Active Directory Enumeration with PowerShell

By Haboob Team
Research@haboob.sa
Table of Contents

Introduction ........................................................................................................................................... 2
Why Powershell? ................................................................................................................................... 2
Attack Demonstration .......................................................................................................................... 2
  Domain Enumeration ......................................................................................................................... 3
  Group Policy (GPO) Enumeration ..................................................................................................... 9
  Domain Trusts Enumeration ............................................................................................................. 10
  User Hunting ................................................................................................................................... 13
  Access Control Lists (ACL) Enumeration ....................................................................................... 15
Conclusion ........................................................................................................................................... 17
References .......................................................................................................................................... 18
INTRODUCTION
Nowadays, most of the environments are using Active Directory to manage their networks and resources. And over the past years, the attackers have been focused to abuse and attack the Active Directory environments using different techniques and methodologies. So in this research paper, we are going to use the power of the PowerShell to enumerate the resources of the Active Directory, like enumerating the domains, users, groups, ACL, GPOs, domain trusts also hunting the users and the domain admins. With this valuable information, we can increase our attack surface to abuse the AD like Privilege escalation, lateral movements and persistence and so on.

WHY POWERSHELL?
Penetration Tests and Red Team operations for secured environments need altered approaches. You cannot afford to touch disk, throw executable and use memory corruption exploits without the risk of being ineffective as a simulated adversary. To enhance offensive tactics and methodologies, PowerShell is the tool of choice.

PowerShell has changed the way Windows networks are attacked. It is Microsoft’s shell and scripting language available by default in all modern Windows computers. It could interact with .Net, WMI, COM, Windows API, Registry and other computers on a Windows Domain. This makes it imperative for Penetration Testers and Red Teamers to learn PowerShell.

ATTACK DEMONSTRATION
In the attack demonstration, we are going to use the tool PowerView. PowerView is a PowerShell script which was developed by Will Schroeder and is part of PowerSploit framework. The script relies solely on PowerShell and WMI (Windows Management Instrumentation) queries.

We have built an Active Directory lab that simulates a real world environment with a set of machines, users, domains, misconfigurations. In this lab, we will simulate the attack as we have a limited shell on a Windows machine (joined-domain). From there, we will enumerate the domain using only PowerShell and we will not rely on any exploits or attack platform (like Kali Linux).
**DOMAIN ENUMERATION**

Let’s start with enumerating the domains, like enumerating the users, groups, some interesting fields and resources.

**Get-NetDomain**

This command will give us information about the current domain like the domain name and the domain controller:

```
PS C:\Users\yasser\Desktop> Get-NetDomain

Forest          : Fanzy.com
DomainControllers : (DC-01.Fanzy.com)
Children         : (WSH.Fanzy.com)
DomainNode       : (DC-01.Fanzy.com)
Parent           : (DC-01.Fanzy.com)
PdcRoleOwner     : DC-01.Fanzy.com
RidRoleOwner     : DC-01.Fanzy.com
InfrastructureRoleOwner : (DC-01.Fanzy.com)
Name             : Fanzy.com

(Additional output omitted for brevity.)
```

As shown above, the domain name is *(Fanzy.com)* and the DC is *(DC-01.Fanzy.com)*

**Get-NetDomain -domain “Domain Name”**

If you want to get the same results for another domain, use the above command.

```
PS C:\Users\yasser\Desktop> Get-NetDomain -Domain Dumpy

Forest          : Dumpy.com
DomainControllers : (DC-02.Dumpy.com)
Children         : ()
DomainNode       : (DC-02.Dumpy.com)
Parent           : (DC-02.Dumpy.com)
PdcRoleOwner     : DC-02.Dumpy.com
RidRoleOwner     : DC-02.Dumpy.com
InfrastructureRoleOwner : (DC-02.Dumpy.com)
Name             : Dumpy.com

(Additional output omitted for brevity.)
```

**Get-DomainSID**

Use this command to get the domain SID (Security IDentifier is a unique ID number that a computer or domain controller uses to identify you).

```
PS C:\Users\yasser\Desktop> Get-DomainSID

SID-1-5-21-3156372763-3995679764-3492621305
```

**Get-DomainPolicy**

 *(Get-DomainPolicy).”system access”*

Use this command to get the policy of the current domain.

```
PS C:\Users\yasser\Desktop> (Get-DomainPolicy).”system access”

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PasswordComplexity</td>
<td>15</td>
</tr>
<tr>
<td>MinimumPasswordHistory</td>
<td>22</td>
</tr>
<tr>
<td>MinimumPasswordLength</td>
<td>22</td>
</tr>
<tr>
<td>ForceLogoffWhenPasswordExpire</td>
<td>0</td>
</tr>
<tr>
<td>LDAPAnonymousNameLookup</td>
<td>0</td>
</tr>
<tr>
<td>LockoutEndCount</td>
<td>0</td>
</tr>
<tr>
<td>PasswordHistorySize</td>
<td>24</td>
</tr>
<tr>
<td>MinimumPasswordAge</td>
<td>1</td>
</tr>
<tr>
<td>ClearTextPassword</td>
<td>0</td>
</tr>
<tr>
<td>RequireLogonToChangePassword</td>
<td>0</td>
</tr>
</tbody>
</table>
```
**Get-NetDomainController**

Use this command to get information about the current domain controller (DC).

