Weaponizing Active   
Directory

Text, whiteboard

Description automatically generated

Summary

Attack Explains: In previous attack, we have gained access to the windows 10 using evil-winrm and brailee.ogden credentials. Now, we can execute ASMI Bypass to run malicious activity in the windows 10. We are going to use the tool Sharphound to gather the Active Directory information, and using the tool BloodHound to analyze domain users, and path to gain privilege in the domain.

Target Address: 192.168.3.80

Target System: Windows 10 Password: ‘Winter2022’

Account Compromised: brailee.ogden (windows account)

Tools: SSh, Evil-winrm, Invoke-Snow.ps1, Proxychains, SharpHound, BloodHound.

First off, we are going to download Sharphound.ps1 from github and put it into exefiles directory for easy access for uploadin the first in the windows 10.

Text

Description automatically generated

Verify the SharpHound.ps1 is in the exefiles

Text

Description automatically generated

After established the ssh reverseshell from previous technique, we use proxychains to pivot and hide our identity. And add – s path-to-scripts-file and – e path-to-execute-files which where SharpHound.ps1 is.

Then execute, Innoke-Snows.ps1 to AMSI bypass so you can run SharpHounds.ps

After that, run “menu” command to show the options of Invoke-BloodHound.ps1

Text

Description automatically generated

Then select Invoke-BloodHound and execute the command “Invoke-BloodHound -ldapusername <usersname> -ldappassword <password> -domain <domain >”

Text

Description automatically generated

After execute the command, wait a few minutes because it creates a big file that has the info of the domain.

If it appears a file “xxxxx\_BloodHound.zip” meaning the Invoke-BloodHound.ps1 execute properly.

Graphical user interface, text

Description automatically generated

Create a downloads directory in your evil-winrm folder for downloading files from Evil-winrm.

Graphical user interface, application, website

Description automatically generated

Now we are going to download the BloodHound.zip file to kali using download command

“download path-to-download-directory” and rename it. And it shows in the info: Download successful!

Graphical user interface, text, application

Description automatically generated

We are going to install BloodHound, you can use “apt-get install BloodHound” to download BloodHound. In this case, for compatibility issue. I am going to downgrade to 3.0.5 version from web browser and download the right file, in this case, the linux-x64.zip version for kali linux proper compatibility.

Graphical user interface, text

Description automatically generated

Install neo4j using “apt-get install neo4j” this is to establish database service for BloodHound. and access the <http://localhost:7474> to set up bloodhould access credential.

Text

Description automatically generated

Go to Download directory and unzip BloodHound. and use linux ./ execute command to run 3.0.5 downgraded bloodhound

Graphical user interface, text, application, chat or text message

Description automatically generated

Insert the credentials that you set up in the <http://localhost:7474> to gain access bloodhound programe

Graphical user interface, text, application

Description automatically generated

On the right top corner, you can clink on “upload data” icon to upload the BloodHound.zip which the info were gather in the windows 10.

A screenshot of a computer

Description automatically generated with medium confidence

After successful upload, the database info will shows the data number on the left corner.

Graphical user interface

Description automatically generated

We are going to run three queries to find some sensitive info about the domain

Find all Domain Admins  
Find Shortest Paths to Domain Admins  
Shortest path to High Value Targets

This is the Shortest Paths to Domain Admins

A picture containing graphical user interface

Description automatically generated

These are all Domain Admins

A picture containing chart

Description automatically generated

Shortest path to High Value Targets

Diagram

Description automatically generated

Three found Admin Domain members are

[ansible@windomain.local](mailto:ansible@windomain.local)

[administrator@windomain.local](mailto:administrator@windomain.local)

[laser.service@windomain.local](mailto:laser.service@windomain.local)

Graphical user interface, application

Description automatically generated