

POWERSHELL

POWERVIEW

Active Directory Enumeration Guide
For

Red Teamers

Contents

Introduction.....	4
Get-NetUser.....	4
Get-UserProperty.....	9
Find-UserField.....	10
Invoke-UserHunter.....	11
Get-NetDomain.....	12
Get-NetDomainController	13
Get-NetComputer	14
Get-UserProperty.....	17
Get-NetForest	18
Get-NetForestDomain	20
Get-NetLoggedon.....	20
Get-DomainPolicy	21
Get-NetOU.....	22
Get-NetGroup	23
Get-NetGroupMember.....	29
Get-NetGPO.....	31
Find-GPOLocation	33
Invoke-EnumerateLocalAdmin	33
Get-NetProcess	34
Invoke-ShareFinder	35
Invoke-FileFinder	36
Invoke-ACLScanner	36
Find-LocalAdminAccess	37

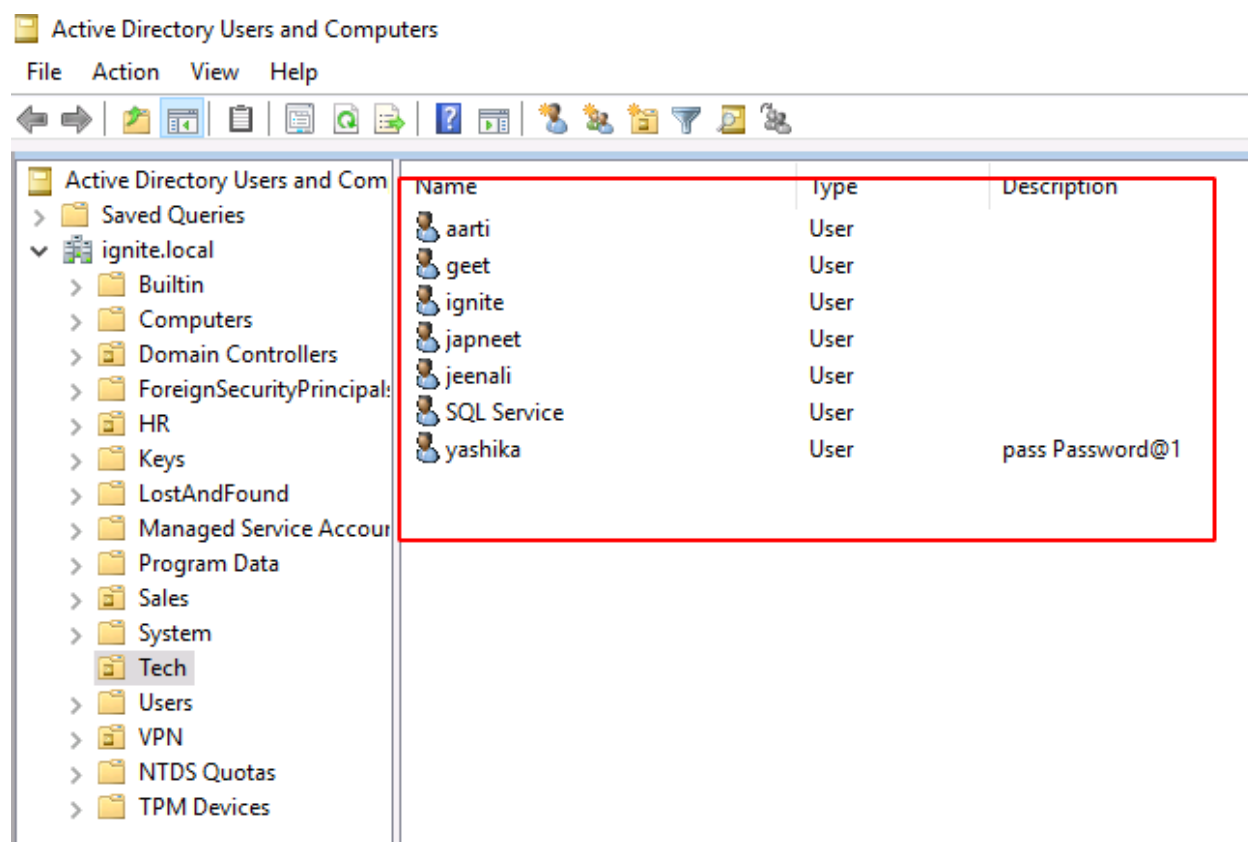
Get-NetSession	38
Conclusion	38

Introduction

We have configured an Active Directory Lab that mimics a real-life environment with a bunch of users, machines, and vulnerabilities. In this demonstration, we are focused on our ability to enumerate information that can be further used to elevate privileges or be able to help with lateral movement. A tool by the name of PowerView was developed and integrated by [Will Schroeder \(a.k.a harmj0y\)](#). It soon became an integral toolkit to perform Active Directory Attacks and Enumeration. For this demonstration, we will assume that we have gained the initial foothold. Now we will use PowerShell with PowerView to enumerate the machine and the domain. In case you run into difficulties running any of the commands depicted, use the official [GitHub](#) for the installation process.

Get-NetUser

In our Active Directory Lab Setup, we created 7 users with different roles and privileges. We can confirm this by viewing the Active Directory Users and Computers as shown in the image.



This was to show and co-relate the information that we are about to enumerate using PowerShell. The attacker has transferred the PowerView to the Target System. To run the PowerShell Script on the System, the Execution Policy must be set to Bypass as shown in the image. Next, import the modules from the PowerView Script. This was a one-time process. After this, the attacker can directly use the modules to

perform enumeration. To get the users that are active on the network, the attacker ran the following command.

```
powershell -ep bypass
Import-Module .\powerview.ps1
Get-NetUser
```

```
PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Desktop> Import-Module .\powerview.ps1
PS C:\Users\Administrator\Desktop> Get-NetUser

logoncount           : 90
badpasswordtime      : 4/7/2021 7:25:25 AM
description           : Built-in account for administering the computer/domain
distinguishedname     : CN=Administrator,CN=Users,DC=ignite,DC=local
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 4/2/2021 1:34:59 PM
name                  : Administrator
objectsid             : S-1-5-21-501555289-2168925624-2051597760-500
samaccountname        : Administrator
admincount            : 1
codepage              : 0
samaccounttype        : 805306368
whenchanged           : 4/2/2021 8:34:59 PM
accountexpires        : 9223372036854775807
countrycode           : 0
adspath               : LDAP:///CN=Administrator,CN=Users,DC=ignite,DC=local
instancetype          : 4
objectguid            : c00f6d7e-69c7-44cf-ba81-0a513e8aaac4
lastlogon             : 4/11/2021 3:32:09 AM
lastlogoff            : 12/31/1600 4:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=ignite,DC=local
dscorepropagationdata : {7/6/2020 5:39:37 PM, 7/6/2020 5:39:37 PM, 6/29/2020 4:54:4
memberof              : {CN=Group Policy Creator Owners,CN=Users,DC=ignite,DC=local
whencreated           : 6/29/2020 4:54:05 PM
iscriticalsystemobject : True
badpwdcount           : 0
cn                    : Administrator
useraccountcontrol     : 66048
usncreated             : 8196
primarygroupid         : 513
pwdlastset             : 6/29/2020 9:40:26 AM
usnchanged             : 106631

pwdlastset            : 12/31/1600 4:00:00 PM
logoncount             : 0
badpasswordtime        : 12/31/1600 4:00:00 PM
description            : Built-in account for guest access to the computer/domain
```