**Get-NetUser**

Use this command to list all the users in the current domain with information about each user.

**Get-UserProperty –Properties pwdlastset**

Use this command to see the last password set of each user in the current domain.
Find-UserField -SearchField Description –SearchTerm “pass”
Most of the system administrators are lazy and they don’t care about how to save the passwords! The above command will search for the word “pass” in the field “description” for each user in the domain.

To make it more clear, here what it looks like in the description of the user “Rashed” from the Active Directory:

Get-NetComputer
Use this command to list all the computers in the current domain.

Get-NetComputer –OperatingSystem "Windows 7 Ultimate"
Use this command to list all the operating systems “Windows 7 Ultimate”.
**Get-NetComputer -Ping**

Use this command to get all the pingable computers (live hosts) in the current domain.

```
PS C:\Users\jasser\Desktop> Get-NetComputer -Ping
DC-01.Fanzy.com
Client-02.Fanzy.com
CLIENT-01.Fanzy.com
```

**Get-NetGroup**

Use this command to get all the groups in the current domain.

```
PS C:\Users\jasser\Desktop> Get-NetGroup
Administrators
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_USERS
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
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
```

**Get-NetGroup *admin***

Use this command to get all the groups that contain the word “admin” in the group name.

```
PS C:\Users\jasser\Desktop> Get-NetGroup *admin*
Administrators
Hyper-V Administrators
Schema Admins
Enterprise Admins
Domain Admins
DNSAdmin
DHCP Administrators
IT_Admin
```
Get-NetGroupMember -GroupName "Domain Admins"
Use this command to get the members of the group “Domain Admin”.

```
PFE CI(User)\user\Desktop> Get-NetGroupMember -GroupName "Domain Admins"
```

Get-NetGroup -UserName "khalid"
Use this command to get the group membership of the user “Khalid”

```
PFE CI(User)\user\Desktop> Get-NetGroup -UserName "Khalid"
```

Get-NetLocalGroup -ComputerName Client-02
Use this command to get all the local administrators on a machine. (Note that it needs administrative rights).

```
PFE CI(User)\user\Desktop> Get-NetLocalGroup -ComputerName Client-02
```
Get-NetLoggedon –ComputerName “Client-02”
Use this command to get actively logged users on a computer (Note that it needs administrative rights)

```
P => C:\Users\khello\Desktop> Get-NetLoggedon –ComputerName Client-02
```

Get-LastLoggedOn –ComputerName Client-02
Use this command to get the last logged user on a computer (Note that it needs administrative rights)

```
P => C:\Users\khello\Desktop> Get-LastLoggedOn –ComputerName Client-02
```

Invoke-ShareFinder
Use this command to find shares on the hosts in the current domain.

```
P => C:\Users\vasser\Desktop> Invoke-ShareFinder
```
GROUP POLICY (GPO) ENUMERATION

In an Active Directory environment, Group Policy is an easy way to configure computer and user settings on computers that are part of the domain. Group Policy allows you to centralize the management of computers on your network without having to physically go to and configure each computer individually.

So let’s go to enumerate the GPO on the domain environment.

Get-NetGPO -ComputerName client-02.fanzy.com

Use this command to get a list of the GPO in the computer (Client-02).

We can see that there is a group policy name (Firewall OFF) which it’s clearly that it turns off the firewall on all the computers on the current domain.

Find-GPOComputerAdmin -Computername client-02.fanzy.com

Use this command to find users who have local admin rights over the machine Client-02 through GPO.

