

Report Threat Intelligence & IOC

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:

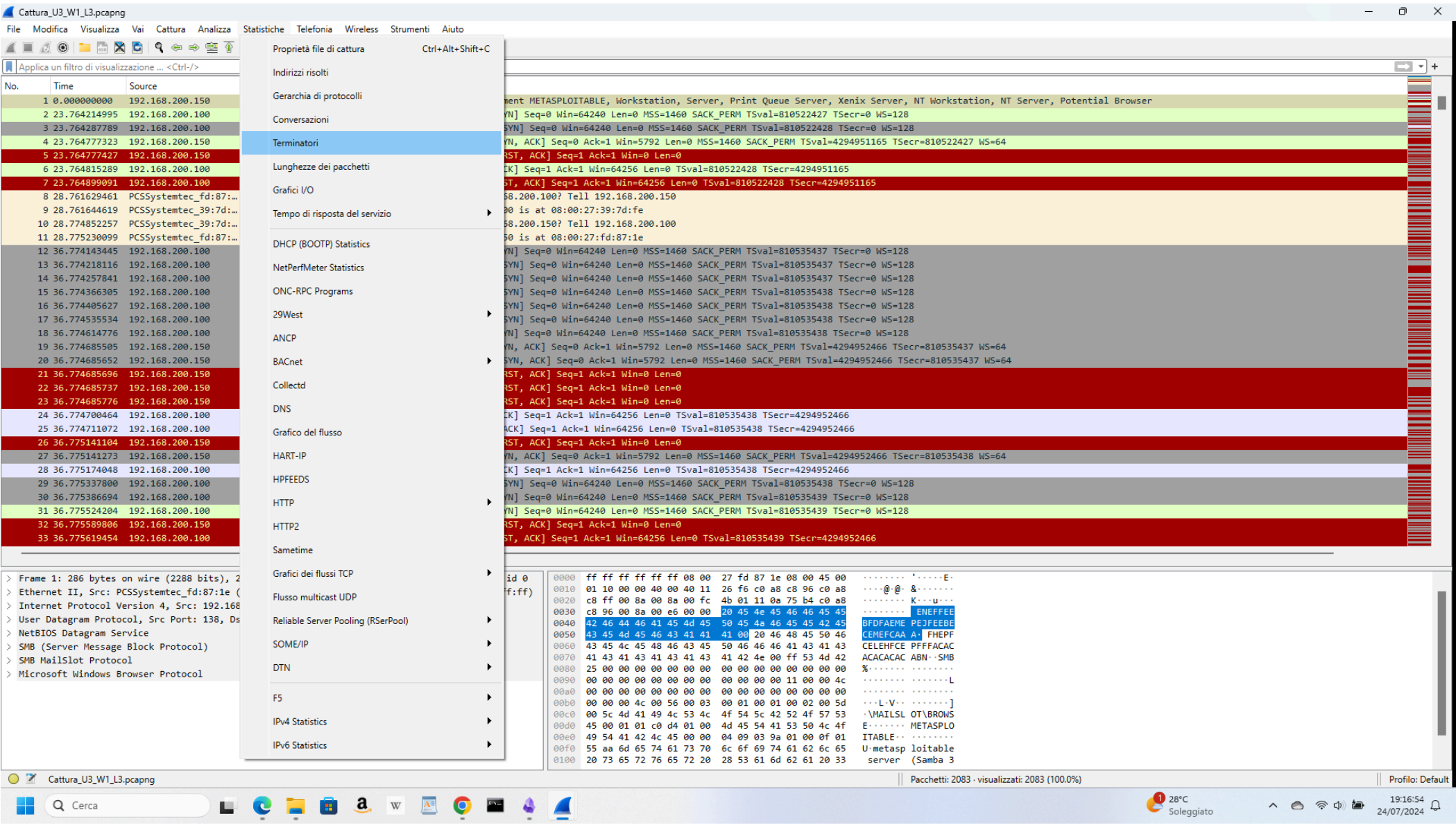
- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un’azione per ridurre gli impatti dell’attacco

Che cos’è WireShark e come può essere utile per individuare IOC nel traffico di rete

Wireshark è un analizzatore di protocollo di rete open-source che consente di catturare e analizzare il traffico di rete in tempo reale ed è un potente strumento per individuare **Indicatori di Compromissione (IOC)** nel traffico di rete. Infatti, 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.

Identificazione di IOC e potenziali vettori di attacco utilizzati

All'interno di Wireshark, nel menù in cima all'applicazione selezioniamo **Statistiche** e poi **Terminatori** e come si può ben notare vi sono tre endpoint. Visionando attentamente gli indirizzi IP presenti, ci accorgiamo subito che sono sulla stessa rete dove troviamo un indirizzo che termina in 255 e dunque è l’indirizzo di broadcast e gli altri terminano rispettivamente in 100 e 150, quindi possiamo supporre appartengano a due macchine comunicanti fra loro.



