



Getting the goods with smbexec

Eric Milam – Brav0hax

Don't you know who I am?

- Attack & Pen -> Accuvant LABS
- Open Source Projects -> easy-creds, smbexec, ettercap, Kali Linux



DOUCHEBAGS

Meet your god



What's this all about?

What is smbexec?

What does it do?

Why should I care?

- There's nothing 0 day here! BOO!
- Yes, but automation is awesome!
- You can use this tool immediately
- It will make post-exploitation much easier



What is smbexec?

- Bash script, yes, a bash script...
 - 1 week of work, consuming a years worth of Mountain Dew
- Power of the tool lies in smbclient & winexe
 - smbclient to get/put files
 - winexe to execute



Why write smbexec?

- Standard msf payloads with psexec module kept getting popped by AV
 - Custom exes also popped because AV trigger is on injection (service protection)
 - Damn you trend micro, but thanks for the motivation
- Blog post from Carnal0wnage
 - Upload and execute your payload



What have you done for me lately?

I want my shells and I want them now!

- Creates an obfuscated payload that will bypass most commercial AV
 - Enable Hyperion Crypter to encrypt the payload
- Creates a Metasploit rc file and launches a Metasploit listener to make things “easy.”
 - Attack can be launched in xterm or screen



Going Native

What? You can get all this great stuff with winexe and native windows commands?



Move Along - Nothing to see here...

- winexe is similar to sysinternals psexec and the --system flag is awesome
- No “payload” necessary
- Looks like normal Windows traffic to OPSEC.
 - Successful logins and not much else



Master and Commander

Execute commands as SYSTEM, the possibilities are virtually limitless

- Dump hashes from workstations and servers
- Create a Volume Shadow Copy
- Run other tools (as SYSTEM)
- Disable or bypass UAC
- Check systems for DA/EA accounts logged in or running a process



smbexec – grab local & dcc hashes

- Dump hashes workstation/servers
- reg.exe save (HKLM SYS,SEC,SAM)
 - SYS+SAM=Local Hashes
 - SYS+SEC=Domain Cached Creds
- creddump converts to hashes in John format for you



smbexec – clear text passwords

WCE FTW!

- Incorporated into smbexec with permission from the owner
- wce.exe and the -w flag
- Runs automagically as part of the hash grab functionality



smbexec – automated VSC

- Creates a Volume Shadow Copy, grabs the SYS reg key and get the hashes from ntds.dit
- Fully automated to grab all the goods and cleans up after you
- NTDSXtract & libesedb runs automatically if grabbing the NTDS.dit and SYS key is successful
- ntds.output file converted into a list of hashes in John format
- Tab separated cred list created for other functionality



smbexec hashgrab demo



CEILING CAT

IS WATCHING YOU MASTURBATE



The caveats...there's always something

You need a credential with admin rights for the system (local or domain)

- administrator:password can usually get you started in 9 out of 10 corporate networks
- NBNS spoofing
- ettercap
- Of course there's always MS08-067 ;-)



When they're blue teaming...

- winexe creates a service, could be stopped or become a red flag
- Sometimes AV doesn't like wce
 - wce included with smbexec has been obfuscated with the approval of the original developer
- Authentication over port 139 or 445 is required
- Locard's exchange principle "Every contact leaves a trace"



Where can I get smbexec?

Sourceforge or GitHub

Metasploit Modules

- Royce Davis (@r3dy__) from pentestgeek.com
 - psexec_command
 - ntds_grab

Impacket

- Developed in python based on the work by Royce

smbexec v2.0

- Ruby port
- Brandon McCann (@zeknox) and Thomas McCarthy (smilingraccoon) from pentestgeek.com



Credit where it's due!

- wce.exe - Hernan Ochoa Amplia Security
- smbclient & winexe Hash Passing patch JoMokun, Emilio Escobar, Skip Duckwall
- vanish.sh Original concept Astr0baby edits by Vanish3r and Hostess
- Samba Team
- winexe - ahajda & Thomas Hood
- Metasploit Team
- Nmap Team
- Creddump - Brendan Dolan-Gavitt
- NTDSXtract - Csaba Barta
- libesedb - Joachim Metz
- Bernardo Damele's Blog posts



Questions

- Twitter -> @Brav0Hax
- IRC -> J0hnnnyBrav0



ACCUVANT
LABS

