SMB Weakness  
(Blue)

Text

Description automatically generated with medium confidence

Tools to Accomplish the Attack

According to MITRE ATTACK FRAMEWORK. [CrackMapExec](https://attack.mitre.org/software/S0488), or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. [CrackMapExec](https://attack.mitre.org/software/S0488) collects Active Directory information to conduct lateral movement through targeted networks.[[1]](https://github.com/byt3bl33d3r/CrackMapExec/wiki/SMB-Command-Reference" \t "_blank)

(SMB Command Execution) ipconfig

We can use the crackmapexec to windows domain, as we see the domain name is Windomain.local, I assume it can be windows system. As research found that SMB protocol is vulnerability for windows. We use smb for crackmapexe to execute “ifconfig” to test out.

Graphical user interface, text

Description automatically generated

(WinRM Execution) Whoami

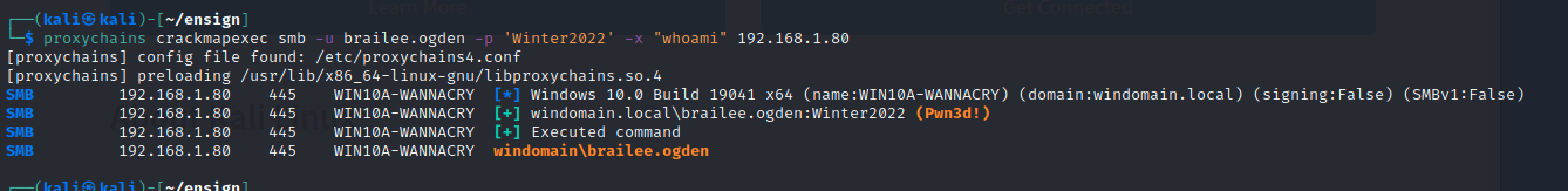
However, I tried to execute “whoami” with winrm protocol on crackmapexec, and it is not executable. It looks like winrm is disable in the windows server.

Text

Description automatically generated

Trying to execute same command “whoami” with smb, and it executed successfully.

(-x meaing to execute cmd command lines)



CrackMapExec (Powershell Execution)

As I changed -x to -X upper case, it changed to powershell execution, using Get-service command which is pwershell command to test out, and it executes successfully.

Timeline

Description automatically generated

Identify Services Running

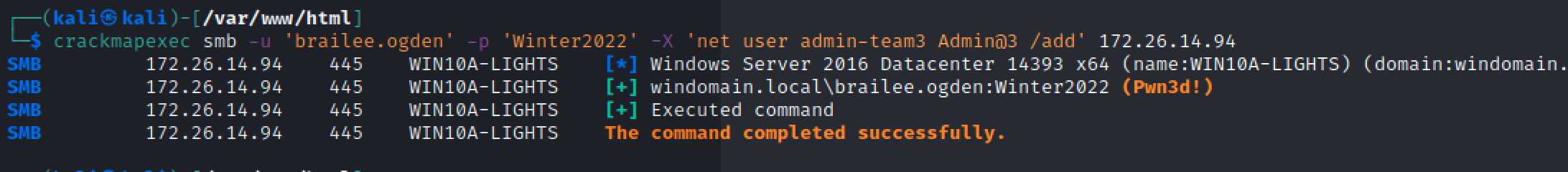
Text

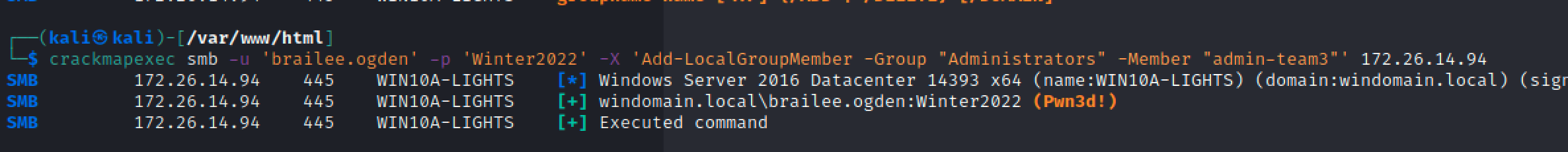
Description automatically generated

Find local user accounts

Timeline

Description automatically generated  
Create a user account called admin-teamx

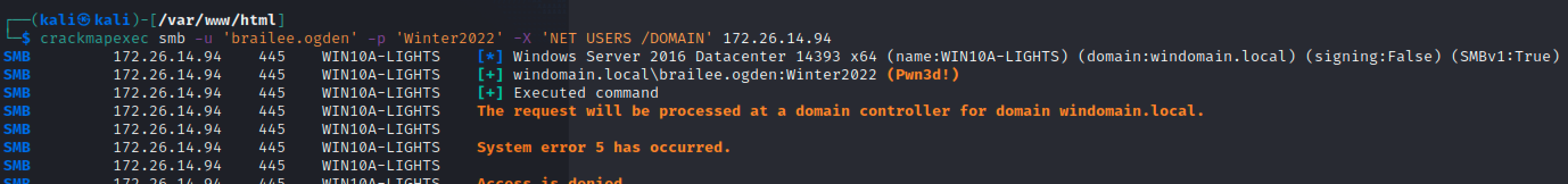
  
● Add the account as a local administrator

  
 ● Check Scheduled Tasks

Text

Description automatically generated  
● Find domain user accounts

No found

  
● Identify network connections

A picture containing text

Description automatically generated  
● Disable the Windows Firewall

A screenshot of a computer

Description automatically generated