בדיקות חוסן בסביבות AD | 7 שעות תוכן | 50 שעות תירגול | פרוייקט גמר

1.בניית סביבת מעבדה

- וירטואליזציה Vmware/VirtualBox
- טעינת Kali Linux
- טעינת Windows Server 2012
- טעינת Windows7
- טעינת Windows10

2. פרוטוקולים בסביבות דומיין

- WPAD
- NBNS
- mDNS
- LLMNR
- IMGPv3
- Kerberos
- NTLM
- SMB
- Ntlmssp

3. הגדרת Windows Server 2012

- הגדרת תיקיות שיתופיות
- הרשאות לקבצים ותיקיות
- הגדרת Gpo's
- הגדרת Script Logon
- נתיבים, תיקיות וקבצי מערכת חשובים
- הכרות עם Sysinternals
- התקנת Active Directory
- התקנת שרת IIS

4. איסוף מידע

- איסוף מידע Linkdin
- איסוף מידע Shodan
- איסוף מידע The Harvester
- איסוף מידע Maltego
- איסוף מידע פנימי באירגון
- מיפויי רשת באמצעות BloodHound
- חילוץ תעבורת רשת Wireshark
- חילוץ תעבורה NetworkMiner
- השתלטות על נתב מרוחק

5.Advanced Weaponization

- היכרות עם Macro Code
- שימוש ב Unicorn
- שימוש ב Macropack
- PPT פישינג
- Office Formula Injection
- Office Word Reverse Shell
- תקיפות בצד לקוח SEToolkit
- הקמת שרת AWS לתקיפות פישינג
- שימוש מתקדם ב Metasploit
- שימוש מתקדם ב Meterpreter

6. Exploitation And Pivoting

- Man in the middle
- SmbrelayX
- NtlmrelayX
- Advanced Responder
- IIS Manipulation
- MITM Mitigation
- Port Forward MSF
- Port Forward SSH
- Tunneling Chisel
- Tunneling Sshuttle
- Tunneling Plink

7. Lateral Movement & AD Attacks

- Intro to AD attacks
- Psexec PE
- The Power Of PowerShell
- AD Enumeration
- Deep Dive On Lsass
- RDP Session Hijacking
- DcSync
- Golden Ticket
- Shadow Volume Copy
- Spray Passwords
- Kerberoasting

8. Post Exploitation

- חיפושי מידע רגיש
- פיצוח קבצי PDF חסויים
- פיצוח מפתחות ASR
- יצוא סיסמאות

9. Wifi Cracking

- תקשורת Wireless ופרוטוקולים
- Handshake Point
- Airmon-ng
- Airdump -ng
- Airplay-ng
- Aircrack-ng
- Wifi Password Cracking
- אוטומציה לתקיפות Wifi

ITSAFE
POWERED BY CYSOURCE