Spostandoci successivamente su Statistiche e selezionando conversazioni è possibile notare che la tab TCP è quella con più entries e di conseguenza ci spostiamo lì

Wireshark - Conversazioni - Cattura_U3_W1_L3.pcapng

Conversation Settings

☐ Risoluzione dei nomi

☐ Ora iniziale assoluta

☒ Limita al filtro di visualizzazione

Copia

Segui il flusso...

Grafico...

Protocollo

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☒ TCP

☐ Token-Ring

☒ UDP

☐ USB

☐ Zircon

Elenco di filtri per specifico tipo

Ethernet · 2IPv4 · 2IPv6TCP · 1026UDP · 1

Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Pacchetti totali	Percentuale filtrati	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B	Bits/s B → A
192.168.200.100	32792	192.168.200.150	218	2	134 byte	526	2	100.00%	1	74 byte	1	60 byte	36.829887	0.0002		
192.168.200.100	32794	192.168.200.150	641	2	134 byte	931	2	100.00%	1	74 byte	1	60 byte	36.870238	0.0002		
192.168.200.100	32820	192.168.200.150	49	2	134 byte	518	2	100.00%	1	74 byte	1	60 byte	36.828836	0.0001		
192.168.200.100	32852	192.168.200.150	688	2	134 byte	948	2	100.00%	1	74 byte	1	60 byte	36.871590	0.0002		
192.168.200.100	32896	192.168.200.150	890	2	134 byte	637	2	100.00%	1	74 byte	1	60 byte	36.838788	0.0006		
192.168.200.100	32912	192.168.200.150	382	2	134 byte	287	2	100.00%	1	74 byte	1	60 byte	36.806271	0.0003		
192.168.200.100	32922	192.168.200.150	41	2	134 byte	999	2	100.00%	1	74 byte	1	60 byte	36.875958	0.0002		
192.168.200.100	32950	192.168.200.150	570	2	134 byte	74	2	100.00%	1	74 byte	1	60 byte	36.782215	0.0002		
192.168.200.100	32976	192.168.200.150	690	2	134 byte	734	2	100.00%	1	74 byte	1	60 byte	36.848545	0.0003		
192.168.200.100	32996	192.168.200.150	1021	2	134 byte	425	2	100.00%	1	74 byte	1	60 byte	36.819978	0.0003		
192.168.200.100	33042	192.168.200.150	445	4	280 byte	15	4	100.00%	3	206 byte	1	74 byte	36.776386	0.0015		
192.168.200.100	33050	192.168.200.150	448	2	134 byte	809	2	100.00%	1	74 byte	1	60 byte	36.855530	0.0002		
192.168.200.100	33050	192.168.200.150	373	2	134 byte	826	2	100.00%	1	74 byte	1	60 byte	36.857281	0.0002		
192.168.200.100	33056	192.168.200.150	521	2	134 byte	157	2	100.00%	1	74 byte	1	60 byte	36.792679	0.0002		
192.168.200.100	33058	192.168.200.150	411	2	134 byte	270	2	100.00%	1	74 byte	1	60 byte	36.804717	0.0002		
192.168.200.100	33058	192.168.200.150	299	2	134 byte	511	2	100.00%	1	74 byte	1	60 byte	36.828373	0.0003		
192.168.200.100	33102	192.168.200.150	51	2	134 byte	79	2	100.00%	1	74 byte	1	60 byte	36.782582	0.0003		
192.168.200.100	33114	192.168.200.150	348	2	134 byte	262	2	100.00%	1	74 byte	1	60 byte	36.803843	0.0002		
192.168.200.100	33206	192.168.200.150	143	2	134 byte	18	2	100.00%	1	74 byte	1	60 byte	36.776496	0.0004		
192.168.200.100	33250	192.168.200.150	355	2	134 byte	299	2	100.00%	1	74 byte	1	60 byte	36.807513	0.0002		
192.168.200.100	33280	192.168.200.150	982	2	134 byte	234	2	100.00%	1	74 byte	1	60 byte	36.801427	0.0002		
192.168.200.100	33332	192.168.200.150	238	2	134 byte	366	2	100.00%	1	74 byte	1	60 byte	36.813553	0.0003		
