Got Shell
Got System

context

Ruben

ruben.boonen@contextis.co.uk
Twitter: @FuzzySec
http://www.fuzzysecurity.com/

Francesco

francesco.mifsud@contextis.co.uk
Twitter: @GradiusX
http://vulnerable.space/

#DisclamiER!

90-day trial Windows 10 64-bit

Modern IE Virtual Machine

Your money is no good here !

Virtual Machine was not modified before distribution!

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

Got Shell

+ Desktop Lockdown

+ Kiosk's (/ Citrix)

+ AppLocker

[A lot to cover in 4h. Don't worry we are friendly, ask questions!]

Got SYSTEM

+ Enumeration
who, what, how?

+ Security Fail!
configuration weak sauce,
patches, unattended installs

+ Permissions
services, scheduled tasks,
files/folders, group policy

got ShELL...

Desktop Lockdown

- Lockdown policies
- Getting an explorer window (..somehow)
- Bypass folder/type restrictions
- Native shells / custom shells

Lockdown Policies

- Can be set using Group Policy or the registry!

- Group policy registry reference:

  _ https://msdn.microsoft.com/en-us/library/ms815238.aspx

- Keep an eye out for failure!

  _ DisableCMD => 0x00000002 (Disable CMD but allow batch?!)

Getting an Explorer window

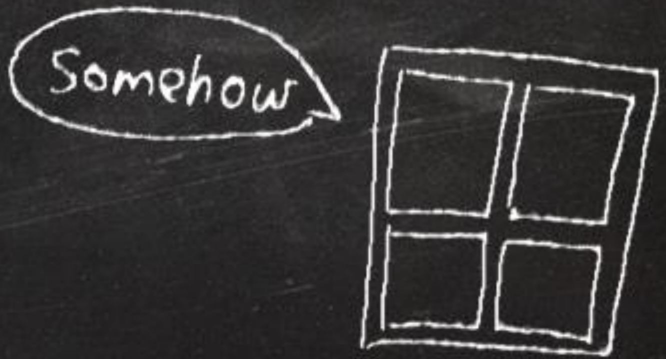
- Native application functionality!

  _ File -> Open
  _ Help menus
  _ print dialogs

- Shortcut keys!

  _ Shift*5
  _ Alt+F4
  _ Win+R
  _ Ctrl+Shift+Esc

**When in doubt,
click on
all the things!**



Bypass FoldER Restrictions

Alternate file paths

_ file:///C:/Windows/System32

_ \\127.0.0.1\C$\Windows\System32

Alternate location schortcuts

_ %WINDIR%, %SYSTEMDRIVE%, %USERPROFILE%

_ shell:System, shell:MyComputerFolder, shell:Personal

Bypass Type Restrictions

- Right-click open :D!
- Drag & Drop execution
- File Shortcuts

  _ create new / modify existing!

Native / Custom Shells

- Native shells

_ cmd, powershell, powershell_ise, FTP, command.com, rundll32

_ batch, vbs, ps1, macros

- A number of executables emulate windows functionality

_ Registry / Command prompt

Kiosk's (/Citrix)

Think lockdown + published application

Real OS under the hood

Apply the techniques we have seen so far!

Applocker

Successor to SRP

White-list Approach
_directory
_publisher
_user/group

Import/Export rules

Audit-only mode yaay!

Applocker Rules

Be wary of configuration failures!

Be wary of exceptions!

By default allows execution of anything in

_ %WINDIR%*

_ %PROGRAMFILES%*

subTEE has Applocker all figured out!

Find "Trusted things that execute things"!

_ rundll32 (yes, again)

_ InstallUtil

_ Regsvr32

Game Over?

got System

Enumeration

Collect all the things

whoami? What groups do I belong to?

