Modul_27_2_14_Isolate_Compromised_Host_Using_5-Tuple

Part 1: Review Alerts in Sguil

f)

What kind of transactions occurred between the client and the server in this attack?

 Útočník si vytvořil údaje pro usera myroot v /etc/shadow a v /etc/passwd (pravděpodobně na zpětné připojení)

Part 2: Pivot to Wireshark

b)

What did you observe? What do the text colors red and blue indicate?

TCP follow stream s dotazy (commandy) útočníka a odpovědi napadeného zařízení.

The attacker issues the whoami command on the target. What does this show about the attacker role on the target computer?

Přes jaký účet se dostal do napadeného zařízení. (metasploitable)

Scroll through the TCP stream. What kind of data has the threat actor been reading?

Data v /etc/shadow (hesla) a v /etc/passwd (údaje o uživatelích).

Part 3: Pivot to Kibana

e)

What are the source and destination IP addresses and port numbers for the FTP traffic?

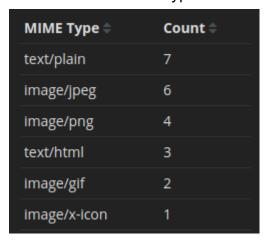
	Time →	source_ip	source_port	destination_ip	destination_port	_id
٠	June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LDjqzXIB B6Cd0 SbfgO
•	June 11th 2020, 03:53:(Q Q	192.168.0.11	52776	209.165.200.235	21	LTjqzXIB B6Cd0 SbfgO

What are the user credentials to access the FTP site?

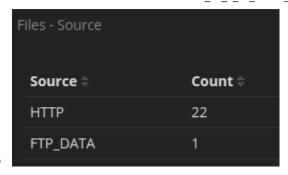
```
SRC: USER analyst
  SRC:
  DST: 331 Please specify the password.
  DST:
  SRC: PASS cyberops
  SRC:
  DST: 230 Login successful.
DST:
  cleková komunikace s FTP
   DST: 220 (vsFTPd 2.3.4)
   DST:
   SRC: USER analyst
   SRC:
   DST: 331 Please specify the password.
   DST:
   SRC: PASS cyberops
   SRC:
   DST: 230 Login successful.
   DST:
   SRC: SYST
   SRC:
   DST: 215 UNIX Type: L8
   SRC: TYPE I
   SRC:
   DST: 200 Switching to Binary mode.
   SRC: PORT 192,168,0,11,194,153
   SRC:
   DST: 200 PORT command successful. Consider using PASV.
   DST:
   SRC: STOR confidential.txt
   SRC:
   DST: 150 Ok to send data.
   DST:
   DST: 226 Transfer complete.
   DST:
   SRC: QUIT
   SRC:
   DST: 221 Goodbye.
   DST:
```

j)

What are the different types of files? Look at the MIME Type section of the screen.

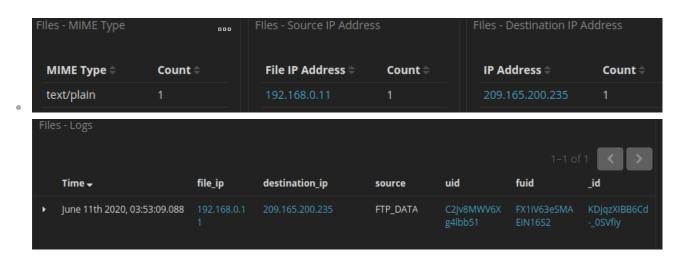


Scroll to the Files - Source heading. What are the file sources listed?



i)

What is the MIME type, source and destination IP address associated with the transfer of the FTP data? When did this transfer occur?



Došlo 11th June 2020 v 3:53

m)

What is the text content of the file that was transferred using FTP?

```
Log entry:
"Ts""2020-06-11T03:53:09.088773Z", "fulid" "FX1IV63eSMAEIN16S2", "tx_hosts"; ["192.168.0.11", "rx_hosts"; ["209.165.200.235"], "conn_uids"; ["C2Jv8MWV6Xg4lbb51"], "source": "FTP_DATA", "depth": 0, "analyzers"; ["SHAI", "MD5"], "mime_type": "text/plain", "duration": 0.0, "is_orig" "false, "seen_bytes": 102, "missing_bytes": 0, "overflow_bytes": 0, "timedout": false, "md5", "e7rocs2c0tot65666365379c91294d536b", "sha1": "f7f54acee0342f6161f8e63a10824ee11b330725")

Sensor Name: seconion-import
Timestamp: 2020-06-11 03:53:09
Connection ID: CLI
Src IP: 192.168.0.11
Dst IP: 209.165.200.235
Src Port: 49817
Dst Port: 20
OS Fingerprint: 209.165.200.235:20 - Linux 2.6 (newer, 1) (up: 1 hrs)
OS Fingerprint: > 192.168.0.11:49917 (distance 0, link: ethernet/modem)
SRC: CONFIDENTIAL DOCUMENT
SRC: DO NOT SHARE
SRC: This document contains information about the last security breach.
SRC:

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817_209.165.200.235:20-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import'AND agent_type='pcap'LiMiT 1
CAPME: Processed transcript in 0.60 seconds: 0.24 0.26 0.00 0.09 0.00

192.168.0.11:49817_209.165.200.235:20-6-516024316.pcap
```

- CONFIDETIA DOCUMENT
- DO NOT SHARE
- This document contains information about the last security breach.

With all the information has gathered so far, what is your recommendation for stopping further unauthorized access?

- Účet byl napadnut (metasploitable), takže lepší zabezpečení a vyhledal bych si jak přesně se to stalo
- Lepší FTP zabezpečení, aby se nedalo jen tak stahovat.