192.168.200.100	33384	192.168.200.150	1020	2	134 byte	640	2	100.00%	1	74 byte	1	60 byte	36.839439	0.0002		
192.168.200.100	33430	192.168.200.150	517	2	134 byte	193	2	100.00%	1	74 byte	1	60 byte	36.796309	0.0003		
192.168.200.100	33452	192.168.200.150	77	2	134 byte	744	2	100.00%	1	74 byte	1	60 byte	36.849410	0.0001		
192.168.200.100	33460	192.168.200.150	112	2	134 byte	673	2	100.00%	1	74 byte	1	60 byte	36.842749	0.0002		
192.168.200.100	33566	192.168.200.150	63	2	134 byte	305	2	100.00%	1	74 byte	1	60 byte	36.808437	0.0002		
192.168.200.100	33618	192.168.200.150	91	2	134 byte	960	2	100.00%	1	74 byte	1	60 byte	36.872641	0.0003		
192.168.200.100	33698	192.168.200.150	615	2	134 byte	558	2	100.00%	1	74 byte	1	60 byte	36.832322	0.0002		
192.168.200.100	33718	192.168.200.150	359	2	134 byte	93	2	100.00%	1	74 byte	1	60 byte	36.785943	0.0003		
192.168.200.100	33782	192.168.200.150	172	2	134 byte	272	2	100.00%	1	74 byte	1	60 byte	36.805267	0.0001		
192.168.200.100	33876	192.168.200.150	443	2	134 byte	1	2	100.00%	1	74 byte	1	60 byte	23.764288	0.0005		
192.168.200.100	33878	192.168.200.150	443	2	134 byte	4	2	100.00%	1	74 byte	1	60 byte	36.774258	0.0004		
192.168.200.100	33884	192.168.200.150	408	2	134 byte	620	2	100.00%	1	74 byte	1	60 byte	36.837045	0.0011		
192.168.200.100	33896	192.168.200.150	763	2	134 byte	149	2	100.00%	1	74 byte	1	60 byte	36.791996	0.0002		
192.168.200.100	33900	192.168.200.150	714	2	134 byte	757	2	100.00%	1	74 byte	1	60 byte	36.850222	0.0007		
192.168.200.100	33910	192.168.200.150	511	2	134 byte	222	2	100.00%	1	74 byte	1	60 byte	36.800059	0.0003		
192.168.200.100	33948	192.168.200.150	390	2	134 byte	957	2	100.00%	1	74 byte	1	60 byte	36.872281	0.0002		
192.168.200.100	33950	192.168.200.150	720	2	134 byte	937	2	100.00%	1	74 byte	1	60 byte	36.870868	0.0001		
192.168.200.100	33994	192.168.200.150	620	2	134 byte	961	2	100.00%	1	74 byte	1	60 byte	36.872660	0.0003		
192.168.200.100	34004	192.168.200.150	528	2	134 byte	203	2	100.00%	1	74 byte	1	60 byte	36.797483	0.0003		
192.168.200.100	34022	192.168.200.150	843	2	134 byte	718	2	100.00%	1	74 byte	1	60 byte	36.847269	0.0002		
192.168.200.100	34024	192.168.200.150	833	2	134 byte	395	2	100.00%	1	74 byte	1	60 byte	36.816349	0.0002		
192.168.200.100	34030	192.168.200.150	1005	2	134 byte	843	2	100.00%	1	74 byte	1	60 byte	36.861458	0.0004		
192.168.200.100	34064	192.168.200.150	96	2	134 byte	421	2	100.00%	1	74 byte	1	60 byte	36.819024	0.0006		
192.168.200.100	34094	192.168.200.150	645	2	134 byte	662	2	100.00%	1	74 byte	1	60 byte	36.841512	0.0003		
192.168.200.100	34120	192.168.200.150	98	2	134 byte	26	2	100.00%	1	74 byte	1	60 byte	36.777303	0.0003		
192.168.200.100	34130	192.168.200.150	230	2	134 byte	979	2	100.00%	1	74 byte	1	60 byte	36.874531	0.0002		
192.168.200.100	34180	192.168.200.150	666	2	134 byte	934	2	100.00%	1	74 byte	1	60 byte	36.870574	0.0002		
192.168.200.100	34182	192.168.200.150	177	2	134 byte	326	2	100.00%	1	74 byte	1	60 byte	36.810645	0.0002		

