



WINspect

Information Security Inc.

Contents

- About WINspect
- WINspect Features
- QuickTest standalone workstation (Windows 10 x64)
- QuickTest domain-joined workstation (Windows 10 x64)
- References

About WINspect

- WINspect is part of a larger project for auditing different areas of Windows environments
- It focuses on enumerating different parts of a Windows machine to identify security weaknesses and point to components that need further hardening
- The main targets for the current version are domain-joined windows machines. However, some of the functions still apply for standalone workstations
- Github > <https://github.com/A-mIn3/WINSpect>

WINspect features

- Checking for installed security products
- Enumerating world-exposed local filesystem shares
- Enumerating domain users and groups with local group membership
- Enumerating registry autoruns
- Enumerating local services that are configurable by Authenticated Users group members
- Enumerating local services for which corresponding binary is writable by Authenticated Users group members

WINspect features

- Enumerating non-system32 Windows Hosted Services and their associated DLLs
- Enumerating local services with unquoted path vulnerability
- Enumerating non-system scheduled tasks
- Checking for DLL hijackability
- Checking for User Account Control settings
- Checking for unattended installs leftovers

QuickTest standalone workstation

- Download and the script

The screenshot shows a GitHub repository page for 'A-min3/WINspect'. The repository is titled 'Powershell-based Windows Security Auditing Toolbox'. It has 19 commits, 1 branch, 0 releases, 1 contributor, and is licensed under GPL-2.0. The current branch is 'master'. A dropdown menu is open, showing a list of files and their latest commit messages:

File	Commit Message
LICENSE	Create LICENSE
README.md	Update README.md
WINspect.ps1	Update WINspect.ps1

On the right side of the dropdown menu, there are options to 'Clone with HTTPS', 'Open in Desktop', and 'Download ZIP'. The 'Download ZIP' button is highlighted with a red box.

QuickTest standalone workstation

- Run the script from powershell
- Make sure to have the Execution Policy configured to “Unrestricted”. Default settings is Undefined hence the script cannot be run
- Execution Policy status can be checked with the following command

```
PS C:\Users\User3\Music\WINSpect-master\WINSpect-master> Get-ExecutionPolicy -List
```

Scope	ExecutionPolicy
MachinePolicy	Undefined
UserPolicy	Undefined
Process	Undefined
CurrentUser	Unrestricted
LocalMachine	Undefined

QuickTest standalone workstation

- The Execution Policy can be modified using the following command

```
PS C:\Users\User3\Music\WINspect-master\WINspect-master> Set-ExecutionPolicy Undefined -Scope CurrentUser -Force
PS C:\Users\User3\Music\WINspect-master\WINspect-master> Get-ExecutionPolicy -List
```

Scope	ExecutionPolicy
MachinePolicy	Undefined
UserPolicy	Undefined
Process	Undefined
CurrentUser	Undefined
LocalMachine	Undefined

QuickTest standalone workstation

- Run the script

```
PS C:\Users\User3\Music\WINSpect-master\WINSpect-master> .\WINSpect.ps1
Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\User3\Music\WINSpect-master\WINSpect-master\WINSpect.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
```

- The script bails out when it couldn't find any domain as per below

```
Administrator: Windows PowerShell
Starting Audit at 9/11/2017 5:50:15 PM
-----
[?] Checking for administrative privileges ..
[?] Checking for Default PowerShell version ..
[+] ----> PowerShell v5
[?] Detecting system role ..
[-] This script needs access to the domain. It can only be run on a domain member machine.
Type any key to continue ... _
```

QuickTest domain-joined machine

- Run the script

```
Administrator: Windows PowerShell
Starting Audit at 9/11/2017 6:18:27 PM
-----
[?] Checking for administrative privileges ..
[?] Checking for Default PowerShell version ..
[+] -----> PowerShell v5
[?] Detecting system role ..
[+] -----> Member Workstation
[?] Checking if Windows Firewall is enabled ..
[?] Checking Firewall Profiles ..
[*] Standard Profile Firewall : Enabled.
[*] Public Profile Firewall : Enabled.
[*] Domain Profile Firewall : Disabled.
[?] Checking for third party Firewall products ..
[-] No other firewall installed.
[?] Checking for installed antivirus products ..
[+] Found 1 AntiVirus solutions.
[?] Checking for product configuration ..
[+] Product Name : Windows Defender.
[+] Service Type : .
[+] Real Time Protection : .
[+] Signature Definitions : Up-to-date.
```

- The script confirms that it's running with admin rights, checks PowerShell version, then inspects Windows Firewall settings

QuickTest domain-joined machine

```
Select Administrator: Windows PowerShell

[?] Checking for UAC configuration ..
    [+] UAC is enabled.
[?]Checking for UAC level ..
    [*] UAC Level : Notify only when apps try to make changes (secure desktop on).

[?] Checking registry keys for autoruns ..
    [*] HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ :
Executable Path
-----
VMware User Process C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmusr
SecurityHealth      C:\Program Files\Windows Defender\MSASCuIL.exe

    [*] HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ :
Executable Path
-----
OneDrive            C:\Users\User3\AppData\Local\Microsoft\OneDrive\OneDrive.exe /background
```

- WINSpect then confirmed that UAC was enabled, and that it should notify only when apps try to make changes, then checked the registry for autorun

QuickTest domain-joined machine

```
Administrator: Windows PowerShell

Q) Checking for configurable services...
Name          Path
-----
NetTcpPortSharing C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMsvchost.exe

Q) Checking for unquoted path services...
[-] Found no service with unquoted pathname.

Q) Checking hosted services (svchost.exe)...
[-] Found no user hosted services.

Q) Checking for DLL hijackability...
Q) Checking for safe DLL search mode...
[-] DLL Safe Search is enabled !
Q) Checking directories in PATH environment variable...
Directory          Writable
-----
C:\WINDOWS\system32 -- False
C:\WINDOWS         False
C:\WINDOWS\system32\wbem     False
C:\WINDOWS\System32\WindowsPowerShell\v1.0\  False

Q) Checking for unattended install leftovers...
[-] No unattended install files were found.

Q) Checking scheduled tasks...
TaskCommand       : C:\Users\User3\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
SecurityContext   : JOINEDDOMAIN\User3
TaskCommand       :
SecurityContext   : NT AUTHORITY\USER
TaskCommand       :
SecurityContext   : NT AUTHORITY\SYSTEM
TaskCommand       :
SecurityContext   : NT AUTHORITY\SYSTEM
TaskCommand       :
SecurityContext   : NT AUTHORITY\SYSTEM

[] Done
Audit completed in 18.5633911 seconds.
```

- WINSpect wrapped up with a quick check of configurable services, DLL Safe Search and no unattended install leftovers

References

- Github

<https://github.com/A-mIn3/WINspect/blob/master/README.md>