POS - EXPLORAÇÃO ADLAB

SONAEL NETO

March 2023

Pós-Exploração - ADLab | Sonael de A. Angelos Neto

- **Como é feito a exploração e o reconhecimento em ambientes com Active Directory?**

  Podem ser realizados de várias maneiras, algumas das quais incluem:

  - **Escaneamento de portas**: Um invasor pode usar ferramentas de escaneamento de portas, como Nmap, para identificar os sistemas que estão em execução no ambiente e os serviços que estão sendo executados nesses sistemas. Isso pode ajudar a identificar sistemas vulneráveis que podem ser explorados.
  - **Enumeração de usuários e grupos**: A enumeração de usuários e grupos pode ser realizada para identificar contas de usuário com privilégios elevados ou contas de serviço que possam ser exploradas.
  - **Coleta de informações do Active Directory**: Um invasor pode usar ferramentas como o PowerView para coletar informações do Active Directory, como informações sobre usuários, grupos, permissões, políticas de grupo e muito mais. Essas informações podem ser usadas para identificar sistemas e usuários vulneráveis.
  - **Exploração de vulnerabilidades**: Depois que as informações sobre o ambiente foram coletadas, um invasor pode usar ferramentas de exploração de vulnerabilidades para identificar sistemas e aplicativos vulneráveis que possam ser explorados para obter acesso não autorizado ao ambiente.
  - **Ataques de phishing**: Ataques de phishing podem ser usados para obter acesso às credenciais de usuários com privilégios elevados. Esses ataques podem ser realizados por meio de e-mails de spear-phishing, que parecem ser enviados por remetentes confiáveis, ou por meio de ataques de engenharia social, nos quais um invasor se passa por um funcionário do suporte técnico e solicita as credenciais do usuário.

  Para reduzir o risco de exploração e reconhecimento em um ambiente Active Directory, é importante implementar medidas de segurança, como a aplicação de atualizações de segurança, práticas de segurança de senha fortes, controle de acesso baseado em função, monitoramento de atividade de usuário e detecção de anomalias. Além disso, é importante educar os usuários sobre os perigos dos ataques de phishing e outras técnicas de engenharia social para que possam estar mais vigilantes e alertas.

- **Como se da a elevação de privilégios em um ambiente Active Directory?**

  A elevação de privilégios em um ambiente Active Directory pode ser realizada de diversas formas, algumas delas incluem:

  - **Uso de credenciais privilegiadas roubadas**: Se um invasor conseguir obter acesso às credenciais de um usuário com privilégios elevados, ele poderá usá-las para se autenticar em outros sistemas e obter acesso privilegiado.
  - **Exploração de vulnerabilidades em software**: Muitas vezes, sistemas e aplicativos em um ambiente Active Directory podem ter vulnerabilidades que permitem que um invasor execute código arbitrário com privilégios elevados. Essa exploração pode permitir que o invasor assuma o controle total do sistema.
  - **Ataques de engenharia social**: Ataques de engenharia social, como phishing ou spear-phishing, podem ser usados para obter acesso às credenciais de usuários com privilégios elevados. Isso pode permitir que o invasor se autentique em outros sistemas e obtenha acesso privilegiado.
  - **Uso de técnicas de escalonamento de privilégios**: Técnicas como "Pass-the-Hash" ou "Pass-the-Ticket" podem ser usadas para obter acesso com privilégios elevados sem a necessidade de obter as credenciais reais do usuário. Essas técnicas exploram vulnerabilidades em protocolos de autenticação.
  - **Uso de backdoors ou malware**: Se um invasor conseguir instalar um backdoor ou malware em um sistema com privilégios elevados, ele poderá usá-lo para obter acesso privilegiado em outros sistemas.

  Para reduzir o risco de elevação de privilégios em um ambiente Active Directory, é importante implementar medidas de segurança como o controle de acesso baseado em função, monitoramento de atividade de usuário e detecção de anomalias, além de aplicar atualizações de segurança e práticas de segurança de senha fortes.

Sumário

Nesse documento iremos explorar um Active Directory.