Chiudi

Aiuto

Cerca

30°C

Soleggiato

20:01:41

24/07/2024

Soffermmandoci in particolar modo sulla colonna "**Porta B**" e cliccando su di essa per ordinare le porte, è possibile notare come siano 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 effettuata molto probabilmente tramite "**Nmap**", un tool comunemente usato per identificare le porte aperte e i servizi attivi su un computer in una rete. In particolar modo, analizzando il caso specifico, si rileva che le richieste TCP provengono dalla macchina con IP 192.168.200.100 e sono dirette verso diverse porte dell'host con IP 192.168.200.150

Wiresark - Conversations - Cattura_U3_W1_L3 pcapng

Conversation Settings

☐ Risoluzione dei nomi

☐ Ora iniziale assoluta

☒ Limita al filtro di visualizzazione

Copia

Segui il flusso...

Grafico...

Protocollo

☐ Bluetooth

☐ BPV7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☒ TCP

☐ Token-Ring

☐ UDP

☐ USB

☐ ZinRee

Elenco di filtri per specifico tipo

Ethernet - 2

IPv4 - 2

IPv6

TCP - 1026

UDP - 1

Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Pacchetti totali	Percentuale filtrati	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B	Bits/s B → A
192.168.200.100	37396	192.168.200.150	1	2	134 byte	874	2	100.00%	1	74 byte	1	60 byte	36.864770	0.0002		
192.168.200.100	34748	192.168.200.150	2	2	134 byte	292	2	100.00%	1	74 byte	1	60 byte	36.806880	0.0002		
192.168.200.100	58938	192.168.200.150	3	2	134 byte	966	2	100.00%	1	74 byte	1	60 byte	36.873582	0.0003		
192.168.200.100	43056	192.168.200.150	4	2	134 byte	557	2	100.00%	1	74 byte	1	60 byte	36.832248	0.0003		
192.168.200.100	54282	192.168.200.150	5	2	134 byte	661	2	100.00%	1	74 byte	1	60 byte	36.841442	0.0003		
192.168.200.100	40874	192.168.200.150	6	2	134 byte	212	2	100.00%	1	74 byte	1	60 byte	36.798733	0.0003		
192.168.200.100	52702	192.168.200.150	7	2	134 byte	505	2	100.00%	1	74 byte	1	60 byte	36.827912	0.0002		
192.168.200.100	47720	192.168.200.150	8	2	134 byte	124	2	100.00%	1	74 byte	1	60 byte	36.790063	0.0001		
192.168.200.100	41348	192.168.200.150	9	2	134 byte	429	2	100.00%	1	74 byte	1	60 byte	36.820242	0.0002		
192.168.200.100	46014	192.168.200.150	10	2	134 byte	216	2	100.00%	1	74 byte	1	60 byte	36.799061	0.0002		
192.168.200.100	37252	192.168.200.150	11	2	134 byte	54	2	100.00%	1	74 byte	1	60 byte	36.780326	0.0003		
192.168.200.100	41700	192.168.200.150	12	2	134 byte	793	2	100.00%	1	74 byte	1	60 byte	36.854291	0.0002		
192.168.200.100	58814	192.168.200.150	13	2	134 byte	235	2	100.00%	1	74 byte	1	60 byte	36.801464	0.0002		
192.168.200.100	53648	192.168.200.150	14	2	134 byte	382	2	100.00%	1	74 byte	1	60 byte	36.815493	0.0003		
192.168.200.100	42454	192.168.200.150	15	2	134 byte	233	2	100.00%	1	74 byte	1	60 byte	36.801319	0.0002		
192.168.200.100	36316	192.168.200.150	16	2	134 byte	748	2	100.00%	1	74 byte	1	60 byte	36.849675	0.0003		
192.168.200.100	39712	192.168.200.150	17	2	134 byte	943	2	100.00%	1	74 byte	1	60 byte	36.871253	0.0002		
192.168.200.100	57066	192.168.200.150	18	2	134 byte	743	2	100.00%	1	74 byte	1	60 byte	36.849341	0.0002		
192.168.200.100	49988	192.168.200.150	19	2	134 byte	102	2	100.00%	1	74 byte	1	60 byte	36.787346	0.0002		
