Powerview-Post Compromise Enumeration

Download the Powerview tool raw from Github and copy in a text editor and save as .ps1 file;

Once we gain a Shell of one of the clients on Network;

Change the shell to powershell;

Update the list of packages

sudo apt update

Install pre-requisite packages.

sudo apt install -y wget apt-transport-https software-properties-common

Download the Microsoft repository GPG keys

wget -q "https://packages.microsoft.com/config/ubuntu/$(lsb_release -rs)/packages-microsoft-prod.deb"

Register the Microsoft repository GPG keys

sudo dpkg -i packages-microsoft-prod.deb

Update the list of packages after adding packages.microsoft.com repository

sudo apt update

Install PowerShell

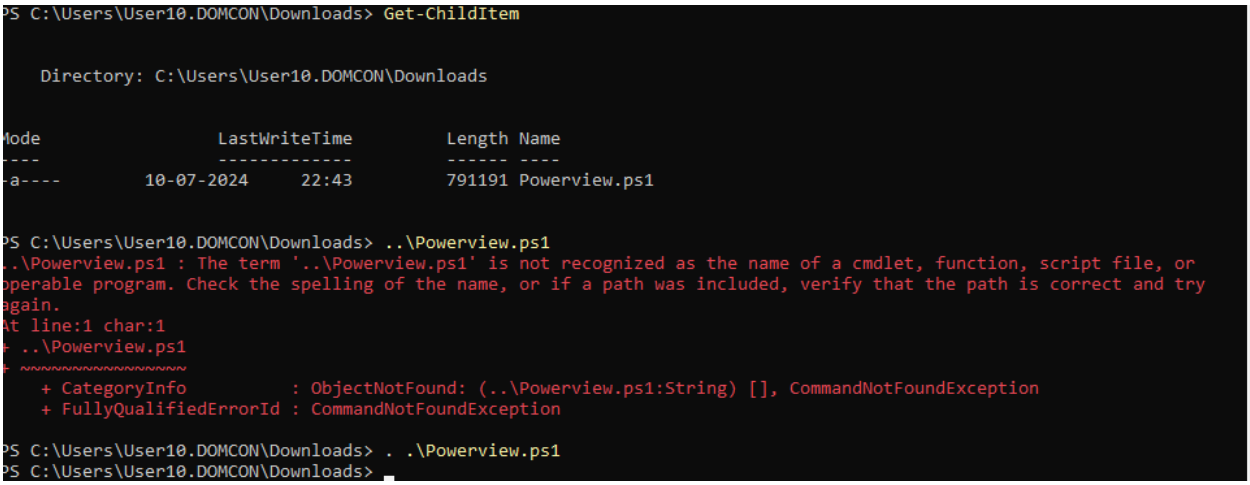
sudo apt install -y powershell

Upload the powerview tool on the shell;

Once uploaded;

Then run the following command:

powershell -ep bypass (this bypass the execution protocol and let's you run commands without interuption)



Make sure to include the space between the two dots. This command will load the functions and cmdlets defined in `PowerView.ps1` into your current session.

Now run the available commands for information

Example of some of the commands

Get-NetDomain

```
PS C:\Users\User10.DOMCON\Downloads> Get-NetDomain


Forest                  : Domcon.com
DomainControllers       : {Server.Domcon.com}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : Server.Domcon.com
RidRoleOwner            : Server.Domcon.com
InfrastructureRoleOwner : Server.Domcon.com
Name                    : Domcon.com
```

Get-NetDomainController

To fetch IPv4

$ipv4Addresses = $domainControllers | ForEach-Object {
$
*.IPAddress | Where-Object { $* -match '^\d{1,3}(\.\d{1,3}){3}$' }
}

```
PS C:\Users\User10.DOMCON\Downloads> Get-NetDomainController


Forest                     : Domcon.com
CurrentTime                : 10-07-2024 17:26:55
HighestCommittedUsn        : 65600
OSVersion                  : Windows Server 2016 Standard Evaluation
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : Domcon.com
IPAddress                  : 2405:201:3031:38d6:3c05:8a42:33ee:77c1
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : Server.Domcon.com
Partitions                 : {DC=Domcon,DC=com, CN=Configuration,DC=Domcon,DC=com,
                             CN=Schema,CN=Configuration,DC=Domcon,DC=com, DC=DomainDnsZones,DC=Domcon,DC=com...}
```

