bytes	826	1	74 bytes	1	60 bytes	36.857281	0.0002		
192.168.200.100	33056	192.168.200.150	521	2	134 bytes	157	1	74 bytes	1	60 bytes	36.792679	0.0002		
192.168.200.100	33058	192.168.200.150	411	2	134 bytes	270	1	74 bytes	1	60 bytes	36.804717	0.0002		
192.168.200.100	33058	192.168.200.150	299	2	134 bytes	511	1	74 bytes	1	60 bytes	36.828373	0.0003		
192.168.200.100	33102	192.168.200.150	51	2	134 bytes	79	1	74 bytes	1	60 bytes	36.782582	0.0003		
192.168.200.100	33114	192.168.200.150	348	2	134 bytes	262	1	74 bytes	1	60 bytes	36.803843	0.0002		
192.168.200.100	33206	192.168.200.150	143	2	134 bytes	18	1	74 bytes	1	60 bytes	36.776496	0.0004		
192.168.200.100	33250	192.168.200.150	355	2	134 bytes	299	1	74 bytes	1	60 bytes	36.807513	0.0002		
192.168.200.100	33280	192.168.200.150	982	2	134 bytes	234	1	74 bytes	1	60 bytes	36.801427	0.0002		
192.168.200.100	33332	192.168.200.150	238	2	134 bytes	366	1	74 bytes	1	60 bytes	36.813553	0.0003		
192.168.200.100	33384	192.168.200.150	1020	2	134 bytes	640	1	74 bytes	1	60 bytes	36.839439	0.0002		
192.168.200.100	33430	192.168.200.150	517	2	134 bytes	193	1	74 bytes	1	60 bytes	36.796309	0.0003		
192.168.200.100	33452	192.168.200.150	77	2	134 bytes	744	1	74 bytes	1	60 bytes	36.849410	0.0001		
192.168.200.100	33460	192.168.200.150	112	2	134 bytes	673	1	74 bytes	1	60 bytes	36.842749	0.0002		
192.168.200.100	33566	192.168.200.150	63	2	134 bytes	305	1	74 bytes	1	60 bytes	36.808437	0.0002		
192.168.200.100	33618	192.168.200.150	91	2	134 bytes	960	1	74 bytes	1	60 bytes	36.872641	0.0003		
192.168.200.100	33698	192.168.200.150	615	2	134 bytes	558	1	74 bytes	1	60 bytes	36.832322	0.0002		
192.168.200.100	33718	192.168.200.150	359	2	134 bytes	93	1	74 bytes	1	60 bytes	36.785943	0.0003		
192.168.200.100	33782	192.168.200.150	172	2	134 bytes	272	1	74 bytes	1	60 bytes	36.805267	0.0001		

Salta all'occhio che nella colonna Port B sono riportate diverse porte. Proviamo ad ordinare la colonna dall'elemento più piccolo al più grande cliccando sopra alla sua intestazione, quindi su Port B:



