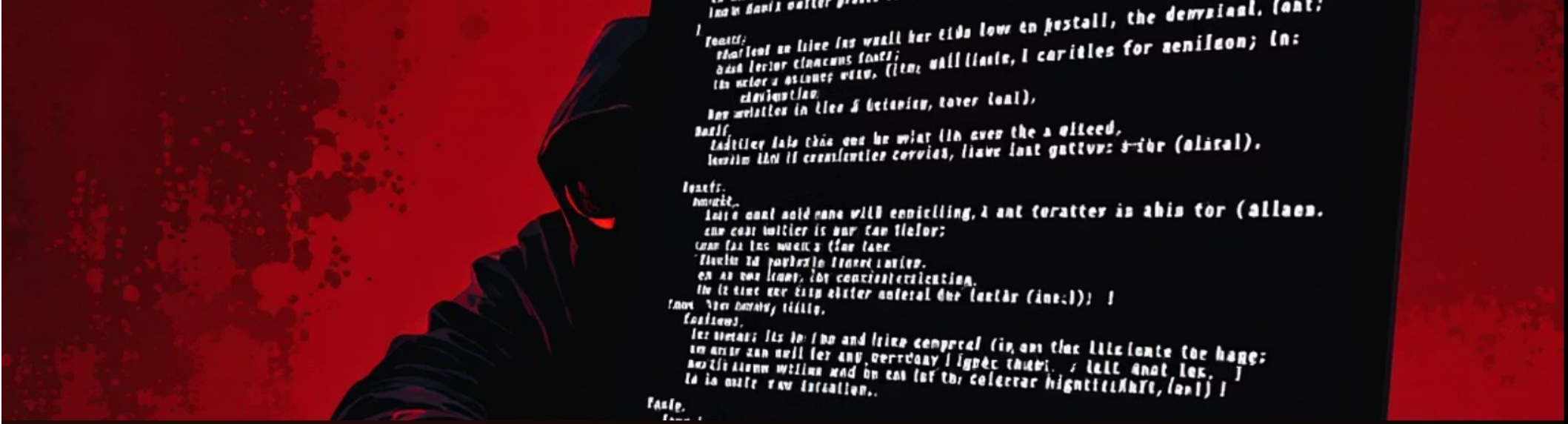


Introduction to Network Pentesting

Fundamental Concepts and Practical Skills

Swipe to unlock powerful network exploitation techniques →

What is Netcat?

Netcat is a versatile networking utility that reads and writes data across TCP or UDP connections. Available on both *NIX and Windows systems, it's essential for cross-platform penetration testing engagements

Netcat is available for both *NIX and Windows operating systems, consequently making it extremely useful for cross-platform engagements..

