CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia cybersecurity

Formación práctica ciberseguridad OT para el sector del agua

Pere Casas
Director Cynexia Cybersecurity

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Taller práctico: Hackeando SASA

Guión

- Información pública
- Reconocimiento
- Ataque inicial
- Descubrimiento interno
- Movimiento lateral
- Explotación
- ☕
- Proceso segurización
- Recap and preguntas

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

🚨 Disclaimer del taller 🚨

- El objetivo es que comprendas cómo piensan los atacantes y cómo operan, para que así puedas defenderte mejor.

- Usaremos herramientas genéricas y accesibles, centradas en la lógica y la técnica detrás de cada ataque, no en la marca de una herramienta específica.

- El objetivo no es mostrar software, herramientas o soluciones “mágicas”.

- El verdadero poder reside en el conocimiento, no en la herramienta.

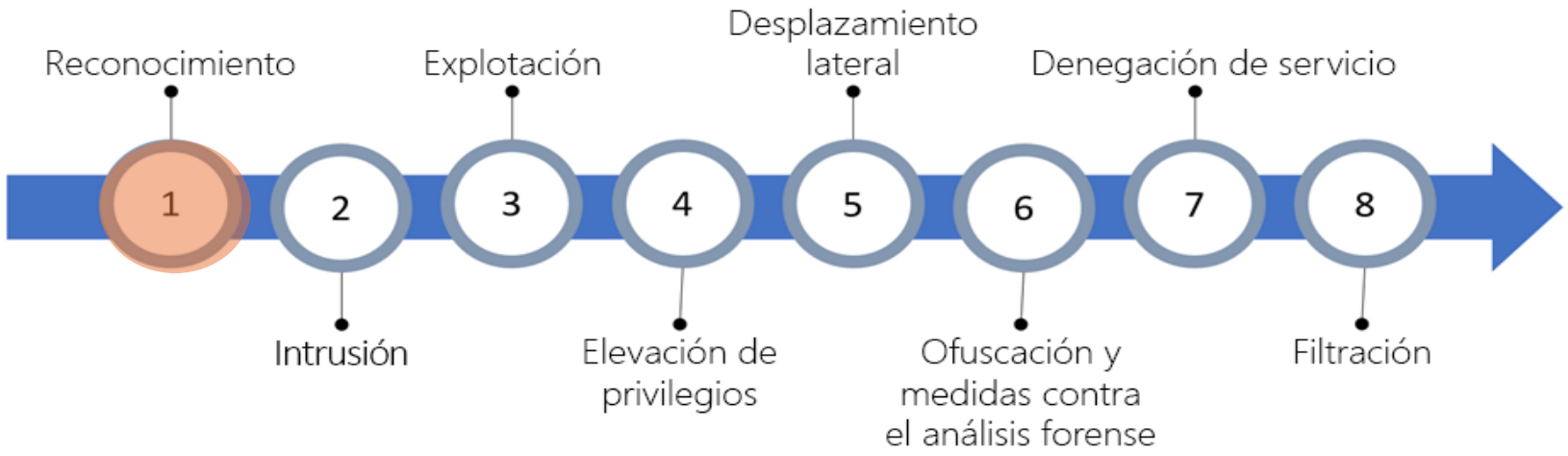
Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Anatomía de un ataque



Información publica

Empresa

- Nombre: Suministradora de Aguas SA
- Alias: SASA
- Facturación: 5M
- Objetivo: Interrumpir suministro de agua

Administrador IT

- Nombre: M.R. (alias ASAP)
- Redes sociales: No usa
- Relación: provedor externo
- Web empresa: https://cyberh2o.es/

Técnico de planta

- Nombre: Desconocido
- Información conocida:
  - Usuario HMI para visualizar KPIs ETAP
  - Administra la HMI usando su móvil conectado al WIFI

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Reconocimiento

ssid: SASA-ETAP-Privat
Pass: **********
WPA2-PSK

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CWP
CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia
cybersecurity

