Packet Tracer - nvestiga un panorama de amenazas

Objetivos

Parte 1: Investigar una vulnerabilidad de configuración de la red

Parte 2: investigar una vulnerabilidad de malware de suplantación de identidad (Phishing)

Parte 3: Investigar una red inalámbrica y la vulnerabilidad de DNS

Aspectos básicos/Situación

El panorama de amenazas consta de todas las vulnerabilidades que los agentes de amenazas pueden aprovechar. Cada incidente de ciberseguridad implica la explotación de vulnerabilidades por diferentes tipos de agentes de amenazas. Algunos agentes de amenazas quieren dinero, otros quieren ser famosos y otros quieren destruir información e infraestructura.

En esta actividad, investigará tres vulnerabilidades que los agentes de amenazas pueden aprovechar.

Nota: En esta actividad, tanto el centro de datos como los sitios de ISP / Telco están bloqueados.

Instrucciones

NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB O LO REALIZADO POR USTED.

Parte 1: Investigar una vulnerabilidad de configuración de la red

A veces, las vulnerabilidades de seguridad de la red pueden ocurrir por accidente. Por ejemplo, olvidarse de actualizar el software de servidor o host puede exponer vulnerabilidades conocidas que podrían mitigarse fácilmente con una simple actualización. De manera similar, pueden introducirse vulnerabilidades cuando un dispositivo de red no está configurado correctamente o un dispositivo es defectuoso. En esta parte, explorará una vulnerabilidad que resulta de un dispositivo que no está configurado correctamente con las mejores prácticas de seguridad.

Paso 1: Use una red de invitados para obtener acceso a otros dispositivos en la red.

a. En **Greenville**, ubique el **Smartphone 3** a las afueras de la ubicación de **Home**.

Mary es la dueña de este smartphone. Es amiga de Bob, quien vive en la casa. Mary está estudiando para eventualmente obtener un trabajo en defensa de ciberseguridad y está familiarizada con las pruebas de penetración de la red. Se dio cuenta de que una red inalámbrica para invitados está abierta y accesible para todos. Se conectó a la red de invitados y usó Nmap para ejecutar un análisis, que puede identificar y descubrir detalles sobre todos los dispositivos activos. Uno de los dispositivos parece ser una cámara web. Su dirección IP es 192.168.100.101.

b. Haga clic en **Smartphone 3**, y luego en **Command Prompt**. Introduzca el comando ping **192.168.100.101**. Después de uno o dos mensajes de "Tiempo de espera de solicitud agotado", los pings restantes deben ser correctos.

Mary informa a Bob que la red es muy vulnerable a los ataques. Alguien podría tomar el control de la cámara web, por ejemplo, y ver videos desde el interior de la casa. Bob invita a María a entrar, investigar el problema y proponer una solución.

Paso 2: Explore la red doméstica para identificar la vulnerabilidad.

a. Haga clic en **Home**. Sabiendo que los routers domésticos generalmente controlan las redes inalámbricas domésticas, Mary se dirige directamente a la oficina en casa y se sienta detrás del escritorio. Utilizará la **Home Office PC** para conectarse al router. Pero primero debe determinar la dirección IP.

b. Haga clic en **Home Office PC** > Pestaña **Desktop** > **Command Prompt** y escriba el comando **ipconfig**.

El gateway predeterminado es la dirección IP del **Home Wireless Router**.

¿Cuál es la dirección IP?

c. A continuación, Mary utiliza el **Web Browser** para conectarse al **Home Wireless Router**. Cierre el **Command Prompt (Símbolo del sistema)** y haga click en **Web Browser (Navegador Web)**. Ingrese la dirección IP del gateway predeterminado.

d. Bob no tiene la documentación del router ni conoce las credenciales de inicio de sesión. Mary busca el modelo de router en Internet y descubre que las credenciales predeterminadas usan **admin** tanto para el nombre de usuario como para la contraseña. Inicie sesión en el **Home Wireless Router**.

e. Haga clic en **Wireless** (Inalámbrico). Revise la **Basic Wireless Settings** para cada una de las tres radios que forman parte del router inalámbrico.

¿Cuáles de las radios están activas?

¿Cuáles son los SSID asignados a estas radios?

f. Haga clic en el submenú **Wireless Security** (Seguridad inalámbrica).

¿La seguridad está activada para cada una de las radios? ¿Se configuran las contraseñas?

g. Mary pudo acceder a la red desde el exterior sin iniciar sesión; por lo tanto, ella investiga más a fondo. Haga clic en el submenú **Guest Network** e investigue la configuración.

