Another

03 March 2025 19:10

GEOLOCATION

Cd BillChipher
Sudo su
Python3 Billchipher.py

DNS ZONE TRANSFER ALLOW / NOT?

Dig url axfr

LDAP ENUM how many user acc associated domain ? Or, LDAP version on DC

ldapsearch -x -h **DCIP** -b "DC=**ABCORG**,DC=com" "objectclass=user" enm

[2049] NFS port

DNS ENUM find name server?

Dnsenum url

SMB ENUM MSG SIGN EN/DIS?

Nmap -sV -T4 -A IP

PASS auditing on a svr. Find the pass a user john?
Win > sys hacking > lc7

MAL ANALY: .elf FILE CPU ARCHTECH FIND
Win > malwa anz > GHIDRARUN.bat

MALICIOUS APK using which PERMISSION check ?
Web > sisik.eu

CMS identify ?
Wig url

IDENTIFY LOAD BALANCING on a srvce?
Ibd domain (lin)

BANNER GRAB web app & find ETAG target sys?
Uniscan -u domain [find IP]
Curl -I IP

Enumerate Domain Users

net user /domain
Lists all users in the Active Directory domain.

2. Get Detailed Information on a Specific User

net user <username> /domain
Shows detailed information about a specific domain user (replace <username> with the target username).

3. List Domain Groups

net group /domain
Lists all groups in the Active Directory domain.

4. Get Detailed Information on a Specific Group

net group "<group_name>" /domain
Displays detailed information about a specific domain group, including its members (replace <group_name> with the group name).

5. Enumerate Domain Admins

net group "Domain Admins" /domain
Lists all members of the "Domain Admins" group.

6. Enumerate Local Administrators

net localgroup Administrators
Lists all members of the local Administrators group on the system.

7. List Computers in the Domain

net view /domain
Displays all computers in the domain.

8. Get Information on a Specific Computer

net view \\<computer_name>
Shows shared resources on a specific computer (replace <computer_name> with the target computer's name).

9. Enumerate Domain Controllers

net group "Domain Controllers" /domain
Lists all Domain Controllers within the domain.

10. List All Network Shared Resources

net share
Lists all shared resources on the local machine.

11. Enumerate Sessions on a Remote Machine

net session \\<computer_name>
Lists all active sessions on a specific computer (replace <computer_name> with the target computer's name).

12. Enumerate Trust Relationships

netdom trust <domain> /domain:<other_domain> /enumerate
Lists trust relationships with other domains (requires netdom tool, replace <domain> and <other_domain> with the respective domains).

13. View Active Directory Domain Policies

net accounts /domain
Shows account policies for the Active Directory domain, including password policies and lockout policies.

14. List Global Group Members

net group "<group_name>" /domain
Shows all members of a specified global group (replace <group_name> with the name of the global group).

15. Display Logged-in Users on the Network

net user
Lists users currently logged into the network.

Get-ADUser -Identity gordon.stevens -Server za.tryhackme.com -Properties *

Get-ADUser -Filter 'Name -like "*stevens"' -Server za.tryhackme.com | Format-Table Name,SamAccountName -A

Get-ADGroup -Identity Administrators -Server za.tryhackme.com

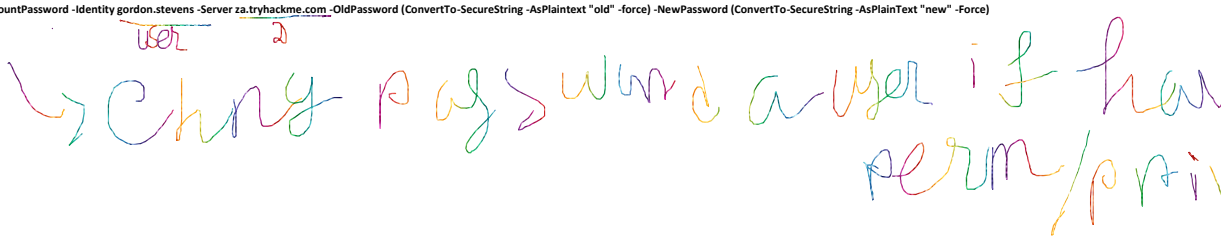
Get-ADGroupMember -Identity Administrators -Server za.tryhackme.com

```
$ChangeDate = New-Object DateTime(2022, 02, 28, 12, 00, 00)
Get-ADObject -Filter 'whenChanged -gt $ChangeDate' -includeDeletedObjects -Server za.tryhackme.com
```

if we are looking for all AD objects that were changed after a specific date:

Get-ADDomain -Server za.tryhackme.com

Set-ADAccountPassword -Identity gordon.stevens -Server za.tryhackme.com -OldPassword (ConvertTo-SecureString -AsPlaintext "old" -force) -NewPassword (ConvertTo-SecureString -AsPlainText "new" -Force)



PS AD ENUM:

value of the title attribute of BETH NOLAN
Get-ADUser -Identity beth.nolan -Server DOMAIN -Properties *

value of the DistinguishedName attribute of Annette Manning
Get-ADUser -Identity USERNAME -Server DOMAIN -Properties *

When tier 2 admins group created
Get-ADGroup -Identity "Tier 2 Admins" -Server DOMAIN
Get-ADGroup -Identity "GROUPNAME" -Server DOMAIN -Properties *

value of the SID attribute of the Enterprise Admins group
Get-ADGroup -Identity "GROUPNAME" -Server DOMAIN -Properties *

Which container is used to store deleted AD obj
Get-ADDomain -Server DOMAIN