ACADEMIA CISCO - ESPOL

Ethical Hacking

OBJETIVOS

En este curso se introduce a los estudiantes a los conceptos básicos del hacking y su aplicación a fin de encontrar vulnerabilidades en una red corporativa. Los estudiantes entenderán la mentalidad y motivos típicos de un hacker, facilitando reproducir o intuir sus acciones en determinadas situaciones. El curso es altamente práctico, y se enfoca en el lado ofensivo de la seguridad informática, o dicho de otro modo, desde el punto de vista del atacante.

Objetivos específicos

Al finalizar el curso, el alumno deberá estar capacitado profesionalmente para:

- Desarrollar habilidades para el reconocimiento y enumeración de servicios activos.
- Aprender diversas técnicas efectivas para el descubrimiento de dispositivos de red y su topología.
- Entender el funcionamiento de los exploits basados en buffer overflow.
- Ganar destrezas en el uso de herramientas de explotación de vulnerabilidades.
- Obtención de acceso a sistemas operativos mediante ataques de password.
- Entender, descubrir y explotar vulnerabilidades de aplicaciones WEB.

.

REQUISITOS

Conocimientos básicos de TCP/IP (Indispensable)
Conocimientos básicos de SQL (Recomendado)

CONTENIDO

Programa Resumido

Capítulo 1: Introducción al Hacking Ético
Capítulo 2: Footprinting and Reconnaissance
Capítulo 3: Scanning Networks
Capítulo 4: Buffer Overflow
Capítulo 5: Using Exploits
Capítulo 6: Password Attacks
Capítulo 7: Vulnerabilidades Web
Capítulo 8: Malware
Capítulo 9: Wargame

ACADEMIA CISCO - ESPOL

Programa Detallado

Capítulo 1: Introducción al Ethical Hacking

- **1.1** ¿Qué es Hacking ?
- **1.2** Mentalidad de un Hacker
- **1.3** Tipos de Hackers
- **1.4** Ethical Hacking
- **1.5** Fases del ethical hacking
  - **1.5.1** Reconocimiento
  - **1.5.2** Scanning
  - **1.5.3** Ganando Acceso
  - **1.5.4** Manteniendo Acceso
  - **1.5.5** Cubriendo Rastros
- **1.6** Tipos de Ataques
  - **1.6.1** Ataques al Sistema Operativo
  - **1.6.2** Ataques a Nivel de Aplicación
  - **1.6.3** Ataques Shrink Wrap Code
  - **1.6.4** Ataques a Configuraciones Erróneas
- **1.7** Defensa en profundidad
- **1.8** Categorización de Vulnerabilidades
- **1.9** Test de Penetración
- **1.10** Introducción a Backtrack
- **1.11** Escondiendo tus pasos
  - **1.11.1** Utilización de Proxies
  - **1.11.2** Anonymizers
  - **1.11.3** VPNs
  - **1.11.4** TOR

Capítulo 2: Footprinting y Reconocimiento

- **2.1** Concepto de Footprinting
- **2.2** Footprinting Pasivo
  - **2.2.1** Google hacking
  - **2.2.2** Whois
  - **2.2.3** Shodan
  - **2.2.4** Redes sociales
  - **2.2.5** Pipl
  - **2.2.6** Otras herramientas en linea
- **2.3** Footprinting Activo
  - **2.3.1** DNS Discovery
  - **2.3.2** Banner Grabbing (netcat,amap)
  - **2.3.3** SMTP
  - **2.3.4** Netbios
  - **2.3.5** SNMP
  - **2.3.6** LDAP
- **2.4** Mirroring Web Sites
- **2.5** Rastreando e-mails
- **2.6** Maltego
- **2.7** Contramedidas

Capítulo 3: Scanning Networks

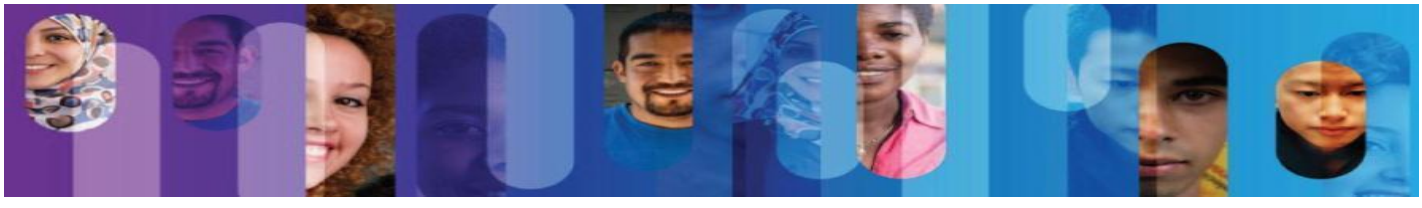
- **3.1** Concepto
- **3.2** Metodología de Scanning
- **3.3** Fundamentos de TCP/IP
- **3.4** NMAP
  - **3.4.1** Técnicas de Scanning
  - **3.4.2** Banner Grabbing
  - **3.4.3** Identificación de Sistemas Operativos
  - **3.4.4** Zenmap
- **3.5** UnicornScan
- **3.6** Detectando Firewalls
  - **3.6.1** Firewalk
- **3.7** War dialing
- **3.8** Graficando topologías de red
- **3.9** IP Spoofing
- **3.10** Hping2 / Hping3
- **3.11** No escanear estos rangos
- **3.12** Contramedidas