Ferramentas utilizadas:

- **Active Directory Explorer**
  - Utilizaremos o Active Directory Explorer para explorar o Active Directory.
- **ldapdomaindump**
  - Utilizaremos o ldapdomaindump para explorar o Active Directory.

• Qual o “nome” do domínio?

Para saber o nome do domínio, utilizaremos o comando "`wmic computersystem get domain`":

```
PS C:\Users\cooten.TH> wmic computersystem get domain
Domain
th.local
```

Também podemos utilizar o comando `systeminfo`:

```
PS C:\Users\cooten.TH> systeminfo

Host Name:                 win10
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          N/A
Registered Organization:   N/A
Product ID:                00329-00000-00003-AA248
Original Install Date:     3/16/2023, 6:07:57 AM
System Boot Time:          3/16/2023, 6:23:41 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2594 Mhz
BIOS Version:              Microsoft Corporation Hyper-V UEFI Release v4.1, 5/9/2022
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Total Physical Memory:     2,047 MB
Available Physical Memory: 521 MB
Virtual Memory: Max Size:  2,559 MB
Virtual Memory: Available: 557 MB
Virtual Memory: In Use:    2,002 MB
Page File Location(s):     D:\pagefile.sys
Domain:                    th.local
Logon Server:              \\dc
Hotfix(s):                 5 Hotfix(s) Installed.
```

Com isso, temos o nome do domínio: `th.local`.

• Qual o nome de todos os computadores do domínio?

Para saber o nome de todos os computadores do domínio, utilizaremos o comando "`net group "domain computers" /domain`":

```
PS C:\Users\cooten.TH> net group "domain computers" /domain
The request will be processed at a domain controller for domain th.local.

Group name     Domain Computers
Comment        All workstations and servers joined to the domain

Members

-------------------------------------------------------------------------------
Colin                  Tony                   WIN10$
WINSERV2019$
The command completed successfully.
```

Note que apenas os nomes que possuem **$** no final são computadores do domínio.

Então, temos os seguintes computadores do domínio:

- `WINSERV2019$`
- `WIN10$`

• Qual o IP do controlador de domínio?

Para saber o IP do controlador de domínio, utilizaremos o comando "`nslookup th.local`":

```
PS C:\Users\cooten.TH> nslookup th.local
Server:  dc.internal.cloudapp.net
Address:  10.13.37.10

Name:    th.local
Address:  10.13.37.10
```

Também podemos utilizar o comando `ipconfig \all` pois normalmente o controlador de domínio é o primeiro servidor DNS:

```
PS C:\Users\cooten.TH> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : win10
   Primary Dns Suffix  . . . . . . . : th.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : th.local
                                       zr4kvnzgbiwetiu2pfm2j5j1ub.bx.internal.cloudapp.net

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : zr4kvnzgbiwetiu2pfm2j5j1ub.bx.internal.cloudapp.net
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-0D-3A-13-45-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9312:7ae3:96a6:834e%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.13.37.150(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, March 16, 2023 6:23:47 AM
   Lease Expires . . . . . . . . . . : Sunday, April 22, 2159 2:23:51 PM
   Default Gateway . . . . . . . . . : 10.13.37.1
   DHCP Server . . . . . . . . . . . : 168.63.129.16
   DHCPv6 IAID . . . . . . . . . . . : 100666682
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-A4-5C-3C-00-0D-3A-13-45-C8
   DNS Servers . . . . . . . . . . . : 10.13.37.10
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Com isso temos que o IP do controlador de domínio é "`10.13.37.10`".

• Qual o servidor dns da rede?

Como visto anteriormente o servidor DNS é o controlador de domínio, então o ip do servidor DNS é o mesmo do controlador de domínio "`10.13.37.10`".

• Qual a police de senhas do domínio?

Para saber a police de senhas do domínio, utilizaremos o comando "`net accounts /domain`":

```
PS C:\Users\cooten.TH> net accounts /domain
The request will be processed at a domain controller for domain th.local.

