Windows Enterprise Network PenTest

JOAS ANTONIO

Windows Features - AMSI

- The Windows Antimalware Scan Interface (AMSI) is a versatile interface standard that allows your applications and services to integrate with any antimalware product that's present on a machine. AMSI provides enhanced malware protection for your end-users and their data, applications, and workloads.
- AMSI is agnostic of antimalware vendor; it's designed to allow for the most common malware scanning and protection techniques provided by today's antimalware products that can be integrated into applications. It supports a calling structure allowing for file and memory or stream scanning, content source URL/IP reputation checks, and other techniques.
- AMSI also supports the notion of a session so that antimalware vendors can correlate different scan requests. For instance, the different fragments of a malicious payload can be associated to reach a more informed decision, which would be much harder to reach just by looking at those fragments in isolation.
- https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal

Windows Features - COM

- The Microsoft Component Object Model (COM) is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. COM is the foundation technology for Microsoft's OLE (compound documents), ActiveX (Internet-enabled components), as well as others.
- To understand COM (and therefore all COM-based technologies), it is crucial to understand that it is not an object-oriented language but a standard. Nor does COM specify how an application should be structured; language, structure, and implementation details are left to the application developer. Rather, COM specifies an object model and programming requirements that enable COM objects (also called COM components, or sometimes simply objects) to interact with other objects. These objects can be within a single process, in other processes, and can even be on remote computers. They can be written in different languages, and they may be structurally quite dissimilar, which is why COM is referred to as a binary standard; a standard that applies after a program has been translated to binary machine code.
- https://docs.microsoft.com/en-us/windows/win32/com/the-component-object-model

Windows Features - UAC

- User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.
- UAC allows all users to log on to their computers using a standard user account. Processes launched using a standard user token may perform tasks using access rights granted to a standard user. For instance, Windows Explorer automatically inherits standard user level permissions. Additionally, any apps that are started using Windows Explorer (for example, by double-clicking a shortcut) also run with the standard set of user permissions. Many apps, including those that are included with the operating system itself, are designed to work properly in this way.
- Other apps, especially those that were not specifically designed with security settings in mind, often require additional permissions to run successfully. These types of apps are referred to as legacy apps. Additionally, actions such as installing new software and making configuration changes to the Windows Firewall, require more permissions than what is available to a standard user account.
- When an app needs to run with more than standard user rights, UAC allows users to run apps with their administrator token (with administrative groups and privileges) instead of their default, standard user access token. Users continue to operate in the standard user security context, while enabling certain apps to run with elevated privileges, if needed.
- https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview

Windows Features - AppLocker

AppLocker can help you:

- Define rules based on file attributes that persist across app updates, such as the publisher name (derived from the digital signature), product name, file name, and file version. You can also create rules based on the file path and hash.
- Assign a rule to a security group or an individual user.
- Create exceptions to rules. For example, you can create a rule that allows all users to run all Windows binaries, except the Registry Editor (regedit.exe).
- Use audit-only mode to deploy the policy and understand its impact before enforcing it.
- Create rules on a staging server, test them, then export them to your production environment and import them into a Group Policy Object.
- Simplify creating and managing AppLocker rules by using Windows PowerShell.
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

Windows Features - Sandbox

Windows Sandbox is a new lightweight desktop environment tailored for safely running applications in isolation.

- How many times have you downloaded an executable file, but were afraid to run it? Have you ever been in a situation which required a clean installation of Windows, but didn't want to set up a virtual machine?
- At Microsoft we regularly encounter these situations, so we developed **Windows Sandbox**: an isolated, temporary, desktop environment where you can run untrusted software without the fear of lasting impact to your PC. Any software installed in Windows Sandbox stays only in the sandbox and cannot affect your host. Once Windows Sandbox is closed, all the software with all its files and state are permanently deleted.

Windows Sandbox has the following properties:

- **Part of Windows** – everything required for this feature ships with Windows 10 Pro and Enterprise. No need to download a VHD!
- **Pristine** – every time Windows Sandbox runs, it's as clean as a brand-new installation of Windows
- **Disposable** – nothing persists on the device; everything is discarded after you close the application
- **Secure** – uses hardware-based virtualization for kernel isolation, which relies on the Microsoft's hypervisor to run a separate kernel which isolates Windows Sandbox from the host
- **Efficient** – uses integrated kernel scheduler, smart memory management, and virtual GPU

https://techcommunity.microsoft.com/t5/windows-kernel-internals-blog/windows-sandbox/ba-p/301849

