BOOTCAMP CIBERSEGURIDAD

RED TEAM OPS DEVELOPER

Spartan-Cybersecurity

ADVERTENCIA

Todos los derechos reservados. Ninguna parte de esta publicación, en su totalidad o en parte, puede ser reproducida copiada, transferida o cualquier otro derecho reservado a su propietario, incluyendo la fotocopia y cualquier otra copia, cualquier transferencia o transmisión utilizando cualquier red u otros medios de comunicación, cualquier emisión para el aprendizaje a distancia, en cualquier forma o por cualquier medio, como cualquier sistema de almacenamiento, transmisión o recuperación de información, sin autorización escrita del autor.

TODO nuestro contenido publicado se realiza con fines educativos, informativos y éticos.

TODAS las técnicas expuestas en este curso son desarrolladas y ejecutadas en entornos controlados.

¡NO SOMOS RESPONSABLES DEL MAL USO QUE LE PUEDAN DAR!

TABLA DE CONTENIDO

    e. Fuerza bruta HTTP, autenticación básica
    f. Call Windows API
    g. FindProcess
    h. Compilación cruzada
        i. Linux
        ii. Windows
6. Proccess injection
    a. CreateThread
        i. VirtualAlloc
        ii. WaitForSingleObject
        iii. VirtualProtect
        iv. RtlCopyMemory
    b. CreateRemoteThread
        i. VirtualAllocEx
        ii. WriteProcessMemory
        iii. VirtualProtectEx
        iv. CreateRemoteThreadEx
    c. ntdll.dll
        i. Banana Syscall
        ii. NtOpenProccess
        iii. NtAllocateVirtualMemory
        iv. NtWriteVirtualMemory
        v. NtCreateThreadEx
7. SPAWN
    a. cmd
    b. powershell
8. Persistencia
    a. startup
    b. registro
    c. task scheduler
    d. PE
    e. DLL

9. Generador de ShellCode
    a. Argumentos
    b. Integración con donut
    c. Codificación y cifrado
10. ShellCode Runner
    a. Shell Loader (Basic)
    b. Shell Loader (Cypher)
    c. Syscalls
11. Diseño DLL Maliciosas
    a. Compilación GCC(CGO)
    b. Validación de DLL exportadas
    c. RunDLL
12. Técnicas de evasión
    a. Padding bytes,
    b. Patch ETW
    c. Patch AMSI
    d. Ofuscación
    e. Cifrado
13. Redirector HTTP
14. Proyecto C2 en HTTP
    a. Conexión cliente-servidor
    b. Reconocimiento S.O.
    c. ScreenShot
    d. Persistencia
    e. Multicliente
    f. Redirector

15. Proyecto Shell reverse en HTTPS
    a. Contexto
    b. Conexión cliente-servidor
    c. Generación de certificados
    d. Instalación de certificados
    e. Reconocimiento S.O
    f. ScreenShot
    g. Persistencia
    h. Proxy inverso
16. Proyecto Shell reverso TCP
    a. Conexión cliente-servidor
    b. Conexión cifrada
17. Técnicas Anti-VirtualMachine
18. Proyecto Desarrollo de Dropper
    a. Validación del entorno (S.O., AVS, MaquinaVirtual)
    b. Checker de conectividad
    c. Descarga de implante
19. Laboratorio post-explotación
    a. Reconocimiento
    b. Log4shell
    c. Evasión
    d. Pivote
    e. Fuerza Bruta
    f. Persistencia

DETALLES DEL CURSO

Fecha de inicio: 2022/11/01

Sesiones en vivo: 8:00 pm a 9:30 pm (CO).

Si no puedes asistir se entrega clase grabada más recursos.

Duración: Entre 10 y 13 clases de 1 hora y 30 minutos por sesión.

Material entregable:

- Guía PDF
- Entorno de Laboratorio con 4 Máquinas Virtuales
- Certificado verificado en línea
- +7 horas de contenido adicional de cursos previos de desarrollo

Requisitos mínimos del sistema:

- 12 GB RAM
- Procesador Core i5 o superior
- Espacio en disco duro 120 GB
- Virtualización VMware

Costo del curso: $150 USD

Comunícate con el área de ventas:

Whatsapp: https://wa.link/j265a0

Telegram: https://t.me/Spartan_Cybersecurity

CUPOS LIMITADOS.