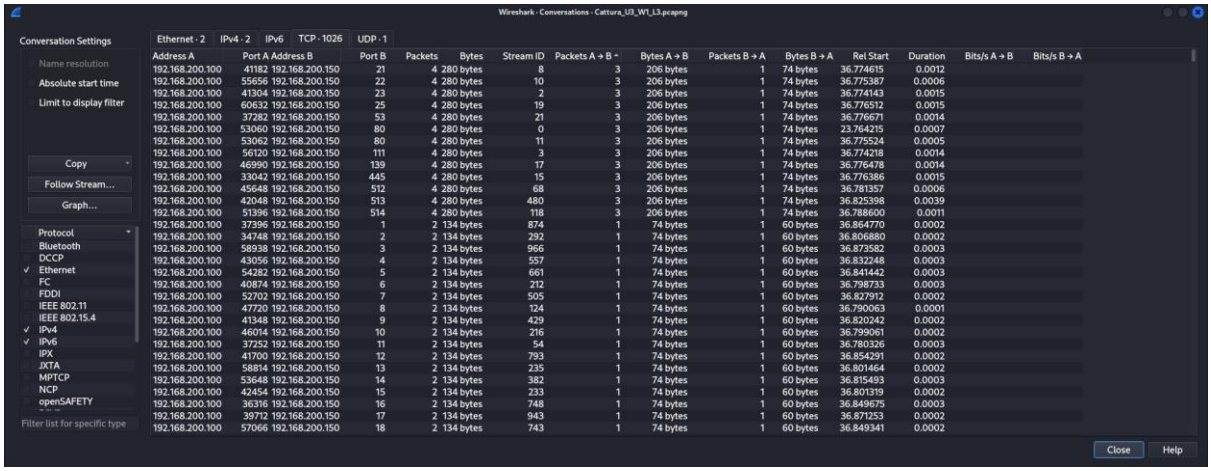
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.200.100	37396	192.168.200.150	1	2	134 bytes	874	1	74 bytes	1	60 bytes	36.864770	0.0002		
192.168.200.100	34748	192.168.200.150	2	2	134 bytes	292	1	74 bytes	1	60 bytes	36.806880	0.0002		
192.168.200.100	58938	192.168.200.150	3	2	134 bytes	966	1	74 bytes	1	60 bytes	36.873582	0.0003		
192.168.200.100	43056	192.168.200.150	4	2	134 bytes	557	1	74 bytes	1	60 bytes	36.832248	0.0003		
192.168.200.100	54282	192.168.200.150	5	2	134 bytes	661	1	74 bytes	1	60 bytes	36.841442	0.0003		
192.168.200.100	40874	192.168.200.150	6	2	134 bytes	212	1	74 bytes	1	60 bytes	36.798733	0.0003		
192.168.200.100	52702	192.168.200.150	7	2	134 bytes	505	1	74 bytes	1	60 bytes	36.827912	0.0002		
192.168.200.100	47720	192.168.200.150	8	2	134 bytes	124	1	74 bytes	1	60 bytes	36.790063	0.0001		
192.168.200.100	41348	192.168.200.150	9	2	134 bytes	429	1	74 bytes	1	60 bytes	36.820242	0.0002		
192.168.200.100	46014	192.168.200.150	10	2	134 bytes	216	1	74 bytes	1	60 bytes	36.799061	0.0002		
192.168.200.100	37252	192.168.200.150	11	2	134 bytes	54	1	74 bytes	1	60 bytes	36.780326	0.0003		
192.168.200.100	41700	192.168.200.150	12	2	134 bytes	793	1	74 bytes	1	60 bytes	36.854291	0.0002		
192.168.200.100	58814	192.168.200.150	13	2	134 bytes	235	1	74 bytes	1	60 bytes	36.801464	0.0002		
192.168.200.100	53648	192.168.200.150	14	2	134 bytes	382	1	74 bytes	1	60 bytes	36.815493	0.0003		
192.168.200.100	42454	192.168.200.150	15	2	134 bytes	233	1	74 bytes	1	60 bytes	36.801319	0.0002		
192.168.200.100	36316	192.168.200.150	16	2	134 bytes	748	1	74 bytes	1	60 bytes	36.849675	0.0003		
192.168.200.100	39712	192.168.200.150	17	2	134 bytes	943	1	74 bytes	1	60 bytes	36.871253	0.0002		
192.168.200.100	57066	192.168.200.150	18	2	134 bytes	743	1	74 bytes	1	60 bytes	36.849341	0.0002		
192.168.200.100	49988	192.168.200.150	19	2	134 bytes	102	1	74 bytes	1	60 bytes	36.787346	0.0002		
192.168.200.100	48812	192.168.200.150	20	2	134 bytes	285	1	74 bytes	1	60 bytes	36.806168	0.0003		
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes	1	74 bytes	36.774615	0.0012		
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3	206 bytes	1	74 bytes	36.775387	0.0006		
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes	36.774143	0.0015		
192.168.200.100	37888	192.168.200.150	24	2	134 bytes	800	1	74 bytes	1	60 bytes	36.854687	0.0002		
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes	1	74 bytes	36.776512	0.0015		
192.168.200.100	34782	192.168.200.150	26	2	134 bytes	159	1	74 bytes	1	60 bytes	36.792890	0.0002		
192.168.200.100	52294	192.168.200.150	27	2	134 bytes	407	1	74 bytes	1	60 bytes	36.817415	0.0002		
192.168.200.100	40542	192.168.200.150	28	2	134 bytes	489	1	74 bytes	1	60 bytes	36.826423	0.0002		
192.168.200.100	57172	192.168.200.150	29	2	134 bytes	686	1	74 bytes	1	60 bytes	36.844094	0.0002		
192.168.200.100	50624	192.168.200.150	30	2	134 bytes	647	1	74 bytes	1	60 bytes	36.840149	0.0004		
192.168.200.100	42462	192.168.200.150	31	2	134 bytes	623	1	74 bytes	1	60 bytes	36.837395	0.0008		

