



CURSO PROFESIONAL DE PENTESTING CONTRA ACTIVE DIRECTORY

Spartan-Cybersecurity



CPAD-100



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. CURSO DE PENTESTING CONTRA DIRECTORIO ACTIVO
2. Introducción a Active Directory
3. Enumeración sobre un AD
 - a. Introducción a Powershell
 - b. Enumeración de recursos compartidos
 - c. Introducción a PowerView
 - i. Enumerando usuarios
 - ii. Enumerando grupos
 - iii. Enumerando Computadoras
 - iv. Enumerando ACL del dominio
 - v. Enumerando GPO
 - vi. Enumerando bosques y relaciones de confianza
 - d. Enumeración con ADPeas
 - e. Enumeración con Microsoft.ActiveDirectory.Management.dll
 - f. Introducción a PowerUp
 - g. Introducción a BloodHound
4. Introducción a la escalación de privilegios local en Windows
 - a. Enumeración manual
 - b. Enumeración con WinPEAS
 - c. Enumeración sobre mecanismos de seguridad en Windows
 - i. Introducción a User Account Control – (UAC)
 - ii. Introducción a AppLocker
 - iii. Introducción a Credential Guard
 - iv. Introducción a Antivirus y AMSI
 - v. Introducción a SYSMON
 - d. Búsqueda de credenciales
 - e. Identificando y abusando de vulnerabilidades en el Kernel
 - f. Identificando y abusando de permisos inseguros en servicios
 - g. Identificando y abusando de Unquoted Service Path
 - h. Identificando y abusando de Tokens de Acceso en Windows



5. Movimiento lateral en entornos Windows
 - a. PowerShell remoting – WinRM
 - b. Psexec
 - c. WMI
 - d. RDP Hijacking con tscon
6. Transferencia de archivos en entornos Windows
 - a. Utilizando HTTP
 - b. Utilizando SAMBA
7. Capturando y crackeando Net-NTLMv2/NTLMv2 hashes
8. Ataques de relaying
 - a. SMB Signing Deshabilitado
9. Password spraying
 - a. Fuerza bruta sobre Kerberos pre-auth
 - b. Fuerza bruta con diccionarios personalizados
 - c. Fuerza bruta sobre RDP
10. Identificando y abusando malas configuraciones en Kerberos
 - a. Detectando información sensible en atributos
 - b. Ataque Kerberoasting
 - c. Ataque ASRepRoasting
 - d. Pass The Hash
 - e. OverPass the Hash
 - f. Ataque Constrained Delegation – (Computadora y Usuario)
 - g. Ataque Unconstrained Delegation
 - h. Ataque Constrained Delegation basado en recurso
 - i. Abusando de ACL
 - i. Write ACL sobre usuario
 - ii. Write ACL sobre computadora
 - iii. Write ACL sobre grupo
 - iv. Write ACL sobre GPO
 - v. WriteDACL sobre el dominio
 - j. Abusando del grupo de DNS Admins



11. Post-Explotacion en Kerberos
 - a. Pass The Ticket
 - i. Silver Ticket
 1. Utilizando CIFS
 2. Utilizando Scheduled Tasks
 3. Utilizando WinRM
 4. Utilizando PowerShell Remoting
 5. Utilizando WMI
 - ii. Golden Ticket
 - b. Abuso de relaciones de confianzas entre dominios
 - c. Extracción total de credenciales del Active Directory
 - i. Extracción de hashes desde ntds.dit
 - ii. Usando Mimikatz DCSync
 - iii. Usando Mimikatz sekurlsa
 - iv. Cracking de hashes de NTLM con hashcat
12. Explotación de ZeroLogon sobre un Active Directory



DETALLES DEL CURSO

Fecha de inicio: 2023/11/06

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 a laboratorio durante 1 mes.
- ✓ Acceso a más de 20 horas de contenido EN VIVO.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ Certificado del CPAD-100 por parte de Spartan-Cybersecurity.

Costo del curso: \$200 USD

Comunícate con el área de ventas:

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

Telegram: https://t.me/Spartan_Cybersecurity

CUPOS LIMITADOS.