הסלמת הרשאות ווינדוס | 2 שעות תוכן | 20 שעות תירגול | פרוייקט גמר

Introduction & Lab Setup.1
- Windows10
- Kali Linux
- Groups & Members in Windows
- ACL's, Services, Registry, Directories

Must Known Tools.2
- PowerUP
- SharpUP
- SeatBelt
- winPEAS
- Accesschk
- JuicyPotato
- Procmon

Spawn a shell & Kernel .3 Exploits
- Reverse Shell Over MSFvenom
- Netcat
- Psexec to System
- Manual Kernel Enumeration
- Automatic Kernel Enumeration

Service Exploits .4
- Insecure Properties
  - Enumeration & Exploitation
- Unquoted Path
  - Enumeration & Exploitation
- Weak Registry Permissions
  - Enumeration & Exploitation
- Insecure Service executables
  - Enumeration & Exploitation
- DLL Hijacking

Registry Exploits.5
- Manual Registry Enumeration
- Automatic Registry Enumeration
- Registry Explotiation
- Query Registry Services
- Manual AIE Enumeration
- Automatic AIE Enumeration
- AIE Exploitation

Passwords.6
- Manual Password Enumeration
- Automatic Password Enumeration
- Query Registry Passwords Store
- Saved Creds man & auto Enum
- Configurations Files
- Recursive Configuration Files
- SAM & System locations
- SAM & System Hash Dump
- SAM & System Hash Crack
- PTH-Winexe

Scheduled Tasks .7
- Manual Schduled Tasks Enum
- Scheduled Tasks Exploitation

Insecure GUI Apps .8
- Insecure GUI Apps Enumeration
- Insecure GUI Apps Exploitation
- Startup Apps Enumeration
- Startup Apps Exploitation

Insecure GUI Apps .9
- Vulnerability Research Wan
- Vulnerability Research winPEAS

ITSAFE
POWERED BY CYSOURCE