בדיקות חוסן תשתית | 15 שעות תוכן | 110 שעות תירגול | פרוייקט גמר

1. הקמת סביבת מעבדות

- וירטואליזציה עם VirtualBox
- טעינת Kali Linux
- טעינת Windows
- טעינת Metasploitable2

2. היכרות עם עולם בדיקות החוסן

- טרמינולוגיה בעולם התקיפה
- סוגי בדיקות תשתית
- תהליכי סריקה וזיהוי פגיעויות
- השגת שליטה וחשיבותה
- אחיזות על מכונה נתקפת

3. אבני יסוד בתקיפה

- מימוש תקשורת Reverse Shell
- מימוש תקשורת Bind Shell
- האזנה בפרוטוקולי TCP/UDP
- העברת קבצים Netcat
- סריקות בסיסיות Netcat
- היכרות עם Wireshark
- פילטרים ב-Wireshark
- חילוץ מידע מקבצי PCAP

4. איסוף מידע פאסיבי ואקטיבי

- Google Dorks
- איסוף ואיתור כתובות מיילים
- איסוף מידע פאסיבי OpenSource
- DNS Enumeration
- תקשורת מול שרתי DNS
- כלי מחקר מול שרתי DNS
- DNS Forward Lookup
- DNS Reverse Lookup

5. סריקת פורטים

- לחיצת יד משולשת ותקשורת TCP
- סריקות UDP
- טעויות נפוצות בסריקות פורטים
- סריקות פורטים ע"י NMAP
- סריקות מתקדמות NMAP NSE
- עקיפות Firewalls
- זיהוי מערכות הפעלה
- Service Enumeration

6. היכרות ועבודה עם Metasploit

- היכרות עם Metasploit
- מודולים ב-Metasploit
- היכרות עם Payloads
- היכרות עם Auxiliaries
- היכרות עם Exploits
- תקיפת FTP עם חולשת RCE
- SMB Windows Brute Force
- Hydra Brute Force
- פרופילי סיסמאות
- Enumeration Tactics
- הזרקות Shellcode
- מעבר בין תהליכים
- תקיפות Wordpress & Drupal
- LFI/RFI
- Log injections
- Environ&Fuzzing
- Remote Code Execution
- Command Injections
- סוסים טרויאנים Msfvenom
- שליטה ב-Meterpreter
- Tomcat
- Backdooring
- AdvanceMeterpreter
- Keylogging
- Download/Upload Functions
- SMTP Enumeration

7. העברת קבצים

- העברת קבצים באמצעות פייתון
- העברת קבצים ב-Windows ע"י Powershell
- העברת קבצים בין Windows ל- Linux ע"י FTP
- העברת קבצים באמצעות שרת SMB
- שיטות נוספות להעברת קבצים

8. הסלמת הרשאות Windows

- UAC Bypass - User Interaction
- UAC Bypass - No User Interaction
- PE Suggester
- Patch enumeration
- Unquoted Path
- Insecure Service
- Zero Click PE

9. הסלמת הרשאות Linux

- Basic Enumerations
- Kernel Exploits
- suid Exploitation
- Sudo Abuse
- Word Writable
- CronTab PE
- Sensitive Files
- Http Methods

10. חקר חולשות

- היכרות עם x86
- היכרות והבנה של תהליכי זיכרון
- זיכרון של בינארי
- CPU Registers
- BufferOverflow Introduction
- OlyDBG Introduction
- Overflowing the buffer
- Fuzzing
- Dealing with crash
- EIP Control
- Shellcode space locating
- Bad Charactars
- Execution flow redirection
- Return Address
- Shellccoding with Metasploit
- Getting a shell

11. סיסמאות

- הזדהות Challenge Response
- גיבוב LM/NTLM
- SAM
- Password Flow
- Mimikatz
- Hash extraction SamDump
- Hash extraction SecretDump
- SecretDump Remoting
- Password cracking Hashcat/John
- Pass the hash
- Reponder & LLMNR intro
- Responder to capture NTLMv2

ITSAFE
POWERED BY CYSOURCE