Windows Features - WDEG

- Windows Defender Exploit Guard is a new set of intrusion prevention capabilities that ships with the Windows 10 Fall Creators Update. The four components of Windows Defender Exploit Guard are designed to lock down the device against a wide variety of attack vectors and block behaviors commonly used in malware attacks, while enabling enterprises to balance their security risk and productivity requirements.
- Traditional antivirus technologies are an integral aspect of the endpoint security stack through the identification and removal of malicious executables using a combination of cloud-based machine learning and heuristics. Despite advances in antivirus detection capabilities, attackers are continuously adapting and have been expanding their arsenal of tricks and techniques to compromise endpoints, steal credentials, and execute ransomware attacks without ever needing to write anything to disk. This emerging trend of fileless attacks, which compose over 50% of all threats, are extremely dangerous, constantly changing, and designed to evade traditional AV. Fileless attacks have two types: those that use non-traditional executable files (e.g., documents with active content in them), and those that exploit vulnerabilities.
- Windows Defender Exploit Guard utilizes the capabilities of the Microsoft Intelligent Security Graph (ISG) and the world-class security research team at Microsoft to identify active exploits and common behaviors to stop these types of attacks at various stages of the kill chain. Although the underlying vulnerability being exploited varies, the delivery mechanism differs, and the payload changes, there is a core set of behaviors and vectors that many different attacks adhere to. By correlating streams of events to various malicious behaviors with the ISG, Windows Defender Exploit Guard provides the capability and controls needed to handle these types of emerging threats.
- https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/

Windows Features – WDAC e WDAG

- https://github.com/MicrosoftDocs/WDAC-Toolkit
- https://hightechnews.info/windows-defender-application-guard-wdag-no-google-chrome-e-firefox/
- https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/install-md-app-guard
- https://docs.microsoft.com/pt-br/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview

Windows Features - WSUS

- https://www.youtube.com/watch?v=LkeGluvR6C8
- https://www.techtarget.com/searchwindowsserver/definition/Windows-Server-Update-Services-WSUS
- https://study.com/academy/lesson/windows-server-update-services-wsus-definition-uses-setup.html
- https://www.utilizewindows.com/introduction-to-windows-server-update-services-wsus/
- https://www.solarwinds.com/resources/it-glossary/wsus-windows-server-update-services


Exploitation

Windows API

- https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/how-to-documentation/raisers-edge-how-to/raisers-edge-user-guides-administration/api.pdf?sfvrsn=ec9ab9a2_11
- https://docs.microsoft.com/en-us/windows/win32/learnwin32/learn-to-program-for-windows
- https://github.com/xamarin/Essentials
- https://en.wikipedia.org/wiki/Windows_Essentials
- https://www.mentebinaria.com.br/forums/topic/307-lista-de-fun%C3%A7%C3%B5es-da-api-do-windows-interessantes-para-er/

Windows API 2

- https://mentebinaria.gitbook.io/engenharia-reversa/apendices/funcoes-api-win
- https://docs.microsoft.com/en-us/visualstudio/debugger/how-can-i-debug-windows-api-functions-q?view=vs-2019
- https://www.vbmigration.com/BookChapters/ProgrammingVB6_AppA.pdf
- https://zetcode.com/gui/winapi/system/
- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list

Windows API Abuse

- https://infocondb.org/con/def-con/def-con-22/getting-windows-to-play-with-itself-a-hackers-guide-to-windows-api-abuse
- https://attack.mitre.org/techniques/T1106/
- http://www.irongeek.com/i.php?page=videos/derbycon4/t122-getting-windows-to-play-with-itself-a-pen-testers-guide-to-windows-api-abuse-brady-bloxham
- https://www.ired.team/offensive-security/defense-evasion/windows-api-hashing-in-malware
- https://www.giac.org/paper/grem/89/malcode-context-api-abuse/108874

Unmanaged vs Managed Code C#

- https://docs.microsoft.com/en-us/dotnet/framework/interop/#:~:text=Code%20that%20executes%20under%20the,are%20examples%20of%20unmanaged%20code
- https://stackoverflow.com/questions/334326/what-is-managed-or-unmanaged-code-in-programming
- https://www.partech.nl/en/publications/2021/03/managed-and-unmanaged-code---key-differences
- https://www.c-sharpcorner.com/uploadfile/puranindia/managed-code-and-unmanaged-code-in-net/
- https://www.geeksforgeeks.org/difference-between-managed-and-unmanaged-code-in-net/
- https://docs.microsoft.com/en-us/dotnet/standard/managed-code
- https://www.tutorialspoint.com/managed-code-vs-unmanaged-code-in-chash