Get-DomainPolicy

```
PS C:\Users\User10.DOMCON\Downloads> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=7; PasswordComplexity=1;
                 PasswordHistorySize=24; LockoutBadCount=0; RequireLogonToChangePassword=0;
                 ForceLogoffWhenHourExpire=0; ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Version        : @{signature="$CHICAGO$"; Revision=1}
Path           : \\Domcon.com\sysvol\Domcon.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windo
                 ws NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

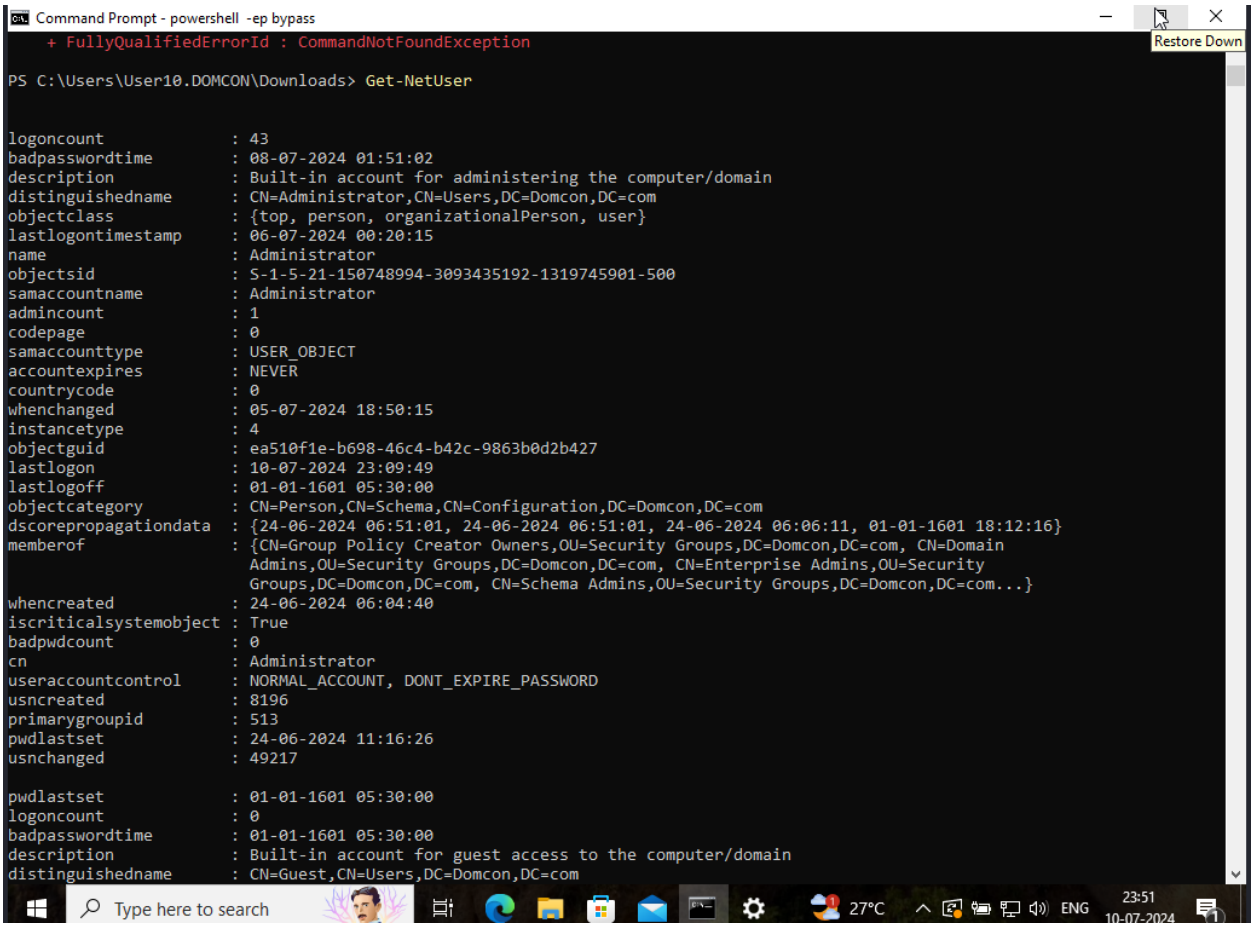
(Get-DomainPolicy).”system access”

