NetExec (NXC) Cheat Sheet

Getting Started

- Installation
- Selecting Protocol
- Target Formats
- Authentication
- Username / Password
- NTLM Hash
- Kerberos
- Credential Database
- Password Spraying
- Brute Force

Core Capabilities

- Authentication Testing
- Enumeration
- Command Execution
- Credential Dumping
- File Upload / Download
- Privilege Escalation
- Lateral Movement

WINRM

- Password Spraying
- Authentication
- Command Execution
- Credential Extraction

LDAP

- Domain User Enumeration
- Domain Group Enumeration
- LDAP Queries
- ASREP Roasting
- Kerberoasting
- Delegation Enumeration
- Domain Trust Enumeration
- BloodHound Collection
- gMSA Credential Dump

SMB

- Authentication
- Share Enumeration
- User Enumeration
- Group Enumeration
- Password Spraying
- Command Execution
- Spider Shares
- File Upload / Download
- Credential Dumping
- LAPS Enumeration
- Spooler Check
- User Impersonation

MSSQL

- Authentication
- Privilege Escalation
- xp_cmdshell Execution
- Linked Servers
- File Upload / Download

SSH

- Password Spraying
- Authentication
- Command Execution
- File Transfer

FTP

- Password Spraying
- File Listing
- File Upload / Download

NFS

- Enumeration
- File Upload / Download
- Root Filesystem Escape

WMI

- Password Spraying
- Authentication
- Command Execution

RDP

- Password Spraying
- Screenshot
- Screenshot without NLA
- Command Execution

VNC

- Authentication
- Password Spraying
- Command Execution

Credential Management

- Credential Database
- Credential IDs
- Workspace Separation
- Credential Reuse

Modules and Automation

- spider_plus
- enum_av
- coerce_plus
- change-password
- backup_operator
- Custom Modules

www.hackingarticles.in