

Got SYSTEM ?



Ruben Boonen

ruben.boonen@contextis.co.uk

@FuzzySec

<http://www.fuzzysecurity.com/>

Francesco Mifsud

francesco.mifsud@contextis.co.uk

@GradiusX

Disclaimer!

90-day trial Windows 7 32-bit
[Modern IE Virtual Machine]

Your money is no good here!

Virtual Machine was not modified
before distribution!



Why are we here?

85% of home and corporate network
infrastructure is Windows based

Bob is ok, but
SYSTEM is better

Forget about UNIX,
priv esc on Windows is **awesome!**



We are in it
for the sh3llzz!

Agenda



A lot to cover in 2h.
Don't worry we are
friendly.
Ask questions!

+ Enumeration

[who, what, how?]

+ Security Fail!

[configuration weak sauce, patches,
unattended installs]

+ Permissions

[services, scheduled tasks,
files/folders, group policy]

= Enumeration =

Collect all the things

+ whoami? What groups do I belong to?

+ What is this place?

[version, architecture, drives, network access, patchlevel]

+ What does this place do?

[software, startup, tasks, services, registry]

The more info we have the better our chances at getting SYSTEM!



whoami

“Whoami” or
“echo %username%”

net user USERNAME
(Remember to check group
membership!)

net users

whereami

```
systeminfo  
| findstr /B /C:"OS Name"  
/C:"OS Version "
```

```
driverquery
```

```
ipconfig /all
```

```
route print
```

Patches: Systeminfo (Warning!)

```
"wmic qfe get Caption,Description,HotFixID,InstalledOn"
```

SYMPTOMS

When using SystemInfo.exe in Windows Server 2003 to display a list of installed hotfixes, some hotfixes may not be listed if over 200 are installed.

whatami

```
schtasks /query /fo LIST /v
```

```
wmic batch script
```


= Security Fail! =

+ Configuration Weak Sauce

[passwords in files/registry, GPP Cached Passwords]

+ Patches

[Missing patches -> Pwnd!]

+ Unattended Installs

[unattend.xml & sysprep.xml]



Configuration Weak Sauce

```
dir /s *pass* == *cred* == *vnc* == *.config*
```

```
findstr /si password *.xml *.ini *.txt
```

```
reg query HKLM(HKCU) /f password /t REG_SZ /s
```

```
GPP Cached Passwords (Powersploit/Metasploit)
```



Patches

- All patches to date

Microsoft Bulletin: <https://www.microsoft.com/en-us/download/details.aspx?id=36982>

- Currently Installed Patches

```
wmic qfe get HotFixID
```

- Cross-Reference

Powershell Script



```
c:\sysprep.xml
```

```
c:\sysprep\sysprep.xml
```

Unattended Installs

```
%WINDIR%\Panther\Unattend\Unattend.xml
```

```
%WINDIR%\Panther\Unattend.xml
```

Check entire OS!

= Permissions =

+ Services

[unquoted service paths, folder permissions, service permissions]

+ Scheduled Task

[configuration fubar!]

+ AlwaysInstallElevated

[Eurmm ... WTF?!]

+ 303 Name Not Found

[Procmon -> Pwnd!]



Services \ **Unquoted** Service Paths

Searching for Unquoted Service Paths

Service Binpath

C:\BSides Exercises\Vuln Folder 1\anything.exe
C:\BSides Exercises\Vuln Folder 1\anything.exe
C:\BSides Exercises\Vuln Folder 1\anything.exe
C:\BSides Exercises\Vuln Folder 1\anything.exe

cmd

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

Powershell

```
gwmi win32_service | ?{$_.} | where {($_.pathname -ne $null) -and  
($_.pathname.trim() -ne "")} | where {-not  
$_.pathname.StartsWith("")} | where {($_.pathname.Substring(0,  
$_.pathname.IndexOf(".exe") + 4)) -match ".\."}
```



Services \ Weak Folder Permissions

- Checking Folder Permissions

- |_ accesschk.exe -dqv C:\Some\Path

- |_ accesschk.exe -uwdqs UserGroup c:\



Services \\ Weak **Service** Permissions

- Checking Service Permissions

 - |_ accesschk.exe -ucqv ServiceName

 - |_ accesschk.exe -ucvq * <Any_Service>

- Check Service Write Access

 - |_ accesschk.exe -uwcqv UserGroup *





Scheduled Tasks

- Output for all tasks

```
|_ schtasks /query /fo LIST /v > tasks.txt
```

- Specific task

```
|_ schtasks /query /fo LIST /v /tn TaskName
```



AlwaysInstallElevated

- Group Policy Setting that allows any *.msi to install with elevated privilege
- Why is this even an option?
- Attack: Compile payload as *.msi
- Profit!



303 Name Not Found

- A large number of applications/services load non-existent resources
- The file search order includes folders in the system path
|_ echo %path%
- Write access to a folder in the system path -> Game Over!

= Resources & Special Thanks =

+ Encyclopaedia Of Windows Privilege Escalation (Brett Moore)

|_ <http://www.youtube.com/watch?v=kMG8IsCohHA>

|_ <https://www.insomniasec.com/downloads/publications/WindowsPrivEsc.ppt>

+ Windows Attacks: AT is the new black (Chris Gates & Rob Fuller)

|_ http://www.youtube.com/watch?v=_8xJaaQlpBo

+ Elevating privileges by exploiting weak folder permissions (Parvez Anwar)

|_ <http://www.greyhathacker.net/?p=738>

+ CIS Build Review Benchmarks

|_ <https://benchmarks.cisecurity.org/downloads/multiform/index.cfm>

+ Windows Privilege Escalation Fundamentals (Ruben Boonen)

|_ <http://www.fuzzysecurity.com/tutorials/16.html>





Questions ?

Contact Us:

ruben.boonen@contextis.co.uk
@FuzzySec

francesco.mifsud@contextis.co.uk
@GradiusX