

REPORT CS0124 S9L3

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

No.			Destination		Length Info
			192.168.200.255	BROWSER	286 Host Announcement METASPLOITABLE, Workstation, Server, Pri
			192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
			192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
			192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
			192.168.200.100	TCP	60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
			192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105224
			192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81€
		PCSSystemtec_fd:87:1e			60 Who has 192.168.200.100? Tell 192.168.200.150
		PCSSystemtec_39:7d:fe			42 192.168.200.100 is at 08:00:27:39:7d:fe
		PCSSystemtec_39:7d:fe			42 Who has 192.168.200.150? Tell 192.168.200.100 60 192.168.200.150 is at 08:00:27:fd:87:1e
		PCSSystemtec_fd:87:1e 192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM
			192.168.200.150	TCP	74 41304 → 23 [SYN] Seq=0 Win=04240 Len=0 MSS=1460 SACK_PERM 74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
			192.168.200.150	TCP	74 30120 → 111 [SYN] Seq=0 Win=04240 Len=0 MSS=1400 SACK_PERM 74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
			192.168.200.150	TCP	74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM =
			192.168.200.150	TCP	74 58030 → 334 [STN] Seq=0 Win=04240 Len=0 MSS=1400 SACK_PERM
			192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
			192.168.200.150	TCP	74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
			192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seg=0 Ack=1 Win=5792 Len=0 MSS=1460
			192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
			192.168.200.100	TCP	60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
			192.168.200.100	TCP	60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
			192.168.200.100	TCP	60 135 → 52358 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
Frame		n wire (2288 bits), 28			
		SSystemtec_fd:87:1e (0			01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8 @ @ &
		rsion 4, Src: 192.168.			c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8 K. u.
		ol, Src Port: 138, Dst		. 2001. 20	c8 96 00 8a 00 e6 00 00 20 45 4e 45 46 46 45 45 ENEFFEE
	OS Datagram Ser			.0	42 46 44 46 41 45 4d 45 50 45 4a 46 45 45 42 45 BFDFAEME PEJFEEBE
		ct_group datagram (17)		0	43 45 4d 45 46 43 41 41 41 00 20 46 48 45 50 46 CEMEFCAA A. FHEPF
• 🖺	NBDGM message typ	e (nbdgm.type), 1 byte			Packets: 2083 · Displayed: 2083 (100.0%) Profile: Default

Come possiamo vedere dallo screenshot eseguito su kali si evince che ci sono ripetute richieste TCP dalle macchine source alla macchina destination, fanendo intendere che l'attaccante sta eseguendo una scansione dei servizi e delle porte aperte.

CONCLUSIONI

Per sventare una possibile scansione delle porte e servizi vulnerabili e contrastare un possibile attacco possiamo utilizzare diversi metodi a nostra disposizione.

Uno di questi e' attivare un firewall sulla macchina target in modo tale da bloccare o droppare qualsiasi richiesta da parte di indirizzi ip attaccanti.

Un altro metodo potrebbe essere quello di andare a risolvere le singole vulnerabilita' all'interno della macchina o server target così da eliminare o ridurre il rischio di attacchi interni \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\