Qui per semplicità di fruizione riportiamo solo la prima parte della scansione, ma scorrendo l'elenco è possibile notare che sono indicate tutte le porte dalla 1 alla 1024, che sappiamo essere il numero di porte "ben note", ovvero su cui solitamente stanno in ascolto i servizi noti e ben definiti.

Questo è indice di una scansione da una macchina verso l'altra che ha interessato tutte le porte ben note per capire se fossero aperte. Sì, ma che tipo di scansione?

Spostando l'attenzione sulla colonna Packets A -> B, possiamo notare che vi sono alcune entrate dove il valore della colonna è 1 e alcune dove il valore della colonna è 3. Questo ci ricorda il three way handshake, da cui possiamo ipotizzare che le porte con 3 pacchetti fossero aperte e quelle con 1 pacchetto chiuse.

Ordiniamo gli elementi di quella colonna questa volta dal più grande al più piccolo con un doppio click; questo farà sì che in cima alla lista vi siano le entries dove i pacchetti scambiati sono 3:



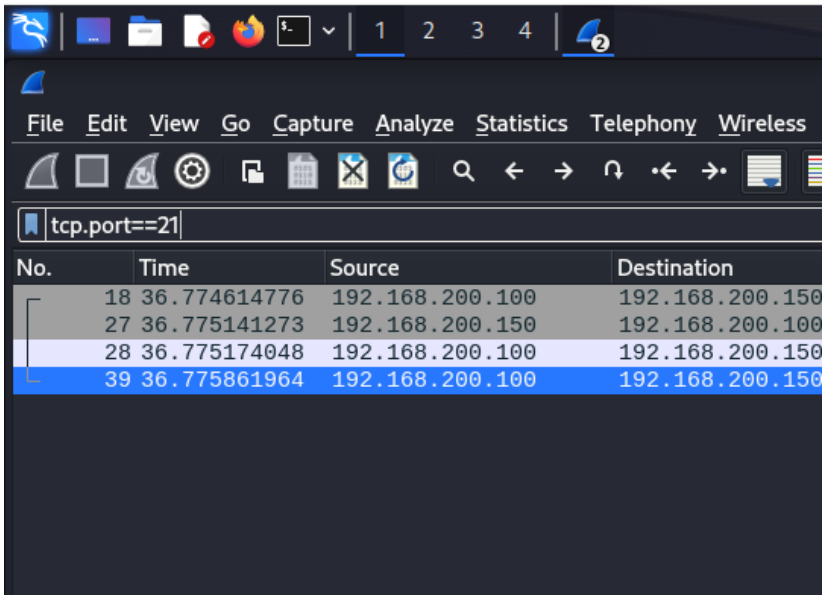
In effetti, le porte in oggetto (terza colonna) sono le porte tipicamente associate ai servizi più comuni. Solo per fare alcuni esempi non esaustivi: la porta 21 è associata al protocollo FTP (File Transfer Protocol), utilizzato per il trasferimento di file; la porta 80 è riservata al protocollo HTTP (Hypertext Transfer Protocol), comunemente utilizzato per il traffico Web non crittografato; la porta 445 è comunemente associata al protocollo SMB (Server Message Block) usato per la condivisione di file e risorse in reti Microsoft Windows.