¿La red de usuarios temporales está activa? Si es así, ¿en qué radio?

Una red inalámbrica de usuarios invitados solo debe proporcionar acceso a Internet a los usuarios invitados. No debe permitir que los invitados accedan a los dispositivos en la red local dentro de la casa. En este caso, los invitados pueden acceder a la red local. Esto indica que el router doméstico está mal configurado.

¿Qué propondría que haga Bob para proteger esta red?

Parte 2: Investigar una vulnerabilidad de malware de suplantación de identidad

La suplantación de identidad es un tipo de ataque de ingeniería social en el que un agente de amenazas se disfraza como una fuente legítima y confiable para engañarlo para que instale malware en su dispositivo o para compartir información personal o financiera. Los ataques de suplantación de identidad generalmente ocurren a través de correos electrónicos o llamadas telefónicas. A diferencia de otras vulnerabilidades de red, la principal vulnerabilidad en los ataques de suplantación de identidad son los usuarios de la red. Por este motivo, una defensa importante contra la suplantación de identidad es capacitar a los usuarios sobre cómo prevenir ataques de suplantación de identidad.

En esta parte, simulará e investigará un ataque de suplantación de identidad.

Nota: Esta actividad es solo para fines de demostración. Escribir y enviar mensajes de correo electrónico de suplantación de identidad no es ético y se considera un ataque criminal en la mayoría de las jurisdicciones.

Paso 1: Actúe como un agente de amenazas y cree un correo electrónico de suplantación de identidad.

a. Vaya a la red del **Cafe**

b. Haga clic en **Cafe Hacker Laptop** > Pestaña **Desktop** > **Email**.

c. Haga clic en **Compose**.

Utilice su imaginación para escribir un correo electrónico de suplantación de identidad. Su objetivo es persuadir al usuario para que copie y pegue una URL de su mensaje de correo electrónico en su navegador. Incluya el enlace **pix.example.com** en el correo electrónico. Puede buscar, por ejemplo, correos electrónicos de suplantación de identidad en línea para ver cómo los agentes de amenazas escriben este tipo de correo electrónico.

Nota: Los enlaces en correos electrónicos de suplantación de identidad suelen ser enlaces activos o "activos". Todo lo que la víctima tiene que hacer es hacer clic. Sin embargo, Packet Tracer no admite el uso de enlaces activos dentro del cliente de correo electrónico.

d. Envíe su correo electrónico a tres personas dentro de la red de la **Branch Office**. Sus direcciones de correo electrónico son las siguientes:

- user1@mail.isp.net
- user2@mail.isp.net
- user3@mail.isp.net

Paso 2: Abra los correos electrónicos recibidos del agente de amenazas.

a. Acceda a la **Branch Office**.

b. Haga clic en uno de los dispositivos, ya sea **PC-BR1**, **Laptop BR-1**, o **Laptop BR-2**.

c. Haga clic en Pestaña **Desktop** > **Email**, y finalmente en **Receive**. Debería recibir el correo electrónico que acaba de enviar.

Nota: Packet Tracer puede tardar varios segundos en converger. Es posible que deba hacer clic en **Receive** varias veces si el correo electrónico no se recupera correctamente.

d. Opcional: vaya a los otros dispositivos de la víctima, abra su cliente de **Email** y haga clic en **Receive** para verificar que también recibió su correo electrónico de suplantación de identidad.

Paso 3: Actúe como una víctima y siga las instrucciones de suplantación de identidad.

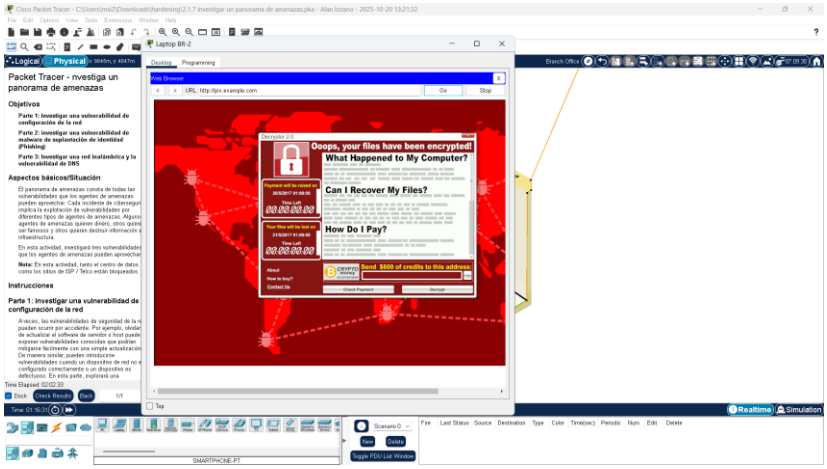
a. Lea el correo electrónico y copie la dirección del sitio web.

b. Cierre el **Mail Browser**, y luego haga clic en el **Web Browser**.

c. Pegue la URL en el campo **URL** y luego **Go**.

