ZERO

SEGURIDAD INFORMÁTICA

Hola a todos, el equipo de Zero Seguridad Informática tiene a su disposición este curso presencial de Python abordando los temas que a continuación se describirán.

Certificación de Hacking con Python

1.- Introducción al lenguaje Python

- .- Configuración del laboratorio
- .- Primer programa en Python
- .- Tipos de datos (Strings, Int, Float)
- .- Operadores con Python (Booleanos, aritméticos, relacionales, lógicos)
- .- Entrada de datos, condicionales y loops (raw_input, if, elif, while y for)
- .- Estructuras de datos (Listas, Tuplas, Diccionarios y list comprehension)

2.- Manejo intermedio del lenguaje Python

- 2.1 Repaso de la unidad anterior
- 2.2 Manejo de ficheros con Python (Escritura, lectura y adición)
- 2.3 Manejo de funciones (Uso de funciones, argumentos en funciones)
- 2.4 Introducción a la programación orientada a objetos (Manejo de clases y decoradores)
- 2.5 Manejo de errores (Try, Except, Finally)
- 2.6 Módulos y paquetes

3.- Uso avanzado de Python

- 3.1 Repaso de la lección anterior
- 3.2 Introducción al Hacking con Python
- 3.3 Interacción con sitios web (métodos HTTP, detección de headers, envió de datos por POST, interacción con formularios)
- 3.4 Interacción de CMS (Enumeración de temas instalados, Usuarios de Wordpress, temas, versiones, versiones de Joomla)
- 3.5 Interacción con registros (Información de zonas DNS, Fuerza bruta a los DNS, Whois desde Python, reverse ip lookup, detección de cloudflare)

4.- Uso avanzado de Python parte 2

- 4.1 Repaso de la lección anterior
- 4.2 Interacción con sistemas operativos (Modulo OS, Ejecución de comandos, interpretación de salidas, extracción de información, creación de gusanos)
- 4.3 Trabajo con el módulo socket para el desarrollo de Malware (Recolección de banners, modelo client-server, desarrollo de backdoors y funciones avanzadas)
- 4.4 Interactuando con Shodan desde Python (Información de hosts, búsquedas masivas e incorporación de argumentos)

5.- Uso avanzado de Python parte 3

- 5.1 Repaso de la lección anterior
- 5.2 Nmap y Python (Incorporación de nmap con Python para el scaneo de redes)
- 5.3 Ataques de fuerza bruta a servicios FTP y SSH
- 5.4 Password Cracking (Fuerza bruta a hashes, uso de HASHLIB, ataque online y offline con diccionarios)
- 5.5 Introducción al web scrapping (Manejo de el modulo RE & BS4)

6.- Modo Ninja con Python

- 6.1 Repaso de la lección anterior
- 6.2 Creación de keyloggers con Python (Registro de pulsaciones, envió remoto de logs, ejecución en segundo plano)
- 6.3 Explotación de vulnerabilidades web (LFI & RFI)
- 6.4 Ataques en redes locales con Scapy (ARP Spoofing, Escaners de red, Sniffers FTP & HTTP)

7.- Despedida

- Entrega de certificados

El costo total de duración en horas se tiene estimado en 1 semana tomando 4 horas diarias, los reconocimientos que otorguemos contarán con validez oficial por parte de la UTNA(Universidad Tecnológica del Norte de Aguascalientes)