Appuntiamoci i numeri di queste porte, torniamo alla schermata principale di Wireshark e applichiamo dei filtri che ci permettano volta per volta di selezionare solamente i pacchetti scambiati tramite le porte TCP scelte.

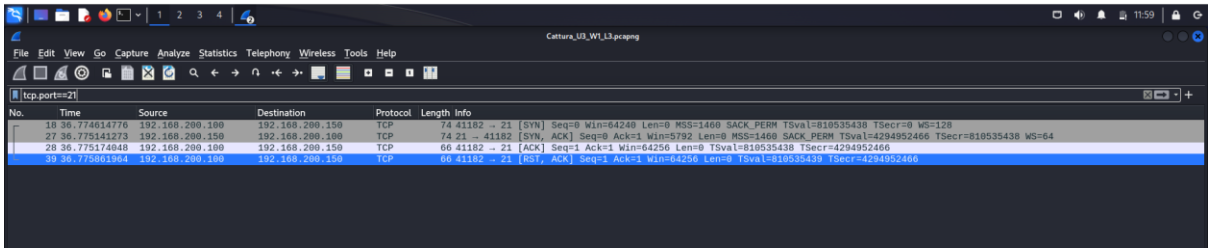
Il comando da digitare nel campo del filtro per fare questo è il seguente:

tcp.port==[numero porta]

Nel nostro caso, digitiamo: tcp.port==21:



Otteniamo questo output:



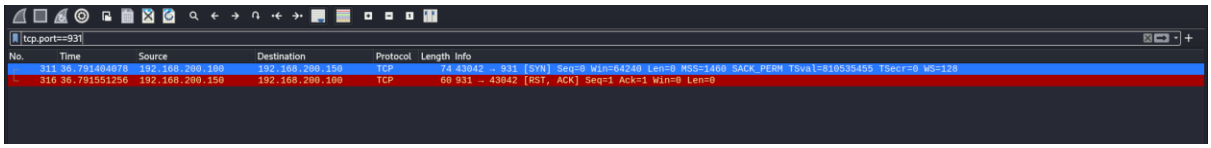
Nella colonna INFO è possibile vedere la sequenza SYN, SYN ACK, ACK, tipica di una scansione TCP con Nmap, ovvero una scansione che completa la connessione.

Nello specifico, la sequenza è la seguente:

1. 192.168.200.100 invia una richiesta SYN a 192.168.200.150 tramite la porta 80;
2. 192.168.200.150 risponde con SYN-ACK;
3. 192.168.200.100 risponde con ACK e completa la connessione;
4. 192.168.200.100 chiude la connessione con RST.

Da cui abbiamo avuto anche la conferma che 192.168.200.100 è la macchina attaccante e 192.168.200.150 è la macchina vittima.

Proviamo ora ad analizzare una porta che non riportava uno scambio di 3 pacchetti, per esempio la 931:



Vediamo che in questo caso alla richiesta SYN da parte dell'attaccante, la porta ha risposto con RST, ovvero RESET, rifiutando la connessione perché chiusa.

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

Abbiamo dedotto che:

192.168.200.100 è la macchina attaccante;
192.168.200.150 è la macchina vittima;

L'attacco è consistito in una scansione TCP, quindi completa, ragionevolmente effettuata con Nmap.

Le porte aperte sono risultate essere le seguenti: 21, 22, 23, 25, 53, 80, 111, 139, 512, 513, 514.

Consigliate un’azione per ridurre gli impatti dell’attacco

Per evitare che un attaccante possa effettuare una scansione Nmap sulla propria macchina, è consigliabile configurare un Firewall che rifiuti tutte le richieste provenienti da IP che non sono in Whitelist.