Capítulo 4: Buffer Overflow (Teórico: 2 Horas – Practico: 3 Horas)

- **4.1** Arquitectura de un Ordenador
- **4.2** Entendiendo los Buffer Overflows (BoF)
  - **4.2.1** Stack-Based Buffer Overflow
  - **4.2.2** Heap-Based Buffer Overflow
- **4.3** OllyDbg Debugger
  - **4.3.1.** Análisis de BoF en una Aplicación Real
  - **4.3.2.** Smashing the Stack
- **4.4** Mutando un Exploit de Buffer Overflow
- **4.5** Identificación de Buffer Overflow
  - **4.4.1.** Fuzzing
- **4.6** Defendiéndose contra Buffer Overflows
- **4.7** Contramedidas
- **4.8** Buffer Overflow en Pen Testing

Capítulo 5: Utilizando Exploits Existentes

- **5.1** Shells y Reverse Shells
  - **5.1.1** Jugando con Netcat
- **5.2** Utilizando Exploits Públicos
  - **5.2.1** Exploits en Backtrack
  - **5.2.2** Exploits en la Web
- **5.3** Metasploit
  - **5.3.1** Arquitectura
  - **5.3.2** Exploits
  - **5.3.3** Payloads
  - **5.3.4** Módulos Auxiliares
  - **5.3.5** Meterpreter
- **5.4** Otros Frameworks de Explotación



Capítulo 6: Ataques a Passwords

- **6.1** Online Password Attacks
  - **6.1.1** Hydra
  - **6.1.2** Medusa
  - **6.1.3** Cain y Abel
- **6.2** Offline Password Attacks
  - **6.2.1** Windows SAM
  - **6.2.2** Windows Hash Dumpling
    - **6.2.2.1** PWDump
    - **6.2.2.2** FGDump
  - **6.2.3** John the Ripper
  - **6.2.4** L0phtCrack / Cain y Abel
  - **6.2.5** Rainbow Tables
  - **6.2.6** Ophcrack
- **6.3** Ataques Pass the hash
- **6.4** Password profiling (CeWl)
- **6.5** Ataques de Acceso Físico
  - **6.5.1** Windows
  - **6.5.2** Linux
  - **6.5.3** Dispositivos de Red

Capítulo 7: Vulnerabilidades Web

- **7.1** Protocolo HTTP
- **7.2** Arquitectura de un Servidor Web
- **7.3** Footprinting de Webservers
- **7.4** Parameter Tampering
  - **7.4.1** Tamper Data
  - **7.4.2** Burp Proxy
  - **7.4.3** Paros Proxy
- **7.5** XSS
- **7.6** CSRF
- **7.7** PathTraversal
  - **7.7.1** Null Byte Attack
- **7.8** OS Command Injection
- **7.9** LFI/RFI
- **7.10** Information Disclosure
- **7.11** SQL Injection
- **7.12** Directory/File Bruteforcing
  - **7.12.1** Dirb
  - **7.12.2** Dir Buster
- **7.13** Nikto
- **7.14** OWASP Top10

Capítulo 8: Malware

- **8.1** Troyanos
  - **8.1.1** Definición

8.1.2 Maneras en que un Troyano Infecta un Equipo
8.1.3 Técnicas de Evasión de Anti-Virus
8.1.4 Tipos de Troyanos
8.1.5 Wrapping
8.1.6 Detección de Troyanos
8.1.7 Contramedidas
8.2 Backdoors
8.3 Viruses
8.3.1 Definición
8.3.2 Estadísticas Mundiales
8.3.3 Ciclo de Vida de un Virus
8.3.4 ¿Por qué se Crean Virus?
8.3.5 Maneras en que un Virus Infecta un Equipo
8.3.6 Virus Hoaxes
8.3.7 Tipos de Virus
8.3.8 Escribiendo un Virus Sencillo
8.3.9 Métodos de Detección
8.4 Gusanos / Worms
8.4.1 Diferencias con un Virus
8.4.2 8.4.2. Ejemplo de Gusano: Conficker
8.5 Covert Channels
8.6 Spyware
8.7 Keyloggers
8.8 Servicios de Análisis de Malware en Línea
8.9 Contramedidas de Malware
8.10 Herramientas Anti-Virus

Capítulo 9: Wargame

DURACIÓN

50 Horas