Nota: Packet Tracer puede tardar varios segundos en converger. Pueden hacer clic en **Fast Forward Time (Adelantar el tiempo)** (Alt+D) para acelerar el proceso.

¿Qué sucedió cuando se cargó la página web?



Se le abrió un malware

¿Cómo se llama este tipo de ataque?

ransonware

En una situación del mundo real, este correo electrónico generalmente se transmite por un virus que envía automáticamente correos electrónicos maliciosos a todas las direcciones de su lista de contactos.

Describa el daño que este tipo de ataque puede causar dentro de una organización.

Los empleados deben recibir capacitación sobre cómo identificar los correos electrónicos de suplantación de identidad y las medidas que se deben tomar para evitar que sufran daños. Además, las organizaciones pueden configurar firewalls, sistemas de prevención de intrusiones y otros dispositivos y software de seguridad para bloquear correos electrónicos de suplantación de identidad antes de ingresar a la red. Algunas empresas se suscriben a servicios que recopilan y mantienen listas de sitios web maliciosos. Los dispositivos de seguridad de la organización pueden utilizar estas listas para actualizar automáticamente los filtros para bloquear el tráfico malicioso.

Parte 3: Investigue una red inalámbrica y una vulnerabilidad de DNS

El usuario promedio de la red tiende a confiar en las redes Wi-Fi abiertas en lugares públicos. El uso de Wi-Fi en su lugar, los servicios de datos móviles pueden proporcionar velocidades de transmisión de datos más rápidas y ser más rentables. Sin embargo, los agentes de amenazas pueden configurar una computadora portátil con una interfaz Wi-Fi que pueda actuar como punto de acceso y cliente de Wi-Fi. Esto significa que

los creadores de amenazas pueden crear sus propias redes inalámbricas y transmitir un SSID convincente a las posibles víctimas en lugares públicos. Los actores de amenazas utilizan estos puntos de acceso dudosos para crear ataques de ataque principal. En este ataque, los creadores de amenazas pueden capturar y leer todo el tráfico inalámbrico de los dispositivos que se asocian con el punto de acceso dudoso, lo que posiblemente aprenda nombres de usuario, contraseñas y otra información confidencial.

En esta parte, investigará cómo se puede utilizar un punto de acceso dudoso para atraer a los usuarios a conectarse a una red inalámbrica falsa. Cuando se combinan con servicios de red como DHCP y DNS, los usuarios pueden ser víctimas de ataques maliciosos a sitios web mediante el secuestro de DNS.

Paso 1: Conéctese a la red inalámbrica del agente de amenazas.

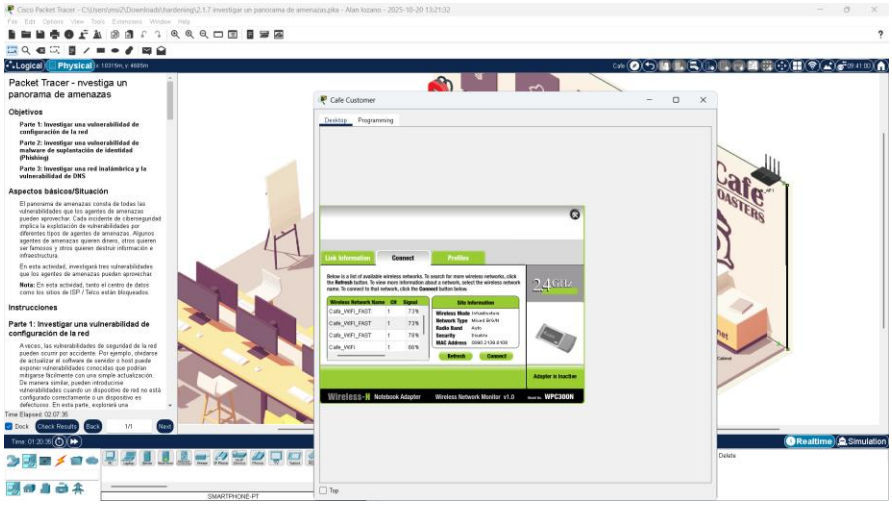
a. Navegue hasta el **Cafe**. Observe al actor de amenazas sentado en la esquina.

b. Haga clic en la **Hacker Backpack** e investigue el contenido. En su mochila, tiene un router inalámbrico y un sniffer de red. Su objetivo es interceptar el tráfico de usuarios y dirigirlo a un servidor malicioso.

c. Regrese a **Cafe** y haga clic en la computadora portátil del **Cafe Customer** > Pestaña **Desktop** > Aplicación **PC Wireless**.

d. Haga clic en la pestaña **Connect**. Será necesario que haga clic en **Refresh** para ver la lista de redes disponibles.

