
ALCORN
GROUP


ALCORN
GROUP

The Count's {A..Z} of Windows Privilege Escalation

Lukasz Gogolkiewicz

A

About

Lukasz Gogolkiewicz

- Managing Consultant

Aaaah What we Talking About?

Alphabet

- Each Letter Has a Technique

Windows Environment

- Kiosk
- Locked Down Environments
- Zero/Thin Clients
- Published Desktops
- Low -> High Priv

A

Autorun(s)

Sysinternals

- Autoruns / Autorunsc
- A Utility to view which services are configured to start on boot

https://technet.microsoft.com/en-au/sysinternals/bb963902.aspx

B

Binary Replacement/Planting

Classic!

- Still Works.

Replace a Binary that…

- Starts as a service
- Starts as a privileged process
- Called by a privileged process?

Example?

- C:\Windows\System32\sethc.exe

C

Configuration Files

Another Classic

- Like its 1999!

Look locally at files

- Unattend.[txt|xml|ini]
- Vnc.ini
- Web.Config (password resuse?)
- VSFtpd Config
- SNMP Config?
  - Write Strings
  - Other Devices?
- Scripts
  - BobAutoAdd.ps1

D

DLL Attacks

DLL Injection

- Requires Privileges

DLL Redirection

- Needs Write Access

DLL Hijacking / Search Path

- Winner Winner, Chicken Dinner

DLL Attacks

Search Order

- The directory from which the application is loaded
- C:\Windows\System32
- C:\Windows\System
- C:\Windows
- The current working directory
- Directories in the system PATH environment variable
- Directories in the user PATH environment variable

https://pentestlab.blog/2017/03/27/dll-hijacking/

E

Exploits

Out of Date Software

- Known Exploits
  - Sophail
  - McAfee

Misconfigurations

- Love you Tomcat!
- Love you more Jenkins!

F

File Permissions

Classic

- Love you Windows!

Check Permissions of Files and Folders

- Configuration Files?
- “New Folder” outside system directories
- Replace a binary?
- Startup Folder for All Users…
  - The Admin logs onto this system right?

G

Group Policy

Exploit GPUpdate in Transit

- MS15-011 and MS15-014

Configuration Issues with Group Policy

- Applocker
  - *PS C:\> Get-AppLockerPolicy*

Get Group Policty and Review (GPResult / RSOP)

- Configuration issues?
- Have a look at what is locked down tight…might be something interesting

H

Hot Potato

The Chaining is Real

- Exhaust UDP ports so DNS lookup fails
- Local NetBIOS Name Service (NBNS) Spoof
- Fake WPAD Proxy Server to Control Proxy
- Windows / Defender Update
- HTTP → SMB NTLM relay
- Update redirects and points locally, proxy relays creds locally with ‘New System’ service and ‘User-Defined’ Command

Stephen Breen @breenmachine
http://foxglovesecurity.com/2016/01/16/hot-potato/

Images

Virtual Image Backups / Storage

- VMDK
- VHD / VHDX
- OVA
- ISO
- .IMG

J

Jump on the Web

Google Everything You See

- Source code of applications running

Configuration Settings / Manuals

- Default passwords for installed applications
- Default configuration file locations

K

Kerberos

Abuse the Kerberos

- KRBTGT Hash
- Domain SID
- Domain Name

Passing All The Things

- Pass-the-Hash
- Pass-the-Ticket
- Kerberoasting

Skip DuckWall & Benjamin Delpy
https://www.blackhat.com/docs/us-14/materials/us-14-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It-wp.pdf

L

Logs Files

Web Servers

- Session Tokens
- Usernames and Passwords
  - Credential Reuse?
  - Access to Application Functionality?
- Apache Local File Include Shell Exec?

SQL Server

- Connection Strings
- SQL Transactions

Custom Applications

- Usernames and Passwords?
- Calling Other Binaries We Controls?

M

Memory Access

System Memory Access via Physical Access?

- Firewire
- Thunderbolt
- ExpressCard
- PC Card
- PCI/PCIe Interfaces

Inception

- Extract First 4 Jigabytes of Memory

N

Network Shares

Stuff Stored on Network Shares?

- Backups (Images)
- Scripts
- Shortcuts (Hidden Shares)
- “Encrypted” Admin Password in SysVol
- Application Installers
  - Increase Attack Surface
- Users Sharing Local Drives with ‘inetpub’ Having Write Access?

O

Other Users

Shared Computing Environment

- Citrix
- VMWare
- VDI / Remote Desktop Services
- Internet Kiosks

P

Piss Poor Passwords Prevent Persistence Plus Pwnage

Default Passwords

- Have A Look At Documentation for Systems

Poor Passwords

- Password1
- Welcome1
- Password@123
- toor
- admin / admin
- <client name>1

PXE Boot

Pre-boot Execution Environment

- Boot Images off Network Shares

Do You Have Network Access?

