Relazione Threat Intelligence e IOC

Obiettivo dell'Esercizio

L'obiettivo di questa analisi è individuare eventuali Indicatori di Compromissione (IOC) all'interno di una cattura di rete effettuata tramite Wireshark, valutare la presenza di un attacco in corso e proporre ipotesi sui vettori di attacco utilizzati, insieme ad azioni preventive per futuri incidenti simili.

Il contesto operativo riguarda una rete locale (LAN) in cui sono stati identificati due indirizzi IP principali: 192.168.200.100 (sorgente) e 192.168.200.150 (destinazione). L'analisi mira a determinare se l'attività osservata rappresenta un comportamento normale o un tentativo di compromissione.

Contesto Operativo

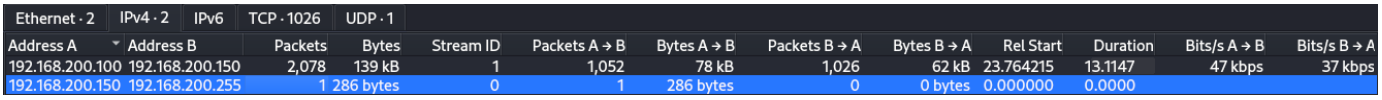
La rete analizzata sembra essere un ambiente di test o laboratorio, dato che uno degli host (192.168.200.150) si identifica come "Metasploitable", una macchina virtuale deliberatamente vulnerabile utilizzata per simulazioni di attacchi. Tuttavia, la presenza di tale sistema in una rete non isolata rappresenta un rischio significativo, poiché Metasploitable espone servizi noti per vulnerabilità critiche.

L'assenza di traffico DNS suggerisce che l'attaccante stia operando direttamente tramite indirizzi IP, senza necessità di risoluzione dei nomi di dominio, il che è coerente con l'uso di strumenti automatizzati come Metasploit o Nmap per esplorare la rete e identificare servizi vulnerabili.

Fasi dell'Analisi

Riepilogo Generale dei Pacchetti

- **Totale pacchetti :** 2083
- **Protocolli individuati :**
    - **TCP:** 2078 pacchetti
    - **ARP:** 4 pacchetti
    - **UDP-BROWSER:** 1 pacchetto
- **Pacchetti HTTP/DNS :** 0

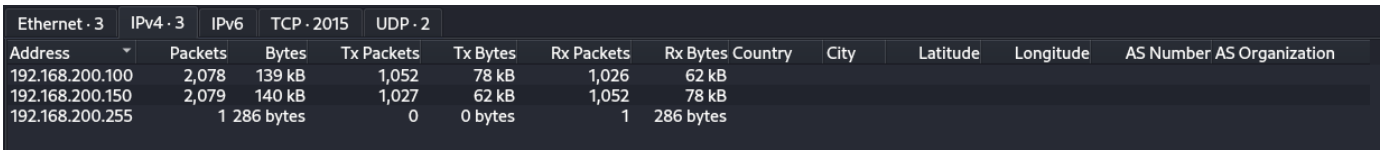


Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.200.100	192.168.200.150	2,078	139 kB	1	1,052	78 kB	1,026	62 kB	23.764215	13.1147	47 kbps	37 kbps
192.168.200.150	192.168.200.255	1	286 bytes	0	1	286 bytes	0	0 bytes	0.000000	0.0000		

Analisi del Traffico di Rete

Nell'analisi del traffico di rete, sono stati individuati due indirizzi IP principali coinvolti nella comunicazione: **192.168.200.100**, che appare come l'host mittente e l'iniziatore delle connessioni con un totale di 1052 pacchetti inviati, e **192.168.200.150**, che agisce come destinatario, ricevendo 1027 pacchetti e rispondendo alle richieste.

