Vulnerable-AD: создание стенда для атак на Active Directory

spy-soft.net/vulnerable-ad-lab-for-attack-active-directory

1 июля 2023 г.

Vulnerable-AD позволяет создать лабораторию (уязвимую Active Directory) и практиковать различные атаки на Active Directory. Давайте рассмотрим, что из себя представляет Vulnerable-AD, как его установить и использовать.

Еще по теме: Пентест Active Directory на HTB Intelligence

Что такое Vulnerable-AD

Active Directory (AD) — это сервис каталога и служба управления доступом, разработанная компанией Microsoft, которая используется для хранения информации о пользователях, компьютерах, группах и других объектах в сетевой среде Windows. AD предоставляет централизованное хранение и управление данными учетных записей и ресурсов, а также обеспечивает механизм аутентификации и авторизации для пользователей и компьютеров в доменной сети. Он широко используется в корпоративных сетях для обеспечения безопасности, централизованного управления и совместного доступа к ресурсам.

Vulnerable-AD — бесплатный инструмент на GitHub, который позволяет создать уязвимую Active Directory для атак. Это может быть полезно для практики пентеста Active Directory и обучения админов.

Список поддерживаемых Vulnerable-AD атак на Active Directory:

- **DCSync** — это метод, при котором злоумышленник с использованием привилегий администратора получает доступ к данным о паролях, хранящимся в Active Directory. Это позволяет получить хэш пароля для любого пользователя домена без его фактического изменения.

- **Silver Ticket** — это вид атаки, при котором злоумышленник создает поддельный билет Kerberos для обхода механизма аутентификации и получения несанкционированного доступа к ресурсам.
- **Golden Ticket** — это более мощный вариант атаки на базе Kerberos, при которой злоумышленник создает фальшивый билет Kerberos с полными привилегиями администратора домена. Это позволяет им обходить любые меры безопасности и контроля доступа в Active Directory.
- **Kerberoasting** — это атака, направленная на получение хэшей паролей пользователей, используя слабые шифровальные алгоритмы, используемые для защиты билетов Kerberos. Злоумышленник может декодировать полученные хэши и использовать их для восстановления фактических паролей.
- **Pass-the-Hash** — атака, при которой злоумышленник использует хэш пароля, полученный в результате атаки или утечки данных, для аутентификации на других компьютерах в сети, обходя необходимость знания фактического пароля.
- **Pass-the-Ticket** — атака, при которой злоумышленник использует украденный билет Kerberos для аутентификации и получения доступа к системам без необходимости знать фактический пароль пользователя.
- **AS-REP Roasting** — это атака, направленная на получение хэшей паролей пользователей, используя уязвимость в процессе аутентификации Kerberos, которая позволяет запросить ответ без предоставления фактического пароля.
- **Abuse DnsAdmins** — это относится к злоупотреблению привилегиями DnsAdmins в Active Directory для получения несанкционированного доступа и контроля над доменом.
- **Password Spraying** — метод атаки, при котором злоумышленник пытается использовать несколько распространенных паролей или пароли из утечек данных для множества пользователей с целью получить доступ к аккаунтам.
- **Abusing ACLs/ACEs** — это относится к злоупотреблению списками контроля доступа (ACL) и записями контроля доступа (ACE) в Active Directory для получения несанкционированного доступа к ресурсам.
- **SMB Signing Disabled** — отключение подписи SMB (Server Message Block) означает, что серверы и клиенты в сети не обязаны подписывать и проверять целостность передаваемых файлов и данных. Это может позволить злоумышленникам внедряться в сеть и выполнять атаки MITM (Man-in-the-Middle) или изменять передаваемые данные без обнаружения.
- **Password in Object Description** — это указывает на ситуацию, когда пароль пользователя или другая конфиденциальная информация сохраняется в описании объекта Active Directory. Это может привести к утечке конфиденциальной информации, если злоумышленник получит доступ к объектам Active Directory.

