S9L5 Analisi Wire Shark.

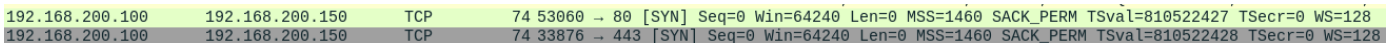
S9L5 Analisi Wire Shark.

Analisi della cattura

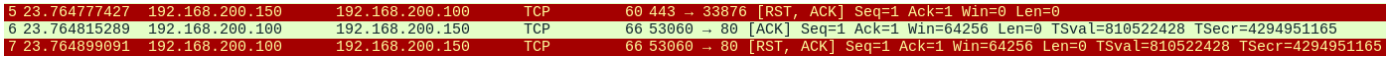
Dall'analisi della cattura di rete fornita sono stati rilevati i seguenti aspetti significativi:

Contesto del traffico

L'indirizzo IP sorgente principale, 192.168.200.100, risulta inviare numerosi pacchetti verso l'indirizzo IP di destinazione, 192.168.200.150.



Si osservano numerosi pacchetti TCP con flag SYN inviati senza una risposta completa dal destinatario, accompagnati da un significativo numero di pacchetti RST (reset delle connessioni).



Sono coinvolte diverse porte, tra cui porte ben note (ad esempio 80 per HTTP e 443 per HTTPS) e porte minori a 1024.

Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

Address A	Port A	Address B	Port B	Pac
192.168.200.100	54220	192.168.200.150	995	
192.168.200.100	54302	192.168.200.150	996	
192.168.200.100	46014	192.168.200.150	997	
192.168.200.100	42016	192.168.200.150	998	
192.168.200.100	52136	192.168.200.150	999	
192.168.200.100	47044	192.168.200.150	1000	
192.168.200.100	48512	192.168.200.150	1001	
192.168.200.100	44018	192.168.200.150	1002	
192.168.200.100	50686	192.168.200.150	1003	
192.168.200.100	38430	192.168.200.150	1004	
192.168.200.100	34030	192.168.200.150	1005	
192.168.200.100	50708	192.168.200.150	1006	
192.168.200.100	42420	192.168.200.150	1007	
192.168.200.100	56076	192.168.200.150	1008	
192.168.200.100	38350	192.168.200.150	1009	
192.168.200.100	47100	192.168.200.150	1010	
192.168.200.100	48408	192.168.200.150	1011	
192.168.200.100	53308	192.168.200.150	1012	
192.168.200.100	43698	192.168.200.150	1013	
192.168.200.100	42700	192.168.200.150	1014	
192.168.200.100	44580	192.168.200.150	1015	
192.168.200.100	39078	192.168.200.150	1016	
192.168.200.100	36474	192.168.200.150	1017	
192.168.200.100	57032	192.168.200.150	1018	
192.168.200.100	40832	192.168.200.150	1019	
192.168.200.100	33384	192.168.200.150	1020	
192.168.200.100	32996	192.168.200.150	1021	
192.168.200.100	38352	192.168.200.150	1022	
192.168.200.100	59292	192.168.200.150	1023	
192.168.200.100	37738	192.168.200.150	1024	

Indicatori di Compromissione (IOC)

- Elevato numero di pacchetti SYN: Questo pattern è tipico di un attacco SYN flood, in cui l'attaccante tenta di esaurire le risorse del sistema bersaglio.
- Presenza di pacchetti RST: L'invio di numerosi pacchetti RST da parte del bersaglio (192.168.200.150) indica che il sistema sta rigettando connessioni non valide o non desiderate.
- Traffico verso porte multiple: L'attività verso diverse porte suggerisce una scansione delle porte, probabilmente volta a identificare servizi attivi o vulnerabili sul bersaglio.

Ipotesi sui vettori di attacco

Scansione delle porte: L'attaccante ha cercato di identificare servizi esposti e vulnerabili sul sistema bersaglio.

- **Azioni consigliate**

Per mitigare gli impatti dell'attacco attuale e prevenire attacchi futuri, si raccomandano le seguenti azioni:

- Bloccare l'IP sorgente
- Implementare sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS)
- Limitare le connessioni SYN incomplete (Se continue e in quantità diventa un SYN flood a tutti gli effetti)
- Ridurre la superficie di attacco
- Verificare quali porte e servizi sono effettivamente necessari sul sistema e disabilitare quelli inutilizzati.
- Assicurarsi che i servizi attivi siano aggiornati con le ultime patch di sicurezza.