Internal Password Spray

Summary

Attack Explains:

We are using socks proxy via vagrant account so we can be hidden our attack, using this we can perform password attack inside of the attack network. Search found that windows OS has vulnerability of smb protocol, we are going to use smb protocol to exploit the vulnerability.

Target Address: 172.26.14.94 Target OS: Windows 10

Target Account: brailee.ogden Password Found: Winter2022

Tools/Techniques: Proxychains, Nmap, Metasploit, smb protocals, SMB\_login

Set up our connections using reverse socks proxy

Text

Description automatically generated

Make use configure proxychins4.cons

Text, logo

Description automatically generated

Delete # to enable quie\_mode

Graphical user interface

Description automatically generated

And make sure the socks proxy is configures

A picture containing shape

Description automatically generated

Verify the socks proxy using nmap via proxychains.

Text

Description automatically generated

Text

Description automatically generated

Perform password spray via Proxychains

This is the passwords and names for the password attack

Text

Description automatically generated

Text

Description automatically generated

Use Metasploit via proxychains to use our identity.

Text

Description automatically generated

We are going to use smb\_login tools in the Metasploit

Graphical user interface, text

Description automatically generated

Set up the configurations that match the target information.

Text

Description automatically generated

As it shows, the password is found and successfully performed via proxychains.

A picture containing text

Description automatically generated