Resources for the OSEP

Github repos

<https://github.com/Mr-Un1k0d3r/SCShell>

<https://github.com/kosh-cyber/OSEP-NOTE>

<https://github.com/chvancooten/OSEP-Code-Snippets>

<https://github.com/r0r0x-xx/OSEP-Pre>

<https://github.com/CyberSecurityUP/OSCE3-Complete-Guide#osep>

Official Documentation

<https://learn.microsoft.com/en-us/docs/>

<https://visualstudio.microsoft.com/msdn-platforms/>

http://www.pinvoke.net/

Websites for help

<https://www.ired.team/>

<https://book.hacktricks.xyz/welcome/readme>

<https://attack.mitre.org>

<https://medium.com>

<https://rastamouse.me/>

<https://www.powershellgallery.com/>

<https://chat.openai.com/>

http://www.pinvoke.net/

C2

<https://github.com/byt3bl33d3r/SILENTTRINITY>

<https://github.com/BC-SECURITY>

Building the lab

<https://www.linkedin.com/posts/zer0verflow_penetrationtesting-activedirectory-building-activity-6906707626684780544-PImf/>

<https://www.linkedin.com/posts/fadymoheb_freepalastine-ad-activedirectory-activity-7127620092472737792-YihL/>

<https://github.com/Orange-Cyberdefense/GOAD>

Some resources that I found interesting.

https://rastamouse.me/exploring-process-injection-opsec-part-1/

https://medium.com/@matterpreter/offensive-p-invoke-leveraging-the-win32-api-from-managed-code-7eef4fdef16d

https://mark-borg.github.io/blog/2017/interop/

https://www.ired.team/offensive-security/defense-evasion/finding-all-rwx-protected-memory-regions

https://learn.microsoft.com/en-us/dotnet/api/system.runtime.interopservices.dllimportattribute?view=netframework-4.8

https://learn.microsoft.com/en-us/dotnet/standard/native-interop/pinvoke

https://learn.microsoft.com/en-us/dotnet/api/system?view=netframework-4.8

https://learn.microsoft.com/en-us/dotnet/api/system.runtime.interopservices?view=netframework-4.8

https://learn.microsoft.com/en-us/dotnet/csharp/language-reference/keywords/using-directive

https://learn.microsoft.com/en-us/dotnet/framework/reflection-and-codedom/reflection

about the reflection

https://www.codeproject.com/Articles/55710/Reflection-in-NET

https://learn.microsoft.com/en-us/dotnet/csharp/advanced-topics/reflection-and-attributes/

https://learn.microsoft.com/en-us/dotnet/framework/reflection-and-codedom/reflection

about process injection

https://rastamouse.me/exploring-process-injection-opsec-part-1/

https://rastamouse.me/exploring-process-injection-opsec-part-2/

https://github.com/3xpl01tc0d3r/ProcessInjection

https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf

https://thewover.github.io/Introducing-Donut/

https://attack.mitre.org/techniques/T1055/

https://github.com/pwndizzle/c-sharp-memory-injection/

https://www.ired.team/offensive-security/code-injection-process-injection

https://infosecwriteups.com/process-injection-series-part-i-pe-injection-615b761513fe

more to learn about the process injection

https://malwaretips.com/

https://www.bleepingcomputer.com/forums/

https://www.malwarecookbook.com/

https://learn.microsoft.com/en-us/windows/win32/SysInfo/windows-system-information

DLL injection

https://github.com/stephenfewer/ReflectiveDLLInjection

https://clymb3r.wordpress.com/2013/04/06/reflective-dll-injection-with-powershell/

https://www.ired.team/offensive-security/code-injection-process-injection/dll-injection

https://cocomelonc.github.io/tutorial/2021/09/20/malware-injection-2.html

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/dll-hijacking

https://tryhackme.com/room/dllhijacking

https://security.stackexchange.com/questions/74586/what-is-the-difference-between-dll-hijacking-and-dll-injection

https://github.com/hasherezade/pe-sieve

https://github.com/m0n0ph1/Process-Hollowing

https://www.kernelmode.info/forum/

https://www.codeproject.com/Articles/4910/ASN-1-Editor

https://0x00sec.org/t/reflective-dll-injection/3080

https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

AV Evasion

https://obscuresecurity.blogspot.com/2012/12/finding-simple-av-signatures-with.html

https://github.com/PowerShellMafia/PowerSploit/blob/master/AntivirusBypass/Find-AVSignature.ps1

----------------------------------------------------------------------------

https://www.eicar.org/download-anti-malware-testfile/

----------------------------------------------------------------------------

Note >> this recourses are maybe consider as random but I kept the only looked interesting

As for the AD part in the OSEP the CRTE should be enough for u If u took a look at the notes I took from it

https://github.com/ali5aled/CRTE\_NOTES