

Threat Intelligence & Indicator of Compromise

Analisi di una cattura di rete effettuata con Whireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	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 TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165

No.	Time	Source	Destination	Protocol	Length	Info
999	36.825892141	192.168.200.100	192.168.200.150	TCP	74	56144 → 680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535489 TSecr=0 WS=128
1000	36.825994262	192.168.200.100	192.168.200.150	TCP	74	58008 → 267 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535489 TSecr=0 WS=128
1001	36.826117618	192.168.200.100	192.168.200.150	TCP	74	35678 → 82 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535489 TSecr=0 WS=128
1002	36.826171483	192.168.200.100	192.168.200.150	TCP	74	34608 → 951 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535489 TSecr=0 WS=128
1003	36.826344161	192.168.200.150	192.168.200.100	TCP	60	680 → 56144 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1004	36.826344247	192.168.200.150	192.168.200.100	TCP	60	267 → 58008 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1005	36.826344288	192.168.200.150	192.168.200.100	TCP	60	82 → 35678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1006	36.826492502	192.168.200.100	192.168.200.150	TCP	74	46854 → 907 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1007	36.826422755	192.168.200.100	192.168.200.150	TCP	74	40542 → 28 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1008	36.826516402	192.168.200.150	192.168.200.100	TCP	60	951 → 34608 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1009	36.826516493	192.168.200.150	192.168.200.100	TCP	60	907 → 46854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1010	36.826591166	192.168.200.100	192.168.200.150	TCP	74	54134 → 127 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1011	36.826656757	192.168.200.150	192.168.200.100	TCP	60	28 → 40542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1012	36.826697422	192.168.200.100	192.168.200.150	TCP	74	53206 → 504 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1013	36.826768060	192.168.200.150	192.168.200.100	TCP	60	127 → 54134 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1014	36.826800114	192.168.200.100	192.168.200.150	TCP	74	46790 → 702 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1015	36.826837499	192.168.200.100	192.168.200.150	TCP	74	42060 → 254 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1016	36.826981067	192.168.200.150	192.168.200.100	TCP	60	504 → 53206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1017	36.826982072	192.168.200.150	192.168.200.100	TCP	60	702 → 46790 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1018	36.826982118	192.168.200.150	192.168.200.100	TCP	60	254 → 42060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1019	36.827033922	192.168.200.100	192.168.200.150	TCP	74	40110 → 79 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128
1020	36.827054204	192.168.200.100	192.168.200.150	TCP	74	35496 → 907 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535490 TSecr=0 WS=128

Identificazioni eventuali IOC

Già dai primi pacchetti si nota che l'host vittima è una Macchina Metasploitable con IP: 192.168.200.150 ed è stato effettuato un

Three Way Handshake da una macchina con IP: 192.168.200.100 .

Dagli oltre mille pacchetti analizzati si può dedurre che stato usato il port scanning Nmap per vedere se Metasploitable avesse porte aperte e, quindi, vulnerabilità da sfruttare.

Sulla macchina vittima come prima cosa, si consiglia di attivare il firewall con regole che limitano il traffico in ingresso ai soli utenti autorizzati, di disabilitare i servizi non in uso, per non lasciare porte aperte inutilizzate, di configurare i servizi usati in modo che solo gli utenti autorizzati possano accedervi ed, infine, conoscendo già un IP di una macchina che ha attaccato il sistema, lo si può inserire in una black list.