Seguridad en Tecnologías Operacionales (SCADA, PLC)

Visión General

Conocer como un atacante puede acceder a un sistema industrial ya sea local o remotamente es importante para tomar medidas y defender mejor el perímetro, diferentes técnicas y vulnerabilidades al igual que en sistemas I.T pueden usarse para sacar provecho, en este curso los estudiantes aprenderán a evaluar como atacar y proteger estos sistemas al igual que descubrir nuevas vulnerabilidades o errores comunes de configuración en entornos industriales.
Se realizaran pruebas en servidores web al igual que otros servicios y protocolos industriales, estos laboratorios son 100% prácticos y el estudiante tendrá que evaluar y auditar estos sistemas como si estuviera en entorno real.

Introducción a las Tecnologías Operacionales

- Introducción, Procesos y roles
- Conociendo el Hardware
- PLC, HMIs, RTUs
- Protocolos de Comunicación
- Equipos de comunicación industrial
- OSINT
- Ataques en tecnologías y aplicaciones web
- Análisis de Firmware
- Evaluación

Ataques en Tecnologías web

- Fugas de información
- Acceso no autorizado / Bypass de autenticación
- Detectando y analizando posibles vulnerabilidades en aplicaciones web
- Vulnerando las aplicaciones web
- Denegaciones de servicio
- Laboratorio
- Evaluación

Equipamiento de Nuestro Laboratorio

- DELL INSPIRON 14-3467 i5-7200U 14" 8GB
- PLC

- Introducción a Protocolos Industriales
- Modbus ,SNMP
- Estableciendo comunicación mediante protocolos usando scripting en Python
- Vulnerabilidades
- Laboratorio
- Evaluación

- Manejo de incidentes
- Administración de dispositivos y contraseñas
- Políticas de seguridad
- Evaluación Final

Información General:

- **Lugar:** Apoquindo 4775, oficina 302, Las Condes, Santiago
- **Horas:** 40 hrs
- **Valor:** 22UF

cybertrust
INSPIRANDO CONFIANZA

www.cybertrust.cl

Teléfono: +562 3224 3551 | +562 3224 3552 Email: contacto@cybertrust.cl

Experiencia

Consultor en Ciberseguridad, conocido en los eventos de seguridad informática más importantes de la industria, como DEFCON, Blackhat en USA, EKOparty en Argentina el HACK.LU en Luxemburgo y Syscan360 en China.

Se le conoce por sus trabajos en investigación de seguridad en protocolos y equipo industrial.
En 2016 demostró por primera vez como un atacante remoto puede interferir en el estudio sismológico de una nación atacando directamente los sismógrafos conectados a internet.

En 2017 libero un fallo en el protocolo SNMP el cual permite a un atacante evadir el mecanismo de autenticación, el fallo afecta a ISPs de Brazil y México los cuales juntos acumulan 1 millón de cable módems afectados.

Speaker Internacional:

- 8.8 Security conference Santiago chile - Explotando y atacando redes sismológicas
- HACK.LU 2016 - Exploiting and attacking seismological networks
- Dragonjar security conference - Explotando y atacando redes sismológicas
- BlackHat ARSENAL 2016 - NetDB Project
- DEFCON 24 2016 - Exploiting and attacking seismological networks.
- Ekoparty 2015 - SSL certificate massive analysis and medical device fingerprinting
- OWASP Latin tour 2015 Costa Rica
- Syscan360 en China

Bertín Bervis
Consultor Senior en Ciberseguridad
CyberTrust