iSEC
information security inc.

WINspect Update1

Information Security Inc.

Contents

- About WINspect
- WINspect Features
- QuickTest standalone 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

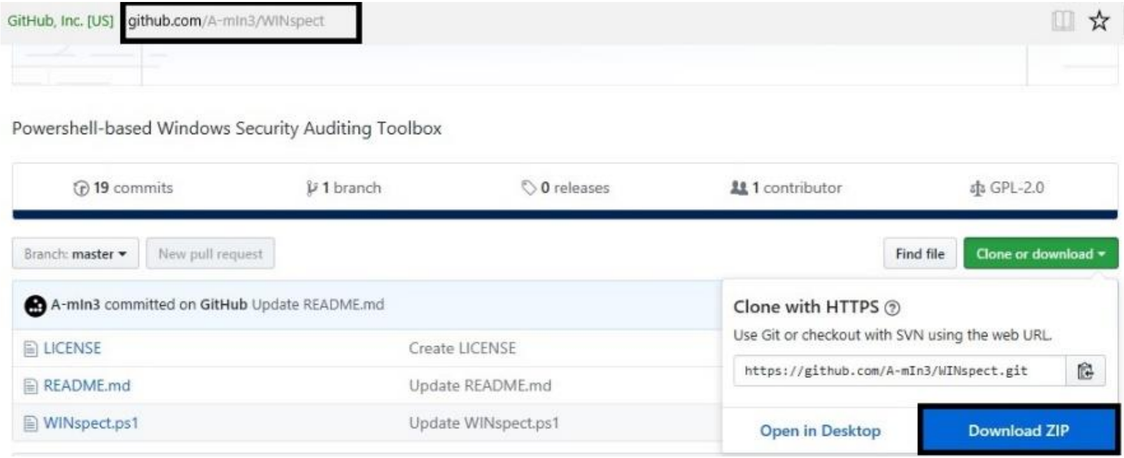
- Checking for installed security products
- Enumerating world-exposed local filesystem shares
- Enumerating domain users and groups with local group membership
- Enumerating registry autoruns
- Enumerating local services that are configurable by Authenticated Users group members
- Enumerating local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



GitHub, Inc. [US] github.com/A-mIn3/WINspect

Powershell-based Windows Security Auditing Toolbox

19 commits · 1 branch · 0 releases · 1 contributor · GPL-2.0

A-mIn3 committed on GitHub Update README.md

LICENSE	Create LICENSE
README.md	Update README.md
WINspect.ps1	Update WINspect.ps1

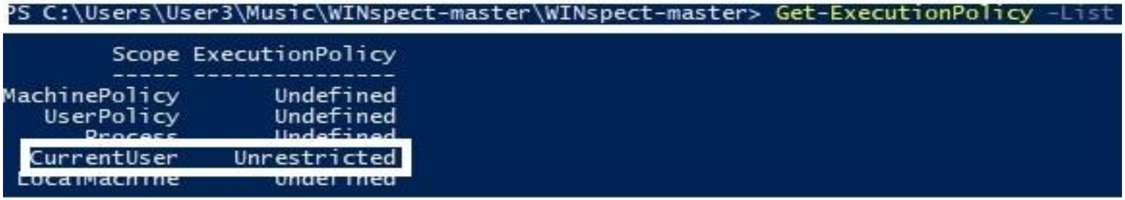
Clone with HTTPS

Use Git or checkout with SVN using the web URL.

```
https://github.com/A-mIn3/WINspect.git
```