Esquema básico interno

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

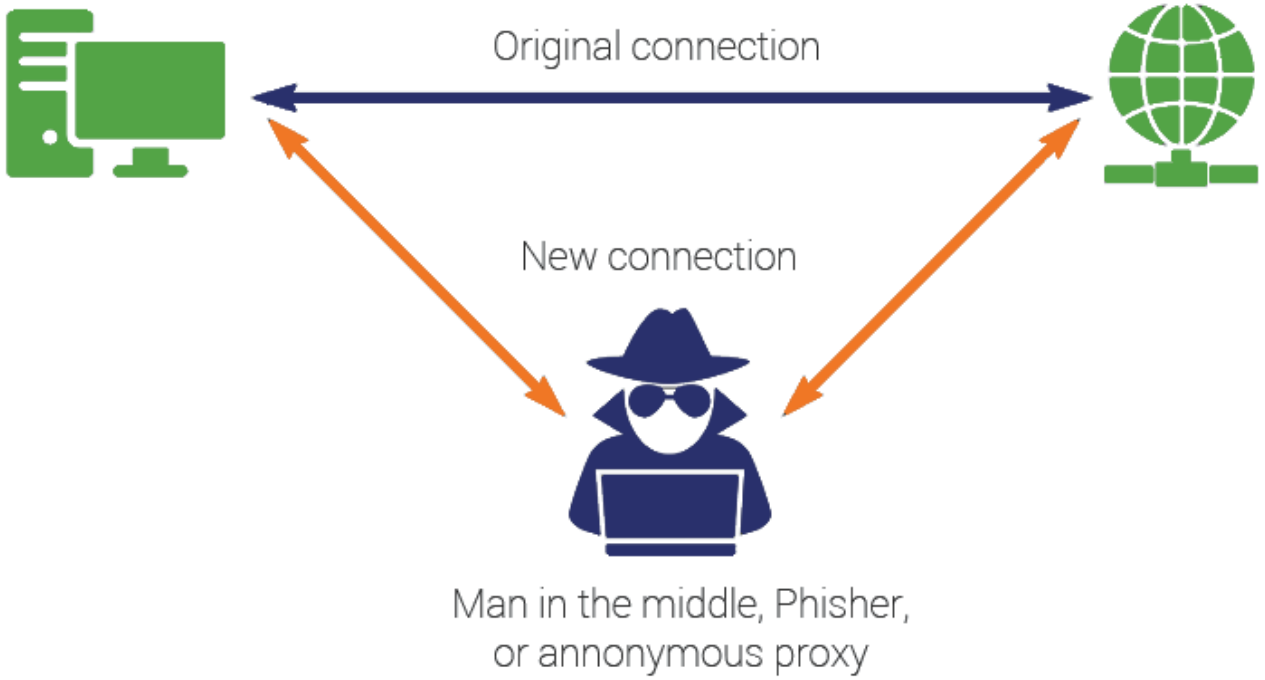
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Conceptos que aprendemos

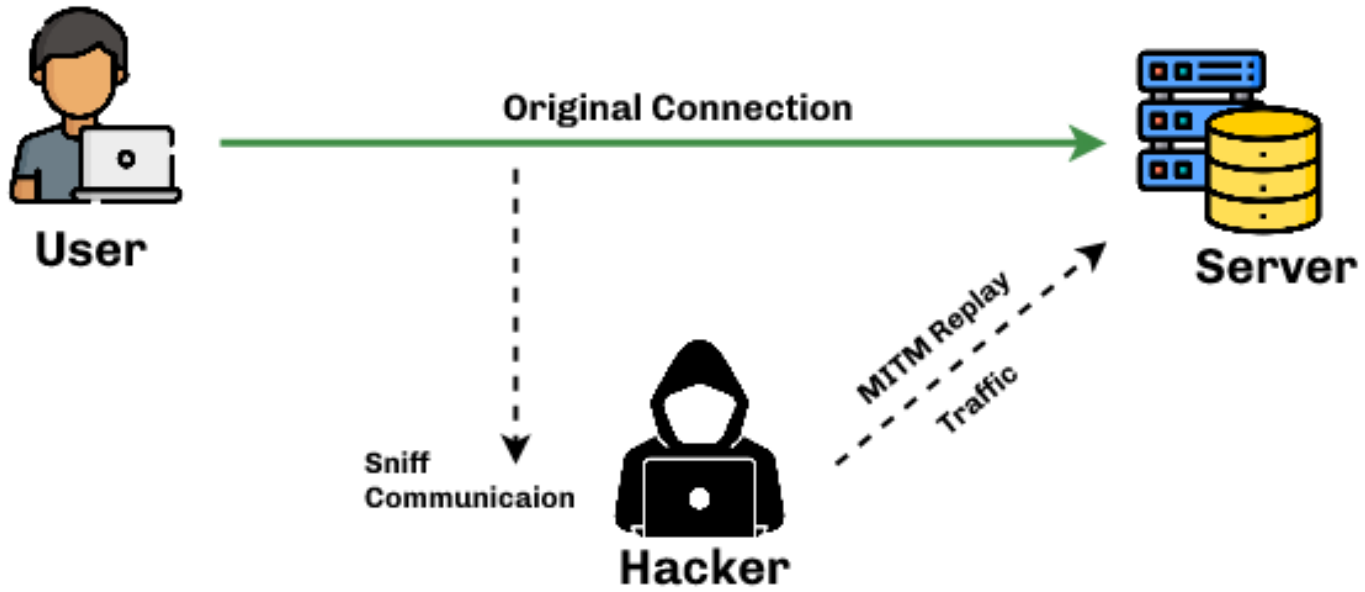
Ataques a redes Wi-Fi (WPA2)
Ataques de fuerza bruta y cracking
Pivoting entre redes
Ataques Man-in-the-Middle (MITM)
Replay attack
Fuzzing de directorios web
Inyección de comandos
Reverse Shell
Escalada de privilegios básica
Persistencia