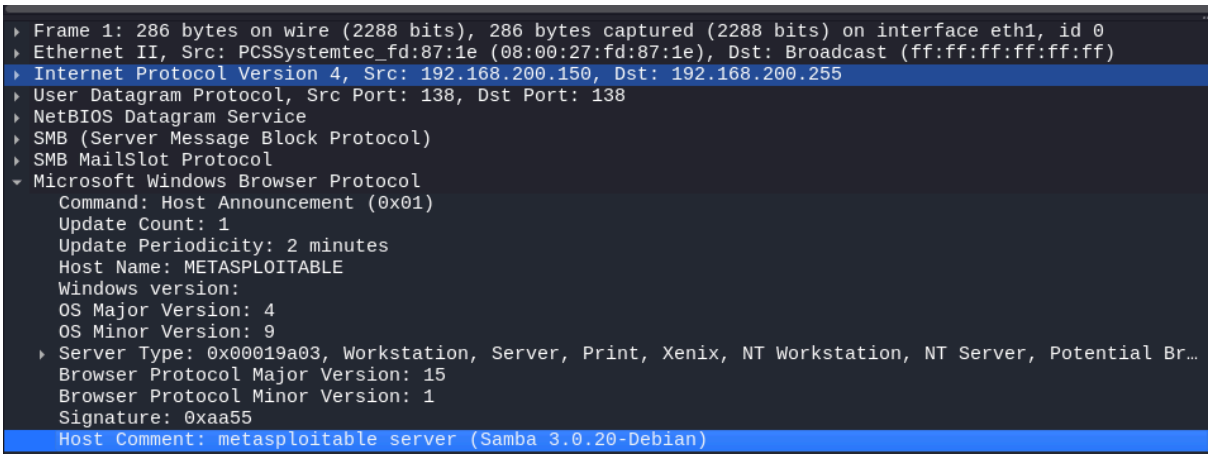


Ethernet · 3 | IPv4 · 3 | IPv6 | TCP · 2015 | UDP · 2

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
192.168.200.100	2,078	139 kB	1,052	78 kB	1,026	62 kB						
192.168.200.150	2,079	140 kB	1,027	62 kB	1,052	78 kB						
192.168.200.255	1	286 bytes	0	0 bytes	1	286 bytes						

Uno dei pacchetti più significativi riguarda l'annuncio di rete inviato da **192.168.200.150**, il quale si identifica come *"METASPLOITABLE"* attraverso il protocollo BROWSER, trasmettendo il messaggio in broadcast all'indirizzo **192.168.200.255**. La presenza di questo hostname all'interno della rete rappresenta un chiaro indicatore di rischio, dato che *Metasploitable* è una macchina volutamente vulnerabile, spesso utilizzata per test di sicurezza ed esercitazioni di attacco.

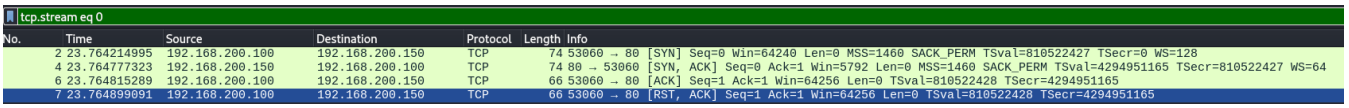
All'interno del pacchetto è inclusa l'informazione relativa alla versione del servizio in esecuzione sulla porta **138**, associata al protocollo **SMB**. In particolare, si tratta di **Samba 3.0.20-Debian**, una versione nota per la presenza di diverse vulnerabilità di sicurezza, potenzialmente sfruttabili per attacchi mirati.



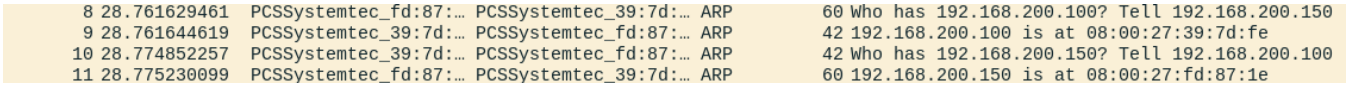
```
▸ Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
▸ Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255
▸ User Datagram Protocol, Src Port: 138, Dst Port: 138
▸ NetBIOS Datagram Service
▸ SMB (Server Message Block Protocol)
▸ SMB MailSlot Protocol
▾ 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 Br…
    Browser Protocol Major Version: 15
    Browser Protocol Minor Version: 1
    Signature: 0xaa55
    Host Comment: metasploitable server (Samba 3.0.20-Debian)
```

