

Report di Analisi Forense del Traffico di Rete: Identificazione di Indicatori di Compromissione (IOC) e Valutazione della Minaccia

Data del Report: 30 Maggio 2025

Autore: Stefano Gugliotta

Riferimento Cattura di Rete: Cattura_U3_W1_L5.pcapng

1. Introduzione e Obiettivo dell'Analisi

Il presente documento costituisce un report di analisi forense del traffico di rete, basato sull'esame del file *Cattura_U3_W1_L5.pcapng*. L'obiettivo primario di questa analisi è l'identificazione di potenziali Indicatori di Compromissione (IOC) che possano suggerire attività malevole o sospette in corso all'interno dell'ambiente di rete monitorato. In aggiunta, il report mira a formulare ipotesi fondate sui vettori di attacco plausibilmente impiegati e a proporre un set di azioni immediate e strategiche per mitigare gli impatti di eventuali attacchi attuali e per rafforzare la postura di sicurezza complessiva, prevenendo incidenti futuri di natura simile.

L'analisi è stata condotta metodicamente utilizzando Wireshark, uno strumento standard del settore per l'analisi dei pacchetti di rete, concentrandosi in particolare sul traffico registrato e integrando evidenze fornite da screenshot aggiuntivi relativi all'analisi stessa.

2. Identificazione e Analisi degli Indicatori di Compromissione (IOC)

L'esame approfondito della cattura di rete ha rivelato una chiara sequenza di attività di ricognizione. Nello specifico, si evidenziano i seguenti indicatori di compromissione principali, che coinvolgono due indirizzi IP interni alla sottorete 192.168.200.0/24:

- **Host Attaccante Sospetto:** 192.168.200.100
- **Host di Destinazione/Target Scansionato:** 192.168.200.150

Gli IOC osservati includono:

- **Tentativi di Connessione Iniziali su Porte Standard (HTTP/HTTPS) con Chiusura Immediata:** L'attività sospetta inizia con una prima comunicazione TCP sulla porta 80 da parte di 192.168.200.100 verso 192.168.200.150. Come mostrato in **Figura 1**, nonostante un classico handshake TCP, il client 192.168.200.100 ha chiuso immediatamente la connessione, suggerendo un'operazione di scansione "half-open" (nmap -sS). Successivamente, il client ha tentato la stessa operazione sulla porta 443,

8 28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230959	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60 192.168.200.150 is at 08:00:27:fd:07:1e
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 36.774495627	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
19 36.774685595	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20 36.774685652	192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64

ma la connessione è stata rifiutata (come evidenziato in **Figura 2**), probabilmente perché il servizio HTTPS non era attivo.

- **Fase di ARP-Scan e Successivo SYN-Scan su Varie Porte:** Dopo i tentativi iniziali, è stata rilevata un'attività di ARP-Scan, indicando una fase di

```
Source Port: 83
Destination Port: 55216
[Stream index: 184]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (37)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2710734741
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... ....0 = Push: Not set
... ..1. = Reset: Set
[Expert Info (Warning/Sequence): Connection reset (RST)]
.... ....0. = Syn: Not set
.... ....0 = Fin: Not set
[TCP Flags: .....A.R..]
```

mappatura attiva della rete locale. Questa è stata rapidamente seguita da un SYN-Scan mirato a un set diversificato di porte. Tutte queste comunicazioni terminano con un reset (RST), come osservato inizialmente, tranne per le porte identificate come aperte.

