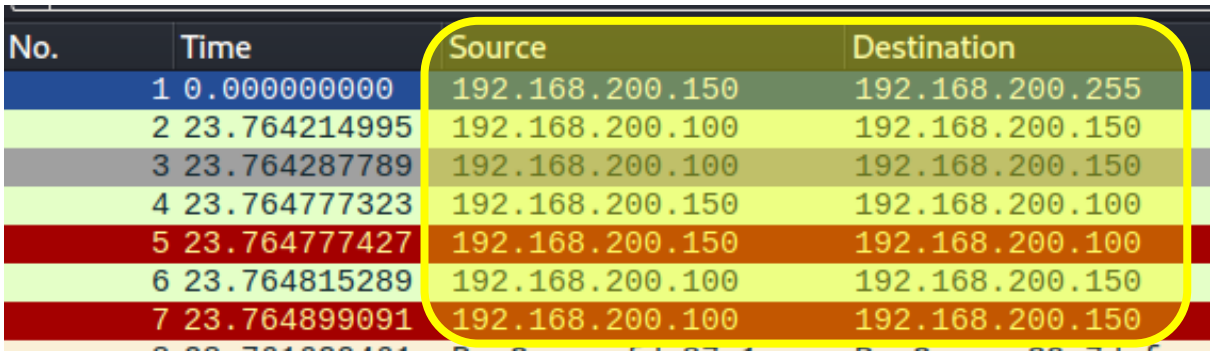
Analisi pacchetti per rilevamento IOC

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

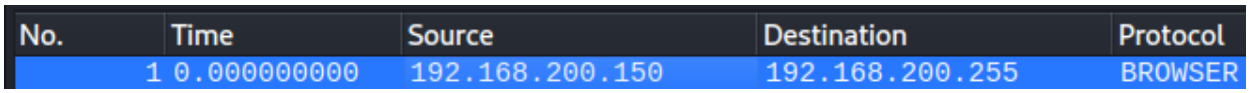
`192.168.200.150` e `192.168.200.100`



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

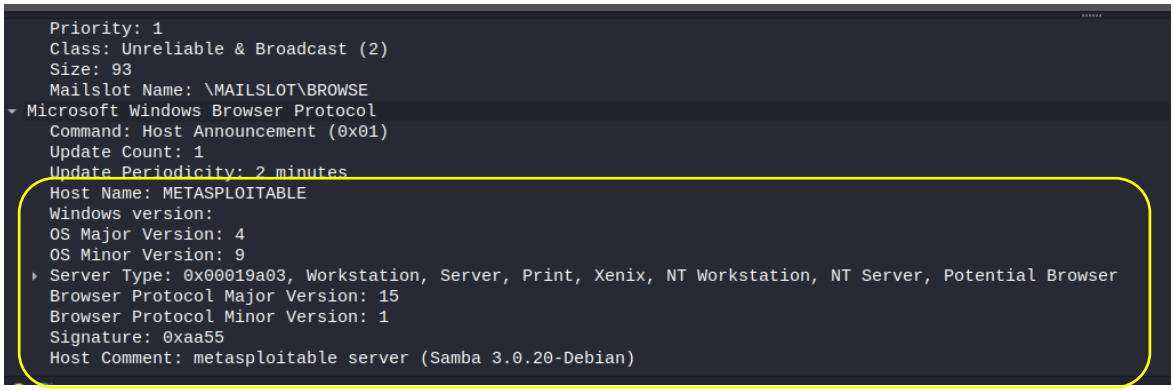
Il primo pacchetto è un messaggio di host announcement (comunicazione della presenza di un host) all'indirizzo di broadcast `192.168.200.255` da parte dell'IP `192.168.200.150`.