Un altro pacchetto rilevante è un tentativo di connessione TCP inviato da **192.168.200.100** alla porta **80** di **192.168.200.150**. Il pacchetto SYN indica l'inizio di una comunicazione HTTP, e se non viene seguito da una connessione stabilita, ma da un pacchetto di reset (RST), potrebbe suggerire una scansione delle porte. In

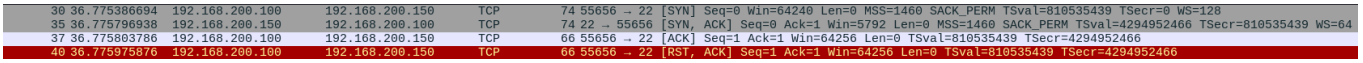
effetti, proprio **192.168.200.150** risponde successivamente con un pacchetto **RST, ACK**, segnalando il rifiuto della connessione, un comportamento spesso associato a tentativi di scansione per individuare servizi attivi sulla macchina bersaglio.



Un'altra attività rilevata è una richiesta ARP proveniente da **192.168.200.100**, con il messaggio *"Who has 192.168.200.150? Tell 192.168.200.100"*. Sebbene le richieste ARP siano normali in qualsiasi rete, una loro ripetizione eccessiva può indicare un tentativo di **ARP scanning**, utile per mappare dispositivi attivi sulla rete locale.

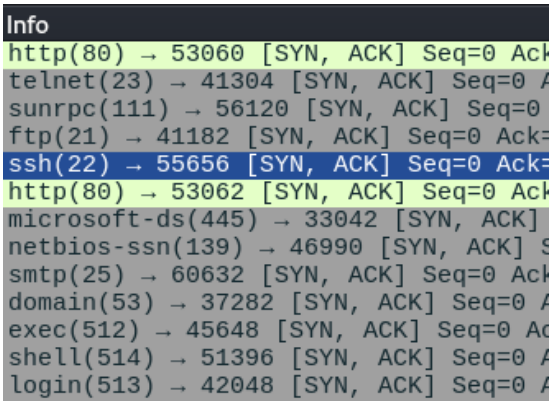


Infine, è stato osservato un pacchetto di trasferimento dati su **porta 22 (SSH)** tra gli stessi due host, con flag **RST, ACK**. L'invio di dati su SSH potrebbe essere parte di una normale attività amministrativa, ma se non autorizzato potrebbe segnalare un **tentativo di accesso remoto illecito**, come un attacco brute-force per indovinare le credenziali dell'host.



L'insieme di questi pacchetti suggerisce un'attività di scansione e potenzialmente di attacco, con particolare attenzione alla presenza di una macchina vulnerabile esposta nella rete.

Elenco Delle Porte Risultanti Aperte



Le porte risultano aperte poiché hanno risposto al pacchetto **SYN** ricevuto con un **SYN-ACK**, confermando la disponibilità del servizio sulla porta di destinazione.

Indicatori di Compromissione (IOC) Osservati

IOC:

Macchina Attaccante:

- **Dettagli:** IP 192.168.200.100, Host PCSSystemtec_39:7d:fe (MAC: 08:00:27:fd:87:1e)
- **Rischio Associato:** Possibile compromissione. L'host risulta coinvolto in attività di scansione, potenzialmente riconducibili a un attacco in corso.
- **Azione Consigliata:** Isolare immediatamente la macchina dalla rete, analizzare i log di sistema

Hostname Anomalo

- **Dettaglio:** "METASPLOITABLE"
- **Rischio Associato:** Sistema vulnerabile con servizi esposti (SSH, FTP, SMB)
- **Azione Consigliata:** Isolare il sistema in una VLAN dedicata.

Pattern TCP Sospetto

- **Dettaglio:** Sequenze SYN + RST
- **Rischio Associato:** Indicatore di scansione di porte o tentativi di exploit.
- **Azione Consigliata:** Configurare IDS/IPS per bloccare traffico SYN.

