WINspect

Information Security Inc.

iSEC
information security inc.

Contents

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

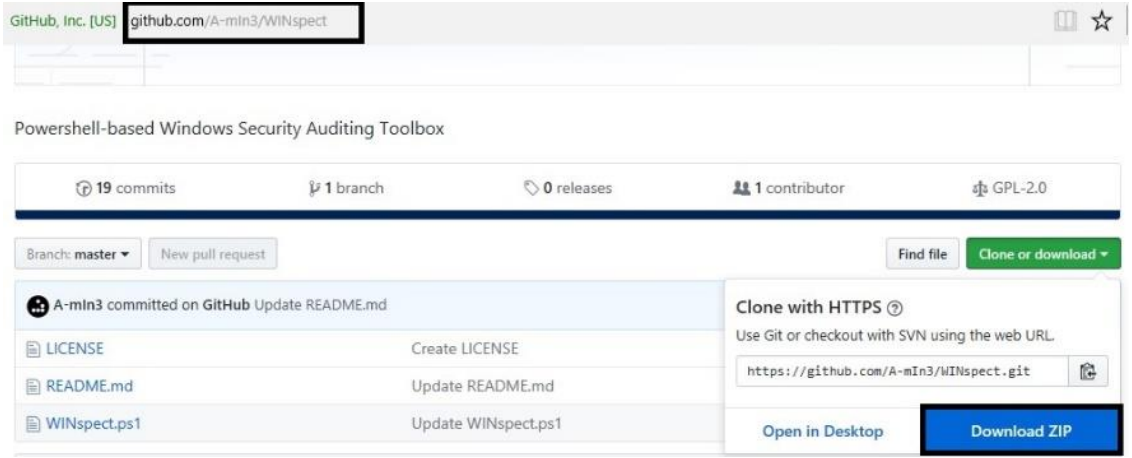
- Checking for installed security products
- Enumerating world-exposed local filesystem shares
- Enumerating domain users and groups with local group membership
- Enumerating registry autoruns
- Enumerating local services that are configurable by Authenticated Users group members
- Enumerating local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