- **Volume Elevato di Pacchetti SYN e RST/ACK:** La maggior parte del traffico tra i due host consiste in pacchetti SYN (richieste di connessione) inviati da 192.168.200.100 verso

192.168.200.150, immediatamente seguiti da pacchetti RST, ACK (reset e conferma) inviati da 192.168.200.150 al mittente. Questo schema si ripete costantemente e con elevata frequenza, come evidenziato in Figura 3 che mostra una sezione estesa della scansione. Questo volume elevato è

```
Transmission Control Protocol, Src Port: 53060, Dst Port: 80, Seq: 1, Ack
Source Port: 53060
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 4]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 802623072
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1271586189
1000 .... = Header Length: 32 bytes (8)
Flags: 0x014 (RST, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... ....0 = Push: Not set
... ..1. = Reset: Set
.... ....0. = Syn: Not set
.... ....0 = Fin: Not set
[TCP Flags: .....A.R..]
Window: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0x1273 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
```

una conseguenza diretta dell'uso di una scansione "half-open" (SYN scan), che invia RST per chiudere le connessioni non appena lo stato di una porta viene determinato, consentendo una scansione rapida e vasta senza completare gli handshake.

- **Tentativi di Connessione su un Set di Porte Comuni, Specifiche Porte Non Standard e Range Alti:** L'host sorgente (192.168.200.100) ha tentato di stabilire connessioni su un set di porte TCP ben note associate a servizi comuni (es. 21, 22, 80). Sono stati rilevati anche tentativi specifici su porte non standard meno comuni come la porta 83 (come si può vedere in **Figura 4**), oltre a porte in range più elevati come 45928, 89, e 980. Questo indica una scansione più ampia rispetto al solo set di porte

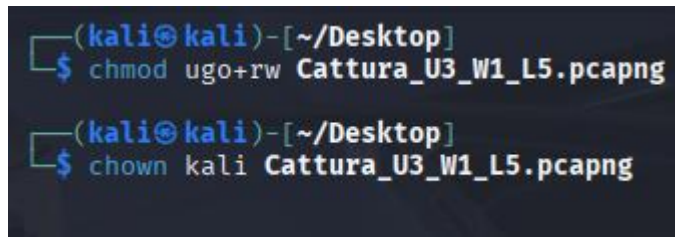
comuni, suggerendo un approccio di ricognizione più approfondito per identificare servizi noti e potenziali servizi non standard o vulnerabili in posizioni meno prevedibili.

- **Rilevamento di Porte TCP Aperte sul Target:** La scansione ha avuto successo nell'identificare diverse porte aperte su 192.168.200.150, come evidenziato dalle risposte SYN-ACK ricevute per specifici tentativi. Le porte TCP identificate come aperte includono:
 - 21 (FTP)
 - 22 (SSH)
 - 23 (Telnet)
 - 25 (SMTP)
 - 53 (DNS)
 - 80 (HTTP)
 - 111 (Portmapper / RPCBind)
 - 139 (NetBIOS Session Service)
 - 445 (SMB/CIFS)
 - 512 (Exec Service)
 - 514 (Shell Service) La presenza di questi servizi attivi sul target 192.168.200.150 espone una superficie di attacco significativa e rende la macchina vulnerabile a potenziali exploit.
- **Traffico Concentrato tra Due Specifici Host Interni:** L'attività anomala è prevalentemente concentrata tra i due indirizzi IP specificati, entrambi residenti nella medesima sottorete interna, come illustrato nelle statistiche delle conversazioni in **Figura 5**. Ciò suggerisce un'interazione mirata all'interno del perimetro di rete dell'organizzazione.

[Inserisci qui lo Screenshot: cattura 3.jpg o cattura 4.jpg per la sezione delle statistiche delle conversazioni] Figura 5: Statistiche delle conversazioni IPv4 che mostrano il traffico concentrato tra 192.168.200.100 e 192.168.200.150.