Assenza di Traffico DNS

- **Dettaglio:** Nessuna richiesta DNS
- **Rischio Associato:** Suggerisce attacco diretto o uso di strumenti automatizzati.
- **Azione Consigliata:** Monitorare traffico interno per anomalie.

Connessioni Ripetute

- **Dettaglio:** Comunicazione costante tra due IP
- **Rischio Associato:** Possibile attacco mirato o scansione.
- **Azione Consigliata:** Bloccare connessioni non autorizzate.

Ipotesi sul Vettore di Attacco

Alla luce delle evidenze raccolte:

1. **Fase di Ricognizione :**
    - L'attaccante (192.168.200.100) sta effettuando una ricognizione attiva per mappare i servizi esposti dal target (192.168.200.150).
    - È plausibile che venga utilizzato Metasploit per testare vulnerabilità note su 192.168.200.150.
2. **Tecniche di Scansione :**
    - Port Scanning : Tentativi di connessione verso diverse porte (es. 80, 443, 22) con pattern SYN + RST.
    - ARP Scanning : Richieste ARP ripetute per identificare dispositivi nella rete locale.
3. **Fase Successiva dell'Attacco :**
    - L'attaccante potrebbe sfruttare vulnerabilità note nei servizi esposti (es. SSH, SMB) per ottenere accesso al sistema.

Azioni Consigliate

Mitigazione dell'Attacco in Corso

1. **Isolamento del Target :**
    - Spostare 192.168.200.150 in una VLAN dedicata per limitare l'esposizione.
2. **Blocco del Traffico Sospetto :**
    - Aggiungere regole al firewall per bloccare connessioni non necessarie sulle porte aperte.
3. **Analisi Forense :**
    - Verificare i log di sistema di 192.168.200.150 per identificare eventuali compromissioni.

Prevenzione Futura

1. **Segmentazione della Rete :**
    - Dividere la rete in subnet isolate per ridurre la superficie di attacco.
2. **Monitoraggio Continuo :**
    - Implementare un SIEM e IDS/IPS per rilevare attività anomale (es. port scanning, ARP scanning).
3. **Patch Management :**
    - Applicare patch critiche ai servizi esposti (es. SSH, SMB) per chiudere vulnerabilità note.
4. **Formazione del Personale :**
    - Sensibilizzare gli utenti sui rischi legati all'uso di sistemi vulnerabili come Metasploitable.

Conclusione

L'analisi della cattura di rete rivela un'intensa attività di scansione delle porte da parte dell'host 192.168.200.100 verso l'host 192.168.200.150. Questo comportamento è evidenziato da pattern TCP sospetti, come sequenze di pacchetti SYN seguiti da RST, e dall'assenza di traffico DNS, che suggerisce un'interazione diretta tramite indirizzi IP all'interno della rete locale. L'identificazione del sistema target come "Metasploitable" rappresenta un indicatore critico, poiché si tratta di una macchina deliberatamente vulnerabile spesso utilizzata per simulazioni di attacchi.

Sebbene non vi siano evidenze dirette di un attacco in corso, l'attività osservata indica chiaramente una fase di ricognizione finalizzata a mappare i servizi esposti dal sistema target. Tale scansione potrebbe essere il preludio a tentativi di exploit su porte critiche (es. SSH, HTTP, SMB) o a ulteriori azioni malevole.

Per mitigare il rischio, è fondamentale isolare sistemi vulnerabili come Metasploitable in ambienti controllati (es. VLAN dedicate), monitorare il traffico di rete per rilevare attività anomale e implementare misure preventive come IDS/IPS e regole firewall restrittive. Inoltre, è essenziale promuovere una cultura della sicurezza per evitare l'esposizione accidentale di sistemi vulnerabili in reti operative.

Questa analisi sottolinea l'importanza di identificare e gestire adeguatamente le fasi iniziali di esplorazione della rete, al fine di prevenire potenziali escalation verso attacchi più complessi.