Si estuviera en el Cafe, ¿a qué red inalámbrica elegiría conectarse? Explique.



En la de café wifi por que esa red es mas segura

e. Haga clic en cualquiera de los nombres de red de **Cafe_WI-FI_FAST** y luego en **Connect**.

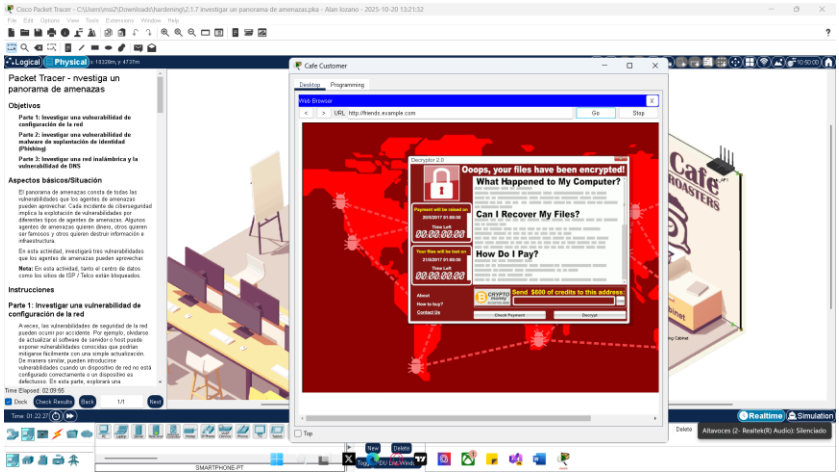
Paso 2: Visite su sitio de medios sociales favorito.

a. Cierre la aplicación **PC Wireless** y haga clic en **Web Browser**.

b. En el campo URL, ingrese **friends.example.com** y haga clic en **Go**. Se supone que este sitio web es una red social legítima en esta simulación.

¿Qué ocurrió?

Un ataque de ransonware



¿Cuál fue la URL del servidor de malware que se utilizó en el escenario de ataque de suplantación de identidad? ¿Es lo mismo?

friends.example.com

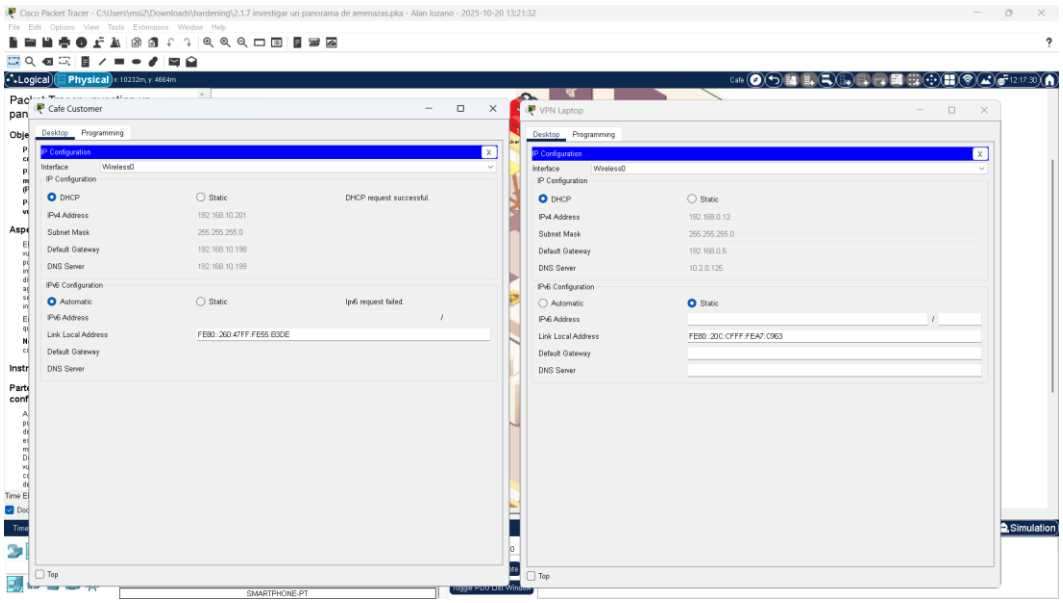
Paso 3: Investigar el origen del ataque.

a. Cierre el **Web Browser** y luego haga clic en **IP Configuration (Configuración de IP)**.

b. En el **Cafe**, haga clic en **VPN Laptop** > Pestaña **Desktop** > **IP Configuration**.

