STEALING THE CROWN – ADVANCED RED TEAM ADVERSARY OPERATIONS AND TACTICS

Trainers: Javier Antúnez & Diego Bruno

Descripción general:

En este entrenamiento explicaremos Técnicas, Tácticas y Procedimientos (TTPs) actuales para infiltrarse en las redes, mantener persistencia, moverse lateralmente e ir escalando hasta conseguir los objetivos buscados dentro de la red.

Para aquellos dedicados al pentesting y que quieren acercarse al Red Teaming, permite conocer las técnicas tácticas y procedimientos (TTPs) utilizados por atacantes reales.

Todo el training se hará emulando una campaña de red team sobre una organización real simulada, operando a través de herramientas de command and control (C2) como ocurriría en un escenario real. En algunos casos nos valdremos también de ataques file less y herramientas externas al C2 para completar el toolset.

Comenzaremos desde una situación de compromiso inicial de un equipo, iremos aplicando lo aprendido hasta comprometer diferentes servidores, utilizando técnicas diversas de compromiso, persistencia, movimiento lateral y escalamiento de privilegios locales y de red.

Los ataques mostrados se basan puramente en funcionalidad y configuraciones comunes en redes Active Directory, por lo que no estaremos atados a utilizar de vulnerabilidades que dependan de parches faltantes en la red víctima, es decir que todo lo aprendido nos permitirá atacar incluso redes que tienen todos los parches al día.

En nuestra opinión, una de las mejores formas de realizar ataques exitosos es entender cómo funcionan los objetivos, que herramientas hay disponibles y cuales podemos modificar por nuestra cuenta para aprovechar debilidades y funcionalidades de los sistemas AD.

Por esto, se explicarán los conceptos necesarios para comprender el funcionamiento de las técnicas y ataques, para luego aplicarlas y verlas en acción y sobre un entorno de laboratorio controlado. Este enfoque te permitirá entender qué está sucediendo, más allá de que herramienta estés utilizando.

Temario:

Algunos de los temas tratados serán:

- Conceptos generales
- Introducción de Arquitectura del S.O.
- Active Directory Kill chain
- Compromiso inicial
- Creación de payloads
- Persistencia local
- Reconocimiento local
- Compromiso de credenciales locales
- Escalamiento de privilegios
- Reconocimiento de red y dominio
- Ejecución remota y Movimiento lateral
- Abuso de ACLs de active directory
- Ataques de kerberos
- Persistencia en Active Directory

Conocimientos previos:

Este es un curso para personas con conocimientos en seguridad de la información que busquen ganar conocimientos y habilidades en el campo de red team. Como prerrequisitos, los asistentes deben tener conocimientos básicos y entendimiento claro de:

- Administración de Servidores Windows.
- Active Directory
- Scripting y programación (Powershell -C# puede ser beneficioso-)
- Protocolos de red
- Group Policy Objects.
- Uso de herramientas de virtualización en escritorio (VMWare)

Equipamiento necesario:

- Notebook con procesador i5 o superior (o equivalente).
- Soporte de virtualización habilitado (Intel VT o AMD-V).
- Memoria RAM 8 GB o superior
- 60 GB de espacio en disco

Nota: si la notebook no cuenta con sistema operativo Windows (ej: Linux o MacOS) el equipo debe tener suficiente memoria RAM como para ejecutar una VM adicional con Windows 10 (aproximadamente 4GB adicionales sobre el requerimiento mínimo -recomendamos 16 GB de RAM para una experiencia más cómoda-).

Reservá tu lugar

Costo:

USD 2.000

Reservá tu lugar

CONSULTAS

Para realizar consultas sobre el training o alguno de sus beneficios, escribir a: capacitacion@ekoparty.org

Trainers:

Javier Antúnez

Desde el año 1999 se dedica al área de Seguridad Informática, donde se ha desempeñado en cargos como Administrador, Auditor y Analista, y como consultor independiente para empresas de primer nivel. Es Licenciado en Sistemas por la Universidad de Morón, CRTP (Certified Red Team Professional), CISSP (Certified Information Systems Security Profesional), CARTP (Certified Azure Red Team Professional) y Auditor Líder en ISO/IEC 27001 por TÜV Rheinland. Es egresado del Programa de Dirección en Seguridad del Capítulo Argentino de ASIS (American Society for Industrial Security).

Cuenta con experiencia en análisis y diseño de seguridad de red, revisiones de seguridad en sistemas operativos y redes, penetration testing, desarrollo de políticas y estándares de seguridad, infraestructura de clave pública, administración de firewalls, implantación y soporte de herramientas de cifrado, análisis de riesgo, capacitación y programas de concientización. También participa activamente en proyectos de desarrollo de aplicaciones web e infraestructuras basadas en SOA y automatización de controles.

Se ha desempeñado como instructor en cursos de capacitación en seguridad informática para empresas de primer nivel, y ha dictado seminarios y conferencias sobre Biometría, Desarrollo seguro de aplicaciones web, Criptografía, seguridad en Windows y las normas ISO/IEC 27001 y 27002, entre otros.

Fue socio fundador del capítulo argentino de ISSA (Information Systems Security Association), y se desempeñó sucesivamente como Vice-presidente, Presidente y Secretario del mismo. Formó parte del Consejo Argentino de Seguridad de la Información (CASI) y del capítulo Argentina de ISC2.

Diego Bruno

Se dedica al campo de la seguridad informática desde hace 10 años habiendo alcanzado además varias certificaciones internacionales a lo largo de su carrera como el CRTP (Certified Red Team Professional), CCNA (Certified Cisco Network Associate) – MCSA (Microsoft Certified System Administrator) – AS|PT (Attack-Secure Penetration Tester) y CEHv7 (EC-Council Certified Ethical Hacker) e ISO 27001:2013 Lead Auditor. Cuenta con amplia experiencia real en análisis y diseño de seguridad de red, revisiones de seguridad en sistemas operativos y redes, penetration testing y Vulnerability Assesments (VA), desarrollo de políticas y estándares de seguridad, infraestructura de clave pública, administración de firewalls, implantación y soporte de herramientas de encriptación, análisis de riesgo, capacitación y programas de concientización.

Ha trabajado tanto en su rol de consultor como así también como arquitecto y analista de seguridad en empresas de primer nivel como Visa, Citibank, HSBC, Emepa, Scania, Claro, Telefónica y varias otras.

Se ha desempeñado como instructor en cursos de capacitación en seguridad informática para empresas de primer nivel, y ha dictado seminarios y conferencias sobre Hardening de plataformas Windows, Criptografía, Ethical Hacking y seguridad en ambientes virtualizados y la familia de las normas ISO/IEC 27000 en reconocidas conferencias locales e internacionales como RiseCon, 8.8, etc.