Offensive Powershell 101

[AFK.conf]

PS > env

- Offensive Security > Morphus
- Twitter / GitHub > @g0ttfrid
- Linkedin > in/yurimaia

PS > Agenda

- Powershell
- Security features
- Bypass security features (Hands-on)
- Load artifacts in memory (Hands-on)

PS > What is Powershell?

- Command-line Shell
- Scripting language
- Automation platform
- Configuration management

https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.3

PS > What is Powershell?

- Native to Windows
- Able to call the Windows API
- Able to run commands without writing to the disk

PS > Security Features

- Execution Policy*
- Constrained Language Mode
- Module and script block logging
- Antimalware Scan Interface (AMSI)
- Application Control (AppLocker)

PS > Execution Policy

- Load Configuration Files
- Run Scripts

- AllSigned
- Bypass
- Default
- RemoteSigned
- Restricted
- Undefined
- Unrestricted

PS > Constrained Language Mode

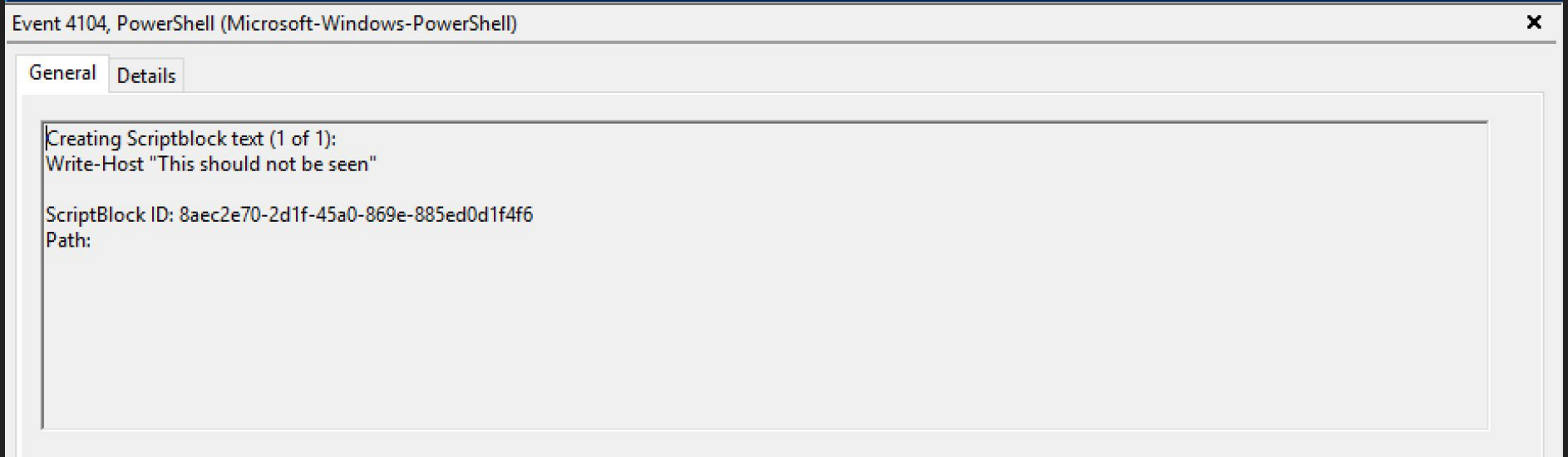
- COM objects
- .NET objects (Import Windows API)
- New data types (with Add-Type)

