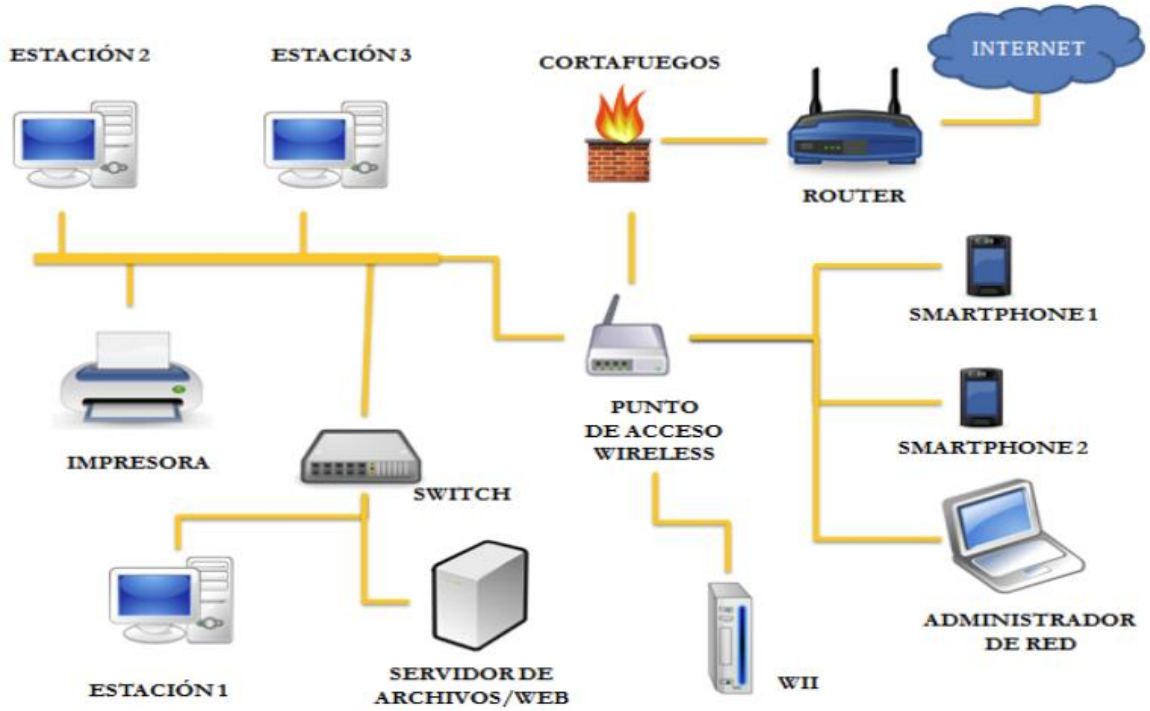
Experto Universitario en Ethical Hacking

Reconocimiento Pasivo/Activo

Ejercicio 1 – Unidad 1

Si miramos con atención la gráfica a continuación, ¿cuántos puntos posibles de ingreso/intrusión, creen que son posibles?



Respuesta:

En esta red, hay varios puntos de posible ingreso o intrusión que se pueden analizar. Basándonos en los dispositivos visibles y considerando otros factores, los puntos de ingreso potenciales son:

1. **Router**: Es uno de los puntos principales de conexión a internet y puede ser objetivo de ataques externos, especialmente si tiene una configuración de seguridad débil.
2. **Punto de acceso inalámbrico**: Un punto de acceso wireless es vulnerable a intrusiones si la red WiFi no está correctamente asegurada (por ejemplo, con una contraseña débil o sin cifrado WPA2 o WPA3).
3. **Firewall**: Aunque su función es proteger la red, una configuración incorrecta podría abrir puertas de acceso a la red.

