CURSO DE PENTESTING CONTRA LA NUBE DE AZURE Y OFFICE 365

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

16) Introducción a Microsoft Identity Services
    a) Microsoft Active Directory (Microsoft Ad)
    b) Microsoft Active Directory Federated Services (Ad Fs)
    c) Azure Active Directory (Azure Ad)
    d) Azure Active Directory Domain Services (Azure Ad Ds)
    e) Diferencias entre Active Directory VS Azure AD
17) Pentesting Azure Active Directory (Azure Ad)
    a) Enumeración Manual de Azure Ad
        i) Enumerando Recursos
        ii) Enumerando Roles
        iii) Enumerando Usuarios
        iv) Enumerando Grupos
        v) Enumerando Dispositivos
        vi) Enumerando Enterprise Applications
    b) ¿Qué es el control de acceso basado en rol de Azure (RBAC)?
        i) Identificando los usuarios y roles más privilegiados dentro de un tenant
    c) Enumeración utilizando Tokens sobre APIs - MS Graph
        i) Azure API via Powershell
        ii) Azure API via Python Version
18) Extraccion de credenciales almacenadas en un Automation accounts con Get-AzPasswords
19) Introducción a reglas condicionales de acceso
    a) Evasión sobre reglas condicionales de acceso
20) Introducción a Azure Blob Storage
    a) ¿Qué es un Storage Account?
    b) ¿Qué Es Azure Blob Storage?
    c) ¿Qué Es Un Block Blobs?
    d) ¿Qué Es Un Append Blobs?
    e) ¿Qué Es Un Page Blobs?
    f) ¿Qué Son Los Azure Storage Security Features?

21) Pentesting contra Azure Blob Storage
    a) Enumeración Manual de Azure Blob Storage
        i) Enumerando Azure Blob Storage Con MicroBurst
        ii) Enumerando Azure Blob Storage por medio de una URL SAS
        iii) Identificando información sensible alojada en Container y Shares de Azure Storage Account
22)Introducción a Azure Functions
    a) ¿Qué Es Una Función de Azure Functions?
    b) ¿Qué Lenguajes Admite Azure Functions?
    c) ¿Qué Tipo de Código Puede Ejecutarse En Azure Functions?
23)Pentesting Azure Functions
    a) Enumeración Manual de Azure Functions
        i) Enumerando Azure Functions
    b) Casos de Estudio
        i) Post-Explotación sobre un Azure Functions luego de un RCE
24) Introducción a Azure Web App Services
    a) ¿Qué Es Una App Service?
    b) Sistemas operativos utilizados por un App Service
    c) Lenguajes de programación compatibles para desarrollar un App Services
25)Pentesting Azure Web App Services
    a) Enumeración de Azure Web App Services
        i) Enumerando App Service
    b) Casos de Estudio
        i) Post-Explotacion Sobre Web App Services luego de obtener un webshell
26) Introducción a Azure Vms – (Azure Virtual Machines)
    a) ¿Qué Es Una Instancia Vm?
    b) ¿Qué Es Un Grupo de Seguridad de Vms?
    c) ¿Qué Es Un Backdoor?
        i) ¿Cómo Backdorizar Una Instancia Vms?

27)Introducción a Azure Key Vault
   a) ¿Qué Datos Confidenciales Puede Administrar Azure Key Vault?
28) Pentesting Azure Key Vault
   a) Enumeración Manual de Azure Key Vault
      i) Enumerando Azure Key Vault
      ii) Extracción de datos sensibles después de un acceso inicial
29) Pentesting Azure Virtual Machines (Vms)
   a) Enumeración Manual de Azure Vms
      i) Enumerando Instancias
   b) Casos de Estudio
      i) Post-Explotacion abusando del permiso Microsoft.Compute/virtualMachines/runCommand/action por medio de RunPowerShellScript
      ii) Post-Explotacion abusando de los privilegios sobre Intunes Administration
30) Movimiento lateral en la nube
   a) Realizando la técnica Pass The PRT para migrar una sesión en Windows hacia el portal web de Azure y hacer un bypass del MFA
31) Phising contra usuarios de Office365
   a) Ataque illicit Consent Grant – 365Stealer
32)Introducción a Azure virtual network (VNET)
   a) ¿Cuáles son los componentes de Azure vnet?
   b) ¿Cómo puedo proteger las instancias vms que se ejecutan en mi vnet?
   c) ¿Qué diferencias existen entre los grupos de seguridad que están en una VNET y las ACL de red de una vnet?

33) Pentesting hacia VNET
   a) Enumeración Manual de Vnet
      i) Enumerando Vnet
      ii) Identificando la configuración del networking de los componentes de azure
   b) Casos de Estudio
      i) Utilizando nuestros privilegios para manipular reglas de entrada de Azure Firewall y tener acceso servicios desplegados en una VM
34) Pentesting Contra Arquitectos de Azure
   a) Exfiltración de Credenciales Dentro de Un Repositorio de Github
35) Análisis de Vulnerabilidades Con Herramientas Automatizadas
   a) Utilizando Scout Suite
   b) Utilizando powerzure
   c) Detectando información sensible en Deployment Template
36) Introducción A Blue Team En Azure
   a) Azure Web Application Firewall
   b) Azure Security Center.
   c) Azure Bastion.
   d) Azure Sentinel.
37) Post-explotacion en Active directory sincronizados con Azure
   a) Extracción de credenciales sobre Azure AD Connect
      i) DCSync utilizando el usuario MSOL
      ii) Silver Ticket utilizando AZUREADSSOACC
38.) Técnicas de persistencia en Azure AD
      iii) Creando cuentas de Azure AD
      iv) Creando una cuenta de invitado al Tenant

DETALLES DEL CURSO

Material entregable:

- ✓ Acceso a más de 20 horas de contenido en MATERIAL GRABADO.
- ✓ Libro PDF de 300 páginas.
- ✓ Acceso a laboratorio vulnerable para practicar durante 1 mes.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ Certificado del CPAZ por parte de Spartan-Cybersecurity.

Costo del curso: $200 USD

Comunícate con el área de ventas para conocer nuestros descuentos:

WhatsApp: https://wa.link/j265a0

Telegram: https://t.me/Spartan_Cybersecurity

CUPOS LIMITADOS.