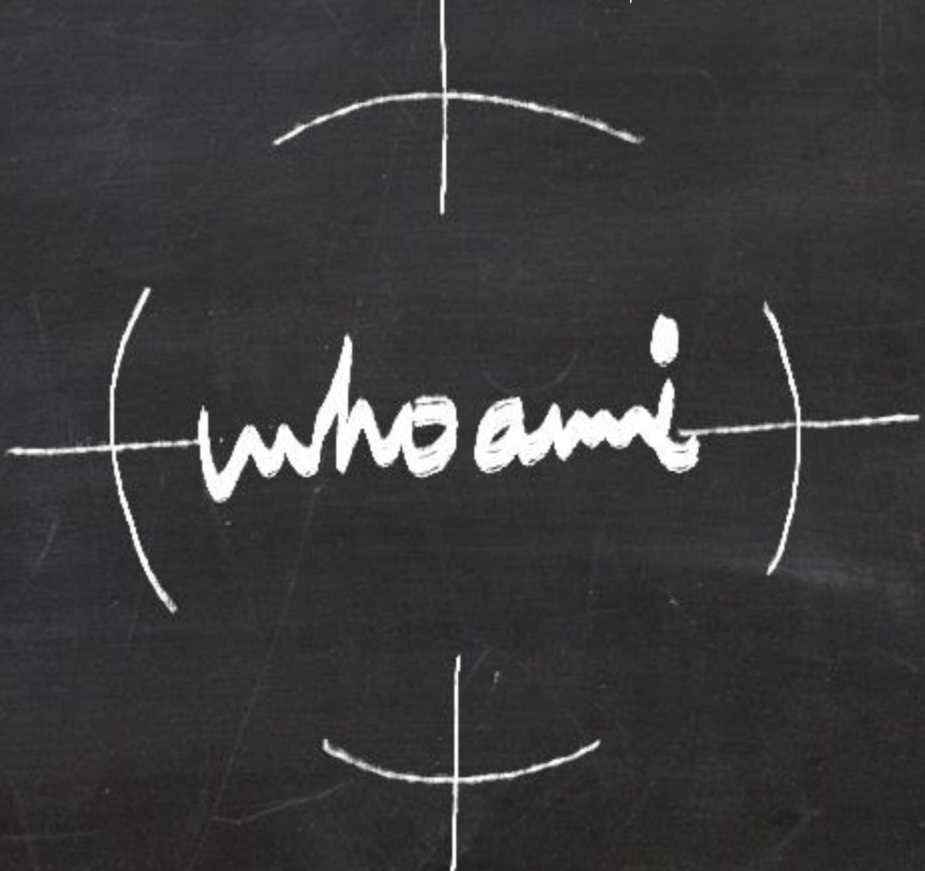
What is this place?
_ version, architecture, drives, network access, patchlevel

What does this place do?
_ software, startup, tasks, services, registry

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

“whoami” or “echo %username%”

net users

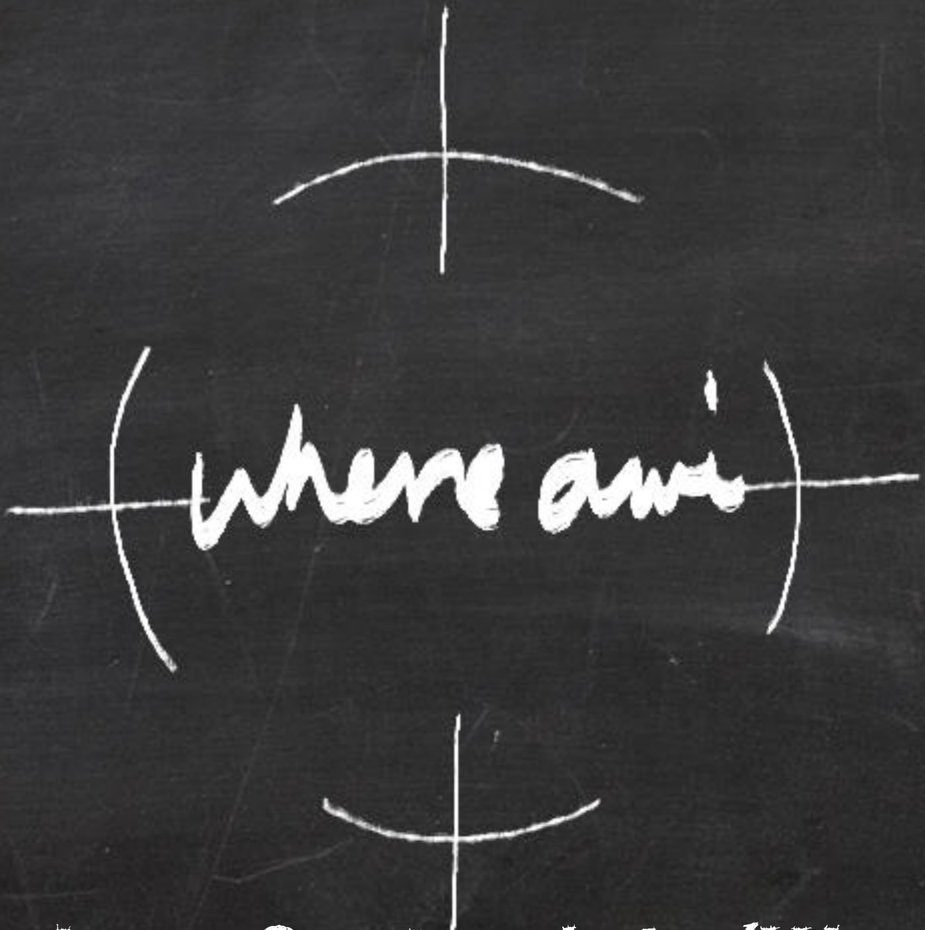


net user USERNAME

(Remember to check group membership!)