QuickTest standalone workstation

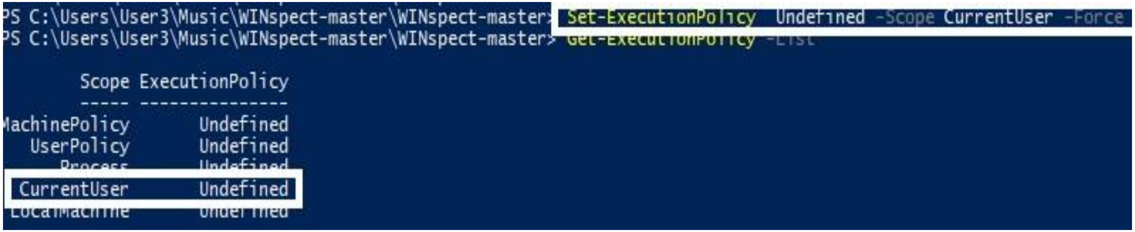
- Run the script from powershell
- Make sure to have the Execution Policy configured to “Unrestricted”. Default settings is Undefined hence the script cannot be run
- Execution Policy status can be checked with the following command



```
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

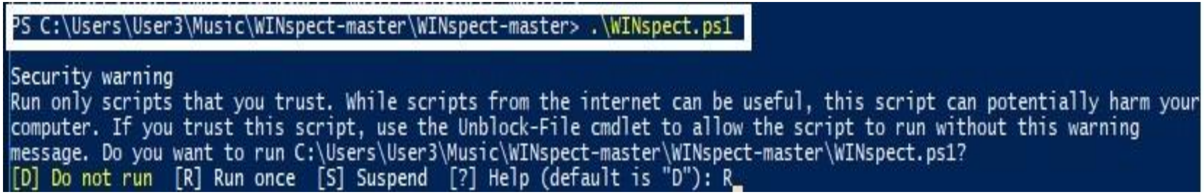
- The Execution Policy can be modified using the following command



```
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

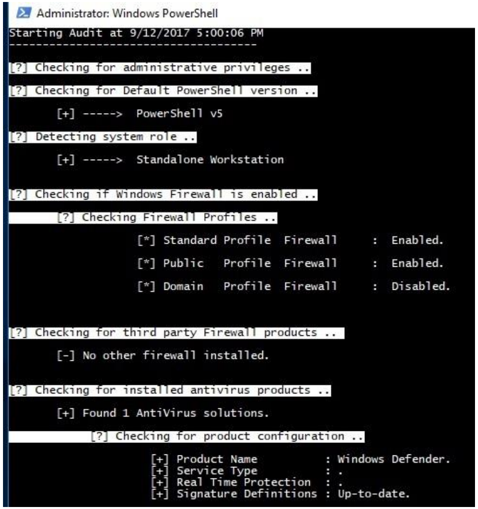
- Run the script



```
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
```

QuickTest standalone workstation

Run the script

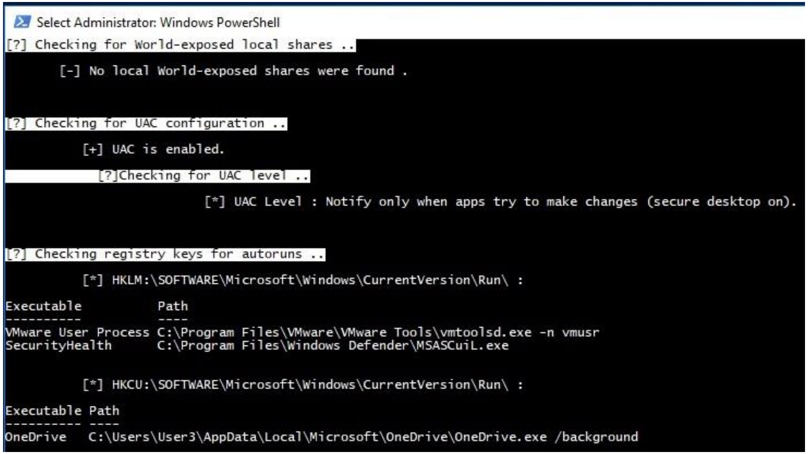


```
Starting Audit at 9/12/2017 5:00:06 PM
-------------------------------------

[?] Checking for administrative privileges ..

[?] Checking for Default PowerShell version ..

       [+] ----->  PowerShell v5

[?] Detecting system role ..

       [+] ----->  Standalone 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 standalone workstation

- 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



Select Administrator: Windows PowerShell

```
[?] Checking for World-exposed local shares ..

       [-] No local World-exposed shares were found .


[?] 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
```

References

- Github

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