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    Never
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        PRIMARY
The command completed successfully.
```

Também podemos utilizar o script "`ldapdomaindump.py`" para obter a police de senhas do domínio.

Primeiro vamos gerar um dump do domínio com o comando "`python .\ldapdomaindump.py -u "th.local\cooten" -p "OlIrk8VS0ARWHGbP"-o domainthlocal -m 10.13.37.10`"

Agora vamos abrir o arquivo "`domain_policy.html`" e ver a police de senhas do domínio:

Domain policy

distinguishedName	Lockout time window	Lockout Duration	Lockout Threshold	Max password age	Min password age	Min password length	Password history length	Password properties	Machine Account Quota
DC=th,DC=local	10.0 minutes	10.0 minutes	0	42.00 days	1.00 days	7	24	PASSWORD_COMPLEX	10

onde temos que a police de senhas do domínio é:

- **Force user logoff how long after time expires:** `Never`
- **Minimum password age (days):** `1`
- **Maximum password age (days):** `42`
- **Minimum password length:** `7`
- **Length of password history maintained:** `24`
- **Lockout threshold:** `Never`
- **Lockout duration (minutes):** `10`
- **Lockout observation window (minutes):** `10`
- **Computer role:** `PRIMARY`

• Quantos grupos esse domínio possui?

Para saber quantos grupos esse domínio possui, utilizaremos o comando "`net group /domain`":

Com isso temos que o domínio possui `144` grupos.

• Quantos usuários são Administradores de domínio? E enterprise admins?

Para saber quantos usuários são **Domain Admins**, utilizaremos o comando "`net group /domain "Domain Admins"`":

E para saber quantos usuários são **Enterprise admins**, utilizaremos o comando "`net group /domain "Enterprise Admins"`":

Então temos que o domínio possui `6` membros **Domain Admins** e `1` membros **Enterprise admins**.

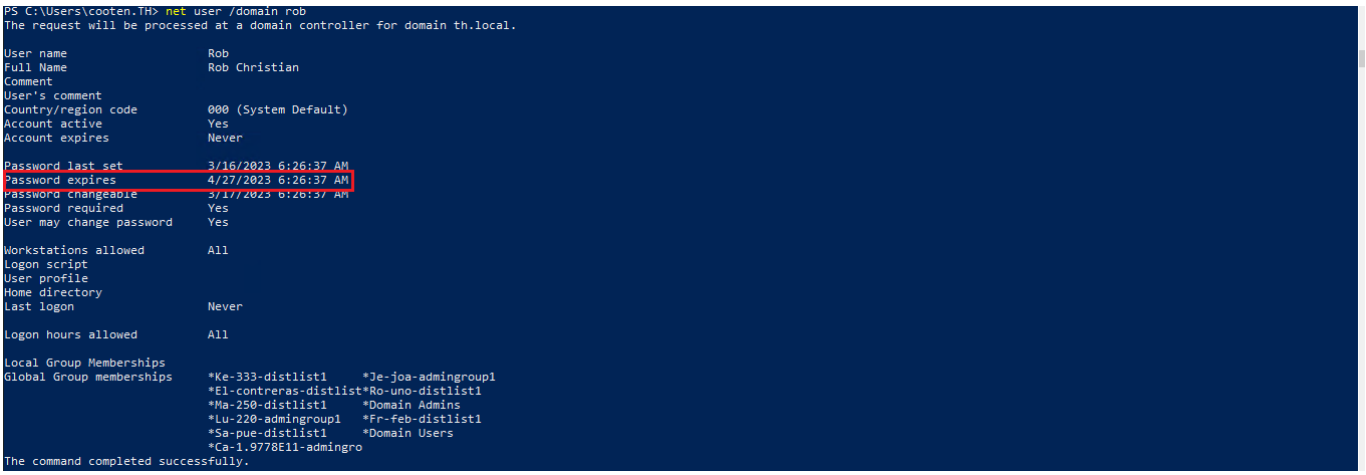
• Quais usuários são administradores do domínio?

De acordo com o resultado anterior, temos que os membros que pertencem ao grupo **Domain Admins** são:

- `cooten`
- `Jordan`
- `Cornelia`
- `Krista`
- `Dianne`
- `Rob`

• Existe algum administrador de domínio que a senha não expira? Se sim, qual?

Para saber se existe algum administrador de domínio que a senha não expira, utilizaremos o comando "`net user /domain NAME_USER`" para cada usuário do grupo **Domain Admins**:



Com isso, verificando todos os usuários do grupo **Domain Admins**, temos que não existe nenhum administrador de domínio que a senha não expira.

• Algum administrador possui algum comentário interessante no seu usuário? Se sim, qual?

O único membro do grupo **Domain Admins** que possui um comentário é o usuário `cooten`:

```
PS C:\Users\cooten.TH> net user /domain cooten
The request will be processed at a domain controller for domain th.local.