Users that are enumerated are not just restricted to usernames. Data collected consists of logoncount that can give an idea of an active or inactive user in the network. Next, there is a badpasswordtime which tells the last time and date that an attempt to log on was made with an invalid password on this account. Then a small description of the user with the names of groups that this particular user is part of. Finally, it

shows the date and time since the last password change. All this information is very important when the attacker is trying to learn about the user's behaviour.


```

logoncount : 60
badpasswordtime : 4/7/2021 7:12:41 AM
description : pass Password@1
distinguishedname : CN=yashika,OU=Tech,DC=ignite,DC=local
objectclass : {top, person, organizationalPerson, user}
displayname : yashika
lastlogontimestamp : 4/7/2021 7:12:47 AM
userprincipalname : yashika@ignite.local
name : yashika
objectsid : S-1-5-21-501555289-2168925624-2051597760-1103
samaccountname : yashika
admincount : 1
codepage : 0
samaccounttype : 805306368
whenchanged : 4/10/2021 2:08:59 PM
accountexpires : 9223372036854775807
countrycode : 0
adspath : LDAP://CN=yashika,OU=Tech,DC=ignite,DC=local
instancetype : 4
objectguid : d2ff2fb0-5f92-471b-b94c-a1bc5be262f2
lastlogon : 4/10/2021 7:26:55 AM
lastlogoff : 12/31/1600 4:00:00 PM
objectcategory : CN=Person,CN=Schema,CN=Configuration,DC=ignite,DC=local
dscorepropagationdata : {3/26/2021 6:37:49 PM, 1/1/1601 12:00:00 AM}
givenname : yashika
memberof : CN=Domain Admins,CN=Users,DC=ignite,DC=local
whencreated : 6/29/2020 5:08:49 PM
badpwdcount : 0
cn : yashika
useraccountcontrol : 66048
usncreated : 16577
primarygroupid : 513
pwdlastset : 6/29/2020 10:08:49 AM
usnchanged : 200768

logoncount : 1
badpasswordtime : 12/31/1600 4:00:00 PM
distinguishedname : CN=geet,OU=Tech,DC=ignite,DC=local
objectclass : {top, person, organizationalPerson, user}
displayname : geet
lastlogontimestamp : 4/7/2021 7:23:57 AM
userprincipalname : geet@ignite.local
name : geet
objectsid : S-1-5-21-501555289-2168925624-2051597760-1104
samaccountname : geet
admincount : 1
codepage : 0
samaccounttype : 805306368
whenchanged : 4/7/2021 2:23:57 PM
accountexpires : 9223372036854775807
countrycode : 0
adspath : LDAP://CN=geet,OU=Tech,DC=ignite,DC=local
instancetype : 4
usncreated : 16584
objectguid : 944569dc-bae7-400b-8ba3-68bd6849a8ef
lastlogoff : 12/31/1600 4:00:00 PM
objectcategory : CN=Person,CN=Schema,CN=Configuration,DC=ignite,DC=local
dscorepropagationdata : {4/7/2021 1:47:03 PM, 1/1/1601 12:00:00 AM}
givenname : geet
memberof : CN=Backup Operators,CN=Builtin,DC=ignite,DC=local
lastlogon : 4/7/2021 7:23:57 AM
badpwdcount : 0
cn : geet

```

Similar information is available for the users Yashika and Geet.

To get an abstract list of users created on the network, grab the common name by using the select command on the output of the Get-NetUser Module.

Get-NetUser | select cn

```
PS C:\Users\Administrator\Desktop> Get-NetUser | select cn
cn
--
Administrator
Guest
DefaultAccount
krbtgt
yashika
geet
aarti
Raj
pavan
SQL Service
jeenali
japneet
ignite
```

The Administrator, Yashika, Geet, Aarti, Raj, Pavan, Jeenali, Japneet, etc. are the various users in this network environment.

Similarly, to gather information about a particular user. For example, after the attacker extracted users in the previous section, a specific user was chosen to be targeted. More information about a particular user is required now. This can be done by using a flag-username with the username that the attacker wants to target. In this case, the attacker chose Yashika User.

Get-NetUser -UserName yashika


```

PS C:\Users\Administrator\Desktop> Get-NetUser -UserName yashika
logoncount : 60
badpasswordtime : 4/7/2021 7:12:41 AM
description : pass Password@1
distinguishedname : CN=yashika,OU=Tech,DC=ignite,DC=local
objectclass : {top, person, organizationalPerson, user}
displayname : yashika
lastlogontimestamp : 4/7/2021 7:12:47 AM
userprincipalname : yashika@ignite.local
name : yashika
objectsid : S-1-5-21-501555289-2168925624-2051597760-1103
samaccountname : yashika
admincount : 1
codepage : 0
samaccounttype : 805306368
whenchanged : 4/10/2021 2:08:59 PM
accountexpires : 9223372036854775807
countrycode : 0
adspath : LDAP://CN=yashika,OU=Tech,DC=ignite,DC=local
instancetype : 4
objectguid : d2ff2fb0-5f92-471b-b94c-a1bc5be262f2
lastlogon : 4/10/2021 7:26:55 AM
lastlogoff : 12/31/1600 4:00:00 PM
objectcategory : CN=Person,CN=Schema,CN=Configuration,DC=ignite,DC=local
dscorepropagationdata : {3/26/2021 6:37:49 PM, 1/1/1601 12:00:00 AM}
givenname : yashika
memberof : CN=Domain Admins,CN=Users,DC=ignite,DC=local
whencreated : 6/29/2020 5:08:49 PM
badpwdcount : 0
cn : yashika
useraccountcontrol : 66048
usncreated : 16577
primarygroupid : 513
pwdlastset : 6/29/2020 10:08:49 AM
usnchanged : 200768

```

A streamlined but detailed output regarding the Yashika User is extracted by the attacker.

Get-UserProperty

When working with the users and their properties, we see that there is a variable named `pwdlastset`. We can use this to check which users are reluctant to change their passwords. This can be set to any of the properties extracted in the previous step. For this demonstration, we will be extracting the password last set property of all the users.

Get-UserProperty -Properties pwdlastset

```
PS C:\Users\Administrator\Desktop> Get-UserProperty -Properties pwdlastset
name                pwdlastset
-----
Administrator       6/29/2020 9:40:26 AM
Guest               12/31/1600 4:00:00 PM
DefaultAccount      12/31/1600 4:00:00 PM
krbtgt              6/29/2020 9:54:43 AM
yashika             6/29/2020 10:08:49 AM
geet                6/29/2020 10:09:17 AM
aarti               6/29/2020 10:10:52 AM
Raj                 7/6/2020 10:33:10 AM
pavan               7/6/2020 12:24:15 PM
SQL Service         4/3/2021 9:17:09 AM
jeenali             4/5/2021 12:31:09 PM
japneet             4/5/2021 12:32:28 PM
ignite              4/9/2021 8:43:37 AM
```

Find-UserField

There are times when there are so many users on the network that it becomes very difficult for the domain administrator to keep track of all users or their credentials. To save the credentials information, they resort to some of the riskiest techniques. A good example that I have seen more than ever in the real environment is saving the credentials or important information about the user in their description. This can be extracted by the use of Find-UserField with a search term. In this demonstration, we used the term "pass" to search for potential passwords. The user Yashika has their password written and saved in their description. This is not limited to this type of information. Lots of different data can also be extracted by using the right set of keywords, such as "built." This will extract the attacker from the accounts that are built-in accounts.