Offensive CSharp

- https://github.com/matterpreter/OffensiveCSharp

AbandonedCOMKeys	Enumerates abandoned COM keys (specifically `InprocServer32`). Useful for persistence as you can, in some cases, write to the missing location and call with `rundll32.exe -sta {CLSID}`. Technique referenced in this post by @bohops	4.0
COMHunter	Enumerates COM servers set in `LocalServer32` and `InProc32` keys on a system using WMI	4.0
CredPhisher	Prompts the current user for their credentials using the `CredUIPromptForWindowsCredentials` WinAPI function. Supports an argument to provide the message text that will be shown to the user.	3.5
DriverQuery	Collect details about drivers on the system and optionally filter to find only ones not signed by Microsoft	3.5
EncryptedZIP	Compresses a directory or file and then encrypts the ZIP file with a supplied key using AES256 CFB. This assembly also clears the key out of memory using `RtlZeroMemory`. Use the included Decrypter progam to decrypt the archive.	3.5
ETWEventSubscription	Similar to WMI event subscriptions but leverages Event Tracing for Windows. When the event on the system occurs, currently either when any user logs in or a specified process is started, the `DoEvil()` method is executed.	4.6
GPSCoordinates	Tracks the system's GPS coordinates (accurate within 1km currently) if Location Services are enabled. Works on Windows 10 currently, but hoping to cover all versions 7+.	4.0
HijackHunter	Parses a target's PE header in order to find lined DLLs vulnerable to hijacking. Provides reasoning and abuse techniques for each detected hijack opportunity	4.0
HookDetector	Detects hooked Native API functions in the current process, indicating the presence of EDR	4.0

Bypass Antivíruses with C#

- https://damonmohammadbagher.github.io/Posts/ebookBypassingAVsByCsharpProgramming/index.htm?page=Chapter%201.html
- https://holdmybeersecurity.com/2016/09/11/c-to-windows-meterpreter-in-10mins/
- https://github.com/DamonMohammadbagher/NativePayload_Reverse_tcp
- https://github.com/padovah4ck/RedSharp
- https://www.ired.team/offensive-security/code-execution/using-msbuild-to-execute-shellcode-in-c
- https://reposhub.com/dotnet/miscellaneous/plackyhacker-Suspended-Thread-Injection.html
- https://pt.slideshare.net/mvelazco/defcon-27
- https://tbhaxor.com/execute-unmanaged-code-via-c-pinvoke/
- https://websterprodigy.net/2012/08/31/av-evading-meterpreter-shell-from-a-net-service/
- https://haxtivitiez.wordpress.com/2019/09/25/writing-backdoor-payloads-with-c-part-2-custom-meterpreter-stager/
- https://www.youtube.com/watch?v=VdYfymr44v8
- https://www.purpl3f0xsecur1ty.tech/2021/03/30/av_evasion.html

Process Injection

- https://redcanary.com/threat-detection-report/techniques/process-injection/#:~:text=Process%20injection%20is%20a%20method,resources%2C%20and%20possibly%20elevated%20privileges.
- https://www.elastic.co/pt/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
- https://attack.mitre.org/techniques/T1055/
- https://medium.com/csg-govtech/process-injection-techniques-used-by-malware-1a34c078612c
- https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All.pdf
- https://www.youtube.com/watch?v=xewv122qxnk
- https://www.youtube.com/watch?v=tBR1-1J5Jec
- https://www.youtube.com/watch?v=CwglaQRejio
- https://www.secarma.com/process-injection-part-1-the-theory/
- https://www.ired.team/offensive-security/code-injection-process-injection
- https://malgamy.github.io/malware-analysis/DLL-Injection/
- https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11578/Balaoura_MTE1623.pdf?sequence=1&isAllowed=y
- https://www.socinvestigation.com/process-injection-techniques-used-by-malware-detection-analysis/

Bypass Windows Account

- https://www.youtube.com/watch?v=YhkcQziQt8Y
- https://www.youtube.com/watch?v=7MeiiBygFWQ
- https://www.youtube.com/watch?v=LEFV3bc0q7E
- https://www.tomshardware.com/how-to/bypass-windows-11-tpm-requirement
- https://www.youtube.com/watch?v=MVfQx9yhsgw
- https://www.youtube.com/watch?v=LroJNedIvNw

WDAC Bypass

- https://github.com/bohops/UltimateWDACBypassList
- https://fortynorthsecurity.com/blog/how-to-bypass-wdac-with-dbgsrv-exe/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0951
- https://bohops.com/2020/10/15/exploring-the-wdac-microsoft-recommended-block-rules-visualuiaverifynative/
- https://cloud7.news/security/update-your-powershell-to-fix-the-wdac-bypass-vulnerability/
- https://mattifestation.medium.com/windows-defender-application-control-wdac-resources-9cad7026a943
- https://www.cirt.gov.bd/cve-2020-0951-windows-defender-application-control-security-feature-bypass-vulnerability/
- https://cs.beta.fletch.ai/p/microsoft-asks-admins-to-patch-powershell-to-fix-wdac-bypass
- https://debricked.com/en/vulnerability-database/vulnerability/CVE-2019-0733
- https://cyware.com/news/microsoft-asks-admins-to-patch-powershell-to-fix-wdac-bypass-d52778dd/
- https://www.youtube.com/watch?v=GU5OS7UN8nY