Client Mode

Connect to any TCP/UDP port or Netcat listener

Server Mode

Listen for incoming connections on specific ports

Bind Shells Explained

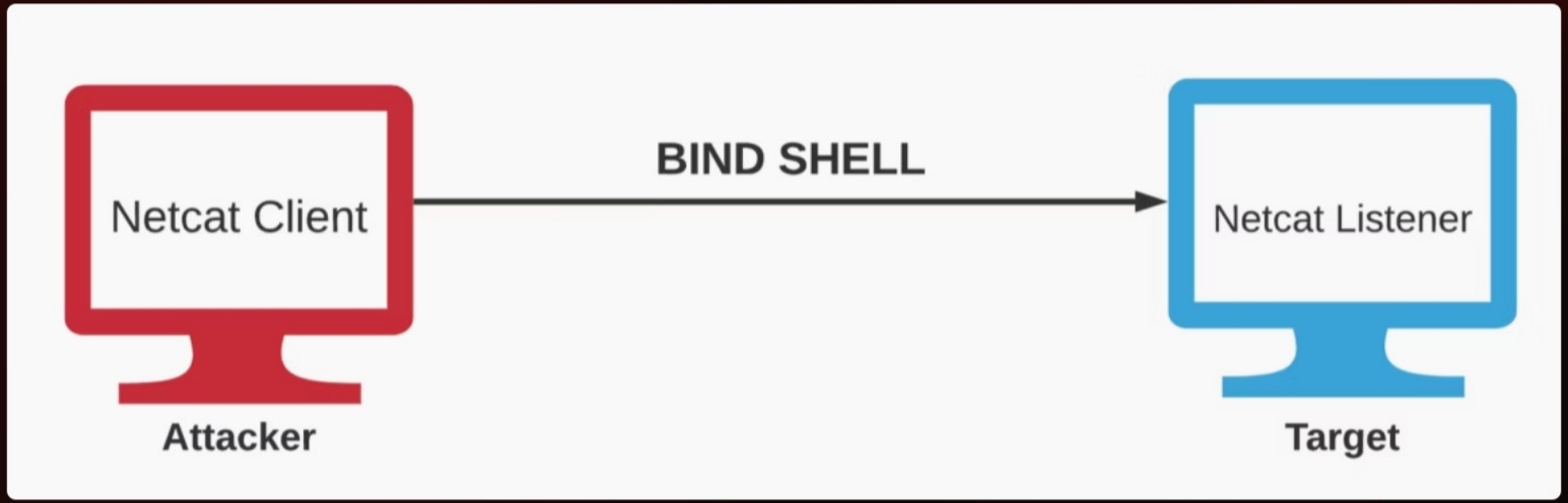
Attack Flow

A bind shell creates a listener on the target system that executes commands when the attacker connects.

Key characteristic: Attacker initiates the connection directly to the compromised target.

The listener can execute cmd.exe or /bin/bash upon connection.

Bind Shells Explained



Reverse Shells Explained

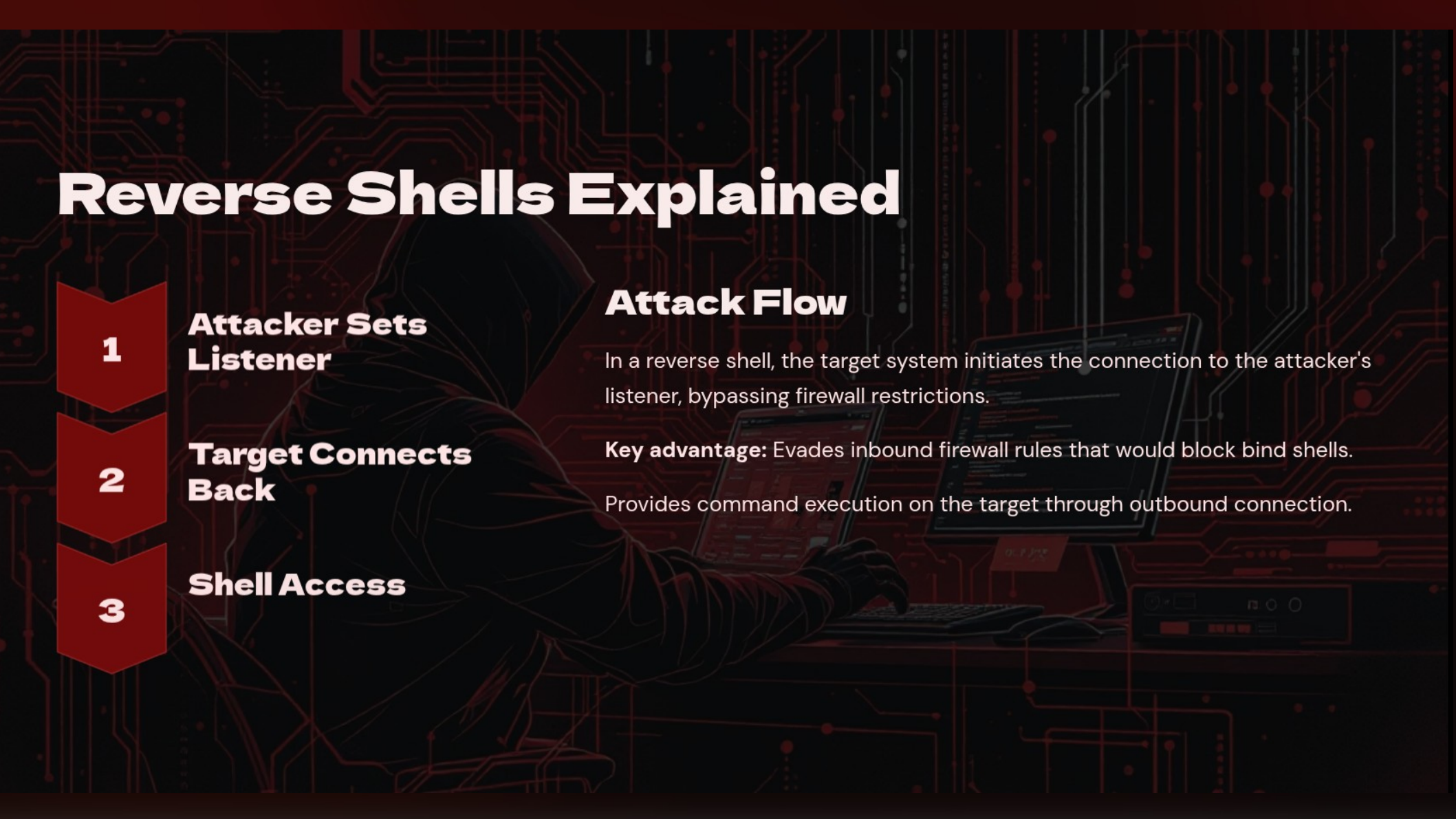
1. **Attacker Sets Listener**
2. **Target Connects Back**
3. **Shell Access**