Find-UserField -SearchField Description -SearchTerm "pass"

Find-UserField -SearchField Description -SearchTerm "built"

```
PS C:\Users\Administrator\Desktop> Find-UserField -SearchField Description -SearchTerm "pass"
samaccountname description
-----
yashika         pass Password@1

PS C:\Users\Administrator\Desktop> Find-UserField -SearchField Description -SearchTerm "built"
samaccountname description
-----
Administrator   Built-in account for administering the computer/domain
Guest            Built-in account for guest access to the computer/domain
```

The information that is extracted using UserField is the information stored in the properties of that user. While on the server, this can be viewed by opening the list of users and then right-clicking on any particular user. Then choose Properties. This will lead to a window similar to the one shown in the image below. Here, we can see that the administrator has provided the password in their description field. This goes

without saying that this should not be done at all. From the attacker's point of view, always check for such descriptions as they will contain some clue that can help you get further.

yashika Properties

Published Certificates Member Of Password Replication Dial-in Object

Security Environment Sessions Remote control

Remote Desktop Services Profile COM+ Attribute Editor

General Address Account Profile Telephones Organization

yashika

First name: yashika Initials:

Last name:

Display name: yashika

Description: pass Password@1

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

Invoke-UserHunter

While enumerating the domain, the attacker that has a targeted approach will be able to extract more data and that faster. The setup at home servers that we practise on does not impose a time constraint on attackers. In real-life red teaming assessments, if the attacker is taking their sweet time extracting data, they pose a risk of being detected and getting thrown out of their initial access or even getting captured. This is where some reconnaissance comes in handy. During the recon, the attacker can have a list of specific users that they have priority to enumerate first, and it is possible that those users will help the attacker to elevate access so they won't need to enumerate other users. This reduces the time as well as the noise and logs that will be created when the attacker enumerates users. This is solved using Invoke-UserHunter. It assists the attacker in searching for, or "hunting" for, those specific users. It will accept

usernames, and if the attacker has a handy list of usernames, it will graciously accept them as well. It accepts the domain group and host lists as well. It uses a mix of Get-NetSessions and Get-NetLoggedon against every server and then compares the result against the target user set. Then again, it raises the question of the amount of noise it will generate. But giving it a smaller number of usernames in the list or even giving it a single username will help the attacker reduce the noise significantly. It is worth noting that Invoke-UserHunter will run without any administrator privileges. To demonstrate, the attacker executes the Invoke-UserHunter command without any users or options. It will run against all users that it can find, which usually is the Administrator. It can be observed that the information extracted is pretty basic but useful in the case of profiling a user.

Invoke-UserHunter

```
PS C:\Users\Administrator\Desktop> Invoke-UserHunter  
  
UserDomain : IGNITE  
UserName : Administrator  
ComputerName : DC1.ignite.local  
IP : 192.168.1.172  
SessionFrom :  
LocalAdmin :
```

A pretty nifty feature that was interesting enough to be added was the CheckAccess function. This feature enables the attacker to check for local administrator access for the user or list of users that they provided. In the demonstration, the attacker tested the access of the administrator, which without surprise came to be True.

Invoke-UserHunter -CheckAccess

```
PS C:\Users\Administrator\Desktop> Invoke-UserHunter -CheckAccess  
  
UserDomain : IGNITE  
UserName : Administrator  
ComputerName : DC1.ignite.local  
IP : 192.168.1.172  
SessionFrom :  
LocalAdmin : True
```

Get-NetDomain

Get-NetDomain is useful when an attacker needs to extract domain-related information directly from the target server. It pretty much extracts the domain data that includes the forest name, domain controllers with children (that might be configured on a real environment server). Then there is the Name of the Parents with the RidRoleOwner, which is a DC Object that holds the relative identifier (RID) master role, and PDC RoleOwner, another DC Object that holds the PDC emulator role for that specific domain.

Get-NetDomain

```
PS C:\Users\Administrator\Desktop> Get-NetDomain  
  
Forest : ignite.local  
DomainControllers : {DC1.ignite.local}  
Children : {}  
DomainMode : Unknown  
DomainModeLevel : 7  
Parent :  
PdcRoleOwner : DC1.ignite.local  
RidRoleOwner : DC1.ignite.local  
InfrastructureRoleOwner : DC1.ignite.local  
Name : ignite.local
```

If the attacker wants to go after a specific domain, they can use the domain option by providing the name of the domain they are looking for, and Get-NetDomain will extract the data for that specific domain.

Get-NetDomain -domain "ignite.local"

```
PS C:\Users\Administrator\Desktop> Get-NetDomain -domain "ignite.local"  
  
Forest : ignite.local  
DomainControllers : {DC1.ignite.local}  
Children : {}  
DomainMode : Unknown  
DomainModeLevel : 7  
Parent :  
PdcRoleOwner : DC1.ignite.local  
RidRoleOwner : DC1.ignite.local  
InfrastructureRoleOwner : DC1.ignite.local  
Name : ignite.local
```

Get-NetDomainController

Next in the lineup, we have the Get-NetDomainController. This provides information about the particular server device instead of the domain. When an attacker wants to extract the data from the domain controller machine, this tool can be used. It extracts the forest information, with the time and date configured on the server. IT tells the OS version that can help constrain the search for kernel exploits for the attacker. Then the attacker has the IP addressing data with the inbound and outbound connections.

Get-NetDomainController

```

PS C:\Users\Administrator\Desktop> Get-NetDomainController
Forest : ignite.local
CurrentTime : 4/11/2021 10:45:09 AM
HighestCommittedUsn : 213062
OSVersion : Windows Server 2016 Standard Evaluation
Roles : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain : ignite.local
IPAddress : ::1
SiteName : Default-First-Site-Name
SyncFromAllServersCallback : {}
InboundConnections : {}
OutboundConnections : {}
Name : DC1.ignite.local
Partitions : {DC=ignite,DC=local, CN=Configuration,DC=ignite,DC=local,

```

The Get-NetDomainController, like the Get-NetDomain, can be configured to target a specific domain by the attacker. The scenario is that the attacker might be looking at multiple domains set up with multiple servers, so the attacker can use the -Domain option to target that specific domain controller inside the domain.

Get-NetDomainController -Domain ignite.local

```

PS C:\Users\Administrator\Desktop> Get-NetDomainController -Domain ignite.local
Forest : ignite.local
CurrentTime : 4/11/2021 10:45:24 AM
HighestCommittedUsn : 213062
OSVersion : Windows Server 2016 Standard Evaluation
Roles : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain : ignite.local
IPAddress : ::1
SiteName : Default-First-Site-Name
SyncFromAllServersCallback : {}
InboundConnections : {}
OutboundConnections : {}
Name : DC1.ignite.local
Partitions : {DC=ignite,DC=local, CN=Configuration,DC=ignite,DC=local,

```

Get-NetComputer

What seems to be a pretty simple option can turn out to be one of the most used tools to extract a huge amount of data from either the domain controller or even a single device. If the attacker executes the Get-NetComputer command directly on the Domain Controller machine, it will reveal the computer names of all the devices connected to the Domain.

Get-NetComputer


```
PS C:\Users\Administrator\Desktop> Get-NetComputer  
DC1.ignite.local  
client.ignite.local  
DESKTOP-ATNONJ9.ignite.local  
WIN-3Q7NEBI2561.ignite.local
```

Moving on, if the attacker decides to use the "-Ping Option", then they can get the list of all the devices that can be pinged from the machine they are running the Get-NetComputer from.

Get-NetComputer -Ping

```
PS C:\Users\Administrator\Desktop> Get-NetComputer -Ping  
DC1.ignite.local
```

If the attacker doesn't want to extract the data one parameter at a time, there is an option to extract all the data from the machine. This can be done with the FullData option, but keep in mind that a large amount of data extraction leads to a large chance of getting detected.