- **Esecuzione di Comandi di Gestione File (chmod e chown) sul File di Cattura:** Un'ulteriore osservazione significativa riguarda l'esecuzione dei comandi chmod ugo+rw Cattura_U3_W1_L5.pcapng e chown kali Cattura_U3_W1_L5.pcapng, come mostrato in **Figura 6**. Questi comandi sono stati eseguiti sul sistema su cui risiedeva il file della cattura di rete (o un sistema ad esso collegato dove il file è stato elaborato). chmod ugo+rw modifica i permessi del file rendendolo leggibile e scrivibile per tutti gli utenti, mentre chown kali assegna la proprietà del file all'utente kali. Sebbene tali comandi possano essere legittimamente utilizzati da un analista per la gestione dei

permessi e della proprietà del file durante l'analisi, se non fossero stati avviati da un'azione autorizzata, rappresenterebbero un **potenziale indicatore di compromissione a livello di sistema**, suggerendo un accesso non autorizzato al sistema su cui è stata eseguita la cattura o dove è stato gestito il file. È cruciale determinare il contesto e l'autore di queste azioni per valutarne la natura malevola.

A screenshot of a terminal window in Kali Linux. The prompt is (kali@kali) - [~/Desktop]. The first command is \$ chmod ugo+rw Cattura_U3_W1_L5.pcapng. The second command is \$ chown kali Cattura_U3_W1_L5.pcapng.

```
(kali@kali) - [~/Desktop]
$ chmod ugo+rw Cattura_U3_W1_L5.pcapng

(kali@kali) - [~/Desktop]
$ chown kali Cattura_U3_W1_L5.pcapng
```

3. Ipotesi sui Potenziali Vettori di Attacco Utilizzati

Sulla base degli indicatori di compromissione analizzati, l'ipotesi più robusta e fondata riguardo ai vettori di attacco è la seguente:

- **Vettore Principale: Port Scanning (SYN Scan) per Ricognizione Avanzata:**
 - La fase iniziale di ricognizione attiva (ARP-Scan per la mappatura della rete locale e Port Scanning/SYN Scan su un set diversificato di porte) ha avuto successo nell'identificare numerosi servizi attivi sul target 192.168.200.150. Il comportamento osservato nella cattura di rete è perfettamente allineamento con il modo in cui Nmap esegue una scansione SYN, una tecnica "stealth" per identificare le porte aperte senza completare il handshake TCP. L'alto volume di pacchetti SYN e RST/ACK osservato è una caratteristica intrinseca di questa metodologia di scansione, che permette di sondare un vasto numero di porte rapidamente, inviando un RST per terminare la connessione non appena si determina lo stato della porta, piuttosto che un tentativo di esaurire le risorse o saturare la rete. L'inclusione di porte meno comuni o in range più elevati suggerisce che l'attaccante stia cercando di mappare l'intera superficie di attacco, non solo i servizi più ovvi, in preparazione a tentativi di sfruttamento.
- **Strumenti e Caratteristiche del Sistema Attaccante:**
 - L'analisi approfondita dei campi dei pacchetti (come Window_size = 64420 e la presenza di timestamp attivi) suggerisce che la macchina attaccante (192.168.200.100) stia utilizzando un sistema operativo basato su Linux. Inoltre, il numero alto e casuale delle porte sorgente utilizzate per i tentativi di scansione, unito all'ordinamento specifico delle opzioni TCP nei pacchetti SYN, sono indicatori forti e tipici dell'utilizzo di uno strumento di scansione avanzato e popolare come Nmap (Network Mapper). Queste osservazioni sono coerenti con le considerazioni sui log fornite.
- **Potenziale Vettore Aggiuntivo: Accesso a Livello di Sistema (da Verificare):**
 - L'evidenza dell'esecuzione dei comandi chmod e chown sul file della cattura di rete richiede un'indagine approfondita. Se queste azioni non fossero state

eseguite legittimamente da un analista o da un processo autorizzato, allora ciò indicherebbe che l'attaccante è riuscito a ottenere un qualche livello di accesso esecutivo sul sistema su cui è stata effettuata la cattura o dove il file è stato elaborato. Questo accesso potrebbe essere avvenuto tramite lo sfruttamento di una vulnerabilità (anche se non direttamente sul 192.168.200.150) o tramite credenziali compromesse. In tal caso, l'esecuzione di tali comandi rappresenterebbe un'attività di **post-exploitation**, mirata a consolidare l'accesso, modificare la configurazione del sistema o preparare il terreno per ulteriori azioni malevole.

