GitHub - brav0hax/smbexec

By brav0hax

Archived: 2026-04-05 22:53:27 UTC

Folders and files

Name	Name	Last commit message	Last commit date
Latest commit Removed source code compilation as part of install, updated yml to pt… Jun 22, 2015 a54fc14 · Jun 22, 2015 **History** 59 Commits			
certs	certs	Moving smbexec back to where it belongs	Jun 19, 2015
lib	lib	Removed source code compilation as part of install, updated yml to pt…	Jun 22, 2015
patches	patches	Moving smbexec back to where it belongs	Jun 19, 2015
powershell	powershell	Moving smbexec back to where it belongs	Jun 19, 2015

Name	Name	Last commit message	Last commit date
progs	progs	Moving smbexec back to where it belongs	Jun 19, 2015
sources	sources	Moving smbexec back to where it belongs	Jun 19, 2015
Gemfile	Gemfile	Moving smbexec back to where it belongs	Jun 19, 2015
Gemfile.lock	Gemfile.lock	Removed source code compilation as part of install, updated yml to pt…	Jun 22, 2015
README	README	Update README	Jun 19, 2015
TODO	TODO	Moving smbexec back to where it belongs	Jun 19, 2015
WCE-LICENSE.txt	WCE-LICENSE.txt	updated wce to univ binary	Jul 15, 2013
WCE-README	WCE-README	updated wce to univ binary	Jul 15, 2013
about.txt	about.txt	Moving smbexec back to where it belongs	Jun 19, 2015
install.sh	install.sh	Removed source code compilation as part of install, updated yml to pt…	Jun 22, 2015

Name	Name	Last commit message	Last commit date
smbexec.rb	smbexec.rb	Moving smbexec back to where it belongs	Jun 19, 2015
smbexec.yml	smbexec.yml	Removed source code compilation as part of install, updated yml to pt…	Jun 22, 2015