192.168.200.100	48812	192.168.200.150	20	2	134 byte	285	2	100.00%	1	74 byte	1	60 byte	36.806168	0.0003		
192.168.200.100	41182	192.168.200.150	21	4	280 byte	8	4	100.00%	3	206 byte	1	74 byte	36.774615	0.0012		
192.168.200.100	55656	192.168.200.150	22	4	280 byte	10	4	100.00%	3	206 byte	1	74 byte	36.775387	0.0006		
192.168.200.100	41304	192.168.200.150	23	4	280 byte	2	4	100.00%	3	206 byte	1	74 byte	36.774143	0.0015		
192.168.200.100	37888	192.168.200.150	24	2	134 byte	800	2	100.00%	1	74 byte	1	60 byte	36.854687	0.0002		
192.168.200.100	60632	192.168.200.150	25	4	280 byte	19	4	100.00%	3	206 byte	1	74 byte	36.776512	0.0015		
192.168.200.100	34782	192.168.200.150	26	2	134 byte	159	2	100.00%	1	74 byte	1	60 byte	36.792890	0.0002		
192.168.200.100	52294	192.168.200.150	27	2	134 byte	407	2	100.00%	1	74 byte	1	60 byte	36.817415	0.0002		
192.168.200.100	40542	192.168.200.150	28	2	134 byte	489	2	100.00%	1	74 byte	1	60 byte	36.826423	0.0002		
192.168.200.100	57172	192.168.200.150	29	2	134 byte	686	2	100.00%	1	74 byte	1	60 byte	36.844094	0.0002		
192.168.200.100	50624	192.168.200.150	30	2	134 byte	647	2	100.00%	1	74 byte	1	60 byte	36.840149	0.0004		
192.168.200.100	42462	192.168.200.150	31	2	134 byte	623	2	100.00%	1	74 byte	1	60 byte	36.837395	0.0008		
192.168.200.100	58262	192.168.200.150	32	2	134 byte	173	2	100.00%	1	74 byte	1	60 byte	36.794491	0.0003		
192.168.200.100	40194	192.168.200.150	33	2	134 byte	981	2	100.00%	1	74 byte	1	60 byte	36.874668	0.0002		
192.168.200.100	41062	192.168.200.150	34	2	134 byte	841	2	100.00%	1	74 byte	1	60 byte	36.861335	0.0002		
192.168.200.100	37230	192.168.200.150	35	2	134 byte	278	2	100.00%	1	74 byte	1	60 byte	36.805714	0.0002		
192.168.200.100	47180	192.168.200.150	36	2	134 byte	309	2	100.00%	1	74 byte	1	60 byte	36.808661	0.0007		
192.168.200.100	42742	192.168.200.150	37	2	134 byte	597	2	100.00%	1	74 byte	1	60 byte	36.835560	0.0025		
192.168.200.100	47896	192.168.200.150	38	2	134 byte	845	2	100.00%	1	74 byte	1	60 byte	36.861585	0.0002		
192.168.200.100	34288	192.168.200.150	39	2	134 byte	141	2	100.00%	1	74 byte	1	60 byte	36.791383	0.0002		
192.168.200.100	60640	192.168.200.150	40	2	134 byte	1024	2	100.00%	1	74 byte	1	60 byte	36.878560	0.0002		
192.168.200.100	32922	192.168.200.150	41	2	134 byte	999	2	100.00%	1	74 byte	1	60 byte	36.875958	0.0002		
192.168.200.100	40522	192.168.200.150	42	2	134 byte	51	2	100.00%	1	74 byte	1	60 byte	36.779946	0.0003		
192.168.200.100	58382	192.168.200.150	43	2	134 byte	198	2	100.00%	1	74 byte	1	60 byte	36.796827	0.0002		
192.168.200.100	58846	192.168.200.150	44	2	134 byte	232	2	100.00%	1	74 byte	1	60 byte	36.801297	0.0002		
192.168.200.100	54666	192.168.200.150	45	2	134 byte	275	2	100.00%	1	74 byte	1	60 byte	36.805354	0.0003		
192.168.200.100	50164	192.168.200.150	46	2	134 byte	497	2	100.00%	1	74 byte	1	60 byte	36.827121	0.0001		
192.168.200.100	55426	192.168.200.150	47	2	134 byte	986	2	100.00%	1	74 byte	1	60 byte	36.874980	0.0002		
192.168.200.100	36060	192.168.200.150	48	2	134 byte	591	2	100.00%	1	74 byte	1	60 byte	36.835168	0.0028		
192.168.200.100	32820	192.168.200.150	49	2	134 byte	518	2	100.00%	1	74 byte	1	60 byte	36.828836	0.0001		
192.168.200.100	37744	192.168.200.150	50	2	134 byte	825	2	100.00%	1	74 byte	1	60 byte	36.857113	0.0004		