In sintesi, mentre la scansione delle porte è chiaramente un'attività di ricognizione mirata ma estesa, la natura dei comandi `chmod` e `chown` è la chiave per determinare se l'incidente sia progredito a una compromissione più profonda.

4. Raccomandazioni e Azioni Correttive

Data la chiara evidenza di attività di scansione e il potenziale (da verificare) di compromissione del sistema, è imperativo agire con urgenza.

A. Azioni Immediate (Risposta all'Incidente / Contenimento):

1. Determinazione della Natura dei Comandi `chmod` e `chown`:

- **Priorità assoluta:** Indagare immediatamente sul sistema su cui sono stati eseguiti i comandi `chmod ugo+rw Cattura_U3_W1_L5.pcapng` e `chown kali Cattura_U3_W1_L5.pcapng` (come mostrato in **Figura 6**). Determinare se tali azioni siano state legittime (eseguite dall'analista o da un processo autorizzato) o un'attività malevola.
- Se l'azione fosse legittima, le raccomandazioni di compromissione di sistema di seguito sono meno stringenti e l'attenzione si concentra sulla scansione.
- **Se fosse un'azione malevola, considerare il sistema compromesso e procedere immediatamente con le azioni 2 e 3 relative al sistema compromesso.**

2. Identificazione e Isolamento dei Sistemi Coinvolti (se compromessi):

- Identificare e isolare immediatamente l'host attaccante (192.168.200.100) e, **se la compromissione è confermata sul sistema che ha eseguito il `chmod` o sul target 192.168.200.150**, isolare anche questi dalla rete. Questo può essere realizzato bloccando le porte fisiche dello switch, applicando regole di deny sul firewall o segmentando temporaneamente gli host in VLAN di quarantena.

3. Avvio Immediato di Analisi Forense Approfondita (se compromissione confermata):

- **Se si conferma la natura malevola dei comandi chmod/chown o altre evidenze di compromissione**, è cruciale eseguire un'**analisi forense completa** sui sistemi compromessi. Questo include:
 - Identificare la *root cause* dell'accesso (quale vulnerabilità è stata sfruttata, quali credenziali sono state usate).
 - Ricercare malware, backdoor, account utente non autorizzati o privilegi elevati.
 - Analizzare i log di sistema (event viewer, bash history, auth.log, syslog) per attività sospette, inclusa l'esecuzione di comandi.
 - Analizzare il filesystem per modifiche non autorizzate, file creati o modificati.
 - Considerare il **ripristino dei sistemi da un backup pulito e verificato o la ricostruzione da zero**.

4. Allerta e Coordinamento del Team di Sicurezza:

- Comunicare tempestivamente questa attività sospetta e, se confermata, la compromissione al Security Operations Center (SOC) o al team IT/Sicurezza responsabile. Avviare la procedura standard di risposta agli incidenti, inclusa la documentazione dettagliata di tutte le azioni intraprese.

B. Azioni Preventive (Rafforzamento della Sicurezza a Lungo Termine):

1. Segmentazione di Rete Robusta e Regole Firewall Granulari:

- Implementare una robusta **segmentazione di rete** (es. attraverso VLAN, sottoreti dedicate e firewall interni/ACL sugli switch L3) per limitare la comunicazione tra host e sottoreti ai soli flussi strettamente necessari (principio del minimo privilegio).
- Configurare i firewall per implementare regole di denial by default e per applicare funzionalità avanzate di **Rate Limiting** e **Flood Protection** per mitigare le scansioni di porta aggressive.

