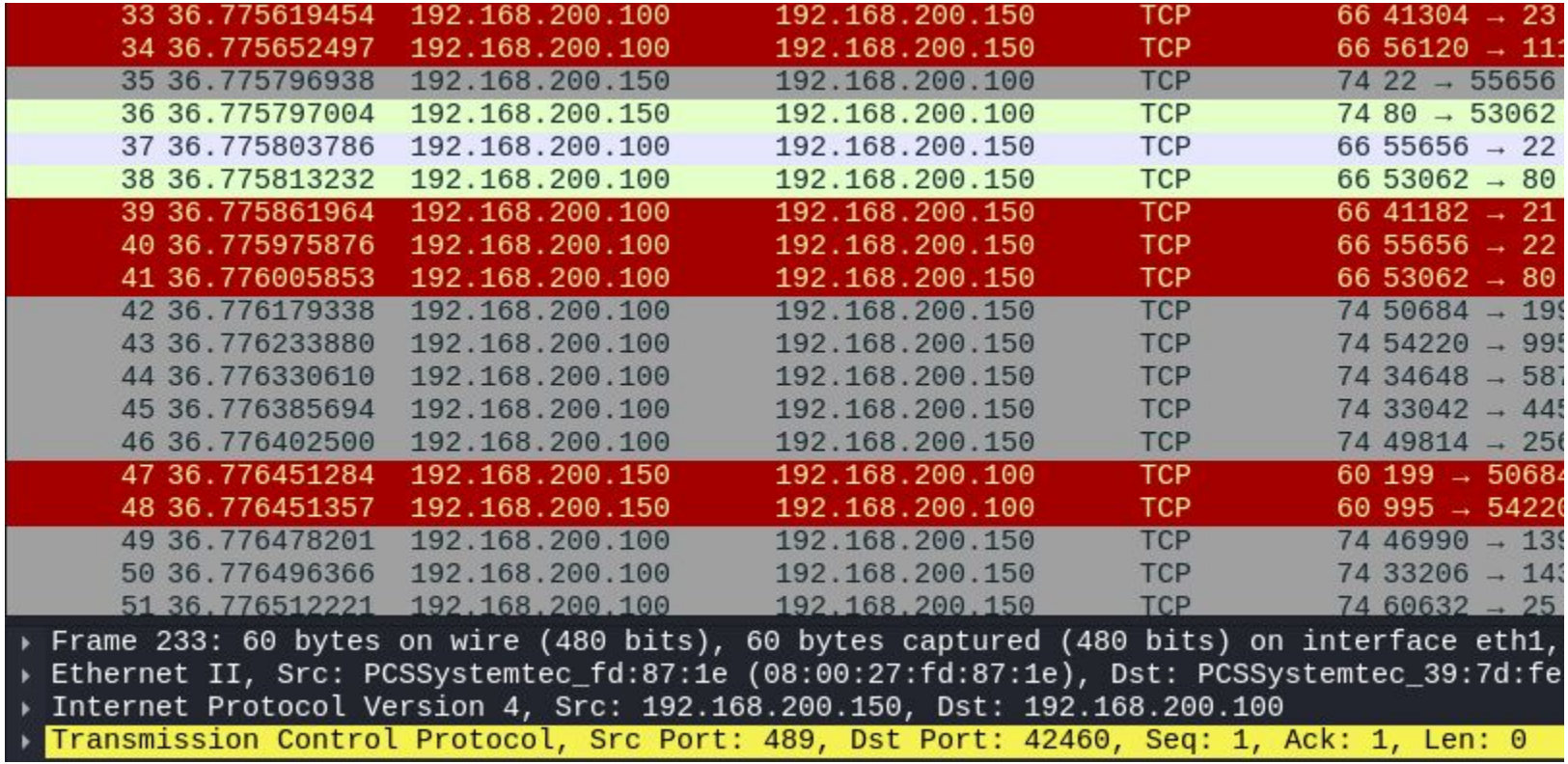
consegna s9-l3

threat intelligence & IOC



possiamo notare nella scansione fornita che l'ip 192.168.200.100 sta tentando un port scanning nei confronti dell'ip 192.168.200.150 in quanto la richiesta e' presente piu' volte nella scansione.

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID
192.168.200.100	43584	192.168.200.150	565	2	134 bytes	984
192.168.200.100	43022	192.168.200.150	564	2	134 bytes	160
192.168.200.100	56914	192.168.200.150	563	2	134 bytes	634
192.168.200.100	52958	192.168.200.150	562	2	134 bytes	855
192.168.200.100	47098	192.168.200.150	561	2	134 bytes	73
192.168.200.100	53378	192.168.200.150	560	2	134 bytes	252
192.168.200.100	37074	192.168.200.150	559	2	134 bytes	865
192.168.200.100	57906	192.168.200.150	558	2	134 bytes	923
192.168.200.100	45764	192.168.200.150	557	2	134 bytes	919
192.168.200.100	51230	192.168.200.150	556	2	134 bytes	578
192.168.200.100	36752	192.168.200.150	555	2	134 bytes	224
192.168.200.100	58636	192.168.200.150	554	2	134 bytes	5
192.168.200.100	52046	192.168.200.150	553	2	134 bytes	401
192.168.200.100	36734	192.168.200.150	552	2	134 bytes	231
192.168.200.100	54570	192.168.200.150	551	2	134 bytes	864
192.168.200.100	57474	192.168.200.150	550	2	134 bytes	816
192.168.200.100	60096	192.168.200.150	549	2	134 bytes	196
192.168.200.100	45808	192.168.200.150	548	2	134 bytes	867
192.168.200.100	53082	192.168.200.150	547	2	134 bytes	998
192.168.200.100	59806	192.168.200.150	546	2	134 bytes	797
192.168.200.100	45416	192.168.200.150	545	2	134 bytes	96
192.168.200.100	49618	192.168.200.150	544	2	134 bytes	209
192.168.200.100	47266	192.168.200.150	543	2	134 bytes	767
192.168.200.100	55892	192.168.200.150	542	2	134 bytes	148
192.168.200.100	56276	192.168.200.150	541	2	134 bytes	853
192.168.200.100	37712	192.168.200.150	540	2	134 bytes	701
192.168.200.100	45276	192.168.200.150	539	2	134 bytes	194
192.168.200.100	48344	192.168.200.150	538	2	134 bytes	179
192.168.200.100	38964	192.168.200.150	537	2	134 bytes	380
192.168.200.100	49214	192.168.200.150	536	2	134 bytes	350

per esserne sicuri isoliamo la “conversazione” tra i due ip che avvengono su TCP e possiamo appunto vedere che la scansione e’ stata eseguita su tutte le porte dalla 1 alla 1024 cio’ fa supporre che l'attaccante stia tentando di trovare una possibile vulnerabilità nel sistema così da eseguire qualche tipo di attacco

consigli per evitare gli attacchi

per evitare un possibile attacco si consiglia di isolare le porte sotto scansione,di cambiare le regole firewall per evitare accessi all'ip attaccante in quanto visibile e statico e formare i dipendenti così da evitare che cadano vittima di tentativi di phishing o altri attacchi che si basano sul social engineering