Find-GPOLocation -UserName Aziz

Use this command to find all computers that “Aziz” has local administrator rights in the current domain through the applied GPO.
Get-NetOU
Use this command to get all the OUs (Organization Units) in the current domain.

```
PS C:\Users\khalid\Desktop> Get-NetOU
LDAP://OU=Domain Controllers,DC=Fanzy,DC=com
LDAP://OU=Lab,DC=Fanzy,DC=com
LDAP://OU=Users,OU=Lab,DC=Fanzy,DC=com
LDAP://OU=Computers,OU=Lab,DC=Fanzy,DC=com
LDAP://OU=IT,OU=Lab,DC=Fanzy,DC=com
LDAP://OU=HR,OU=Lab,DC=Fanzy,DC=com
LDAP://OU=Development,OU=Lab,DC=Fanzy,DC=com
LDAP://OU=Help Desk,OU=Lab,DC=Fanzy,DC=com
PS C:\Users\khalid\Desktop>  
```

**DOMAIN TRUSTS ENUMERATION**
In an AD environment, trust is a relationship between two domains or forests which allows users of one domain or forest to access resources in the other domain or forest. For example, a user in domain A can request or access resources in domain B (like query the computers in the domain B).

**Trusts Direction:**

- **Two-way trust (Bi-directional):** Users from Domain A can access resources in Domain B and vice versa.
- **One-way trust (Unidirectional):** Users in the trusted domain can access resources in the trusting domain but the reverse is not true

**Trusts Transitivity:**

- **Parent-child trust:** It is created automatically between the new domain and the domain that precedes it in the namespace hierarchy, whenever a new domain is added in a tree. For example, usa.fanzy.com is a child of fanzy.com). This trust is always two-way transitive.
- **Tree-root trust:** It is created automatically between whenever a new domain tree is added to a forest root. This trust is always two-way transitive.

**External Trusts:** Between two domains in different forests when forests do not have a trust relationship. It can be one-way or two-way and is nontransitive.

As read teams, it’s important to enumerate the domain trusts in order to expand the attack surface.
Get-NetDomainTrust
Use this command to get a list of all domain trusts for the current domain to map the domain trust.

<table>
<thead>
<tr>
<th>SourceName</th>
<th>TargetName</th>
<th>TrustType</th>
<th>TrustDirection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fanzy.com</td>
<td>USA.Fanzy.com</td>
<td>ParentChild</td>
<td>Bidirectional</td>
</tr>
</tbody>
</table>

Get-NetForest
Use this command to get details about the current forest.

Get-NetForest -Forest dampy.com
Use this command to get details about another forest.

Get-NetForestDomain
Use this command to get all the domains in the current forest.
Get-NetForestCatalog
Use this command to get all global catalogs for the current forest.

Get-NetForestTrust
Use this command to map the trusts of a forest.

From the above result, we can see that the domain (Fanzy.com) has a two-way trust (Bidirectional) with the domain (Dampy.com) as well as with the domain (Lenda.com).

So, from the domain trust we can for example query the computers name of another domain (Dampy.com) as shown below.
USER HUNTING
When we got a foothold on a machine in the AD environment, it’s important to look for the privileged users such as the Local Administrators or the Domain Admins. In this section, we are going to hunt those users in the AD environment in order to gain Domain Admin rights from a domain user (normal user).

Find-LocalAdminAccess
Use this command to find all machines on the current domain where the current user has local admin access.

Invoke-EnumerateLocalAdmin
Use this command to find local admins on all machines of the domain (needs administrator privs on non-dc machines).

Invoke-UserHunter
Use this command to find computers where a domain has logged in.

From the above output, we can see that the Domain Admin (Dona) in logged in the machine (Client-01) with its IP (10.10.10.20).
Invoke-UserHunter -UserName "Aziz"
Use this command to find computers where a specific user has sessions.

```
PS C:\Users\khalid\Desktop> Invoke-UserHunter -UserName "Aziz"
UserDomain : FANZY
UserName   : Aziz
ComputerName : Client-02.Fanzy.com
IPAddress   : 10.10.10.30
```

Invoke-UserHunter -CheckAccess
Use this command to find computers where a domain admin is logged in and current user has access.

```
UserDomain : FANZY
UserName   : Dona
ComputerName : Client-02.Fanzy.com
IPAddress   : 10.10.10.30
SessionFrom : 
SessionFromName : 
LocalAdmin   : True

UserDomain : FANZY
UserName   : Dona
ComputerName : CLIENT-01.Fanzy.com
IPAddress   : 10.10.10.20
SessionFrom : 
SessionFromName : 
LocalAdmin   : True
```
Access Control Lists (ACL) Enumeration

An Access Control List (ACL) is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee. The security descriptor for a securable object can contain two types of ACLs: a DACL and a SACL.

**DACL**: Defines the permissions trustees (a user or group) have on an object.

**SACL**: Logs success and failure audit messages when an object is accessed.

In other words, the ACL is like asking: who has permission and what can be done on an object?

Most of the system administrators are wrongly configuring the ACL (such as granting a normal user to important permissions). So as attackers, we are interested in enumerating the ACL in order to find interesting ACLs!