- README
- License

```
************************************************************
                         smbexec
        A rapid psexec style attack with samba tools
     Original Concept and Script by Brav0Hax & PureHate
   Ported to ruby and modified by Smilingraccoon and Zeknox
                  Codename - Machiavellian
************************************************************

Written because we got sick of Metasploit PSExec getting popped

Special thanks to Carnal0wnage who's blog inspired us to go this route.
http://carnal0wnage.attackresearch.com/2012/01/psexec-fail-upload-and-exec-instead.html

v2.0 - 10/17/2013
UPDATED - Rubified ;)

v1.2.9.1 - 07/31/2013
ADDED - r3dy (pentestgeek.com) created a custom cachedump.rb that is a standalone tool to extract dc

v1.2.9 - 07/15/2013
UPDATED - wce has been updated with a universal binary with new version released by the developer (v
FIXED - on occasion when a Ctrl-C is inititated, if the smbexec proj folder is empty it will delete
FIXED - Typo in the f_dsusers function for sys file path

Windows Credentials Editor v1.41beta
(c) 2010, 2011, 2012, 2013 Amplia Security, Hernan Ochoa
written by: hernan@ampliasecurity.com
http://www.ampliasecurity.com
```

```
v1.2.8.1 - 06/24/2013
UPDATED - Added 'make' install check since libesedb and nmap rely on it for compile
UPDATED - DA/EA checker still not working as I wanted, ugly grep hacks to make it perform better.

v1.2.8 - 05/22/2013
ADDED - If you have crypter.exe installed on your system it will encrypt your payload after obfuscat
ADDED - Will prompt you if you'd like to execute payload as user or SYSTEM
ADDED - Option to gain a command shell from a remote system without a payload
FIXED - DA check gives system error 5 "Access Denied" changed it to complete the tasks as SYSTEM -> 
UPDATED - Fix payload creation issues, triggered DEP when combined with crypter.exe option. Thx to H

v1.2.7 - 04/01/2013
FIXED - False positives from Admin check option
FIXED - Domain cached creds logic I brok in last release
UPDATED - The whole look and feel is less gaudy and borrow heavily from msfconsole

v1.2.6 - 02/25/2013
ADDED - wce.exe for 64 Bit systems
FIXED - DA/EA checker did not check for any errors and would falsely state users were on the system 
FIXED - Option to just create payload and RC file would continue by launching attack. Now operating 
UPDATE - Now checks the target systems processor architecture in order to use the proper wce.exe (wc
UPDATE - dcc hash file & cleartext password file is only moved into logfolder if not empty (common e
UPDATE - source code for samba is now v3.6.12 for compiling smbexeclient binary
UPDATE - Installer now installs nmap verision 6.25 (Only if nmap is not found on the system. It does

v1.2.5 - 02/19/2013
FIXED - Issues with proper mingw identification, especially for 64 Bit systems - Bug reported by Jim
UPDATE - Installer was updated with extra prereqs for winexe compilation.
TESTING - Install and execution of smbexec was tested again on Ubuntu 12.04 and Fedora 17 64Bit syst

v1.2.4 - 02/04/2013
UPDATE - Added UAC functionality. Now you can check systems to see if they have UAC enabled. In addi

v1.2.3 - 01/20/2013
UPDATE - Changed menu layout, was getting crowded on the main page. Combined like tasks.
FIXED - Hash folder creation wasn't checking for existing folder before trying to create. Resulted i

v1.2.2 - 01/17/2013
UPDATE - Check credentials for remote login capabilities
UPDATE - Checks systems for DA/EA users logged in or running processes
UPDATE - If wce.exe is place in the smbexec/progs/ directory it will upload and execute on the targe

NOTE: The wce.exe file that exists in the progs directory has been obfuscated and is included in smb
Hernan retains all rights to the Windows Credential Editor and can ask to have the program removed f

Windows Credentials Editor v1.3beta
```

```
(c) 2010, 2011, 2012 Amplia Security, Hernan Ochoa
written by: hernan@ampliasecurity.com
http://www.ampliasecurity.com

v1.2.0 - 11/30/2012
FIXED - Script now checks to ensure exe's are compiled before running. Alerts user to use installer
UPDATE - Added drive and path variables to ntds hash grab function. (No longer hardcoded to C:\Windo
UPDATE - Checks for available diskspace before copying ntds.dit and sys files to the path provided
UPDATE - Deletes the volume shadow copy created by the ntds hash grab function

v1.1.1 - 11/11/2012
FIXED - Sometimes the IP validation fails even though it is a proper IP address
UPDATE - Installer updated with Samba-3.6.9 source
UPDATE - libesedb project moved to Google Code, installer updated with proper path

Includes
- smbexec.sh
- installer.sh
- patches to compile binaries
- source for samba-3.6.9 and winexe-1.00

Just run the installer and you should be good to go! If not email me... jbrav.hax@gmail.com

Credit where credit is due:
* b00stfr3ak - For multiple pull requests and code contributions
* Pasv - For the kick ass updates to the file finder module
* wce.exe - Hernan Ochoa - An incredible tool that mimikatz CANNOT touch! - http://www.ampliasecurit
* smbclient & winexe Hash Passing patch - JoMo-kun -> http://www.foofus.net/~jmk/passhash.html
        - Patch updated for Samba 3.6.12 by exfil (Emilio Escobar)
* vanish.sh - Original concept Astr0baby stable version edits Vanish3r -> http://www.securitylabs.in
* www.samba.org
* winexe - ahajda -> http://sourceforge.net/users/ahajda
* Metasploit - www.metasploit.com (Thank you HD and team!)
* Nmap - nmap.org (Thank you Fydor!)
* Creddump - Brendan Dolan-Gavitt - http://code.google.com/p/creddump/
* NTDSXtract - Csaba Barta - http://www.ntdsxtract.com/
* libesedb - Joachim Metz - http://libesedb.googlecode.com/

Happy Hunting!
```

Source: https://github.com/brav0hax/smbexec