User name                    cooten
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/15/2023 10:04:56 PM
Password expires             4/26/2023 10:04:56 PM
Password changeable          3/16/2023 10:04:56 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/16/2023 6:36:55 AM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Cryptographic Operato
Global Group memberships     *Group Policy Creator *Schema Admins
                             *St-elchilean-distlist*Tr-enamedina-distlist
                             *Sa-aujourdhu-distlist*We-lachiconi-distlist
                             *Ro-uno-distlist1     *Domain Admins
                             *Enterprise Admins    *An-silvercha-admingro
                             *Yo-19JUNIO20-admingro*Do-NOC-admingroup1
                             *Domain Users         *Wi-905-distlist1
The command completed successfully.
```

Seu comentário diz: **Built-in account for administering the computer/domain**

> Conta integrada para administrar o computador/domínio

Porém olhando o aquivo "`domain_users.html`" gerado pelo script "`ldapdomaindump.py`", podemos ver que o usuário Kerry membro do grupo **Domain Users** possui um comentário interessante:

K.Spence	K.Spence	Kerry	Fr-aureliotq-admingroup1, Ga-cookie369-distlist1, No-siempreju-distlist1, Ro-pegueousi-distlist1, St-686104004-distlist1, Ma-pen-distlist1, Co-Tabouche2-distlist1, Ma-250-distlist1, Em-aureliotq-distlist1	Domain Users	03/16/23 05:26:25	03/16/23 05:26:26	01/01/01 00:00:00	NORMAL_ACCOUNT	03/16/23 05:26:26	1384	Just so I dont forget my password is JYe9!9&fwGgfB7R9UULh6yW2e

Seu comentário diz: **Just so I dont forget my password is JYe9!9&fwGgfB7R9UULh6yW2e**

> Só para não esquecer minha senha é JYe9!9&fwGgfB7R9UULh6yW2e

Temos aqui então uma senha que pode ser utilizada para logar no usuário `Kerry`.

• Dificuldades.

Nenhuma dificuldade relevante. =}

• Conclusão.

O ambiente Active Directory é amplamente utilizado em empresas e organizações para gerenciar usuários, grupos e recursos de rede. No entanto, esse ambiente também pode ser alvo de invasores que buscam obter acesso não autorizado a sistemas e informações confidenciais.

Para proteger o ambiente Active Directory contra ameaças de segurança, é necessário implementar medidas de segurança, como o controle de acesso baseado em função, monitoramento de atividade de usuário e detecção de anomalias, além de aplicar atualizações de segurança e práticas de segurança de senha fortes. É importante também educar os usuários sobre os perigos dos ataques de phishing e outras técnicas de engenharia social.

Por outro lado, para invasores que buscam explorar e reconhecer o ambiente Active Directory, é possível realizar várias técnicas, como escaneamento de portas, enumeração de usuários e grupos, coleta de informações do Active Directory, exploração de vulnerabilidades e ataques de phishing. Com essas técnicas, os invasores podem obter informações valiosas sobre o ambiente e identificar sistemas e usuários vulneráveis que podem ser explorados.

Portanto, é fundamental que empresas e organizações estejam cientes das ameaças de segurança que existem no ambiente Active Directory e implementem medidas de segurança robustas para proteger seus sistemas e informações confidenciais. Além disso, é importante manter-se atualizado sobre as últimas ameaças e vulnerabilidades e estar preparado para agir rapidamente em caso de incidentes de segurança.

• Referências.

- Post-Exploitation Basics In Active Directory Environment
- Windows Active Directory Post Exploitation Cheatsheet
- Active Directory Exploitation Cheat Sheet
- ChatGPT

• Laboratório.

- ADLab