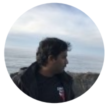

Bbinfosec Follow
Jul 9, 2018 · 2 min read

Windows Active Directory Post Exploitation Cheatsheet

During the course of Pentesting Post exploitation stage is important, The following commands will give you up some cheatsheet/ready made commands for gaining potential information.

The commands listed in this article are native queries to the Active Directory (no binaries or malicious code). Once completed, they return information about any and all resources inside, including: users, servers, applications, identities, and naming conventions.

Try it on your Domain: copy and paste any of the commands into a command line or PowerShell (indicated with brackets next to each command). Perform reconnaissance like an attacker

1. **Fundamental Reconnaissance :**

whoami
 [cmd or PowerShell]
Tells us which user we are authenticated as

gpresult /R
[cmd or PowerShell]
Gives us the effective user permissions and the group policies enabled of the account

nltest /dclist: [cmd or PowerShell] Lists all Domain Controllers

([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).Sites | select Name, Subnets[PowerShell]
Shows us the subnets of the network

2.Servers, Computers & Applications Reconnaissance :

net group "domain computers"/ domain

[cmd or PowerShell] Gives us a full list of all the workstations and servers joined to the Domain *(([adsisearcher]”(name=Computer)”).FindAll()) | Select -Expand*

Properties [PowerShell] Gives us all attributes associated with a particular computer

*([adsisearcher]”(& (objectClass=Computer(servicePrincipalName=*X*))”).FindAll()*

[PowerShell] Enumerates all of the computers and servers in the domain that are running X application (dfs,MSSQL)

3.Identities, Credentials & Privileged Users Reconnaissance:

net group “domain admins ” / domain

[cmd or PowerShell] Gives us a list of the designated administrators joined to the Domain

([adsisearcher]”(&(admincount=1))”).FindAll() [PowerShell]

Filters for all privileged accounts

```
(([adsisearcher]”(name=UserName)”).FindAll()) | Select -Expand Properties
```

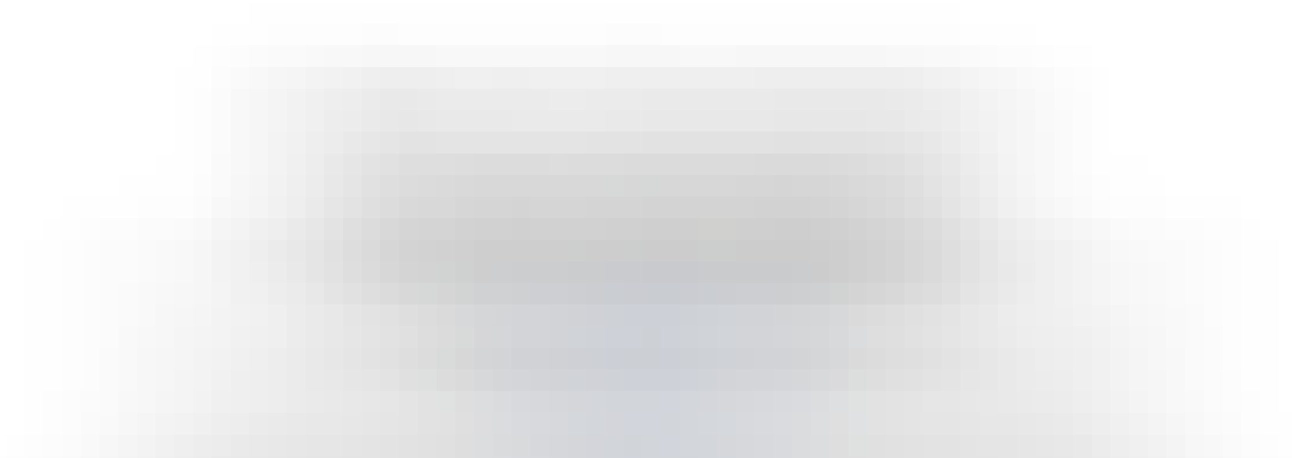
[PowerShell]

Gives us all attributes associated with a particular user.

```
([adsisearcher]”(&(objectClass=User)(primarygroupid=513)(servicePrincipalName=*))”).FindAll()|ForEachObject{“Name:$($_.properties.name)”””SPN:$($_.properties.serviceprincipalname)”””Path:$($_.Path)””””}
```

Enumerates all of the crackable service accounts

Additional Reference :



http://www.handgrep.se/repository/cheatsheets/postexploitation/

Happy Hunting.

Active Directory | Pentesting | Hackernoon | Cheatsheet | Red Team

1 clap

Bbinfosec

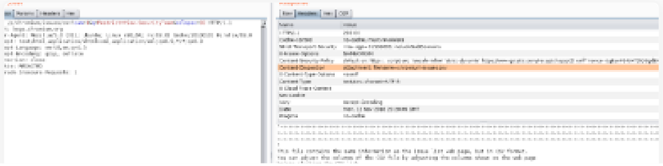
Just another guy whom loves to play around 0 and 1

Follow

Ligoat Security

Got Goat? Security ...

Compromise creds
Remote code execution
Low privileges Lateral movement cycle
Week
Asset recon
Local privilege escalation
High privileges Lateral movement cycle
Months
Remote code execution



Related reads

VulnHub — Kioptrix: Level 3

Mike Bond

Jun 1, 2018 · 14 min rea

233

Also tagged Active Directory

The Art of Cyber Warfare: Defending The Fortress

Rob Webb

Mar 19 · 24 min read

211

Related reads

XS-Searching Google’s bug tracker to find out vulnerable source code

Luan Herrera

Nov 19, 2018 · 6 min r

908

Responses

Write a response...