Get-ObjectACL -SamAccountName "users" -ResolveGUIDs

Use this command to enumerate the ACLs for the users group.

```
PS C:\Users\user\Desktop> Get-ObjectACL -SamAccountName "users" -ResolveGUIDs

PropagationFlags : None
InheritanceFlags  : None
ObjectType        : All
AccessControlType : Allow
ObjectID          : 2-1-5-32-545
InheritedObjectID : None
Inherited         : False
IdentityReference :CN=Users,CN=BuiltIn,DC=Fancy,DC=com
ObjectFlags       : None
ActiveDirectoryRights : GenericRead
InheritanceType   : None

PropagationFlags : None
InheritanceFlags : None
ObjectType        : All
AccessControlType : Allow
ObjectID          : 2-1-5-32-545
InheritedObjectID : None
Inherited         : False
IdentityReference :CN=Users,CN=BuiltIn,DC=Fancy,DC=com
ObjectFlags       : None
ActiveDirectoryRights : GenericRead
InheritanceType   : None

PropagationFlags : None
InheritanceFlags : None
ObjectType        : All
AccessControlType : Allow
ObjectID          : 2-1-5-32-545
InheritedObjectID : None
Inherited         : False
IdentityReference :CN=Users,CN=BuiltIn,DC=Fancy,DC=com
ObjectFlags       : None
ActiveDirectoryRights : GenericRead
InheritanceType   : None
```

Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}

Use this command to see if there is any user has a modification rights to a GPO.

```powershell
PS C:\Users\<user>\Desktop> Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}
```

<table>
<thead>
<tr>
<th>PropagationFlags</th>
<th>InheritOnly</th>
</tr>
</thead>
<tbody>
<tr>
<td>InheritanceFlags</td>
<td>ContainerInherit</td>
</tr>
<tr>
<td>ObjectType</td>
<td>All</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>ObjectSid</td>
<td>Inherited</td>
</tr>
<tr>
<td>ObjectDN</td>
<td>CN=31E2FF14-818D-11D2-945F-88C64F6B84F9, CN=Policy, CN=System, DC=Fanyz, DC=com</td>
</tr>
<tr>
<td>IdentityReference</td>
<td>Creator Creator Owner</td>
</tr>
<tr>
<td>ObjectClass</td>
<td>User</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead, WriteDac</td>
</tr>
<tr>
<td>Owner</td>
<td>Owner</td>
</tr>
<tr>
<td>InheritanceType</td>
<td>Descendants</td>
</tr>
</tbody>
</table>

Get-ObjectAcl -SamAccountName labuser -ResolveGUIDs -RightsFilter "ResetPassword"

Use this command to check if the user “Sarah” has the permission (Reset Password).

```powershell
PS C:\Users\<user>\Desktop> Invoke-AclScanner -ResolveGUIDs ! ?$_.IdentityReference -match "Sarah"
```

<table>
<thead>
<tr>
<th>PropagationFlags</th>
<th>InheritOnly</th>
</tr>
</thead>
<tbody>
<tr>
<td>InheritanceFlags</td>
<td>ContainerInherit</td>
</tr>
<tr>
<td>ObjectType</td>
<td>All</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>ObjectSid</td>
<td>Inherited</td>
</tr>
<tr>
<td>ObjectDN</td>
<td>CN=31E2FF14-818D-11D2-945F-88C64F6B84F9, CN=Policy, CN=System, DC=Fanyz, DC=com</td>
</tr>
<tr>
<td>IdentityReference</td>
<td>&quot;NT AUTHORITY\ENTERPRISE\DOMAIN\CONTROLLERS&quot;</td>
</tr>
<tr>
<td>ObjectClass</td>
<td>User</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead</td>
</tr>
<tr>
<td>Owner</td>
<td>Owner</td>
</tr>
<tr>
<td>InheritanceType</td>
<td>All</td>
</tr>
</tbody>
</table>

We can see that the user “Sarah” has this interesting permission (Reset Password) which she can reset the password of any user in the domain even though that “Sarah” is a normal user!
CONCLUSION
As red teamers, it’s extremely important to enumerate the Active Directory environment whenever we have a foothold on a machine in the AD. Without a proper enumeration, we may don’t achieve our goals as enumerating the AD will help us to gain Domain Admin rights and reach the DC. We can enumerate the domain and the trusts of the domains and the forests, the group policy, the access control list (ACL) and hunting the users in order to reach our goals on an engagement.
REFERENCES

- https://www.harmj0y.net/blog/tag/powerview/
- https://medium.com/tech-jobs-academy/trust-relationships-within-active-directory-directory-services-9f18b3a9e7da