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



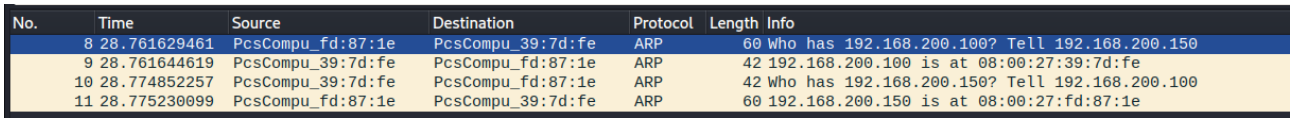
No.	Time	Source	Destination	Protocol
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER

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.



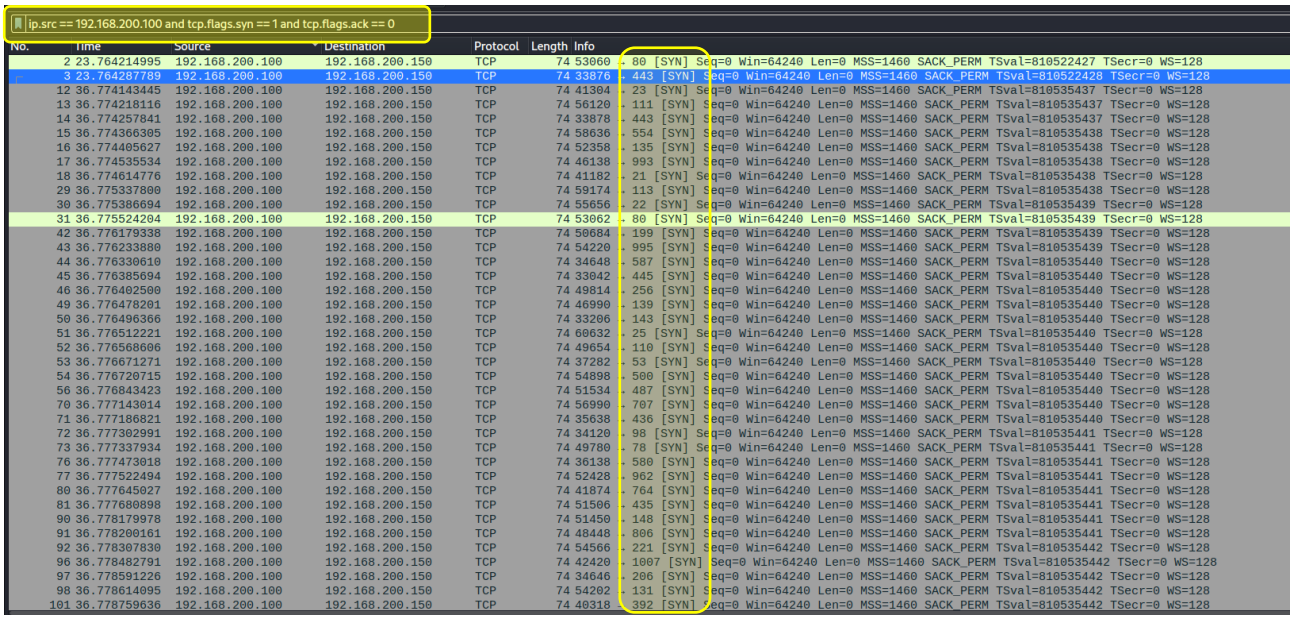
```
    Priority: 1
    Class: Unreliable & Broadcast (2)
    Size: 93
    Mailslot Name: \MAILSLOT\BROWSE
▾ Microsoft Windows Browser Protocol
    Command: Host Announcement (0x01)
    Update Count: 1
    Update Periodicity: 2 minutes
    Host Name: METASPLOITABLE
    Windows version:
    OS Major Version: 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.



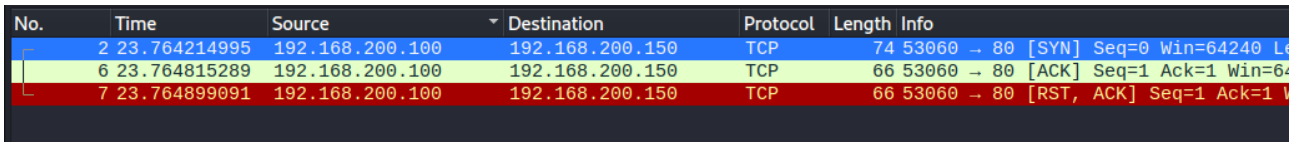
No.	Time	Source	Destination	Protocol	Length	Info
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e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

