

Analisi pacchetti per rilevamento IOC

Apriamo il file con Wireshark vediamo uno scambio di pacchetti tra due IP:

192.168.200.150 e 192.168.200.100

No.	Time	Source	Destination
1	0.000000000	192.168.200.150	192.168.200.255
2	23.764214995	192.168.200.100	192.168.200.150
3	23.764287789	192.168.200.100	192.168.200.150
4	23.764777323	192.168.200.150	192.168.200.100
5	23.764777427	192.168.200.150	192.168.200.100
6	23.764815289	192.168.200.100	192.168.200.150
7	23.764899091	192.168.200.100	192.168.200.150

Il primo pacchetto è un messaggio di host announcement (comunicazione della presenza di un host) all'indirizzo di broadcast 192.168.200.255 da parte dell'IP 192.168.200.150.

L'indirizzo IP 192.168.200.150 sta comunicando la sua presenza alla rete.

No.	Time	Source	Destination	Protocol
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER

Dai dettagli del pacchetto possiamo vedere il nome dell'host (METASPLOITABLE) e altre informazioni. Sembra trattarsi di un "server metasploitable" che esegue Samba 3.0.20-Debian.

Priority: 1
Class: Unreliable & Broadcast (2)
Size: 93
Mailslot Name: \MAILSLOT\BROWSE
Microsoft Windows Browser Protocol
Command: Host Announcement (0x01)
Update Count: 1
Update Periodicity: 2 minutes
Host Name: METASPLOITABLE
Windows version:
OS Major Version: 4
OS Minor Version: 9
Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser
Browser Protocol Major Version: 15
Browser Protocol Minor Version: 1
Signature: 0xaa55
Host Comment: metasploitable server (Samba 3.0.20-Debian)

A seguire, troviamo alcune richieste ARP dove gli IP 192.168.200.100 e 192.168.200.150 associano ciascuno il MAC address del dispositivo dell'altro all'IP corrispondente.

No.	Time	Source	Destination	Protocol	Length	Info
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Il resto dei pacchetti è una serie di richieste TCP con flag SYN che partono da 192.168.200.100 a 192.168.200.150 su un vasto numero di porte:

ip.src == 192.168.200.100 and tcp.flags.syn == 1 and tcp.flags.ack == 0						
No.	Time	Source	Destination	Protocol	Length	Info
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	23.764267768	192.168.200.100	192.168.200.150	TCP	74	53076 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366395	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
29	36.775337809	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775396694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524294	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	58684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233889	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402509	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49	36.776478291	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33280 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776560666	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
70	36.777143914	192.168.200.100	192.168.200.150	TCP	74	66990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34640 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	48310 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128

In alcuni casi vediamo che l'IP 192.168.200.150 risponde con il flag ACK (la porta quindi è aperta).

In questi casi l'IP 192.168.200.100 chiude la connessione inviando un pacchetto RST (non completa il three-way-handshake) a 192.168.200.150:

No.	Time	Source	Destination	Protocol	Length	Info
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
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64240 Len=0
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

In tutti gli altri casi, quando la porta è chiusa, l'IP 192.168.200.150 chiude la connessione inviando un pacchetto RST:

tcp.port == 54898						
No.	Time	Source	Destination	Protocol	Length	Info
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128

No.	Time	Source	Destination	Protocol	Length	Info
447	36.798389913	192.168.200.100	192.168.200.150	TCP	74	49618 → 544 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
451	36.798678087	192.168.200.150	192.168.200.100	TCP	60	544 → 49618 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Non ci sono richieste con protocollo ICMP, ciò significa che non è stato effettuato nessun ping.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info

I pacchetti catturati evidenziano una scansione SYN `nmap` senza ping su un ampio numero di porte (ad esempio `nmap -Pn -sS`) dall'host `192.168.200.100` verso l'host `192.168.200.150`. Ciò significa che l'host `192.168.200.100` sta recuperando informazioni sull'host target (information gathering), indicando così un potenziale futuro attacco vero e proprio.

A seguito di questa scansione, l'host `192.168.200.100` ha recuperato almeno le informazioni sulle porte aperte dell'host `192.168.200.150`. Potrebbe utilizzare queste informazioni per scansioni mirate più invasive, individuando i servizi in esecuzione (banner grabbing), il sistema operativo (OS fingerprinting) della macchina target, nonché eventuali vulnerabilità da sfruttare per un attacco.

Ecco alcune soluzioni che potrebbero essere utili per ridurre l'impatto di una situazione del genere, nonché prevenire il ripetersi di situazioni simili:

Access Control List (ACL):

Una ACL è una lista di regole utilizzata per determinare i permessi di accesso a una risorsa particolare, come una pagina web, un file o una porta di rete. Nelle reti, le ACL sono spesso utilizzate in router e switch per filtrare il traffico, consentendo o negando il passaggio di pacchetti basati su criteri come indirizzo IP, numero di porta, protocollo, ecc.

Network Access Control (NAC):

Il NAC è un approccio alla sicurezza della rete che cerca di definire e implementare una politica sull'esatto tipo di accesso che gli utenti o i dispositivi dovrebbero avere sulla rete. In generale, il NAC verifica l'identità e il ruolo degli utenti o dei dispositivi che cercano di accedere alla rete e applica le policy di sicurezza appropriate. Ad esempio, un sistema NAC potrebbe verificare se un computer ha l'ultima versione di un software antivirus prima di consentirgli l'accesso. Può essere utilizzato per prevenire accessi non autorizzati, isolare dispositivi compromessi o non conformi e garantire che solo dispositivi sicuri e autorizzati possano accedere alla rete.

Firewall:

Un firewall è un dispositivo o un software progettato per filtrare, monitorare e controllare il traffico di rete, consentendo o negando la trasmissione di pacchetti dati basandosi su un insieme di regole di sicurezza predefinite. Funziona come una barriera tra una rete affidabile (ad esempio, una rete aziendale interna) e reti non affidabili (ad esempio, Internet) per prevenire accessi non autorizzati o attacchi malevoli.

E' possibile utilizzare questi strumenti per limitare l'accesso alla rete a indirizzi IP specifici oppure per impedire l'accesso a determinati indirizzi IP.