README.md

i took this from lassehauballe / **Eternalblue**

https://github.com/lassehauballe/Eternalblue
it hasn't been updated in at least two years since this post
if you consider each page as a file, and each chapter as a folder,
for example this is the readme.md
anyways this is entirely for educational purposes coz id like to learn c# and id like to learn about offsec
so I think reading ~~malware~~ offensive cyber security tools is cool :D

Eternalblue in C#

This project is an almost direct translation of https://github.com/EmpireProject/Empire/blob/master/data/module_source/exploitation/Exploit-EternalBlue.ps1. However, the Empire-script did not test if the target is vulnerable. To test for this, I also translated a bit of Metasploits auxiliary/scanner/smb/smb_ms17_010

This was created as an educational project to help myself gain an understanding of how Eternalblue actually works.
Please do use at your own risk, as I have also seen a couple of BSOD during development.
The code has only been tested using msfvenom x64 exec, meterpreter reverse shell shellcode and cobaltstrike. Remember this is the old eternalblue exploit, so should not work on windows 8 and newer.

Updates:

- It is hardcoded with 'Grooms' set to 12
- It can now be run using either "detect or exploit". The first will only detect if its vulnerable or not.
- It can be run with either an IP or the word 'all'. In the latter, it will go through every host on the subnet. At this time, it only spreads on 192.168.XXX.XXX/24 networks.

How to use:

1. Replace the shellcode byte[] called 'buf' in Exploit (line 1028) (The current shellcode just starts notepad.exe (as system))
2. Compile
3. Eternalblue.exe [detect/exploit] [ip/all]

Video: With Cobalt-Strike payload

Eternalblue in C# with Cobalt-Strike payload

Eternalblue.exe running in detect-mode on the entire network

alt text

Eternalblue.exe running in exploit-mode on the entire network

alt text

Revision #3
Created 2023-05-25 02:26:39 UTC by naruzkurai
Updated 2023-05-25 02:41:59 UTC by naruzkurai