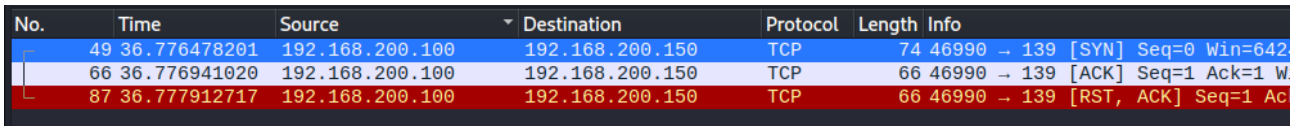
Il resto dei pacchetti è una serie di richieste TCP con flag SYN che partono da `192.168.200.100` a `192.168.200.150` su un vasto numero di porte:



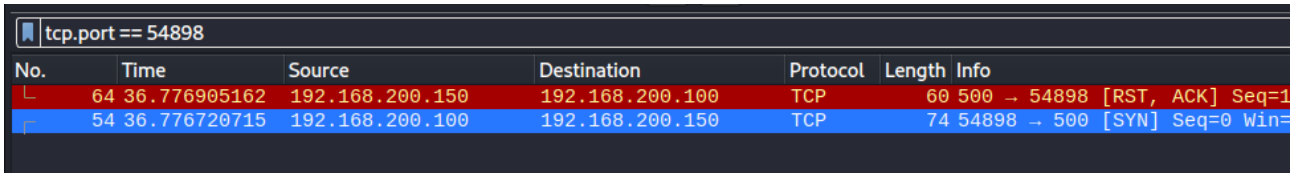
In alcuni casi vediamo che l'IP `192.168.200.150` risponde con il flag ACK (la porta quindi è aperta).

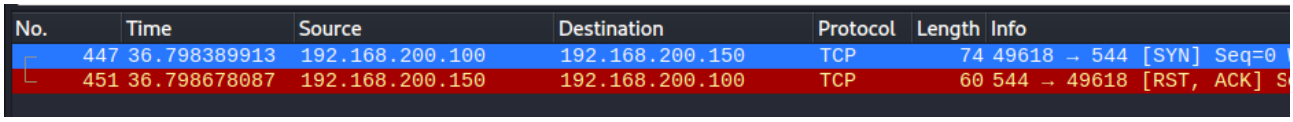
In questi casi l'IP `192.168.200.100` chiude la connessione inviando un pacchetto `RST` (non completa il three-way-handshake) a `192.168.200.150`:



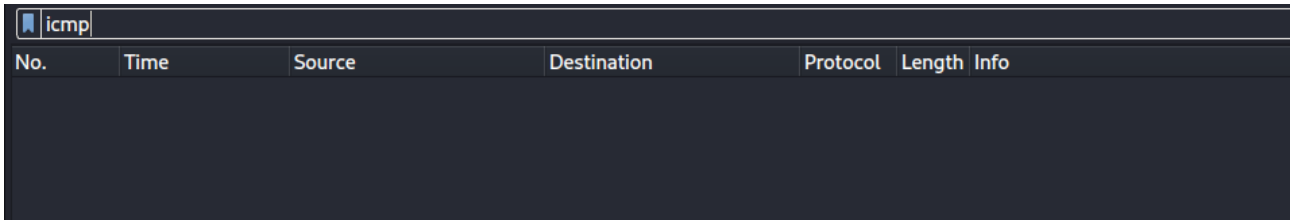


In tutti gli altri casi, quando la porta è chiusa, l'IP `192.168.200.150` chiude la connessione inviando un pacchetto `RST`:





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



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.