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

```
driverquery
ipconfig /all
route print
```



Patches: Systeminfo (Warning!)

```
_“wmic qfe get Caption,Description,HotFixID,InstalledOn”
```

schtasks /query /fo LIST /v

wmic batch script!

Configuration Weak Sauce

_ passwords in files/registry, GPP Cached Passwords

Patches

_ Missing patches -> Pwnd!

Unattended Installs

_ unattend.xml & sysprep.xml

Security Fail!

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)

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

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

Check entire OS!

unattended Installs

PERMISSIONS

Services
_ unquoted service paths,
folder permissions, service permissions

Scheduled Tasks
_ configuration fubar!

AlwaysInstallElevated
_ Eurmm ... WTF?!

303 Name Not Found
_ Procmon -> Pwnd!

Services_
unquoted Service Path

Service Binpath

- C:\Defcon\Vuln Folder 1\anything.exe
- C:\Defcon\Vuln Folder 1\anything.exe
- C:\Defcon\Vuln Folder 1\anything.exe

Searching for Unquoted Service Paths

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

cmd

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

Powershell

Services_ Weak Folder Permissions

Checking Folder Permissions

```
_ accesschk.exe -dqv C:\Some\Path
_ accesschk.exe -dvq UserGroup c:\
```

Services_ Weak Service Permissions

Checking Service Permissions

```
_ accesschk.exe -ucqv ServiceName
_ accesschk.exe -ucvq * <Any_Service>
```

Check Service Write Access

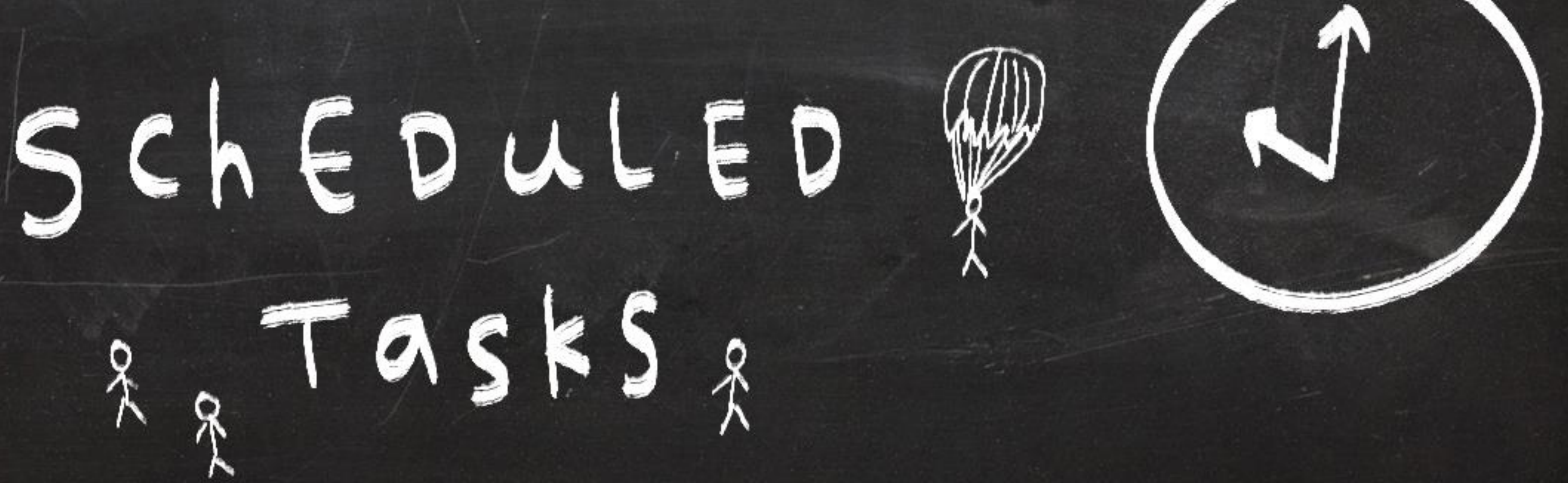
```
_ accesschk.exe -uwcqv UserGroup *
```

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

Oops! 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%

_ set

_ $Env:Path

Write access to a folder in the system path -> Game Over!

Reading Materials

(Resources & Special Thanks)

+ Read everything that SubTee writes!
 _ http://subt0x10.blogspot.com/

+ 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!

Context

Contact Us

+ ruben.boonen@contextis.co.uk _ @FuzzySec

+ francesco.mifsud@contextis.co.uk _ @GradiusX