Get-NetComputer -FullData

```

PS C:\Users\Administrator\Desktop> Get-NetComputer -FullData
pwdlastset : 4/7/2021 5:30:23 AM
logoncount : 147
msds-generationid : {168, 207, 198, 26...}
serverreferencebl : CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Conf
badpasswordtime : 12/31/1600 4:00:00 PM
distinguishedname : CN=DC1,OU=Domain Controllers,DC=ignite,DC=local
objectclass : {top, person, organizationalPerson, user...}
lastlogontimestamp : 4/2/2021 8:36:12 AM
name : DC1
objectsid : S-1-5-21-501555289-2168925624-2051597760-1000
samaccountname : DC1$
localpolicyflags : 0
codepage : 0
samaccounttype : 805306369
whenchanged : 4/7/2021 12:30:23 PM
accountexpires : 9223372036854775807
countrycode : 0
adspath : LDAP://CN=DC1,OU=Domain Controllers,DC=ignite,DC=local
instancetype : 4
msdfsr-computerreferencebl : CN=DC1,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSett
objectguid : de681d91-bd3c-45df-8285-c9ceb8eb7c37
operatingsystem : Windows Server 2016 Standard Evaluation
operatingsystemversion : 10.0 (14393)
lastlogoff : 12/31/1600 4:00:00 PM
objectcategory : CN=Computer,CN=Schema,CN=Configuration,DC=ignite,DC=local
dscorepropagationdata : {6/29/2020 4:54:43 PM, 1/1/1601 12:00:01 AM}
serviceprincipalname : {TERMSRV/DC1, TERMSRV/DC1.ignite.local, Dfsr-12F9A27C-BF97-47
usncreated : 12293
memberof : CN=RAS and IAS Servers,CN=Users,DC=ignite,DC=local
lastlogon : 4/11/2021 3:31:14 AM
badpwdcount : 0
cn : DC1
useraccountcontrol : 532480
whencreated : 6/29/2020 4:54:43 PM
primarygroupid : 516
iscriticalsystemobject : True
msds-supportedencryptiontypes : 28
usnchanged : 147496
ridsetreferences : CN=RID Set,CN=DC1,OU=Domain Controllers,DC=ignite,DC=local
dnshostname : DC1.ignite.local

logoncount : 8
badpasswordtime : 12/31/1600 4:00:00 PM
distinguishedname : CN=CLIENT,CN=Computers,DC=ignite,DC=local
objectclass : {top, person, organizationalPerson, user...}
badpwdcount : 0
lastlogontimestamp : 9/23/2020 10:11:02 AM
objectsid : S-1-5-21-501555289-2168925624-2051597760-2101
samaccountname : CLIENT$
localpolicyflags : 0
codepage : 0

```

Moreover, if the attacker decides to use the -OperatingSystem option with the Get-NetComputer and provides the name of the OS as a parameter, they can extract all the machines that are running that specific operating system.

Get-NetComputer -OperatingSystem "Windows Server 2016 Standard Evaluation"

```


PS C:\Users\Administrator\Desktop> Get-NetComputer -OperatingSystem "Windows Server 2016 Standard Evaluation"
DC1.ignite.local

```

Get-UserProperty

Next on the list is the UserProperty. Up until now, the attacker could extract the users and very little information about them. This was limited, but this problem is solved using UserProperty. With it, the attacker can aim for those niche details about any particular property. Some of the information extractable is checking for Administrator Level Access, Password Time, Password Change Date, Description of the User, checking what group the different users are a part of, and much more.

Get-UserProperty

```
PS C:\Users\Administrator\Desktop> Get-UserProperty   
Name  
----  
accountexpires  
admincount  
adspath  
badpasswordtime  
badpwdcount  
cn  
codepage  
countrycode  
description  
distinguishedname  
dscorepropagationdata  
instancetype  
iscriticalsystemobject  
lastlogoff  
lastlogon  
lastlogontimestamp  
logoncount  
memberof  
name  
objectcategory  
objectclass  
objectguid  
objectsid  
primarygroupid  
pwdlastset  
samaccountname  
samaccounttype  
useraccountcontrol  
usnchanged  
usncreated  
whenchanged  
whenevercreated
```

To target a specific Property, the attacker can use the Properties option and specify the property they want to inquire about. For the demonstration, the property that was inquired here was badpwdcount. This tells the attacker about the unsuccessful attempts that were made against all the users.

Get-UserProperty -Properties badpwdcount

```
PS C:\Users\Administrator\Desktop> Get-UserProperty -Properties badpwdcount
```

name	badpwdcount
Administrator	0
Guest	0
DefaultAccount	0
krbtgt	0
yashika	0
geet	0
aarti	0
Raj	0
pavan	2
SQL Service	0
jeenali	0
japneet	0
ignite	0

The attacker can focus on the logoncount property to get an understanding of which of the users are dormant and which among them are active. In a real-life scenario, inactive users might be the users in a network of ex-employees that have been overlooked by the administrator. This can create a problem as, firstly, these accounts would not adhere to changing their passwords. Also, the attack mounted on these accounts won't raise flags because these users are legit.

Get-UserProperty -Properties logoncount


```
PS C:\Users\Administrator\Desktop> Get-UserProperty -Properties logoncount
```

name	logoncount
Administrator	92
Guest	0
DefaultAccount	0
krbtgt	0
yashika	60
geet	1
aarti	0
Raj	0
pavan	0
SQL Service	0
jeenali	0
japneet	0
ignite	0


Get-NetForest

Apart from the domain information and the user information, the attacker can also gain information about the forests, and there can be multiple forests inside a domain. To procure information about the forest in the current user's domain, use Get-NetForest.

Get-NetForest

```
PS C:\Users\Administrator\Desktop> Get-NetForest   
  
RootDomainSid      : S-1-5-21-501555289-2168925624-2051597760  
Name                : ignite.local  
Sites               : {Default-First-Site-Name}  
Domains             : {ignite.local}  
GlobalCatalogs     : {DC1.ignite.local}  
ApplicationPartitions : {DC=ForestDnsZones,DC=ignite,DC=local, DC=DomainDnsZones}  
ForestModeLevel     : 7  
ForestMode          : Unknown  
RootDomain          : ignite.local  
Schema              : CN=Schema,CN=Configuration,DC=ignite,DC=local  
SchemaRoleOwner     : DC1.ignite.local  
NamingRoleOwner     : DC1.ignite.local
```

Get-NetForestCatalog

```
PS C:\Users\Administrator\Desktop> Get-NetForestCatalog   
  
Forest              : ignite.local  
CurrentTime         : 4/11/2021 10:59:26 AM  
HighestCommittedUsn : 213067  
OSVersion           : Windows Server 2016 Standard Evaluation  
Roles               : {SchemaRole, NamingRole, PdcRole, RidRole...}  
Domain              : ignite.local  
IPAddress            : ::1  
SiteName            : Default-First-Site-Name  
SyncFromAllServersCallback : {}  
InboundConnections  : {}  
OutboundConnections : {}  
Name                : DC1.ignite.local  
Partitions           : {DC=ignite,DC=local, CN=Configuration,DC=ignite,DC=local,}
```

Forests typically have different global catalogues that can help the attacker get some precarious information about the domain. This can be observed from the following demonstration of extracting all the global catalogues of the current forest using Get-NetForestCatalog.

Get-NetForestDomain

```
PS C:\Users\Administrator\Desktop> Get-NetForestDomain
```

Forest	: ignite.local
DomainControllers	: {DC1.ignite.local}
Children	: {}
DomainMode	: Unknown
DomainModeLevel	: 7
Parent	:
PdcRoleOwner	: DC1.ignite.local
RidRoleOwner	: DC1.ignite.local
InfrastructureRoleOwner	: DC1.ignite.local
Name	: ignite.local

Get-NetForestDomain

Moving on from the catalogs, the attacker can also work on extracting the various domains of the forest the current user is located in. This can be done by running Get-NetForestDomain as shown in the demonstration.

Get-NetForestDomain

```
PS C:\Users\Administrator\Desktop> Get-NetForestDomain
```

Forest	: ignite.local
DomainControllers	: {DC1.ignite.local}
Children	: {}
DomainMode	: Unknown
DomainModeLevel	: 7
Parent	:
PdcRoleOwner	: DC1.ignite.local
RidRoleOwner	: DC1.ignite.local
InfrastructureRoleOwner	: DC1.ignite.local
Name	: ignite.local

Get-NetLoggedon

That's enough forest. Getting back to the users on the local or remote machine, the attacker can take advantage of the NetLoggedon module. It should be noted that administrative rights are required to use this module. This module executes the NetWkstaUserEnum Win32API call to extract the users that are currently logged on. If the attacker is in a bit of a hurry, they can enumerate all the users that are logged on to all the machines in the domain by using the Get-DomainComputer and then running the Get-NetLoggedon on that data. This can be concatenated using a pipe.