- Try to PXE boot an Image into a Virtual Machine
- Run Physical Access Checks

Q

QR Codes

Have Access to a Kiosk?

- Try It At Check-in After the Con

Scanning QR Codes

- *Business Class' OR 1=1--*
- *Pilot' OR 1=1--*

Other Attacks?

- Probably Not Sanitising Input
  - Command Injection?

http://goo.gl/Zi7en0 - Using QR Codes as Attack Vector

QR Codes

Gavin Millard @gmillard · 11h

MS14-068 in the real world.

"Welcome Captain. Would you like a coffee before you take off"

#infosec

31 12

QR Codes

Have Access to a Kiosk?

- Try It At Check-in After the Con

Scanning QR Codes

- *Business Class' OR 1=1--*
- *Pilot' OR 1=1--*

Other Attacks?

- Probably Not Sanitising Input
  - Command Injection?

http://goo.gl/Zi7en0 - Using QR Codes as Attack Vector

R

Registry

Check These Keys

- Permissions
- RunAs
- RunOnce
- RenameOnReboot
- AlwaysInstallElevated
- SRP Policy Enumeration
- Application Installed

https://github.com/pentestmonkey/windows-privesc-check

S

Services

Hey…What Services Are Configured to Startup?

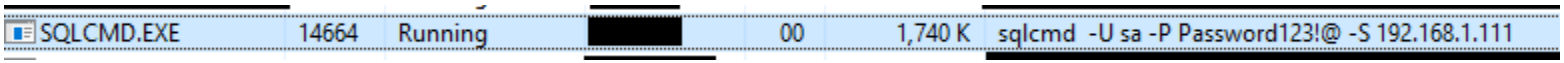
- Check How They Are Starting
- Where Are They Starting From?
- What Privileges Do They Have?
- Also…Do They Call Other Binaries or DLL's?

T

Task Manager / Task List

Have A Look At What is Running

- Web Servers
- SQL Servers
- Other Applications?



Task Manager / Task List

U

Unquoted Service Path

Classic

- Love you Windows!

Issue?

- Spaces Exist In Application Paths Without Being “Quoted”

Check?

- *wmic service get name,displayname,pathname,startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /i /v """*

https://www.gracefulsecurity.com/privesc-unquoted-service-path/

V

Volume Shadow Copy

Sorry

- Required Elevated Privileges

What Can You Get?

- Any Locked Windows File
  - SAM
  - SYSTEM
  - SECURITY
  - NTDS.dit
  - Database Files

How?

- C:\> vssadmin list shadows
- C:\> vssadmin create shadow /For=C:

W

Wireless LAN Passwords

Really??

- Interesting Vector

Kiosk in Airport or Internet Café?

- Grab the WiFi Password
- Connect to WiFi
- Attack Other Kiosks

How??

- *C:\ netsh wlan export profile key=clear*

Wsuspect

Bonus Round

- Another Really Good Attack

Man-in-the-Middle Windows Updates

- Install Drivers via Windows Update

I Want to Know More!

- *https://www.blackhat.com/docs/us-15/materials/us-15-Stone-WSUSpect-Compromising-Windows-Enterprise-Via-Windows-Update.pdf*

X

eXtract NTDS

Please Create More Techniques with X

- Hard to Find Exploit/Technique with X

Have Physical Access?

- Volume Shadow Copy
- PXE Boot

Get Backup of Domain Controller

- Crack Hashes?
- Pass-the-Hash?

Y

YoloMacro!

Sorry…again

- Couldn’t Find One For ‘Y’