- **User Objects With Default Password** — это относится к ситуации, когда объекты пользователей в Active Directory имеют установленный фабричный или стандартный пароль, который не был изменен после создания учетной записи. Это оставляет пользователей уязвимыми для атак, таких как перебор паролей или использование стандартных учетных записей с известными паролями.

Еще по теме: GOAD — лаборатория для практики взлома Active Directory

Установка зависимостей

Вам потребуется установленный Windows-сервер на VBox или Vmware. Я использовал Windows Server 2019 в VMware. У меня уже была настроена служба Active Directory на этом сервере.

Если на вашей виртуальной машине сервер без службы AD, и вы не хотите настраивать Active Directory вручную, можете использовать скрипт:

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

Я не проверял работу скрипта, так как у меня уже была настроена Active Directory.

Установка Vulnerable-AD

Установка и использование Vulnerable-AD можно выполнить следующим образом:

Шаг 1: Войдите в свою машину с контроллером домена (в моем случае — Windows Server 2019).

Шаг 2: Откройте PowerShell.

Шаг 3: Выполните команду:

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

Это загрузит скрипт из репозитория GitHub.

Шаг 4: Вероятно, при первом запуске команды вы получите следующую ошибку:

```
    Directory: C:\Users\Administrator\Desktop\vulnerable-AD


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/6/2022  12:50 AM                .github
-a----         5/6/2022  12:50 AM           1084 LICENSE
-a----         5/6/2022  12:50 AM           1382 README.md
-a----         5/6/2022  12:50 AM          66242 vulnad.ps1


PS C:\Users\Administrator\Desktop\vulnerable-AD> . .\vulnad.ps1
At C:\Users\Administrator\Desktop\vulnerable-AD\vulnad.ps1:24 char:46
+ ...    $banner+= $Global:Spacing + 'â–ˆâ–ˆâ–ˆâ•—   â–ˆâ–ˆâ–ˆâ•—â–ˆâ–ˆâ•—â–ˆâ–ˆâ–ˆâ•—   â–ˆâ–ˆâ–ˆ ...
+                                              ~~~~~~~~~~~~~~~~~~~~
Unexpected token 'â–ˆâ–ˆâ–ˆâ•—â–ˆâ–ˆâ–ˆâ•—' in expression or statement.
At C:\Users\Administrator\Desktop\vulnerable-AD\vulnad.ps1:25 char:46
+ ...    $banner+= $Global:Spacing + 'â–ˆâ–ˆâ–ˆâ•—   â–ˆâ–ˆâ–ˆâ•—â–ˆâ–ˆâ•—â–ˆâ–ˆâ–ˆâ•—   â–ˆâ–ˆâ–ˆ ...
+                                              ~~~~~~~~~~~~~~~~~~~~
Unexpected token 'â–ˆâ–ˆâ–ˆâ•—â–ˆâ–ˆâ–ˆâ•—' in expression or statement.
At C:\Users\Administrator\Desktop\vulnerable-AD\vulnad.ps1:258 char:37
+     Write-Good "SMB Signing Disabled"
+                                     ~
The string is missing the terminator: ".
At C:\Users\Administrator\Desktop\vulnerable-AD\vulnad.ps1:20 char:21
+ function ShowBanner {
+                     ~
Missing closing '}' in statement block or type definition.
    + CategoryInfo          : ParserError: (:) [], ParseException
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\Users\Administrator\Desktop\vulnerable-AD>
```

Это вызвано функцией banner в скрипте. Изучив проблемы на странице GitHub, я нашел решение.

Шаг 5: Чтобы исправить ошибку, клонируйте репозиторий на свою машину:

```
1  git clone https://github.com/WazeHell/vulnerable-AD.git
```