Get-DomainComputer | Get-NetLoggedon

In this demonstration, however, it is shown how to enumerate users that are loggedon on a particular machine with the help of the ComputerName option and providing the Name.

Get-NetLoggedon -ComputerName DC1

```
PS C:\Users\Administrator\Desktop> Get-NetLoggedon -ComputerName DC1
wkui1_username wkui1_logon_domain wkui1_oth_domains wkui1_logon_server
-----
DC1$           IGNITE
Administrator  IGNITE
DC1$           IGNITE
DC1$           IGNITE
DC1$           IGNITE
```

Get-DomainPolicy

Amongst other information, the Domain Policy of a Domain can also reveal some pretty good information. The attacker can use the Get-Domain to extract the policy of the current domain. It reads the default domain policy or the domain controller policy for the current domain or a specified domain/domain controller. To get more focused on a particular domain the Domain option. To extract Domain or Domain Controller using the Source Option or Server option to bind to a particular Active Directory server.

Get-DomainPolicy

```
PS C:\Users\Administrator\Desktop> Get-DomainPolicy
Unicode       : @{Unicode=yes}
SystemAccess  : @{MinimumPasswordAge=1; MaximumPasswordAge=42; LockoutBadCount=0; PasswordComplexity=1;
                MinimumPasswordLength=7}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.String[]}
KerberosPolicy : @{MaxTicketAge=10; MaxServiceAge=600; MaxClockSkew=5; MaxRenewAge=7; TicketValidateClien
Version       : @{Revision=1; signature="$CHICAGO$"}

```

To enumerate Kerberos details, the attacker can try and go after the Kerberos Policy, which contains data such as the Max Ticket Age, Max Renew Age, and several Ticket Validation Clients. This kind of information can come in handy if the attacker is trying to perform a ticket forging attack or similar attack.

(Get-DomainPolicy)."KerberosPolicy"

```
PS C:\Users\Administrator\Desktop> (Get-DomainPolicy)."KerberosPolicy"
MaxTicketAge : 10
MaxServiceAge : 600
MaxClockSkew : 5
MaxRenewAge : 7
TicketValidateClient : 1
```

To extract the data regarding system access, such as the password data that we extracted earlier, like password age, password complexity, and password length, etc.

```
(Get-DomainPolicy)."SystemAccess"
```

```
PS C:\Users\Administrator\Desktop> (Get-DomainPolicy)."SystemAccess"
MinimumPasswordAge : 1
MaximumPasswordAge : 42
LockoutBadCount : 0
PasswordComplexity : 1
RequireLogonToChangePassword : 0
LSAAnonymousNameLookup : 0
ForceLogoffWhenHourExpire : 0
PasswordHistorySize : 3
ClearTextPassword : 0
MinimumPasswordLength : 7
```

Get-NetOU

OUs are the smallest units in the Active Directory system. OU is abbreviated from Organizational Unit. OUs are containers for users, groups, and computers, and they exist within a domain. OUs are useful when an administrator wants to deploy Group Policy settings to a subset of users, groups, and computers within your domain. OUs also allow administrators to delegate admin tasks to users/groups without having to make them an administrator of the directory.

To enumerate, run the following command in PowerShell.

```
Get-NetOU
```

```
PS C:\Users\Administrator\Desktop> Get-NetOU
LDAP://OU=Domain Controllers,DC=ignite,DC=local
LDAP://OU=Tech,DC=ignite,DC=local
LDAP://OU=VPN,DC=ignite,DC=local
LDAP://OU=Sales,DC=ignite,DC=local
LDAP://OU=HR,DC=ignite,DC=local
```

It can be observed that there are 4 OUs on the Target Server. Namely, Tech, VPN, Sales, and HR.

Get-NetGroup

During the enumeration that the attacker is trying to perform, extracting information is one of the most important things that the attacker can enumerate. To get all the groups in the current domain, the attacker can use the Get-NetGroup command as demonstrated.

Get-NetGroup

```
PS C:\Users\Administrator\Desktop> Get-NetGroup
Administrators
Users
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS
Cryptographic Operators
Event Log Readers
Certificate Service DCOM Access
RDS Remote Access Servers
RDS Endpoint Servers
RDS Management Servers
Hyper-V Administrators
Access Control Assistance Operators
Remote Management Users
System Managed Accounts Group
Storage Replica Administrators
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Cert Publishers
Domain Admins
Domain Users
Domain Guests
Group Policy Creator Owners
RAS and IAS Servers
Server Operators
Account Operators
Pre-Windows 2000 Compatible Access
Incoming Forest Trust Builders
Windows Authorization Access Group
Terminal Server License Servers
Allowed RODC Password Replication Group
Denied RODC Password Replication Group
Read-only Domain Controllers
Enterprise Read-only Domain Controllers
Cloneable Domain Controllers
Protected Users
Key Admins
Enterprise Key Admins
DnsAdmins
DnsUpdateProxy
Finance
```

When the attacker requires to extract the groups that consist of the admin keyword, as those might be important or might contain some information regarding the administrator, as this would give all kinds of administrator groups as demonstrated.

Get-NetGroup *admin*

```
PS C:\Users\Administrator\Desktop> Get-NetGroup *admin*
Administrators
Hyper-V Administrators
Storage Replica Administrators
Schema Admins
Enterprise Admins
Domain Admins
Key Admins
Enterprise Key Admins
DnsAdmins
```

Suppose the attacker wanted to check for the membership of a particular user, then they could use the UserName option. This can also be checked as shown in the image below. The attacker extracted the information for the Yashika user.

Get-NetGroup -UserName yashika

```
PS C:\Users\Administrator\Desktop> Get-NetGroup -UserName yashika
BUILTIN\Administrators
IGNITE\Denied RODC Password Replication Group
IGNITE\Domain Admins
```

To target a specific domain, the attacker can use the Domain option with the domain name provided against as shown in the demonstration.

Get-NetGroup -Domain ignite.local

```
PS C:\Users\Administrator\Desktop> Get-NetGroup -Domain ignite.local
Administrators
Users
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS
Cryptographic Operators
Event Log Readers
Certificate Service DCOM Access
RDS Remote Access Servers
RDS Endpoint Servers
RDS Management Servers
Hyper-V Administrators
Access Control Assistance Operators
Remote Management Users
System Managed Accounts Group
Storage Replica Administrators
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Cert Publishers
Domain Admins
Domain Users
Domain Guests
Group Policy Creator Owners
RAS and IAS Servers
Server Operators
Account Operators
Pre-Windows 2000 Compatible Access
Incoming Forest Trust Builders
Windows Authorization Access Group
Terminal Server License Servers
Allowed RODC Password Replication Group
Denied RODC Password Replication Group
Read-only Domain Controllers
Enterprise Read-only Domain Controllers
Cloneable Domain Controllers
Protected Users
Key Admins
```

Furthermore, if the attacker wants to extract all the data regarding the groups working on the domain, they can use the FullData option and extract all the users with their group details. In the demonstration, it can be observed that information is enumerated, such as there is an Admin in this domain, which is a part of the Administrator Group and then other User Groups.

