CONSEGNA S9/L3

di Giuseppe Lupoi

Per l’esercitazione di oggi ci è stato fornito un file contenente una cattura di WireShark, analizzando questo file possiamo notare delle evidenze.

SI evince dalle numerose richieste SYN con protocollo TCP su porte diverse.
Questo fa pensare ad una probabile scansione da parte dell’attaccante sul client a noi fornito con IP 192.168.200.150.

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

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	3
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	3
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	3
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	3
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	3
192.168.200.100	53060	192.168.200.150	80	4	280 bytes	0	3
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	3
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	3
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3
192.168.200.100	32792	192.168.200.150	218	2	134 bytes	526	1
192.168.200.100	32794	192.168.200.150	641	2	134 bytes	931	1
192.168.200.100	32820	192.168.200.150	49	2	134 bytes	518	1
192.168.200.100	32852	192.168.200.150	688	2	134 bytes	948	1
192.168.200.100	32896	192.168.200.150	890	2	134 bytes	637	1
192.168.200.100	32912	192.168.200.150	382	2	134 bytes	287	1
192.168.200.100	32922	192.168.200.150	41	2	134 bytes	999	1

La nostra ipotesi precedentemente esposta sembra essere confermata dal fatto che oltre ad inviare richieste SYN+ACK, che mostrano le porte aperte alla comunicazione, abbiamo anche delle richieste RST+ACK che invece mostrano la comunicazione sulla porta chiusa.

Si potrebbe completamente risolvere questa problematica con l'implementazione di un firewall ed appunto inserendo delle regole che blocchino il traffico sull'indirizzo IP dell'attaccante ovvero 192.168.200.100.

Source	Destination	Protocol	Length	Info
192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810
192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=
192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 T