Откройте в редакторе скрипт **vulnad.ps1** и удалите banner.

```
20  function ShowBanner {
21      $banner = @()
22      $banner+= $Global:Spacing + ''
23      $banner+= $Global:Spacing + '
24      $banner+= $Global:Spacing + '
25      $banner+= $Global:Spacing + '
26      $banner+= $Global:Spacing + '
27      $banner+= $Global:Spacing + '
28      $banner+= $Global:Spacing + '
29      $banner+= $Global:Spacing + ''
30      $banner+= $Global:Spacing + 'By wazehell @safe_buffer'
31      $banner | foreach-object {
32          Write-Host $_ -ForegroundColor (Get-Random -Input @('Green','Cyan','Yellow','gray','white'))
33      }
34  }
35  function VulnAD-GetRandom {
36     Param(
37       [array]$InputList
38     )
39     return Get-Random -InputObject $InputList
40  }
41  function VulnAD-AddADGroup {
42      Param(
43          [array]$GroupList
44      )
```

Как видно на картинке, выделенные строки вызывают ошибки. Удалите их и сохраните скрипт.

Шаг 6: Выполните команду:

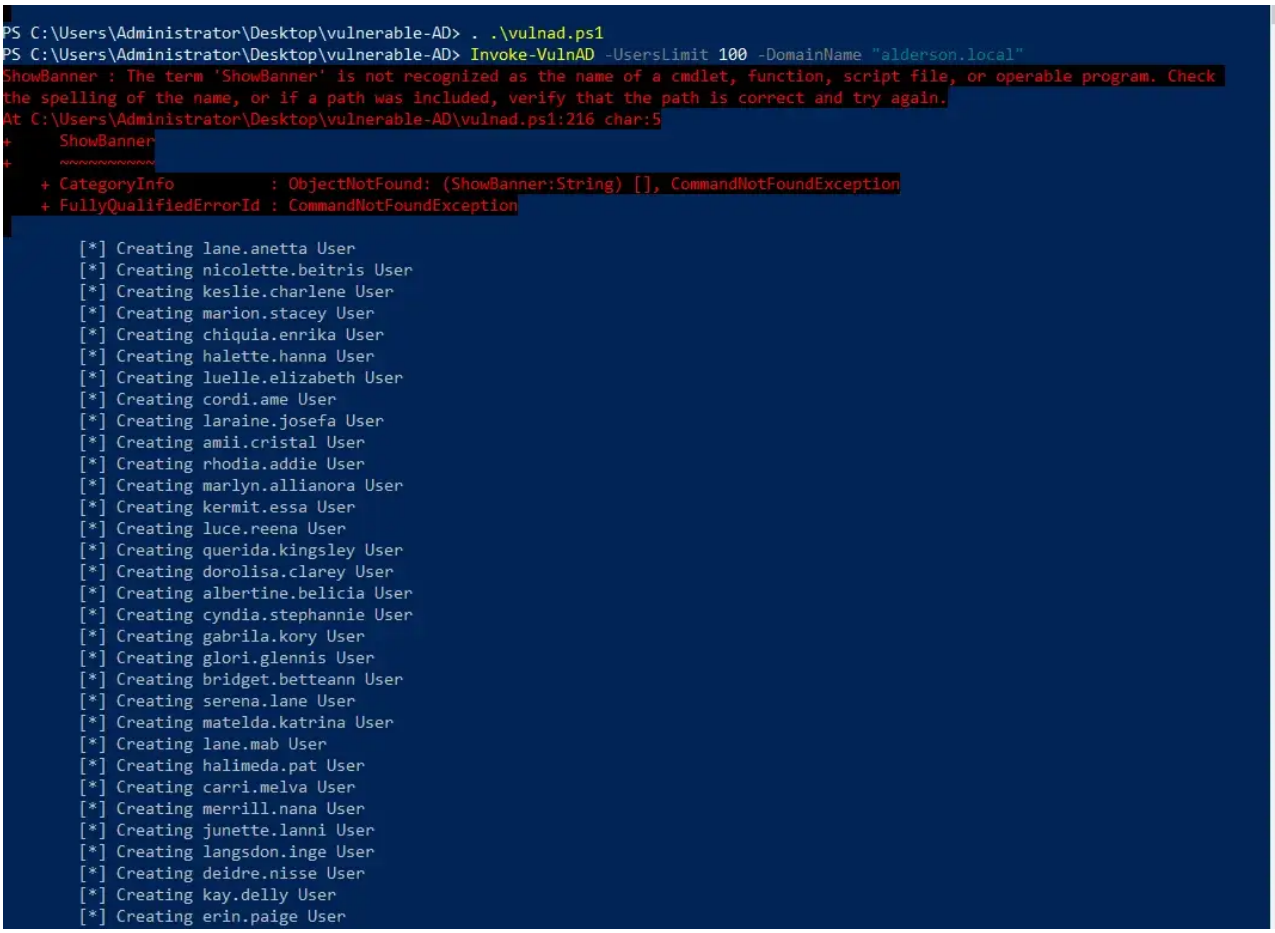
```
. .\vulnad.ps1
```

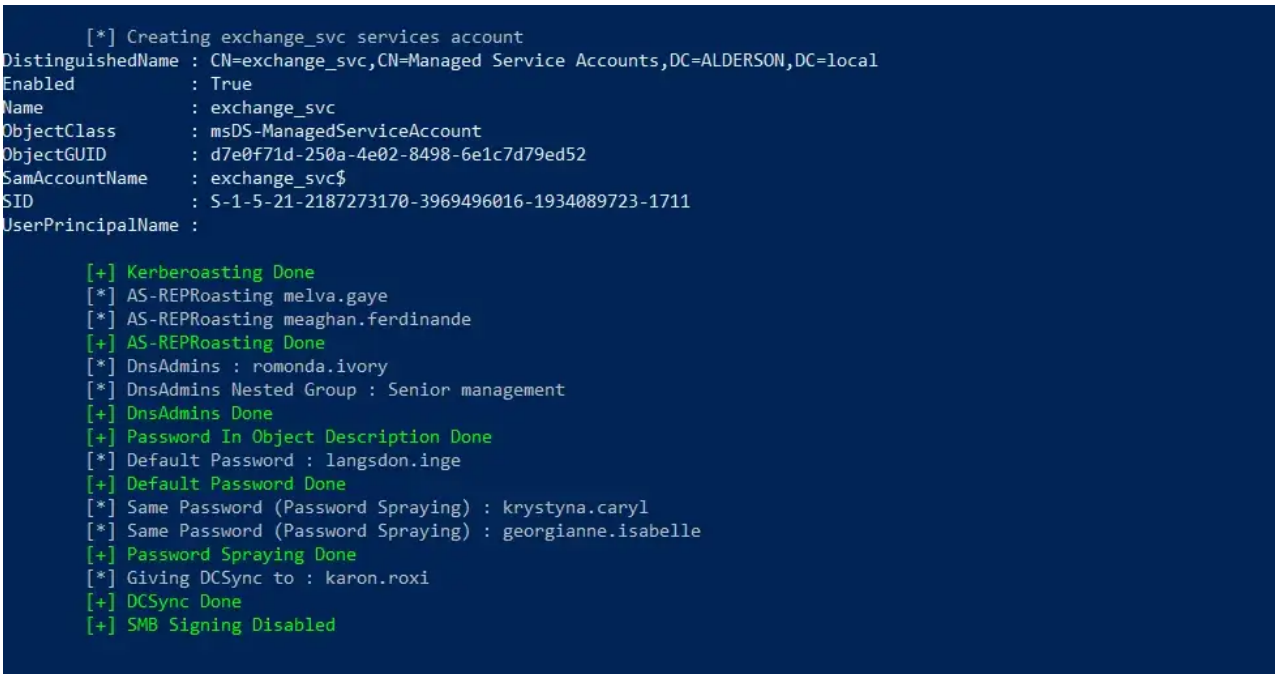
а затем:

```
Invoke-VulnAD -UsersLimit 100 -DomainName "cs.org"
```

Замените **cs.org** на имя вашего домена (в моем случае — alderson.local).

После этого вы должны увидеть следующий вывод:





Теперь с помощью Vulnerable-AD можно работать с уязвимой Active Directory и проводить атаки, не нарушая закон.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Атаки на службы сертификатов Active Directory
- Уклонение от Honeytoken при атаке Active Directory