4. **Estaciones de trabajo (Estación 1, Estación 2, Estación 3)**: Cada estación de trabajo puede representar un punto de ingreso si no tiene un antivirus actualizado, políticas de seguridad o si los usuarios son víctimas de phishing.
5. **Servidor de archivos/web**: Un servidor de archivos o web que está conectado a la red puede ser comprometido mediante vulnerabilidades en el software o configuraciones incorrectas.
6. **Impresora**: Las impresoras modernas pueden ser vulnerables a ataques, especialmente si están conectadas a la red y tienen una interfaz de administración no asegurada.
7. **Smartphones (Smartphone 1 y Smartphone 2)**: Los dispositivos móviles que se conectan a la red pueden ser puntos de entrada si están infectados con malware o si están conectados a través de una red WiFi insegura.
8. **Administrador de red (Laptop)**: Si el administrador de red utiliza una computadora portátil sin las medidas de seguridad adecuadas (como firewall personal, antivirus, etc.), también podría ser un punto de intrusión.
9. **Dispositivo Wii**: Aunque no es un dispositivo típico de ingreso, los dispositivos conectados a la red, como consolas de juegos, pueden ser puntos vulnerables si no se configuran de forma segura.

Además, otros puntos de intrusión potenciales, aunque no estén representados en el diagrama, podrían incluir:

10. **Router del ISP**: El router proporcionado por el proveedor de internet también es un posible punto de entrada, especialmente si no tiene actualizaciones de firmware o una contraseña robusta.
11. **Cámaras IP o dispositivos IoT**: Aunque no están representados aquí, en muchas redes existen cámaras IP o dispositivos IoT que pueden ser accesibles de forma remota.
12. **Paneles de acceso o sensores biométricos**: Si existen estos dispositivos en la red y están conectados, también podrían ser puntos vulnerables.

En resumen, en esta red podríamos identificar al menos **12 puntos posibles de ingreso o intrusión** considerando los dispositivos conectados y los factores externos.

Acerca del Switch:

Si el switch en el diagrama es un switch de capa 3, sería un punto de intrusión potencial. Si es un switch simple de capa 2, el riesgo es mucho menor y generalmente no se considera un objetivo de ataque directo.

Un switch de capa 2 (L2) no tiene capacidades de enrutamiento y, en general, no es administrable, lo que significa que no puede ser configurado o accedido directamente. Estos switches son menos vulnerables a ataques de intrusión directa, ya que su función se limita a la conmutación de paquetes dentro de una misma red local.

Un switch de capa 3 (L3), en cambio, sí tiene capacidades de enrutamiento y, usualmente, es administrable, lo que implica que tiene una interfaz de administración que puede configurarse y, potencialmente, ser explotada. Los switches L3 permiten definir rutas y controlar el tráfico entre subredes, por lo que, si no se asegura adecuadamente, puede ser un punto de intrusión en la red.

Ejercicio 2 - Unidad 1

Seleccionar un sitio web y tratar de buscar información del mismo, haciendo un desarrollo de lo encontrado.

Sitio web seleccionado: https://securion.com.ar

Información obtenida disponible en internet, utilizando CentralOPS, cuitonline.com, Central de deudores del Banco Central de la Republica Argentina:

canonical name: securion.com.ar

IP: 72.167.204.164

CUIT del registrante: 30678239549

CUIT correspondiente a: SECAR SECURITY ARGENTINA S. A. ex SECURITAS ARGENTINA SA

Registrado en NICar el dia 2013-08-28 y modificado el dia 2024-09-12

Rango de IPs: 72.167.0.0 - 72.167.255.255

Servidor alojado en la infraestructura de Go Daddy

DNS en Azure

Puertos abiertos y servicios identificados:

Puerto 21 (FTP) Servicio: Pure-FTPd

Puerto 80 (HTTP v1.1), Servidor Apache, PHP versión: 8.1.30, Sitio web basado en el CMS Wordpress.

Puerto 110 (POP3), Servidor de correo Dovecot

Puerto 143 (IMAP), Servidor de correo Dovecot, envio de credenciales en texto plano pero conexión SSL forzada. Por lo que mitigaría un ataque MITM o visualización a través de sniffer de red.