2. Hardening Approfondito dei Sistemi Operativi e delle Applicazioni:

- Su tutti i sistemi, inclusi il target 192.168.200.150 e i sistemi potenzialmente compromessi, applicare il principio del **minimo privilegio funzionale**: **chiudere tutte le porte non essenziali (in particolare quelle identificate come aperte che non sono strettamente necessarie, come 21, 23, 512, 514)** e disabilitare i servizi di rete non indispensabili.

- Mantenere tutti i sistemi operativi, le applicazioni e i software di rete costantemente **aggiornati** con le ultime patch di sicurezza per correggere le vulnerabilità note (CVE).
- Implementare un rigoroso **monitoraggio dell'integrità dei file (FIM)** e delle modifiche ai permessi di file critici e ai file di configurazione di sistema. Utilizzare strumenti FIM per rilevare immediatamente modifiche sospette (come `chmod ugo+rw` su file o directory non attesi).

3. Implementazione e Ottimizzazione di Sistemi IDS/IPS Avanzati:

- Assicurarsi che i sistemi di Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) siano correttamente configurati, con firme aggiornate, per rilevare e, idealmente, bloccare automaticamente le attività di scansione delle porte e, crucialmente, i tentativi di exploit e le attività di post-exploitation.

4. Monitoraggio e Logging Avanzato con SIEM e SOAR:

- Centralizzare i log di sicurezza (provenienti da firewall, IDS/IPS, server, router, switch e endpoint) in un sistema di **Security Information and Event Management (SIEM)**.
- **Espandere la raccolta log per includere eventi di sistema operativo dettagliati relativi all'esecuzione di comandi (es. bash history, log di auditd per Linux), modifiche ai permessi di file, creazione di nuovi processi, creazione/modifica di account utente e tentativi di login non autorizzati.**
- Configurare regole di correlazione nel SIEM per allertare su sequenze di eventi sospette (es. scansione seguita da tentativo di exploit, login anomalo, e poi modifiche ai permessi o creazione di nuovi processi).
- Considerare l'implementazione di una piattaforma **SOAR (Security Orchestration, Automation and Response)** per automatizzare la risposta a incidenti di alto profilo.

5. Audit di Sicurezza Regolari e Penetration Testing Completì:

- Condurre regolarmente **scansioni di vulnerabilità** interne ed esterne, e **penetration test** (simulazioni di attacco) che includano fasi di post-exploitation. Questo approccio proattivo permette di identificare le debolezze della rete e dei sistemi prima che possano essere scoperte e sfruttate da attori malevoli e di testare la capacità di rilevamento e risposta dell'organizzazione.

Conclusioni Finali:

L'analisi forense del traffico di rete ha rivelato la presenza di una persistente e sistematica attività di ricognizione interna, originata da 192.168.200.100 e mirata a 192.168.200.150. Questa attività, caratteristica dello strumento Nmap su sistema Linux e mirata a un set di

porte comuni, non standard e in range più elevati, ha avuto successo nell'identificare numerosi servizi attivi sul target, rendendo la macchina vulnerabile a potenziali exploit.

L'osservazione dell'esecuzione dei comandi `chmod ugo+rw Cattura_U3_W1_L5.pcapng` e `chown kali Cattura_U3_W1_L5.pcapng` su un sistema che gestisce il file della cattura rappresenta un **potenziale indicatore di compromissione a livello di sistema**. Se tali azioni non fossero state iniziate da un'operazione legittima e autorizzata (es. da un analista per la gestione del file), indicherebbero che l'attaccante ha ottenuto un controllo esecutivo su un sistema all'interno della rete, superando la fase di ricognizione per passare a quella di post-exploitation.

È di **critica importanza e urgenza massima** che l'organizzazione agisca immediatamente per contenere l'incidente, determinare la natura dei comandi `chmod` e `chown` e, se la compromissione fosse confermata, avviare un'analisi forense approfondita. È fondamentale implementare con celerità le raccomandazioni di sicurezza proposte per rafforzare drasticamente la postura di sicurezza, eliminare qualsiasi accesso non autorizzato e prevenire futuri incidenti di questa gravità.