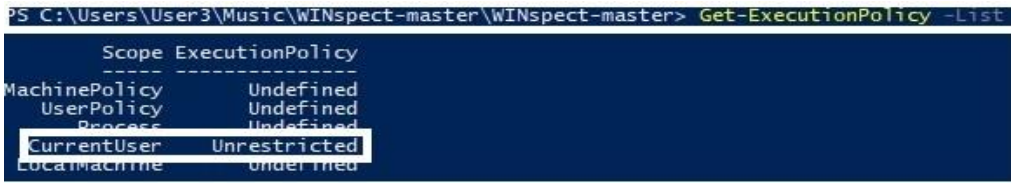
QuickTest standalone workstation

- Download and the script



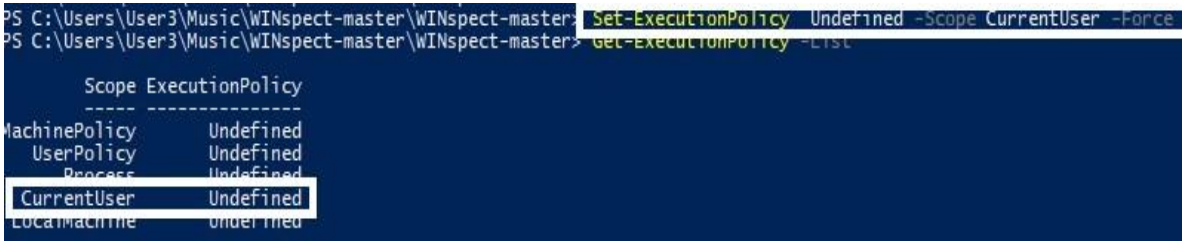
QuickTest standalone workstation

- 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



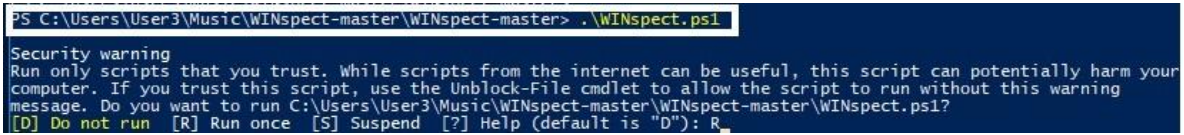
QuickTest standalone workstation

- The Execution Policy can be modified using the following command

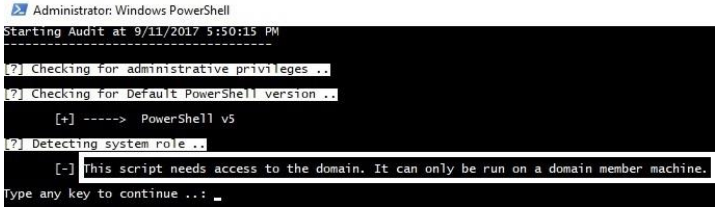


QuickTest standalone workstation

- Run the script

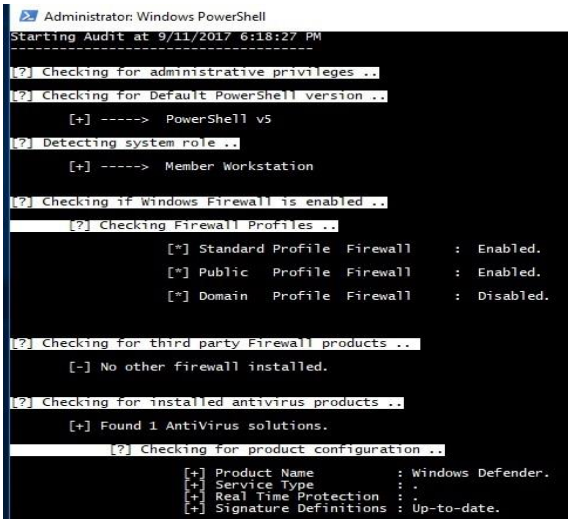


- The script bails out when it couldn't find any domain as per below



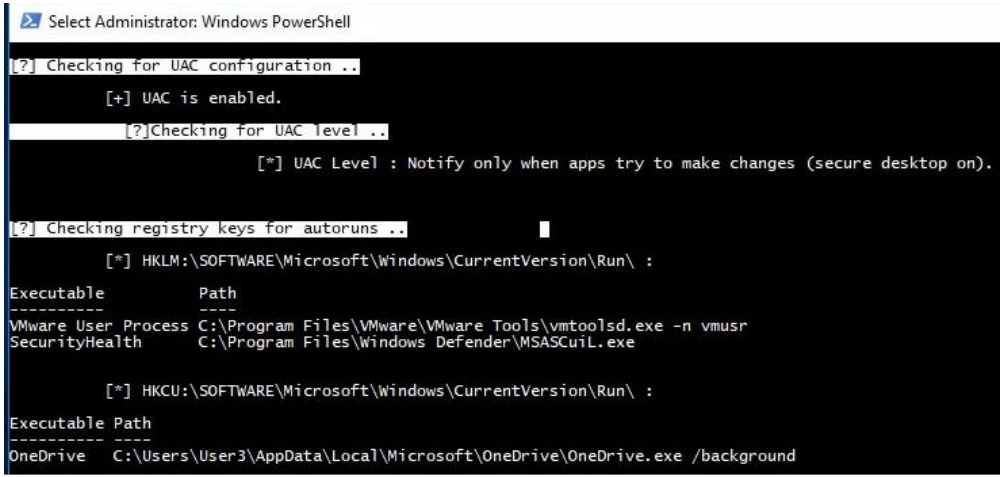
QuickTest domain-joined machine

- Run the script



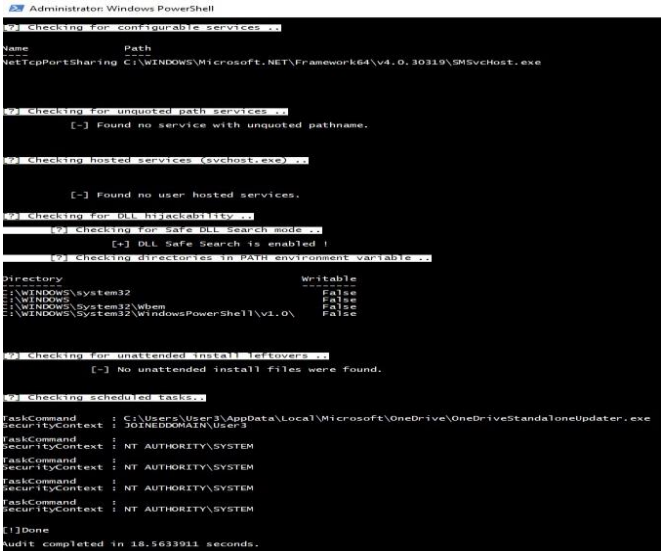
- The script confirms that it's running with admin rights, checks PowerShell version, then inspects Windows Firewall settings

QuickTest domain-joined machine



- 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



- 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