# Tema1.1.3.4.EnriqueGomezTagle

sábado, 3 de febrero de 2024 14:39

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

**Práctica de laboratorio: Visualizar a los Hackers de Sombrero Negro**

## Instrucciones

Phishing a Empresa Financiera

## Situación 1:

a. ¿Quién es el atacante?

Ciberdelincuentes especializados en fraude financiero

b. ¿A qué organización o grupo está asociado el atacante, si lo hay?

Sindicato de Cibercrimen de Europa del Este

c. ¿Cuál es el motivo del atacante?

Obtener acceso a cuentas para robar fondos

d. ¿Qué método de ataque se utilizó?

phishing a través de correo electrónico simulando ser la entidad financiera.

e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?

Obj: el personal de la empresa

Vuln: falta de conciencia sobre seguridad e identificación de correos fraudulentos

f. ¿Cómo se podría prevenir o mitigar este ataque?

- Implementar programas de concientización sobre ciberseguridad para los empleados.
- filtros de correo
- herramientas para detectar y bloquear phishing.

**Práctica de laboratorio: Visualizar a los Hackers de Sombrero Negro**

## Situación 2:

a. ¿Quién es el atacante?

Un ciberdelincuente independiente

b. ¿Con qué organización y/o grupo está asociado el atacante?

Independiente

c. ¿Cuál es el motivo del atacante?

Extorsión económica y demanda de rescate

d. ¿Qué método de ataque se utilizó?

Ransomware, a través de una vulnerabilidad en la red.

e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?

sistemas de información del hospital

Vuln: falta de actualizaciones de seguridad

f. ¿Cómo se podría prevenir o mitigar este ataque?

- Mantener todos los SO y software actualizados y generar copias de seguridad o respaldos.
- Segmentar las redes

**Práctica de laboratorio: Visualizar a los Hackers de Sombrero Negro**

## Situación 3:

a. ¿Quién es el atacante?

Hackers expertos en robar datos de targetas de crédito.

b. ¿Con qué organización y/o grupo está asociado el atacante?

Colectivo de ciberdelincuentes

c. ¿Cuál es el motivo del atacante?

Robar información de TC para compras fraudulentas y venta de info en el mercado negro.

d. ¿Qué método de ataque se utilizó?

Ataque de Fuerza Bruta para encontrar contraseñas débiles de los usuarios.

e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?

Obj: Cuentas de usuarios en sitios de E-comerce
Vuln: contraseñas débiles y predecibles

f. ¿Cómo se podría prevenir o mitigar este ataque?

- políticas de contraseñas
- MFA / TFA
- Fail2Ban
- Monitoreo de intentos de BFA