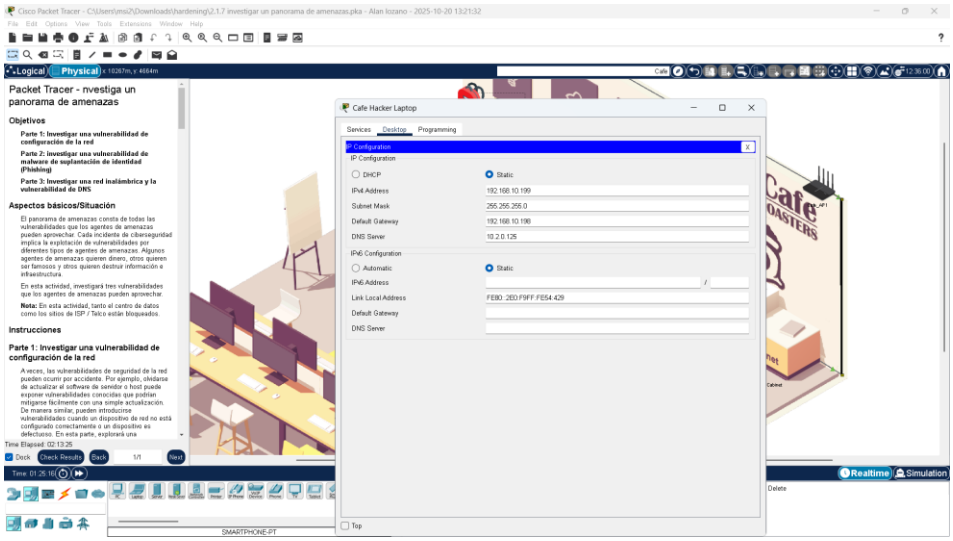
c. Haga clic en **Cafe Customer (Cliente del Café)** en la barra de tareas para volver a verlo y luego organice las dos ventanas de **IP Configuration** una al lado de la otra. Compare los valores entre los dos dispositivos.

¿Cuáles son las diferencias entre las direcciones de las dos computadoras portátiles?



d. Investigar la **Cafe Hacker Laptop**.

¿Cuál es su dirección IP? ¿Por qué es esto significativo?



Por que la ip de la víctima la asigno el hacker

En la computadora **Cafe Hacker Laptop**, haga clic en la pestaña **Services** > **DNS**.

e. Busque el nombre del sitio web de **friends.example.com**. Tenga en cuenta que la dirección IP es la misma dirección IP asociada con **pix.example.com** del ataque de suplantación de identidad anterior.

f. En **Services**, haga clic en **DHCP**. Tenga en cuenta que la dirección del servidor DNS distribuida a los hosts a través de DHCP es la misma asignada al **Cafe Customer**.

¿Cuáles son los pasos en este ataque?

1. **Instalación de la Red Falsa:** Un hacker configura un punto de acceso Wi-Fi falso ("Evil Twin") con un nombre legítimo (ej: "Cafe_Wi-Fi_Fast").
2. **Conexión de la Víctima:** Una víctima se conecta a esta red falsa, creyendo que es auténtica.
3. **Configuración Maliciosa:** La red falsa asigna automáticamente a la víctima una configuración de red que incluye un **Servidor DNS controlado por el hacker**.
4. **Secuestro de Tráfico:** Cuando la víctima intenta visitar un sitio web legítimo (como friends.example.com), el DNS malicioso del hacker **redirige la solicitud a un servidor falso** controlado por él (la misma IP de pix.example.com).
5. **Ataque Final:**
    - La víctima llega a un sitio web falso que puede robar sus credenciales o instalar malware (como ransomware) en su dispositivo.

Consecuencias Principales:

- Robo de contraseñas e información personal.
- Infección de dispositivos con software malicioso.
- Pérdida de datos y posibles extorsiones (ransomware).

Resumen

En esta actividad, hemos analizado tres formas diferentes en las que las vulnerabilidades pueden generar vulnerabilidades. Como usuario informado de la red o profesional de ciberseguridad, es su responsabilidad pensar en las diferentes maneras en que dichas vulnerabilidades pueden detectarse y mitigarse antes de que ocurra un ataque cibernético.