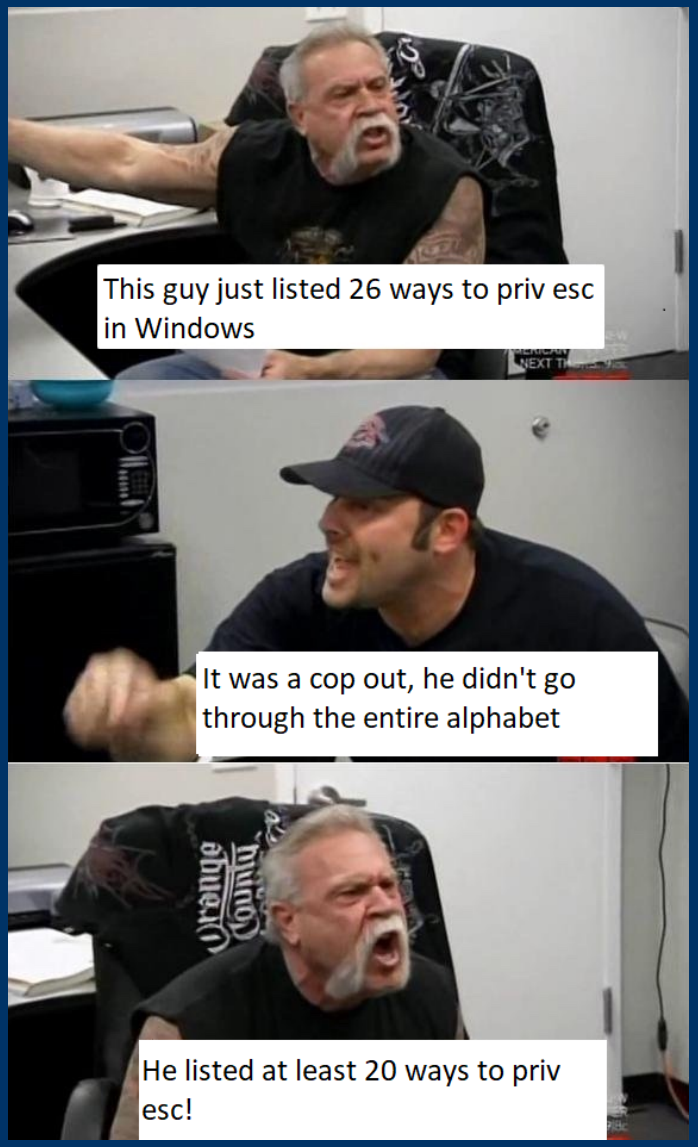
Drop That 0Day

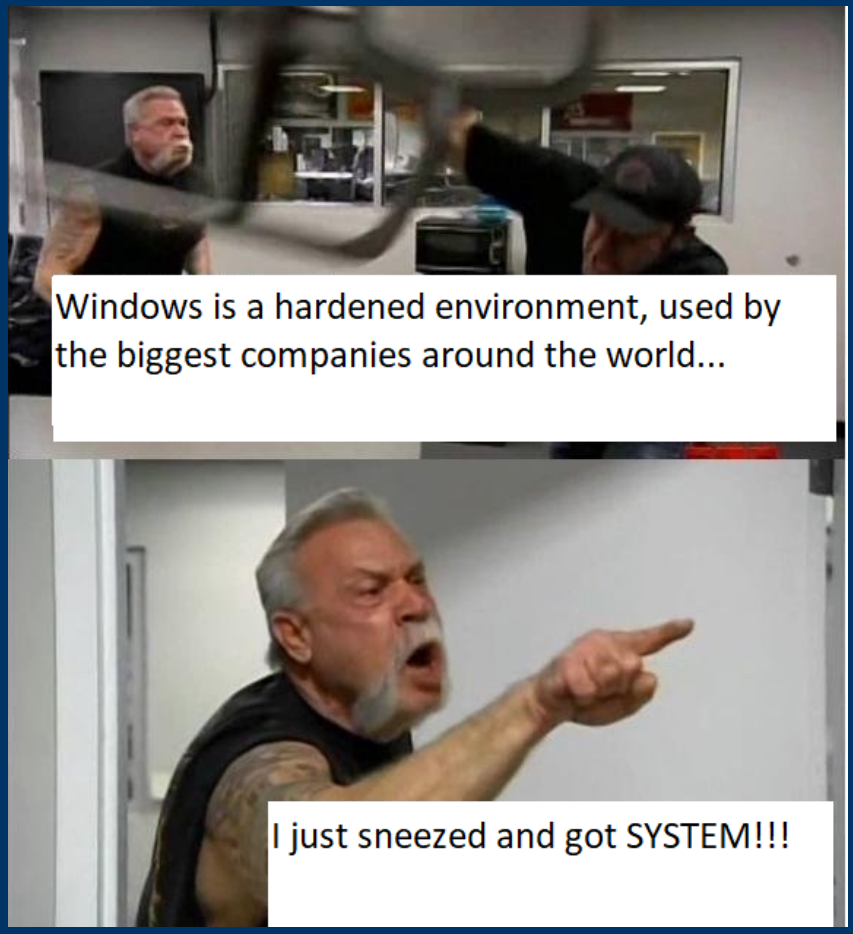
- Loading Template on Share
- Word Broadcasts Share Location
- MiTM / ARP Spoof / DNS Poison / Responder
- Host Template with Macro
- Victim Runs ‘Trusted’ Macro-Enabled Template

Z

Ze End!


THIS IS THE END OF THE PRESENTATION
CLAP NOW
memegenerator.net


This guy just listed 26 ways to priv esc in Windows
It was a cop out, he didn't go through the entire alphabet
He listed at least 20 ways to priv esc!


Windows is a hardened environment, used by the biggest companies around the world...
I just sneezed and got SYSTEM!!!

Resources?

Presentations Better Than Mine

- Brett Moore - Encyclopaedia of Windows Escalation

Blogs Way Better Than Mine

- Carnal0wnage
- Pentest Monkey
- Google Project Zero
- Spectre Ops
- adsecurity

Twitter Feeds Better Than Mine

- @TuskCon
- @subTee
- @harmj0y
- @GentilKiwi
- @tiraniddo
- @mikeloss

See You All @ TuskCon 2018!

Lukasz Gogolkiewicz
@SyNick
Synick on BSides
https://blog.pentester.com.au