Command & Control - level 5 ✍

Title: Memory analysis

Point: 25 Points

Level: Medium

Description: Berthier, the malware seems to be manually maintened on the workstations. Therefore it's likely that the hackers have found all of the computers' passwords. Since ACME's computer fleet seems to be up to date, it's probably only due to password weakness. John, the system administrator doesn't believe you. Prove him wrong!

Find john password.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Solution:

Công cụ sử dụng: `Volatility`, `John the Ripper`
Tiếp tục từ **Command & Control - level 4**. Nhiệm vụ là tìm mật khẩu ông **John** này. (Vì ổng không tin mình ??)

Cái này khá dễ, nhưng mình phải biết đến khái niệm "Security Accounts Manager" (SAM). Reference link

The SAM registry file có được lưu trữ tại `C:\WINDOWS\system32\config`, nhưng nó lúc nào cũng bị lock vào không thể xâm nhập trực tiếp vào. Nhiệm vụ chính là giữ mật khẩu đăng nhập Window dưới dạng hash đê khi người dùng nhập mật khẩu thì nó sẽ hash ra và đối chiếu.
Chúng ta có thể sử dụng công cụ để crack nếu mật khẩu này đủ yếu.

Đầu tiên, hiển thị thông tin danh sách hive. Dùng `hivelist`:

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 hivelist
```

```
┌──(virus㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

Sau đó dump **SAM file** để tìm hash password. Sử dụng `hashdump` với `-y` flag trỏ đến virtual address của `\REGISTRY\MACHINE\SYSTEM` và `-s` trỏ vào `\SystemRoot\System32\Config\SAM`. View usages here

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 hashdump -y 0x8b21c008 -s 0x9aad6148 > ~/hashedPassword.txt
```

Xuất vào file `hashedPassword.txt` cho tiện sử dụng sau này. Xem lướt một chút nội dung của nó

```
┌──(virus㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ cat ~/hashedPassword.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930:::
```

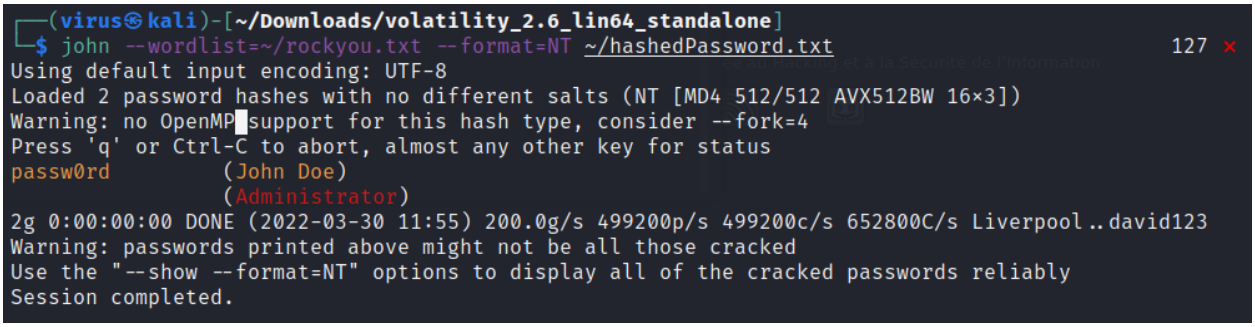
Nếu muốn tìm hiểu chuyên sâu, tham khảo tại SAM file structure / LM and NT hash

Chúng ta chỉ quan tâm đến **NT** hash. Cracking **LM** sẽ không mang lại kết quả, nó chỉ tạo ra để cho tương thích ngược (backward compatibility) nếu Window ở các phiên bản hệ cũ. Mình sử dụng tool có sẵn trong máy **Kali Linux** `john` (hoặc có thể cài đặt tool tương tự `johnny`) để crack hash string, sử dụng `rockyou.txt` có sẵn làm wordlist

```
cp /usr/share/wordlists/rockyou.txt.gz ~ && gzip -d ~/rockyou.txt.gz
```

Chỉ để tiện dùng thui :)) -> Sau đó dùng cái wordlist này đi crack các hash trong file `hashedPassword.txt`:

```
john --wordlist=~/rockyou.txt --format=NT ~/hashedPassword.tx
```



Wonderful !!! `passw0rd` là password cho `(John Doe)`
Flag: **passw0rd**