Puerto 443 (HTTPS)

Dominios asociados:

DNS Name=seguridadargentina.com.ar, DNS Name=aipaa.com.ar, DNS Name=cpanel.securion.com.ar, DNS Name=el-guardian.com.ar, DNS Name=fuegored.com, DNS Name=mail.securion.com.ar, DNS Name=organizacionfiel.com.ar, DNS Name=secarsecurity.com, DNS Name=securion.cl, DNS Name=securion.com.ar, DNS Name=securion.com.co, DNS Name=securion.com.mx, DNS Name=securion.com.pe, DNS Name=seguridadargentina.com.ar, DNS Name=seguridadconosur.com.ar, DNS Name=trailback.com.ar, DNS Name=vigilan.com.ar, DNS Name=webdisk.securion.com.ar, DNS Name=www.aipaa.com.ar, DNS Name=www.el-guardian.com.ar, DNS Name=www.fuegored.com, DNS Name=www.organizacionfiel.com.ar, DNS Name=www.secarsecurity.com, DNS Name=www.securion.cl, DNS Name=www.securion.com.ar, DNS Name=www.securion.com.co, DNS Name=www.securion.com.mx, DNS Name=www.securion.com.pe, DNS Name=www.seguridadargentina.com.ar, DNS Name=www.seguridadconosur.com.ar, DNS Name=www.trailback.com.ar, DNS Name=www.vigilan.com.ar

Descubrimos paneles de logins en:

cpanel.securion.com.ar

webdisk.securion.com.ar

Reconocimiento de relaciones financieras con las siguientes entidades:

Consulta de información para el CUIT-CUIL-CDI 30678239549 - SECAR SECURITY ARGENTINA S. A.

Central de Deudores del Sistema Financiero

En el siguiente cuadro, el monto de deuda se encuentra expresado en miles de pesos.

Denominación del deudor[1]	Entidad[2]	Periodo[3]	Situación[4]	Monto[5]	Días de atraso[6]	Observaciones[7/8]
SECAR SECURITY ARGENTINA S. A.	BANCO INDUSTRIAL S.A.	09/24	1	429805	N/A	-
SECAR SECURITY ARGENTINA S. A.	YPF S.A.	09/24	1	187799	N/A	-
SECAR SECURITY ARGENTINA S. A.	BANCO MACRO S.A.	09/24	1	113728	N/A	-
SECAR SECURITY ARGENTINA S. A.	AMERICAN EXPRESS ARGENTINA S.A.	09/24	1	17398	N/A	-
SECAR SECURITY ARGENTINA S. A.	BANCO SANTANDER ARGENTINA S.A.	09/24	1	8036	N/A	-
SECAR SECURITY ARGENTINA S. A.	Naldo Lombardi S.A.	08/24	1	937	N/A	-
SECAR SECURITY ARGENTINA S. A.	BANCO DE GALICIA Y BUENOS AIRES S.A.U.	09/24	1	855	N/A	-
SECAR SECURITY ARGENTINA S. A.	REBA COMPAÑIA FINANCIERA S.A.	09/24	1	465	N/A	-
SECAR SECURITY ARGENTINA S. A.	BANCO DE LA NACION ARGENTINA	09/24	1	30	N/A	-

Se puede conseguir mucha más información que está de acceso público en internet pero mejor paramos acá ya que creo el punto está demostrado.

Aclaro que lo obtenido es información PUBLICA que se encuentra disponible en INTERNET.

El punto de mostrar entidades financieras relacionadas es para demostrar que podría entrar un ataque de ingeniería social o phishing utilizando esa información. Y por las webs de formularios de login podrían ser objetivo de fuerza bruta o Man in the middle si se utiliza la versión no cifrada (ósea HTTP y no HTTPS) ya que las credenciales se enviarían en texto plano.

Rodrigo Vila.-