Get-NetGroup -FullData


```

PS C:\Users\Administrator\Desktop> Get-NetGroup -FullData
grouptype : -2147483643
admincount : 1
iscriticalsystemobject : True
samaccounttype : 536870912
samaccountname : Administrators
whenchanged : 7/6/2020 5:39:37 PM
objectsid : S-1-5-32-544
objectclass : {top, group}
cn : Administrators
usnchanged : 20539
systemflags : -1946157056
name : Administrators
adspath : LDAP://CN=Administrators,CN=Builtin,DC=ignite,DC=local
dscorepropagationdata : {7/6/2020 5:39:37 PM, 6/29/2020 4:54:43 PM, 1/1/1601 12:00:01 AM}
description : Administrators have complete and unrestricted access to the computer and network resources.
distinguishedname : CN=Administrators,CN=Builtin,DC=ignite,DC=local
member : {CN=Domain Admins,CN=Users,DC=ignite,DC=local, CN=Domain Users,CN=Users,DC=ignite,DC=local, CN=Domain Computers,CN=Computers,DC=ignite,DC=local, CN=Domain Controllers,CN=Controllers,DC=ignite,DC=local}
usncreated : 8200
whencreated : 6/29/2020 4:54:05 PM
instancetype : 4
objectguid : c9afd4ac-f09c-4596-a41e-b69465439363
objectcategory : CN=Group,CN=Schema,CN=Configuration,DC=ignite,DC=local

grouptype : -2147483643
systemflags : -1946157056
iscriticalsystemobject : True
samaccounttype : 536870912
samaccountname : Users
whenchanged : 6/29/2020 4:54:43 PM
objectsid : S-1-5-32-545
objectclass : {top, group}
cn : Users
usnchanged : 12381
dscorepropagationdata : {6/29/2020 4:54:43 PM, 1/1/1601 12:00:01 AM}
name : Users
adspath : LDAP://CN=Users,CN=Builtin,DC=ignite,DC=local
description : Users are prevented from making accidental or intentional changes to the computer and network resources.
distinguishedname : CN=Users,CN=Builtin,DC=ignite,DC=local
member : {CN=Domain Admins,CN=Users,DC=ignite,DC=local, CN=Domain Users,CN=Users,DC=ignite,DC=local, CN=Domain Computers,CN=Computers,DC=ignite,DC=local, CN=Domain Controllers,CN=Controllers,DC=ignite,DC=local}
usncreated : 8203
whencreated : 6/29/2020 4:54:05 PM
instancetype : 4
objectguid : 895d6d29-db2a-4ca2-9eae-9e1b226e5774
objectcategory : CN=Group,CN=Schema,CN=Configuration,DC=ignite,DC=local

```

There is a member named Japneet that is a member of the Tech Group, and while looking for more information about the user groups, it can be observed that there is a user by the name of geet that is a part of the Tech group as well.

```

groupype : -2147483643
admincount : 1
iscriticalsystemobject : True
samaccounttype : 536870912
samaccountname : Print Operators
whenchanged : 4/7/2021 1:45:55 PM
objectsid : S-1-5-32-550
objectclass : {top, group}
cn : Print Operators
usnchanged : 151629
systemflags : -1946157056
name : Print Operators
adspath : LDAP://CN=Print Operators,CN=Builtin,DC=ignite,DC=local
dscorepropagationdata : {7/6/2020 5:39:37 PM, 6/29/2020 4:54:43 PM, 1/1/1601 12:04:16 A
description : Members can administer printers installed on domain controllers
distinguishedname : CN=Print Operators,CN=Builtin,DC=ignite,DC=local
member : CN=japneet,OU=Tech,DC=ignite,DC=local
usncreated : 8212
whencreated : 6/29/2020 4:54:05 PM
instancetype : 4
objectguid : 2cda2d0f-0716-44dd-8ea8-1447d8da4ec6
objectcategory : CN=Group,CN=Schema,CN=Configuration,DC=ignite,DC=local

groupype : -2147483643
admincount : 1
iscriticalsystemobject : True
samaccounttype : 536870912
samaccountname : Backup Operators
whenchanged : 4/9/2021 5:30:20 PM
objectsid : S-1-5-32-551
objectclass : {top, group}
cn : Backup Operators
usnchanged : 192583
systemflags : -1946157056
name : Backup Operators
adspath : LDAP://CN=Backup Operators,CN=Builtin,DC=ignite,DC=local
dscorepropagationdata : {7/6/2020 5:39:37 PM, 6/29/2020 4:54:43 PM, 1/1/1601 12:04:16 A
description : Backup Operators can override security restrictions for the sol
distinguishedname : CN=Backup Operators,CN=Builtin,DC=ignite,DC=local
member : {CN=ignite,OU=Tech,DC=ignite,DC=local, CN=geet,OU=Tech,DC=ignite,DC=local}
usncreated : 8213
whencreated : 6/29/2020 4:54:05 PM
instancetype : 4
objectguid : f2d07966-5803-493b-b7ef-3b77edc0fe15
objectcategory : CN=Group,CN=Schema,CN=Configuration,DC=ignite,DC=local

```

Moving on from the user-based group enumeration to the group-based enumeration by providing the group name as shown in the image below

Get-NetGroup "Domain Admins"

```
PS C:\Users\Administrator\Desktop> Get-NetGroup "Domain Admins"
Domain Admins
```

The attacker can also use multiple options to target a particular group and enumerate all the data about that group, as shown in the demonstration.

Get-NetGroup "Domain Admins" -FullData

```

PS C:\Users\Administrator\Desktop> Get-NetGroup "Domain Admins" -FullData
grouptype           : -2147483646
admincount          : 1
iscriticalsystemobject : True
samaccounttype      : 268435456
samaccountname      : Domain Admins
whenchanged         : 4/7/2021 1:42:38 PM
objectsid           : S-1-5-21-501555289-2168925624-2051597760-512
objectclass         : {top, group}
cn                  : Domain Admins
usnchanged          : 151621
dscorepropagationdata : {7/6/2020 5:39:37 PM, 6/29/2020 4:54:43 PM, 1/1/1601 12:04:16 AM}
memberof           : {CN=Denied RODC Password Replication Group,CN=Users,DC=ignite,DC=local,
CN=Administrators,CN=Builtin,DC=ignite,DC=local}
adspath             : LDAP://CN=Domain Admins,CN=Users,DC=ignite,DC=local
description         : Designated administrators of the domain
distinguishedname   : CN=Domain Admins,CN=Users,DC=ignite,DC=local
name                : Domain Admins
member              : {CN=yashika,OU=Tech,DC=ignite,DC=local, CN=Administrator,CN=Users,DC=ignite,DC=local}
usncreated          : 12345
whencreated         : 6/29/2020 4:54:43 PM
instancetype        : 4
objectguid          : 794d6fc1-b2e0-4462-bcf7-04d6ba921801
objectcategory      : CN=Group,CN=Schema,CN=Configuration,DC=ignite,DC=local

```

There are more possible solutions for the attacker to streamline their enumeration process by providing a bunch of options and parameters to target the exact information. This includes a particular group name option and a domain option.

Get-NetGroup -GroupName *admin* -Domain ignite.local

```

PS C:\Users\Administrator\Desktop> Get-NetGroup -GroupName *admin* -Domain ignite.local
Administrators
Hyper-V Administrators
Storage Replica Administrators
Schema Admins
Enterprise Admins
Domain Admins
Key Admins
Enterprise Key Admins
DnsAdmins

```

Get-NetGroupMember

If the attacker gets to a stage where they have successfully enumerated the group names, then they can use that in collaboration with the Get-NetGroupMember to extract the members of that group. In the demonstration, we extracted the members of the group Domain Admins.