```
PS C:\Users\User10.DOMCON\Downloads> (Get-DomainPolicy)."system access"
PS C:\Users\User10.DOMCON\Downloads> (Get-DomainPolicy)."systemaccess"


MinimumPasswordAge            : 1
MaximumPasswordAge            : 42
MinimumPasswordLength         : 7
PasswordComplexity            : 1
PasswordHistorySize           : 24
LockoutBadCount               : 0
RequireLogonToChangePassword  : 0
ForceLogoffWhenHourExpire     : 0
ClearTextPassword             : 0
LSAAnonymousNameLookup        : 0


PS C:\Users\User10.DOMCON\Downloads>
```

Get-NetUser



This data should also tell us about Honeypot in the network

If any user has not logged in for a long time, that might be a honeypot created just to get us tricked.

Read through the lines while doing the Enumeration

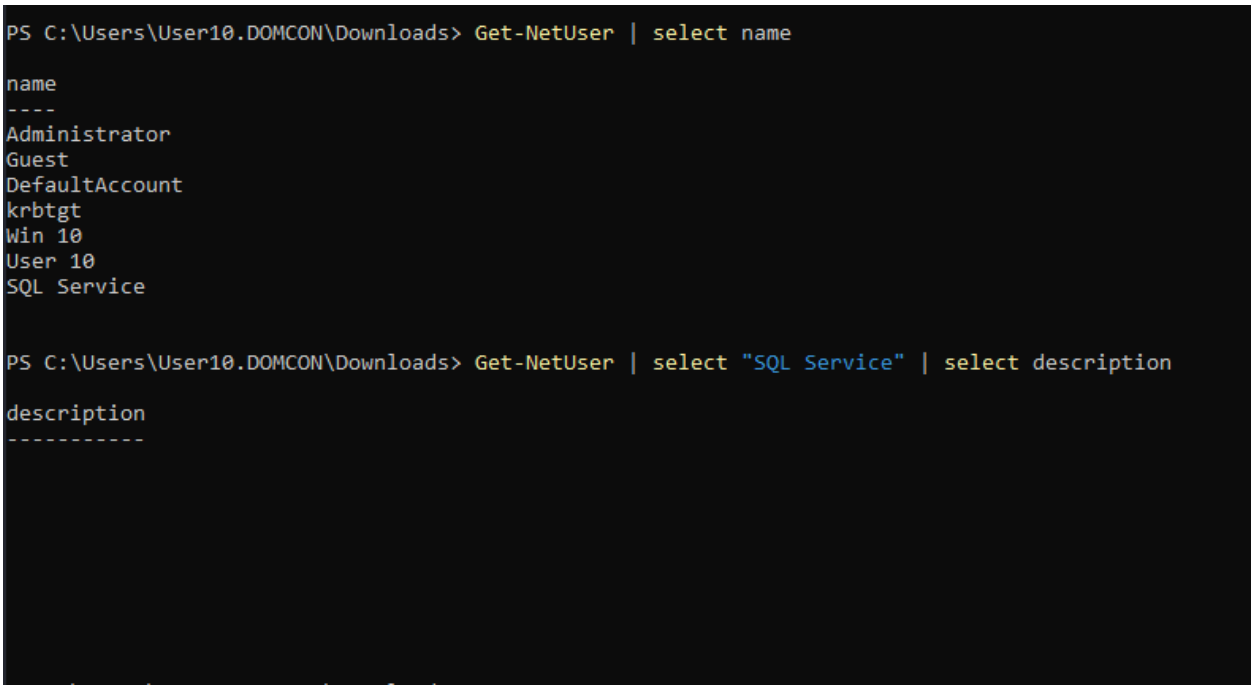
To get the User names

Get-NetUser | select samaccountname

or Get-NetUser | select cn

or Get-NetUser | select name

Anything in the components can be selected at the place of name



Get-UserProperty -Properties logoncount

Get-UserProperty -Properties badpwd

Get-NetComputer -FullData

Get-NetGroup

Get-NetGroup -GroupName “admin”

Get-NetGroupMember -GroupName “group name”

Invoke-Sharefolder

Get-NetGPL (group policy)