Attack Flow

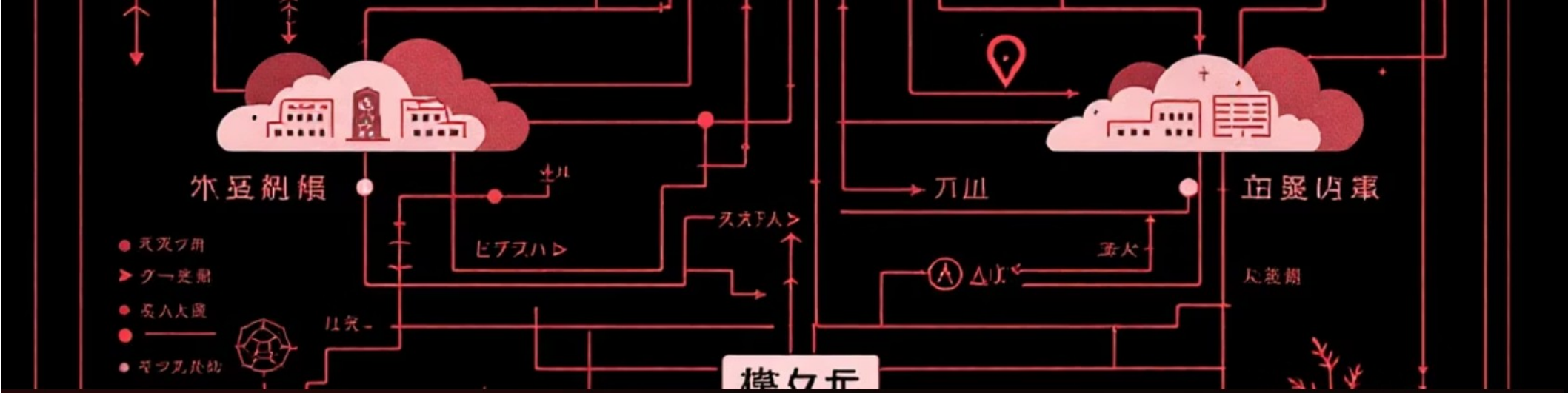
In a reverse shell, the target system initiates the connection to the attacker's listener, bypassing firewall restrictions.