Chiedi

Aiuto

<

Wireshark - Conversations - Cattura_U3_W1_L3.pcapng

Conversation Settings

☐ Risoluzione dei nomi

☐ Ora iniziale assoluta

☒ Limita al filtro di visualizzazio

Copia

Segui il flusso...

Grafico...

Protocollo

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☒ TCP

☐ Token-Ring

☒ UDP

☐ USB

☒ ZinRee

Elenco di filtri per specifico tipo

Ethernet - 2		IPv4 - 2		IPv6	TCP - 1026		UDP - 1											
Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Pacchetti totali	Percentuale filtrati	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B	Bits/s B → A		
192.168.200.100	37738	192.168.200.150	1024	2	134 byte	404	2	100.00%	1	74 byte	1	60 byte	36.817332	0.0003				
192.168.200.100	59292	192.168.200.150	1023	2	134 byte	463	2	100.00%	1	74 byte	1	60 byte	36.823536	0.0003				
192.168.200.100	38352	192.168.200.150	1022	2	134 byte	594	2	100.00%	1	74 byte	1	60 byte	36.835363	0.0026				
192.168.200.100	32996	192.168.200.150	1021	2	134 byte	425	2	100.00%	1	74 byte	1	60 byte	36.819978	0.0003				
192.168.200.100	33384	192.168.200.150	1020	2	134 byte	640	2	100.00%	1	74 byte	1	60 byte	36.839439	0.0002				
192.168.200.100	40832	192.168.200.150	1019	2	134 byte	195	2	100.00%	1	74 byte	1	60 byte	36.796479	0.0001				
192.168.200.100	57032	192.168.200.150	1018	2	134 byte	751	2	100.00%	1	74 byte	1	60 byte	36.849909	0.0001				
192.168.200.100	36474	192.168.200.150	1017	2	134 byte	1017	2	100.00%	1	74 byte	1	60 byte	36.878092	0.0002				
192.168.200.100	39078	192.168.200.150	1016	2	134 byte	273	2	100.00%	1	74 byte	1	60 byte	36.805289	0.0001				
192.168.200.100	44580	192.168.200.150	1015	2	134 byte	260	2	100.00%	1	74 byte	1	60 byte	36.803593	0.0001				
192.168.200.100	42700	192.168.200.150	1014	2	134 byte	66	2	100.00%	1	74 byte	1	60 byte	36.781160	0.0001				
192.168.200.100	43698	192.168.200.150	1013	2	134 byte	615	2	100.00%	1	74 byte	1	60 byte	36.836725	0.0014				
192.168.200.100	53308	192.168.200.150	1012	2	134 byte	895	2	100.00%	1	74 byte	1	60 byte	36.866735	0.0003				
192.168.200.100	48408	192.168.200.150	1011	2	134 byte	860	2	100.00%	1	74 byte	1	60 byte	36.862758	0.0008				
192.168.200.100	47100	192.168.200.150	1010	2	134 byte	579	2	100.00%	1	74 byte	1	60 byte	36.834310	0.0002				
192.168.200.100	38350	192.168.200.150	1009	2	134 byte	555	2	100.00%	1	74 byte	1	60 byte	36.832152	0.0001				
192.168.200.100	56076	192.168.200.150	1008	2	134 byte	379	2	100.00%	1	74 byte	1	60 byte	36.815148	0.0003				
192.168.200.100	42420	192.168.200.150	1007	2	134 byte	35	2	100.00%	1	74 byte	1	60 byte	36.778483	0.0002				
192.168.200.100	50708	192.168.200.150	1006	2	134 byte	176	2	100.00%	1	74 byte	1	60 byte	36.794714	0.0002				
192.168.200.100	34030	192.168.200.150	1005	2	134 byte	843	2	100.00%	1	74 byte	1	60 byte	36.861458	0.0004				
192.168.200.100	38430	192.168.200.150	1004	2	134 byte	177	2	100.00%	1	74 byte	1	60 byte	36.794959	0.0003				
192.168.200.100	50686	192.168.200.150	1003	2	134 byte	521	2	100.00%	1	74 byte	1	60 byte	36.829027	0.0002				
192.168.200.100	44018	192.168.200.150	1002	2	134 byte	933	2	100.00%	1	74 byte	1	60 byte	36.870480	0.0002				
192.168.200.100	48512	192.168.200.150	1001	2	134 byte	402	2	100.00%	1	74 byte	1	60 byte	36.817062	0.0002				
192.168.200.100	47044	192.168.200.150	1000	2	134 byte	651	2	100.00%	1	74 byte	1	60 byte	36.840590	0.0003				
192.168.200.100	52136	192.168.200.150	999	2	134 byte	58	2	100.00%	1	74 byte	1	60 byte	36.780473	0.0001				
192.168.200.100	42016	192.168.200.150	998	2	134 byte	775	2	100.00%	1	74 byte	1	60 byte	36.852296	0.0002				
192.168.200.100	46014	192.168.200.150	997	2	134 byte	301	2	100.00%	1	74 byte	1	60 byte	36.807616	0.0002				
192.168.200.100	54302	192.168.200.150	996	2	134 byte	789	2	100.00%	1	74 byte	1	60 byte	36.853818	0.0002				
192.168.200.100	54220	192.168.200.150	995	2	134 byte	13	2	100.00%	1	74 byte	1	60 byte	36.776234	0.0002				
192.168.200.100	53502	192.168.200.150	994	2	134 byte	706	2	100.00%	1	74 byte	1	60 byte	36.845839	0.0002				
192.168.200.100	46138	192.168.200.150	993	2	134 byte	7	2	100.00%	1	74 byte	1	60 byte	36.774536	0.0006				
192.168.200.100	50072	192.168.200.150	992	2	134 byte	314	2	100.00%	1	74 byte	1	60 byte	36.808923	0.0005				
192.168.200.100	47332	192.168.200.150	991	2	134 byte	202	2	100.00%	1	74 byte	1	60 byte	36.797267	0.0001				
192.168.200.100	35934	192.168.200.150	990	2	134 byte	818	2	100.00%	1	74 byte	1	60 byte	36.856563	0.0001				
192.168.200.100	60578	192.168.200.150	989	2	134 byte	802	2	100.00%	1	74 byte	1	60 byte	36.854971	0.0003				
192.168.200.100	52470	192.168.200.150	988	2	134 byte	391	2	100.00%	1	74 byte	1	60 byte	36.816046	0.0002				
192.168.200.100	40816	192.168.200.150	987	2	134 byte	383	2	100.00%	1	74 byte	1	60 byte	36.815525	0.0002				
192.168.200.100	40772	192.168.200.150	986	2	134 byte	890	2	100.00%	1	74 byte	1	60 byte	36.866250	0.0002				
192.168.200.100	52668	192.168.200.150	985	2	134 byte	886	2	100.00%	1	74 byte	1	60 byte	36.866067	0.0001				
192.168.200.100	45286	192.168.200.150	984	2	134 byte	353	2	100.00%	1	74 byte	1	60 byte	36.812653	0.0001				
192.168.200.100	35486	192.168.200.150	983	2	134 byte	495	2	100.00%	1	74 byte	1	60 byte	36.827054	0.0001				
192.168.200.100	33280	192.168.200.150	982	2	134 byte	234	2	100.00%	1	74 byte	1	60 byte	36.801427	0.0002				
192.168.200.100	51436	192.168.200.150	981	2	134 byte	240	2	100.00%	1	74 byte	1	60 byte	36.801815	0.0005				
192.168.200.100	45816	192.168.200.150	980	2	134 byte	245	2	100.00%	1	74 byte	1	60 byte	36.802264	0.0002				
192.168.200.100	50906	192.168.200.150	979	2	134 byte	552	2	100.00%	1	74 byte	1	60 byte	36.831902	0.0002				
192.168.200.100	37560	192.168.200.150	978	2	134 byte	125	2	100.00%	1	74 byte	1	60 byte	36.790171	0.0002				
192.168.200.100	34346	192.168.200.150	977	2	134 byte	228	2	100.00%	1	74 byte	1	60 byte	36.800807	0.0002				
192.168.200.100	43870	192.168.200.150	976	2	134 byte	471	2	100.00%	1	74 byte	1	60 byte	36.824295	0.0001				
192.168.200.100	38366	192.168.200.150	975	2	134 byte	134	2	100.00%	1	74 byte	1	60 byte	36.790770	0.0003				