Hands-on

PS > Module and script block logging

- Auditing scripts
- Unpack obfuscated scripts

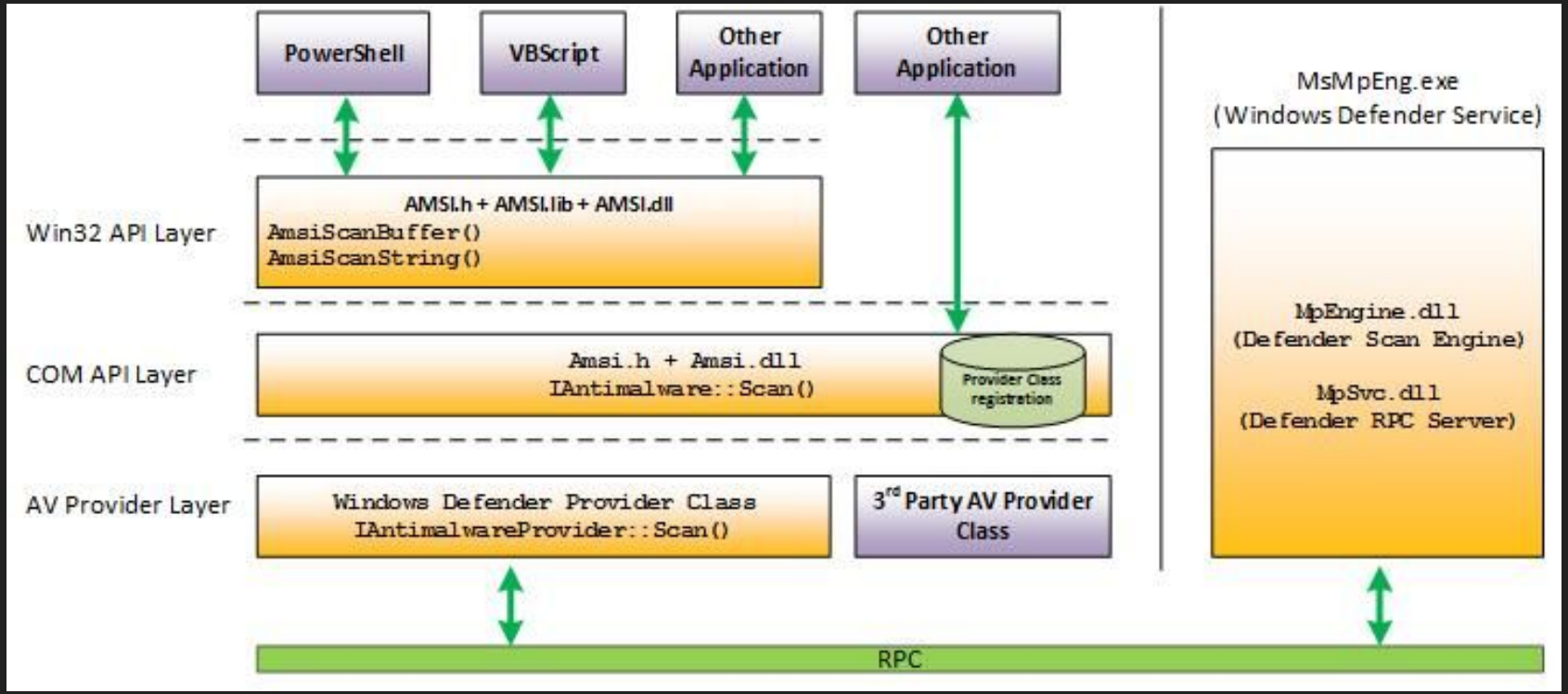
```
PS C:\Users\xpn> InvokE-eXprEssiOn ((("{4}{7}{2}{1}{3}{5}{0}{8}{6}" -f 'ee','ost QENThis should n','te-H','ot b','W','e
s','N','ri','nQE')).RePLace('QEN',[StRINg][CHAr]34) )
This should not be seen
```



PS > Antimalware Scan Interface (AMSI)

- User Account Control, or UAC (elevation of EXE, COM, MSI, or ActiveX installation)
- PowerShell (scripts, interactive use, and dynamic code evaluation)
- Windows Script Host (wscript.exe and cscript.exe)
- JavaScript and VBScript
- Office VBA macros

PS > Antimalware Scan Interface (AMSI)



PS > Application Control (AppLocker)

- Executable files
- Scripts
- Windows installer files
- Dynamic-link libraries (DLLs)
- Packaged apps
- Packaged app installers

Hands-on

PS > refs

https://bestestredteam.com/2019/01/27/powershell-execution-policy-bypass/
https://www.netspi.com/blog/technical/network-penetration-testing/15-ways-to-bypass-the-powershell-execution-policy/
https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell#Patching-amsi.dll-AmsiScanBuffer-by-rasta-mouse
https://rastamouse.me/memory-patching-amsi-bypass/
https://s3cur3th1ssh1t.github.io/Bypass_AMSI_by_manual_modification/
https://s3cur3th1ssh1t.github.io/Powershell-and-the-.NET-AMSI-Interface/
https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/
https://www.mdsec.co.uk/2018/09/applocker-clm-bypass-via-com/
https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/
https://www.blackhillsinfosec.com/constrained-language-mode-bypass-when-pslockdownpolicy-is-used/