Key advantage: Evades inbound firewall rules that would block bind shells.

Provides command execution on the target through outbound connection.



Reverse shell



Bind vs Reverse Shells

Bind Shell

- Target listens on port
- Attacker connects inbound
- Blocked by firewalls
- Simpler to setup

Reverse Shell

- Attacker listens on port
- Target connects outbound
- Bypasses most firewalls
- Preferred in real engagements

Whats a SMB ?

Server Message Block (SMB) is a client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.

- **Port 139 (NetBIOS):** Older session layer protocol running over TCP/IP.
- **Port 445 (Direct TCP):** Modern SMB running directly over TCP, without NetBIOS.
- **Critical Target:** Often misconfigured, offering rich information (users, shares) or critical vulnerabilities (EternalBlue).

Discovery: Nbtscan & Enum4linux

Mapping the Attack Surface

- **nbtscan:** A command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network.
  `nbtscan -r 192.168.1.0/24`
- **enum4linux:** A PERL script wrapper around Samba tools. It aggressively extracts information like:
  - Usernames & Group membership
  - Share lists & Password policies
  - OS Information

Interaction: Smbclient & Smbmap

Accessing Shares

- **smbclient:** Works like an FTP client. Allows you to list shares and transfer files.
  `smbclient -L //10.10.10.5`
  `smbclient //10.10.10.5/backup`
- **smbmap:** A Python tool that visualizes share permissions across the domain. It quickly identifies what you can read or write.
  `smbmap -H 10.10.10.5`
  Key: Look for "READ/WRITE" permissions on non-standard shares.

Interaction: Smbclient & Smbmap

Accessing Shares

```
┌──(root㉿ abhishekmorla)-[/media/…/hackthebox/oscp/pg/Resourced]
└─# smbmap -u V.Ventz -p 'HotelCalifornia194!' -H 192.168.246.175

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.246.175:445     Name: 192.168.246.175           Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        Password Audit                                          READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share

┌──(root㉿ abhishekmorla)-[/media/…/hackthebox/oscp/pg/Resourced]
└─# smbclient \\\\192.168.246.175\\Password\ Audit -U "resourced.local\V.Ventz"
Password for [RESOURCED.LOCAL\V.Ventz]:
Try "help" to get a list of possible commands.
smb: \>
```

SMB enum with Nmap Scripts

Nmap offers powerful scripts to automate SMB discovery and vulnerability detection.

- `--script smb-os-discovery`: Determines the OS, computer name, domain, and workgroup.
- `--script smb-enum-shares`: Lists available shares and their current access levels.
- `--script smb-vuln*`: Checks for known critical vulnerabilities like MS17-010 (EternalBlue) without exploiting them.

```
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse MACHINE_IP
```

FTP & Traffic Analysis

FTP Exploitation

Test for anonymous login, brute force credentials, and exploit vulnerable FTP versions for initial access.

Wireshark Analysis

Capture and analyze network traffic to identify cleartext credentials, unencrypted protocols, and suspicious activity.

```
Port filtering: tcp.port == 443
ip.addr == 192.168.0.1
ip.addr != 192.168.0.1
```

Introduction to Msfconsole

The Metasploit Framework

The Metasploit Framework (MSF) is an open-source, robust penetration testing and exploitation framework that is used by penetration testers and security researchers worldwide.

It provides penetration testers with a robust infrastructure required to automate every stage of the penetration testing life cycle.

The Metasploit Framework

Essential Terminology

- Auxiliary - Scanners and fuzzers that don't deliver payloads.
- Exploit – Code that uses a vulnerability to compromise a target..
- Payload – Piece of code delivered to the target system by an exploit with the objective of executing arbitrary commands or providing remote access to an attacker.
- Listener – A utility that listens for an incoming connection from a target.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search
```

```
       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2489 exploits - 1281 auxiliary - 393 post        ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```