Strumento di cattura

Screenshot copiato negli Appunti e salvato

Seleziona qui per contrassegnare e condividere.

A questo punto, spostandoci sulla colonna **Packets A -> B** e ordinando la colonna dal più grande al più piccolo, possiamo notare come vi siano alcune entrate dove il valore della colonna è 3 e altre dove il valore della colonna è 1. Questo ci ricorda il **three way handshake**, da cui è possibile supporre che la scansione specifica utilizzata sia stata un TCP Connect Scan, indicato dall'opzione -sT in Nmap. Questo tipo di scansione, come dicevamo in precedenza, si avvale del completo three-way handshake, un processo fondamentale nel protocollo TCP, per stabilire una connessione. Il three-way handshake consiste in tre fasi: **SYN** (synchronize), **SYN-ACK** (synchronizeacknowledge), e **ACK** (acknowledge). Quando una porta è aperta, il target risponde con un SYN-ACK dopo aver ricevuto un SYN, e la scansione completa il processo inviando un ACK. Questo è diverso dal SYN Scan (opzione -sS in nmap), che non completa il three-way handshake e si limita a inviare un pacchetto RST (reset) dopo aver ricevuto il SYN-ACK, riducendo così la visibilità della scansione. Di conseguenza, è possibile ipotizzare che le porte con 3 pacchetti fossero aperte e quelle con 1 pacchetto chiuse.

Wireshark - Conversations - Cattura_U3_W1_L3.pcapng

Conversation Settings

☐ Risoluzione dei nomi

☐ Ora iniziale assoluta

☒ Limita al filtro di visualizzazio

Copia

Segui il flusso...

Grafico...

Protocollo

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☒ TCP

☐ Token-Ring

☒ UDP

☐ USB

☒ ZinRee

Elenco di filtri per specifico tipo

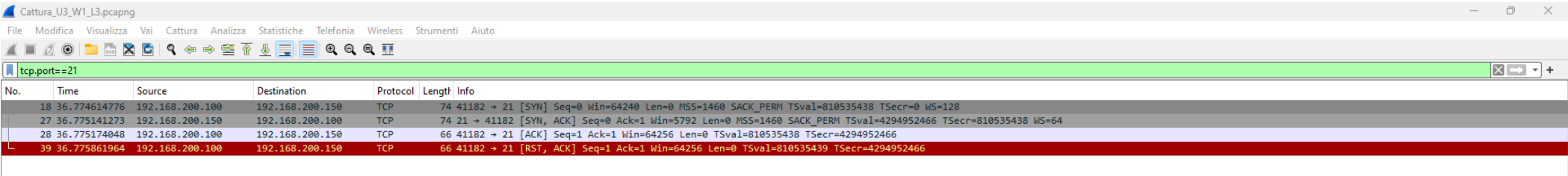
Ethernet - 2		IPv4 - 2		IPv6	TCP - 1026		UDP - 1											
Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Pacchetti totali	Percentuale filtrati	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B	Bits/s B → A		
192.168.200.100	41182	192.168.200.150	21	4	280 byte	8	4	100.00%	3	206 byte	1	74 byte	36.774615	0.0012				
192.168.200.100	55656	192.168.200.150	22	4	280 byte	10	4	100.00%	3	206 byte	1	74 byte	36.775387	0.0006				
192.168.200.100	41304	192.168.200.150	23	4	280 byte	2	4	100.00%	3	206 byte	1	74 byte	36.774143	0.0015				
192.168.200.100	60632	192.168.200.150	25	4	280 byte	19	4	100.00%	3	206 byte	1	74 byte	36.776512	0.0015				
192.168.200.100	37282	192.168.200.150	53	4	280 byte	21	4	100.00%	3	206 byte	1	74 byte	36.776671	0.0014				
192.168.200.100	53060	192.168.200.150	80	4	280 byte	0	4	100.00%	3	206 byte	1	74 byte	23.764215	0.0007				
192.168.200.100	53062	192.168.200.150	80	4	280 byte	11	4	100.00%	3	206 byte	1	74 byte	36.775524	0.0005				
192.168.200.100	56120	192.168.200.150	111	4	280 byte	3	4	100.00%	3	206 byte	1	74 byte	36.774218	0.0014				
192.168.200.100	46990	192.168.200.150	139	4	280 byte	17	4	100.00%	3	206 byte	1	74 byte	36.776478	0.0014				
192.168.200.100	33042	192.168.200.150	445	4	280 byte	15	4	100.00%	3	206 byte	1	74 byte	36.776386	0.0015				
192.168.200.100	45648	192.168.200.150	512	4	280 byte	68	4	100.00%	3	206 byte	1	74 byte	36.781357	0.0006				
192.168.200.100	42048	192.168.200.150	513	4	280 byte	480	4	100.00%	3	206 byte	1	74 byte	36.825398	0.0039				
192.168.200.100	51396	192.168.200.150	514	4	280 byte	118	4	100.00%	3	206 byte	1	74 byte	36.788600	0.0011				
192.168.200.100	37396	192.168.200.150	1	2	134 byte	874	2	100.00%	1	74 byte	1	60 byte	36.864770	0.0002				
192.168.200.100	34748	192.168.200.150	2	2	134 byte	292	2	100.00%	1	74 byte	1							