AppLocker Bypass

- https://github.com/api0cradle/UltimateAppLockerByPassList
- https://www.hacking-tutorial.com/hacking-tutorial/how-to-bypass-windows-applocker/#sthash.7qAGlJus.dpbs
- https://www.youtube.com/watch?v=HY1TNwjE9Ug
- https://www.youtube.com/watch?v=91ZdHFae4-A
- https://www.youtube.com/watch?v=T91iXd_VPVI
- https://blog.pwn.al/security/applocker/bypass/custom/rules/windows/2018/09/13/applocker-custom-rules-bypass.html
- https://depthsecurity.com/blog/bypassing-app-locker-clm-while-evading-edr
- https://infosecaddicts.com/bypass-windows-applocker/
- https://pentestlab.blog/2017/05/22/applocker-bypass-weak-path-rules/
- https://pentestlab.blog/2017/06/16/applocker-bypass-msiexec/
- https://bohops.com/2018/01/07/executing-commands-and-bypassing-applocker-with-powershell-diagnostic-scripts/
- https://www.linkedin.com/pulse/applocker-policy-bypass-using-runas-mohammad-gabr/

LOLBAS

- https://lolbas-project.github.io/
- https://github.com/LOLBAS-Project/LOLBAS

WSL Hacking

- https://medium.com/@gulfsteve/hacking-with-wsl2-ede3e649e08d
- https://infosecwriteups.com/pentesting-on-windows-f88bbe455f7b
- https://www.youtube.com/watch?v=3AvzOWygajA
- https://www.youtube.com/watch?v=_cXmx2qwWts
- https://www.youtube.com/watch?v=8Qlq4GItKb4
- https://reconshell.com/awesome-wsl/
- https://raesene.github.io/blog/2020/05/31/Custom_Pentest_Distributions_With_WSL2/

Process Hollow

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/analyzing-malware-hollow-processes/#:~:text=Process%20hollowing%20is%20a%20technique,hide%20amongst%20normal%20processes%20better.
- https://attack.mitre.org/techniques/T1055/012/
- https://medium.com/@viniciuskmax/process-hollowing-runpe-como-ocultar-c%C3%B3digo-malicioso-por-tr%C3%A1s-de-um-processo-leg%C3%ADtimo-e08ca70ffea7
- https://github.com/m0n0ph1/Process-Hollowing
- https://www.youtube.com/watch?v=BVhHLwhvOf4
- https://www.youtube.com/watch?v=aBKk2KAN0E0
- https://www.ired.team/offensive-security/code-injection-process-injection/process-hollowing-and-pe-image-relocations
- https://www.andreafortuna.org/2017/11/22/runpe-a-practical-example-of-process-hollowing-technique/
- https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1055-process-injection/process-hollowing

Powershell without powershell.exe

- https://www.paloaltonetworks.com/blog/security-operations/stopping-powershell-without-powershell/
- https://www.ired.team/offensive-security/code-execution/powershell-without-powershell
- https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/
- https://bank-security.medium.com/how-to-running-powershell-commands-without-powershell-exe-a6a19595f628
- https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/offensive-security/code-execution/powershell-without-powershell.md
- https://securityonline.info/powerlessshell-run-powershell-command-without-invoking-powershell-exe/
- https://dmcxblue.gitbook.io/red-team-notes/execution/powershell
- https://reposhub.com/python/command-line-tools/Mr-Un1k0d3r-PowerLessShell.html

WSUS Hacking

- https://www.bussink.net/wsus-attacks/
- https://pentestit.com/wsuxploit-weaponized-wsus-exploit-script/
- https://www.gosecure.net/blog/2020/09/03/wsus-attacks-part-1-introducing-pywsus/
- https://github.com/AlsidOfficial/WSUSpendu

Privilege Escalation

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation
- https://book.hacktricks.xyz/windows/checklist-windows-privilege-escalation
- https://hacktricks.boitatech.com.br/windows/checklist-windows-privilege-escalation
- https://github.com/carlospolop/hacktricks/blob/master/windows/checklist-windows-privilege-escalation.md
- https://s3cur3th1ssh1t.github.io/The-most-common-on-premise-vulnerabilities-and-misconfigurations/

Conclusion

- PDF made to raise awareness about depression and disorders, psychological diseases that lead to suicide