Get-NetGroupMember -GroupName "Domain Admins"

```
PS C:\Users\Administrator\Desktop> Get-NetGroupMember -GroupName "Domain Admins"

GroupDomain : ignite.local
GroupName   : Domain Admins
MemberDomain : ignite.local
MemberName  : yashika
MemberSid   : S-1-5-21-501555289-2168925624-2051597760-1103
IsGroup     : False
MemberDN    : CN=yashika,OU=Tech,DC=ignite,DC=local

GroupDomain : ignite.local
GroupName   : Domain Admins
MemberDomain : ignite.local
MemberName  : Administrator
MemberSid   : S-1-5-21-501555289-2168925624-2051597760-500
IsGroup     : False
MemberDN    : CN=Administrator,CN=Users,DC=ignite,DC=local
```

As discussed earlier, Get-NetGroupMember also supports some options to run along, such as Recurse. It helps the attacker extract significant amounts of data about all the users of the group they provided. There is a significant difference between running Get-NetGroupMember with and without Recurse, as evidenced by the screenshots.

```
Get-NetGroupMember -GroupName "Administrators" -Recurse
```

```

PS C:\Users\Administrator\Desktop> Get-NetGroupMember -GroupName 'Administrators' -Recurse
GroupDomain : ignite.local
GroupName : Administrators
MemberDomain : ignite.local
MemberName : Domain Admins
MemberSid : S-1-5-21-501555289-2168925624-2051597760-512
IsGroup : True
MemberDN : CN=Domain Admins,CN=Users,DC=ignite,DC=local

Cannot index into a null array. :
logonCount : 64
badPasswordTime : 4/7/2021 7:12:41 AM
description : pass Password@1
distinguishedName : CN=yashika,OU=Tech,DC=ignite,DC=local
objectClass : {top, person, organizationalPerson, user}
displayName : yashika
lastLogonTimestamp : 4/7/2021 7:12:47 AM
userPrincipalName : yashika@ignite.local
objectSid : S-1-5-21-501555289-2168925624-2051597760-1103
adminCount : 1
codePage : 0
SAMAccountType : 805306368
countryCode : 0
whenChanged : 4/10/2021 2:08:59 PM
instanceType : 4
objectGUID : d2ff2fb0-5f92-471b-b94c-a1bc5be262f2
lastLogoff : 12/31/1600 4:00:00 PM
SAMAccountName : yashika
objectCategory : CN=Person,CN=Schema,CN=Configuration,DC=ignite,DC=local
dSCorePropagationData : {3/26/2021 6:37:49 PM, 1/1/1601 12:00:00 AM}
givenName : yashika
memberOf : CN=Domain Admins,CN=Users,DC=ignite,DC=local
lastLogon : 4/11/2021 4:02:06 AM
badPwdCount : 0
cn : yashika
userAccountControl : 66048
whenCreated : 6/29/2020 5:08:49 PM
primaryGroupID : 513
pwdLastSet : 6/29/2020 10:08:49 AM
name : yashika
GroupDomain : ignite.local
GroupName : Domain Admins
MemberDomain : ignite.local
MemberName : yashika
MemberSid : S-1-5-21-501555289-2168925624-2051597760-1103
IsGroup : False
MemberDN : CN=yashika,OU=Tech,DC=ignite,DC=local

```

Get-NetGPO

Group Policy is very interesting to figure out how the domain is set up and what set of rules and policies are designed by the Administrator to govern it. This can be enumerated using the Get-NetGPO. It will extract all the information regarding group policies that are configured on the target system.

Get-NetGPO

```

PS C:\Users\Administrator\Desktop> Get-NetGPO
usncreated           : 5900
systemflags          : -1946157056
displayname          : Default Domain Policy
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-2488-11D1-A28
-11D1-A28C-00C04FB94F17}]
whenchanged          : 4/8/2021 1:58:58 PM
objectclass           : {top, container, groupPolicyContainer}
gpcfunctionalityversion : 2
showinadvancedviewonly : True
usnchanged            : 163911
dscorepropagationdata : {6/29/2020 4:54:43 PM, 1/1/1601 12:00:00 AM}
name                  : {31B2F340-016D-11D2-945F-00C04FB984F9}
adspath               : LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,C
flags                 : 0
cn                    : {31B2F340-016D-11D2-945F-00C04FB984F9}
iscriticalsystemobject : True
gpcfilesyspath         : \\ignite.local\sysvol\ignite.local\Policies\{31B2F340-016D-11D
distinguishedname      : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste
whencreated            : 6/29/2020 4:54:05 PM
versionnumber          : 7
instancetype           : 4
objectguid             : 4aaf7089-5629-4f93-b6cc-0ecc1c4dba1e
objectcategory          : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=ignite

usncreated           : 5903
systemflags          : -1946157056
displayname          : Default Domain Controllers Policy
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F72-3407-48AE-BA8
whenchanged          : 4/7/2021 4:46:25 PM
objectclass           : {top, container, groupPolicyContainer}
gpcfunctionalityversion : 2
showinadvancedviewonly : True
usnchanged            : 155719
dscorepropagationdata : {6/29/2020 4:54:43 PM, 1/1/1601 12:00:00 AM}
name                  : {6AC1786C-016F-11D2-945F-00C04FB984F9}
adspath               : LDAP://CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,C
flags                 : 0
cn                    : {6AC1786C-016F-11D2-945F-00C04FB984F9}
iscriticalsystemobject : True
gpcfilesyspath         : \\ignite.local\sysvol\ignite.local\Policies\{6AC1786C-016F-11D
distinguishedname      : CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste
whencreated            : 6/29/2020 4:54:05 PM
versionnumber          : 6
instancetype           : 4
objectguid             : f852ef84-af95-4083-ba7c-8eabfa710587

```

As it can be observed from the previous iteration of running the Get-NetGPO, the amount of information is overwhelming. Hence, to get a clean and easy-to-understand output, selection can be used to get those specific names of the policies.

Get-NetGPO | select displayname


```
PS C:\Users\Administrator\Desktop> Get-NetGPO | select displayname
displayname
Default Domain Policy
Default Domain Controllers Policy
New Group Policy Object
```

Find-GPOLocation

Getting the GPO location is a good way to map the abilities of a specific user. It takes the username that is provided to it and checks for the permissions for that user. This means that it will return the locations that are accessible for that user. In this demonstration, we use the Yashika user and we choose the verbose option as well to elaborate on the result to get the most out of it.

Find-GPOLocation -UserName yashika -verbose

```
PS C:\Users\Administrator\Desktop> Find-GPOLocation -UserName yashika -verbose
VERBOSE: Get-DomainSearcher search string: LDAP://DC=ignite,DC=local
VERBOSE: LocalSid: S-1-5-32-544
VERBOSE: TargetSid: S-1-5-21-501555289-2168925624-2051597760-1103
VERBOSE: TargetObjectDistName: CN=yashika,OU=Tech,DC=ignite,DC=local
VERBOSE: Get-DomainSearcher search string: LDAP://DC=ignite,DC=local
VERBOSE: Get-DomainSearcher search string: LDAP://DC=ignite,DC=local
VERBOSE: Effective target sids: S-1-5-21-501555289-2168925624-2051597760-1103 S-1-5-32-544 S-1-5-21-501555289-2168925624-20515
VERBOSE: Get-DomainSearcher search string: LDAP://DC=ignite,DC=local
VERBOSE: Parsing \\ignite.local\sysvol\ignite.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
VERBOSE: Parsing \\ignite.local\sysvol\ignite.local\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
VERBOSE: Parsing \\ignite.local\SysVol\ignite.local\Policies\{46A4D008-D193-4F79-8B62-0B657A945A33}\MACHINE\Microsoft\Windows
VERBOSE: GPOgroups:
```

Invoke-EnumerateLocalAdmin

Invoke-EnumerateLocalAdmin does exactly what the names say. It searched for the local administrators for the domain. In our demonstration, we see that we have extracted the Administrator, Enterprise Admins, and Domain Admins for our domain, ignite. local.