In effetti, le possibili porte aperte identificate nella terza colonna, sono le porte tipicamente associate ai servizi più comuni. Volendo fare alcuni esempi, possiamo vedere la porta 21 che è associata al protocollo FTP (File Transfer Protocol) che è utilizzato per il trasferimento di file; La porta 80 che è riservata al protocollo HTTP (Hypertext Transfer Protocol), comunemente utilizzato per il traffico Web non crittografato e la porta 445 che è comunemente associata al protocollo SMB (Server Message Block) usato per la condivisione di file e risorse in reti Microsoft Windows. A questo punto, appuntiamoci i numeri delle porte identificate, torniamo alla schermata principale di Wireshark e applichiamo dei filtri che ci permettano 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, andremo a ispezionare la porta 21 e quindi a digitare: **tcp.port==21** dove è possibile vedere la sequenza SYN, SYN ACK, ACK, RST ACK, tipica di una scansione TCP con Nmap, ovvero una scansione che completa la connessione.



Consigli per ridurre gli impatti dell’attacco

Alla luce delle vulnerabilità esposte da una scansione delle porte, è fondamentale adottare misure preventive e di mitigazione per ridurre il rischio di attacchi. Ecco alcune raccomandazioni:

- **Chiudere le porte critiche:** nel nostro caso, le porte come ftp (21), ssh (22), telnet (23), SMTP (25), DNS (53), http (80), portmapper RPC (111), netbios (139), smb (445) e quelle per il remote login, se non sono essenziali, devono essere chiuse. Questo riduce la superficie di attacco disponibile. È importante notare che alcune di queste porte potrebbero essere utilizzate da servizi legittimi all'interno dell'organizzazione, pertanto, una valutazione approfondita è necessaria prima di chiuderle.
- **Firewall e accesso limitato:** configurare policy di sicurezza sui firewall per limitare l'accesso ai servizi esposti è cruciale. Questo può includere l'abilitazione di regole che consentono l'accesso solo a specifici indirizzi IP autorizzati. È anche consigliabile impiegare tecniche come il filtraggio degli indirizzi MAC, quando possibile, per un ulteriore livello di sicurezza.
- **Autenticazione forte e controllo accessi:** dove i servizi sono necessari e devono rimanere aperti, assicurarsi che vi siano misure di autenticazione forte e controllo degli accessi. L'uso di password complesse, l'autenticazione a più fattori (MFA) e certificati digitali può notevolmente aumentare la sicurezza.
- **Aggiornamenti e patch di sicurezza:** mantenere aggiornati i sistemi e le applicazioni è fondamentale. Gli aggiornamenti spesso includono patch per vulnerabilità di sicurezza note che potrebbero essere sfruttate da un attaccante.
- **Monitoraggio e analisi del traffico di rete:** implementare soluzioni di monitoraggio del traffico di rete per identificare modelli di traffico insoliti o sospetti. Gli strumenti di rilevamento delle intrusioni (IDS) e i sistemi di prevenzione delle intrusioni (IPS) possono aiutare a identificare e bloccare attività potenzialmente dannose.
- **Sicurezza a livelli multipli (Defense in Depth):** applicare un approccio di sicurezza a più livelli, dove diversi strati di sicurezza lavorano insieme per proteggere gli asset. Questo può includere, oltre ai firewall e al controllo degli accessi, la segregazione della rete, la cifratura dei dati e la formazione degli utenti sulla sicurezza informatica.

- **Valutazioni periodiche di sicurezza:** effettuare regolari valutazioni di sicurezza e penetration test per identificare e mitigare le vulnerabilità prima che possano essere sfruttate.