

Vulnerable AD Configuration:

Create a vulnerable Active Directory that's allowing you to test most of Active Directory attacks in local lab. Supported Attacks Are [Abusing ACLs/ACEs](#), [Kerberoasting](#), [AS-REP Roasting](#), [Abuse DnsAdmins](#), [Password in Object Description](#), [User Objects with Default password](#), [Password Spraying](#), [DCSync](#), [Silver Ticket](#), [Golden Ticket](#), [Pass-the-Hash](#), [Pass-the-Ticket](#) and [SMB Signing Disabled](#).

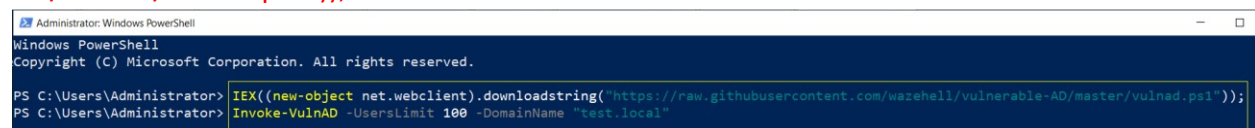
Prerequisites

1. You need to have a Windows Server running in VMware. I had a Windows Server 2019.
2. If you have a Server without an AD in VM, and you don't want to set up the AD manually, you can set it up using the following script.

```
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\\Windows\\NTDS" -  
DomainMode "7" -DomainName "test.local" -DomainNetbiosName "Test" -ForestMode "7" -  
InstallDns:$true -LogPath "C:\\Windows\\NTDS" -NoRebootOnCompletion:$false -SysvolPath  
"C:\\Windows\\SYSVOL" -Force:$true
```

1. Login to your Domain Controller machine in my case Windows Server 2019.
2. Open the PowerShell in Windows Server 2019.
3. Run the following command to download the script from the GitHub repo.

```
IEX((new-object  
net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-  
AD/master/vulnad.ps1"));
```



```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (c) Microsoft Corporation. All rights reserved.  
  
PS C:\Users\Administrator> IEX((new-object net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1"));  
PS C:\Users\Administrator> Invoke-VulnAD -UsersLimit 100 -DomainName "test.local"
```

followed by below command.

```
Invoke-VulnAD -UsersLimit 100 -DomainName "test.local"
```

VULN AD - Vulnerable Active Directory

By wazehell @safe_buffer

```
[*] Creating blondelle.harriette User
[*] Creating agneta.mora User
[*] Creating rana.nady User
[*] Creating fania.filide User
[*] Creating lethia.latrena User
[*] Creating lorrie.elisabetta User
[*] Creating gillan.arlina User
[*] Creating almire.leesa User
[*] Creating kilian.estrella User
[*] Creating annabell.chery User
[*] Creating silvana.letta User
[*] Creating raeann.crystie User
[*] Creating maegan.flor User
[*] Creating darice.brandice User
[*] Creating hester.leo User
[*] Creating ellene.dix User
[*] Creating dotty.elisabeth User
[*] Creating dulcia.florance User
```

And you have successfully set up your vulnerable Active Directory AD.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> IEX((new-object net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1"));
PS C:\Users\Administrator> Invoke-VulnAD -UsersLimit 100 -DomainName "test.local"

[+] Kerberoasting Done
[*] AS-REPRoasting belva.kacey
[*] AS-REPRoasting raeann.crystie
[*] AS-REPRoasting nerty.kent
[+] AS-REPRoasting Done
[*] DnsAdmins : belva.kacey
[*] DnsAdmins : letta.marguerite
[*] DnsAdmins : kaitlin.rani
[*] DnsAdmins : ethelin.evaleen
[*] DnsAdmins : rhoda.lucine
[*] DnsAdmins Nested Group : Senior management
[+] DnsAdmins Done
[*] Password in Description : karoline.amalle
[*] Password in Description : silvana.letta
[+] Password In Object Description Done
[*] Default Password : pearline.lilah
[*] Default Password : leif.adi
[+] Default Password Done
[*] Same Password (Password Spraying) : kilian.estrella
[*] Same Password (Password Spraying) : eimile.janette
[+] Password Spraying Done
[+] DCSync Done
[+] SMB Signing Disabled
```