Invoke-EnumerateLocalAdmin

```

PS C:\Users\Administrator\Desktop> Invoke-EnumerateLocalAdmin ←
Server      : DC1.ignite.local
AccountName : ignite.local/Administrator
SID         : S-1-5-21-501555289-2168925624-2051597760-500
Disabled    : False
IsGroup     : False
IsDomain    : True
LastLogin   : 4/11/2021 5:05:03 AM

Server      : DC1.ignite.local
AccountName : ignite.local/Enterprise Admins
SID         : S-1-5-21-501555289-2168925624-2051597760-519
Disabled    : False
IsGroup     : True
IsDomain    : True
LastLogin   :


Server      : DC1.ignite.local
AccountName : ignite.local/Domain Admins
SID         : S-1-5-21-501555289-2168925624-2051597760-512
Disabled    : False
IsGroup     : True
IsDomain    : True
LastLogin   :

```

Get-NetProcess

Enumerating the running process is one of the things that the attacker should do. It can tell you so much about the target machine. It can extract information about any services that might be vulnerable. It can tell if any process is running with elevated privileges. It also tells the process ID of the process, so if the attacker has access to that process, they can tinker around with it, such as stopping or restarting it.

Get-NetProcess

```
PS C:\Users\Administrator\Desktop> Get-NetProcess 

ComputerName : DC1
ProcessName   : System Idle Process
ProcessID     : 0
Domain        :
User          :

ComputerName : DC1
ProcessName   : System
ProcessID     : 4
Domain        :
User          :

ComputerName : DC1
ProcessName   : smss.exe
ProcessID     : 324
Domain        : NT AUTHORITY
User          : SYSTEM

ComputerName : DC1
ProcessName   : csrss.exe
ProcessID     : 452
Domain        : NT AUTHORITY
User          : SYSTEM

ComputerName : DC1
ProcessName   : wininit.exe
ProcessID     : 564
Domain        : NT AUTHORITY
User          : SYSTEM

ComputerName : DC1
ProcessName   : csrss.exe
ProcessID     : 572
Domain        : NT AUTHORITY
User          : SYSTEM

ComputerName : DC1
ProcessName   : winlogon.exe
ProcessID     : 656
Domain        : NT AUTHORITY
User          : SYSTEM
```

Invoke-ShareFinder

Any inexperienced attacker can tell you why there is a need for enumerating the shares when that can be done externally using the SMB enumeration. But an experienced attacker will know that some shares are not visible to all. It is possible to configure whether a specific share is visible and accessible to all users or to a specific user. Hence, to enumerate the shares in a domain, use Invoke-ShareFinder.

Invoke-ShareFinder

```

PS C:\Users\Administrator\Desktop> Invoke-ShareFinder
\\DC1.ignite.local\ADMIN$ - Remote Admin
\\DC1.ignite.local\C$ - Default share
\\DC1.ignite.local\Confidential - 
\\DC1.ignite.local\IPC$ - Remote IPC
\\DC1.ignite.local\NETLOGON - Logon server share
\\DC1.ignite.local\Sales Report - 
\\DC1.ignite.local\SYSVOL - Logon server share
\\DC1.ignite.local\Users - 

```

Invoke-FileFinder

It is not difficult to conduct a search on the machine where the attacker has gained an initial foothold. But searching for a specific file across the network in the domain can be done using the Invoke FileFinder. It will search for sensitive files such as the Credentials files and other files that can lead to a serious compromise.

Invoke-FileFinder

```

PS C:\Users\Administrator\Desktop> Invoke-FileFinder
FullName      : \\DC1.ignite.local\Users\Administrator
Owner         : NT AUTHORITY\SYSTEM
LastAccessTime : 4/10/2021 8:01:42 AM
LastWriteTime  : 4/10/2021 8:01:42 AM
CreationTime   : 6/29/2020 9:40:36 AM
Length        : 
FullName      : \\DC1.ignite.local\Users\Administrator\AppData\Local\Microsoft\Credentials
Owner         : BUILTIN\Administrators
LastAccessTime : 3/6/2021 8:12:12 AM
LastWriteTime  : 3/6/2021 8:12:12 AM
CreationTime   : 6/29/2020 9:40:37 AM
Length        : 
FullName      : \\DC1.ignite.local\Users\Administrator\AppData\Local\Microsoft_Corporation\
Owner         : BUILTIN\Administrators
LastAccessTime : 4/11/2021 4:40:14 AM
LastWriteTime  : 4/11/2021 4:40:14 AM
CreationTime   : 6/29/2020 9:41:09 AM
Length        : 152966
FullName      : \\DC1.ignite.local\Users\Administrator\AppData\Local\Packages\windows.immer
Owner         : BUILTIN\Administrators
LastAccessTime : 6/29/2020 9:40:54 AM
LastWriteTime  : 7/16/2016 6:18:57 AM
CreationTime   : 6/29/2020 9:40:54 AM
Length        : 1309

```

Invoke-ACLScanner

ACLs, or Access Control Lists, can be scanned on a domain that will return the weak permissions on the files. Bear in mind that domain permission can be a bit challenging to wrap your head around, and the permission that you might find using Invoke-ACLScanner can be difficult to exploit. However, this does not

mean that any attacker should not check for them. In simpler terms, Invoke-ACLScanner finds the permissions that the users and groups have that are potentially subject to exploitation. This is determined by separating the default permission and displaying a list of permissions that do not default or are newly defined by the administrator.

Invoke-ACLScanner -ResolveGUIDs

```
PS C:\Users\Administrator\Desktop> Invoke-ACLScanner -ResolveGUIDs

InheritedObjectType : All
ObjectDN             : CN=MicrosoftDNS,CN=System,DC=ignite,DC=local
ObjectType           : All
IdentityReference    : IGNITE\DnsAdmins
IsInherited          : False
ActiveDirectoryRights : CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedF
PropagationFlags     : None
ObjectFlags          : None
InheritanceFlags     : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID            :
IdentitySID          : S-1-5-21-501555289-2168925624-2051597760-1101

InheritedObjectType : All
ObjectDN             : DC=RootDNSServers,CN=MicrosoftDNS,CN=System,DC=ignite,DC=local
ObjectType           : All
IdentityReference    : IGNITE\DnsAdmins
IsInherited          : True
ActiveDirectoryRights : CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedF
PropagationFlags     : None
ObjectFlags          : None
InheritanceFlags     : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID            :
IdentitySID          : S-1-5-21-501555289-2168925624-2051597760-1101

InheritedObjectType : All
ObjectDN             : DC=@,DC=RootDNSServers,CN=MicrosoftDNS,CN=System,DC=ignite,DC=local
ObjectType           : All
IdentityReference    : IGNITE\DnsAdmins
IsInherited          : True
ActiveDirectoryRights : CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedF
PropagationFlags     : None
ObjectFlags          : None
InheritanceFlags     : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID            :
IdentitySID          : S-1-5-21-501555289-2168925624-2051597760-1101
```

Find-LocalAdminAccess

Find-LocalAdminAccess is also pretty self-defined. It enumerated the machines on the local domain that have the users who have the local administrator access. It checks if the user has local administrator access using Test-AdminAccess. Then it checks for the credential option. If passed, then it uses Invoke-UserImpersonation to impersonate the specified user before enumeration.

Find-LocalAdminAccess

```
PS C:\Users\Administrator\Desktop> Find-LocalAdminAccess  
DC1.ignite.local
```

Get-NetSession

Finally, it's time to shine some light on the sessions that are generated inside a domain. This can be enumerated with the help of the Get-NetSession tool. Upon running this, the attacker can extract the session information for the local or remote machine. This function executes the NetSessionEnum Win32API call for extracting the session information. It can be used as is, or it can be combined with a ComputerName Option to target a specific host.

Get-NetSession

```
PS C:\Users\Administrator\Desktop> Get-NetSession  
sesi10_cname sesi10_username sesi10_time sesi10_idle_time  
-----  
\\[::1] Administrator 0 0
```

Conclusion

Active Directory is extensive and can be confusing for novice security professionals. We provide this detailed resource so that you can enumerate your Active Directory Deployment and understand the information that an attacker can extract. It will also help our Blue Teamers to understand how this kind of information can be extracted and what kind of alerts they need to set up to restrict the attacker.