



RED TEAM DEVELOPMENT COMMAND AND CONTROL

Spartan-Cybersecurity



RTDC-300



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

Módulo 1: Implementación del Entorno de Desarrollo

- ❖ Configuración del entorno de desarrollo: Herramientas, IDEs, y lenguajes de programación.
- ❖ Introducción al stack tecnológico: Golang, MongoDB, WebSocket, SSL/TLS.
- ❖ Generación de certificados SSL: Creación y gestión de certificados para la comunicación segura.
- ❖ Configuración de herramientas de desarrollo auxiliares y de testing.

Módulo 2: Introducción al C2

- ❖ Fundamentos de los sistemas de Comando y Control (C2).
- ❖ Arquitectura y componentes clave de un sistema C2.
- ❖ Consideraciones legales y éticas en el uso de sistemas C2.
- ❖ Diferencias entre un C2 personalizado contra un Cobalt Strike.

Módulo 3: Desarrollo y Seguridad del Agente

- ❖ Inicialización del agente: ID, claves, y comunicación segura.
- ❖ Implementación de SSL/TLS y cifrado híbrido para la seguridad de la transmisión.
- ❖ Recopilación y envío seguro de información del sistema.

Módulo 4: Funcionalidades Avanzadas del Agente

- ❖ Técnicas de captura de pantalla y exfiltración de datos.
- ❖ Ejecución remota de comandos y detección de entornos virtuales.
- ❖ Uso de proxy SOCKS5 y técnicas de pivoting



Módulo 5: Implementación del Servidor C2

- ❖ Configuración del servidor en EC2 y protección con Cloudflare.
- ❖ Gestión de SSL y estrategias de seguridad avanzadas.
- ❖ Implementación de headers HMAC para la autenticación y la integridad de los datos.

Módulo 6: Comunicación y Gestión de Datos

- ❖ Gestión de múltiples agentes y comunicación mediante WSS.
- ❖ Uso de MongoDB para el almacenamiento y análisis de datos.
- ❖ Implementación y gestión de tokens para el control de acceso.

Módulo 7: Seguridad y Firma de Claves

- ❖ Procedimientos para la firma y verificación de claves públicas.
- ❖ Configuración de alertas y monitorización de la actividad del sistema.
- ❖ Prácticas de seguridad para la evasión de detecciones y análisis forenses.

Módulo 8: Desarrollo de la Interfaz de Usuario

- ❖ Implementación de la interfaz de consola con **tcell** y **promptui**.
- ❖ Creación de menús y controles interactivos para la gestión del sistema C2.
- ❖ Visualización y análisis de la actividad en la red de agentes desde la consola.



Módulo 9: Autenticación y Control de Acceso

- ❖ Desarrollo de un sistema de login para el acceso al C2.
- ❖ Implementación de mecanismos de bloqueo y políticas de seguridad para la autenticación.
- ❖ Estrategias para la gestión segura de credenciales y sesiones de usuarios.

Módulo 10: Testing y Análisis

- ❖ Pruebas de penetración y testing de seguridad con Burp Suite.
- ❖ Simulación de ataques y defensa para evaluar la robustez del sistema.
- ❖ Estrategias para la identificación y corrección de vulnerabilidades.

Módulo 11: Implementación de C2 en Cloud

- ❖ Comprensión de los beneficios y desafíos de implementar sistemas C2 en entornos cloud.
- ❖ Despliegue efectivo de un Command and Control en una infraestructura cloud.

Módulo 12: Conclusión y Perspectivas Futuras

- ❖ Recapitulación de mejores prácticas y estrategias clave en desarrollo y operación de sistemas C2.



DETALLES DEL CURSO

Fecha de inicio: 2024/06/03

Sesiones en vivo: 19:00 a 20:30 (GMT-5).

Si no puedes asistir se entrega clase grabada más recursos.

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

Material entregable:

- ✓ Acceso al código fuente de cada proyecto.
- ✓ Acceso a más de 15 horas de contenido EN VIVO.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ Certificado del RTDC-300 por parte de [Spartan-Cybersecurity](https://www.spartan-cybersecurity.com).

Costo del curso: \$200 USD

Comunícate con el área de ventas:

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

Telegram: https://t.me/Spartan_Cybersecurity

CUPOS LIMITADOS.