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

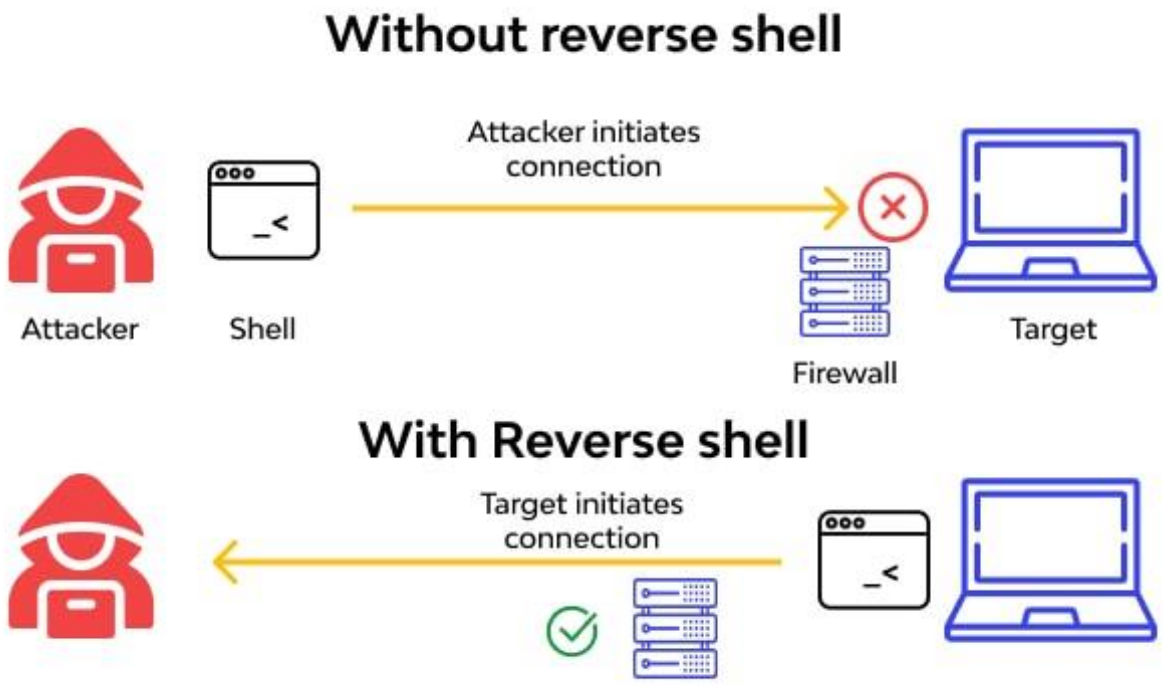
Man-in-the-Middle



Replay attack

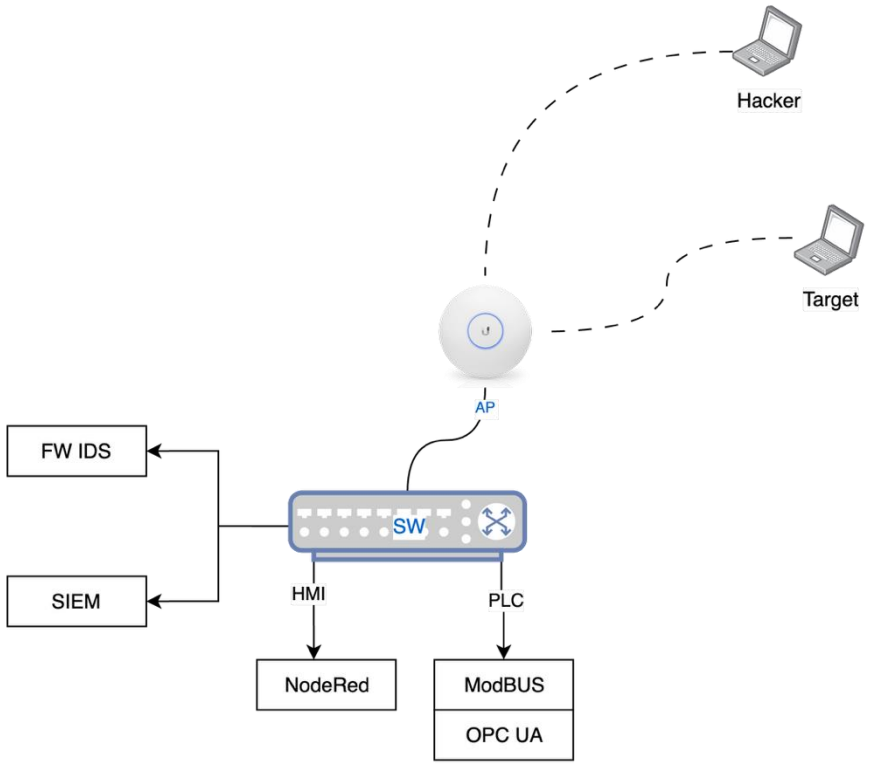


Reverse shell




ETHICAL
HACKING

Esquema final



CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CWP
CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia
cybersecurity

¡Gracias!

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD