

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 interruption)

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

Directory: C:\Users\User10.DOMCON\Downloads

Mode                LastWriteTime         Length Name
----                -
-a-----         10-07-2024    22:43           791191 Powerview.ps1

PS C:\Users\User10.DOMCON\Downloads> ..\Powerview.ps1
..\Powerview.ps1 : The term '..\Powerview.ps1' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
At line:1 char:1
+ ..\Powerview.ps1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (..\Powerview.ps1:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\User10.DOMCON\Downloads> . .\Powerview.ps1
PS C:\Users\User10.DOMCON\Downloads>
```

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}
GPDisplayName : 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

```
Command Prompt - powershell -ep bypass
+ FullyQualifiedErrorId : CommandNotFoundException

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

logoncount           : 43
badpasswordtime      : 08-07-2024 01:51:02
description           : Built-in account for administering the computer/domain
distinguishedname     : CN=Administrator,CN=Users,DC=Domcon,DC=com
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 06-07-2024 00:20:15
name                  : Administrator
objectsid             : S-1-5-21-150748994-3093435192-1319745901-500
samaccountname        : Administrator
admincount            : 1
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 05-07-2024 18:50:15
instancetype          : 4
objectguid            : ea510f1e-b698-46c4-b42c-9863b0d2b427
lastlogon             : 10-07-2024 23:09:49
lastlogoff            : 01-01-1601 05:30:00
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=Domcon,DC=com
dscorepropagationdata : {24-06-2024 06:51:01, 24-06-2024 06:51:01, 24-06-2024 06:06:11, 01-01-1601 18:12:16}
memberof              : {CN=Group Policy Creator Owners,OU=Security Groups,DC=Domcon,DC=com, CN=Domain
                        Admins,OU=Security Groups,DC=Domcon,DC=com, CN=Enterprise Admins,OU=Security
                        Groups,DC=Domcon,DC=com, CN=Schema Admins,OU=Security Groups,DC=Domcon,DC=com...}
whencreated           : 24-06-2024 06:04:40
iscriticalsystemobject : True
badpwdcount           : 0
cn                    : Administrator
useraccountcontrol     : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated             : 8196
primarygroupid         : 513
pwdlastset             : 24-06-2024 11:16:26
usnchanged             : 49217

pwdlastset            : 01-01-1601 05:30:00
logoncount             : 0
badpasswordtime        : 01-01-1601 05:30:00
description            : Built-in account for guest access to the computer/domain
distinguishedname      : CN=Guest,CN=Users,DC=Domcon,DC=com
```

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

```
PS C:\Users\User10.DOMCON\Downloads> Get-NetUser | select name
name
----
Administrator
Guest
DefaultAccount
krbtgt
Win 10
User 10
SQL Service

PS C:\Users\User10.DOMCON\Downloads> Get-NetUser | select "SQL Service" | select description
description
-----
```

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)