



Desarrollo de Malware

CURSO RED TEAM OPS DEVELOPER FOR SENIORS

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

1. Introducción al CURSO INTERMEDIO DE DESARROLLO DE MALWARE PARA REDTEAM
2. Configuración del entorno de desarrollo.
 - a. GoLand IDE
 - b. Instalación de Go (Linux - Windows)
 - c. MinGW-W64 GCC Compiler Installation
3. Programación en GO básica
4. Programación en GO para RedTeam
 - a. Trabajando con archivos (leer, escribir, comprimir, mover, borrar, enumeración)
 - b. Byte array para shellcode
 - c. Criptografía
 - i. Ofuscación
 - ii. Hash
 - iii. Cifrado (AES256, XOR)
 - iv. Codificación (b64, b32, Hex)
5. Redes
 - a. TCP sockets
 - i. Port scanner
 - ii. Cliente-servidor
 - b. UDP cliente-servidor
 - i. Servidor DNS
 - c. HTTP cliente-servidor
 - i. Ejemplo práctico servicio REST
 - ii. Métodos: GET, POST, PUT, DELETE, OPTIONS, HEAD
 - iii. DownloadString
 - d. HTTPS cliente-servidor
 - i. Generación de certificados
 - ii. Instalación de certificados



- e. Fuerza bruta HTTP, autenticación básica
 - f. Call Windows API
 - g. FindProcess
 - h. Compilación cruzada
 - i. Linux
 - ii. Windows
6. Process 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. NtOpenProcess
 - 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



Material entregable:

- ✓ Acceso a más de 20 horas de contenido en MATERIAL GRABADO.
- ✓ Libro PDF de +150 páginas.
- ✓ Acceso a laboratorio con 4 máquinas virtuales.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ Certificado del RTOD-100 por parte de Spartan-Cybersecurity.

Costo del curso: \$150 USD

Comunícate con el área de ventas para conocer nuestros descuentos:

WhatsApp: <https://wa.link/j265a0>

Telegram: https://t.me/Spartan_Cybersecurity

Te esperamos 🤖