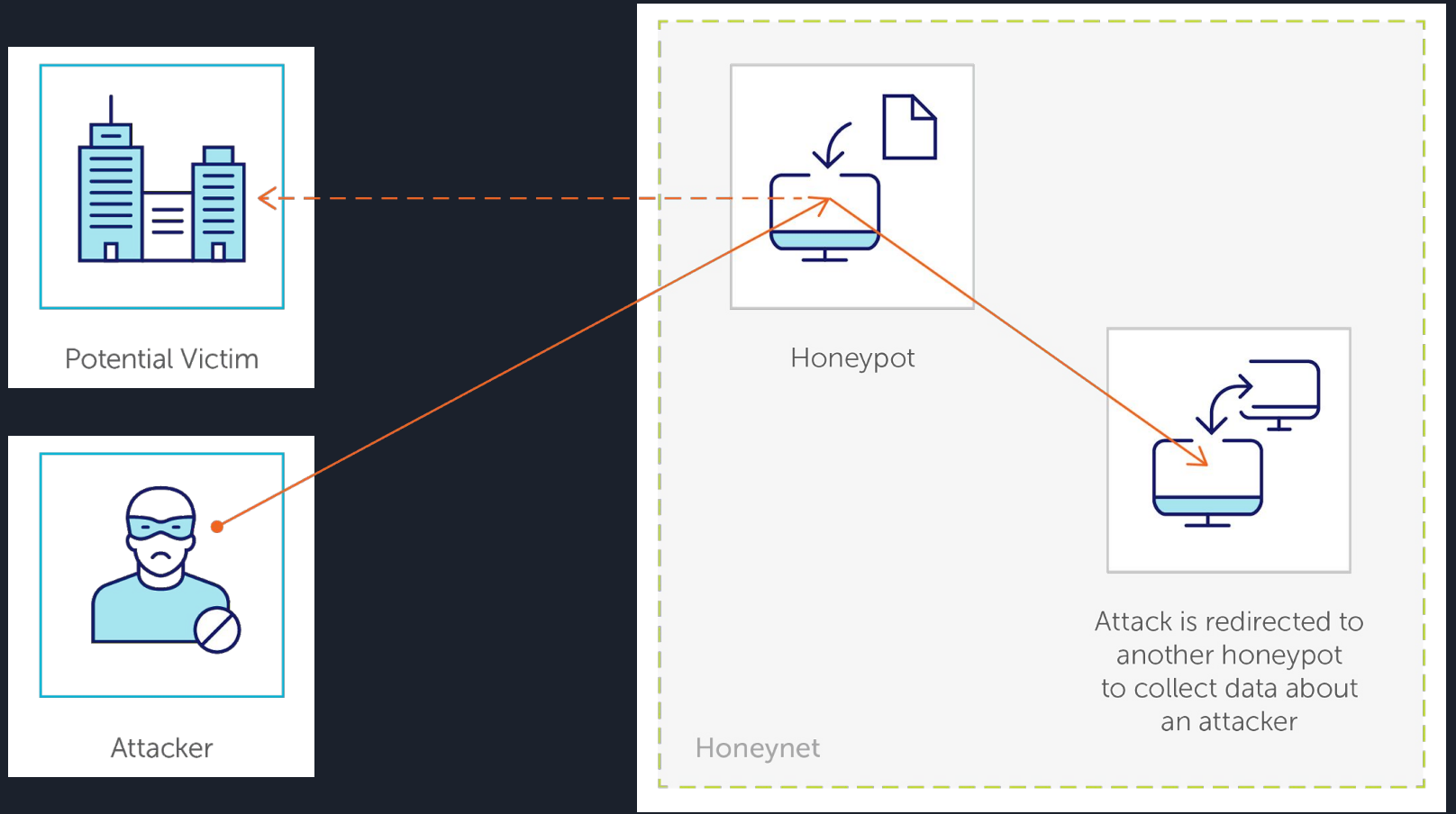
Metodología de garantización de la seguridad en routers

Juan Camilo Tobar N.
Juan Fernando Jaramillo C.
Mauricio Hernández M.

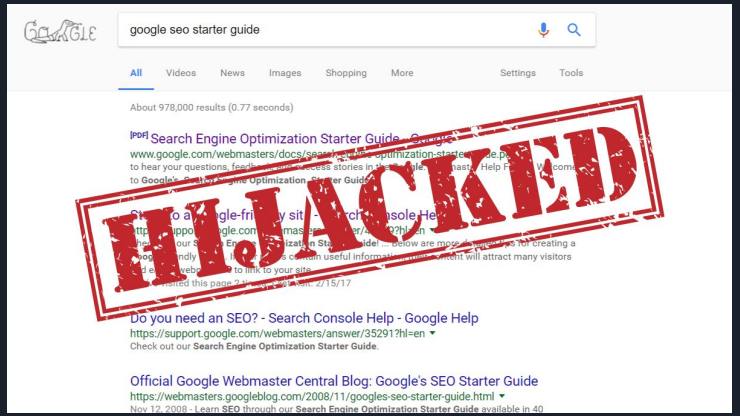


Tomado de: https://www.softserveinc.com/en-us/blogs/security-strategies-fintech/

Tomado de: https://www.welivesecurity.com/la-es/2018/10/01/brasil-aprovechan-vulnerabilidad-en-routers-para-redirigir-usuarios-falsas-paginas-de-bancos/

OTROS CASOS

- Campañas de hijacking afectan a usuarios de Bancos en Brasil.
- aprovechan vulnerabilidades en routers para redirigir a usuarios a páginas falsas de Bancos.
- Vulnerabilidades afectan a más de 7000 routers marca D-Link



¿RouterOS?

Vulnerabilidad

CVE-2018-14847

Permite el **acceso a archivos arbitrarios** de configuración.

Nació en 1997, un año después de la creación de MikroTIk.

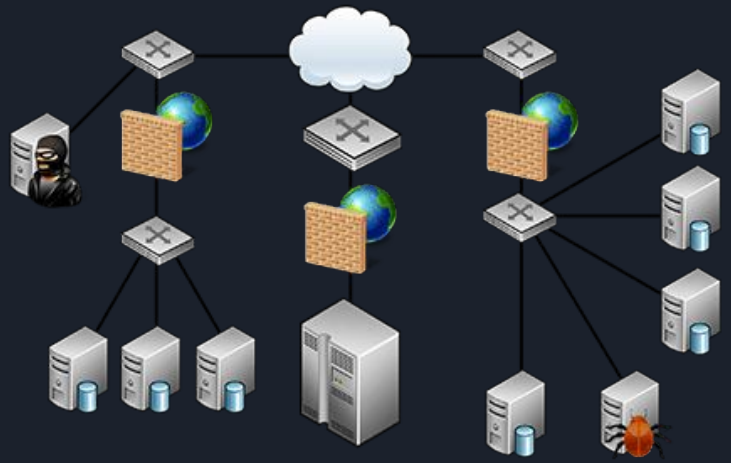
Está basado en Linux y suple funcionalidades usadas por los NSP e ISP.

RouterOS

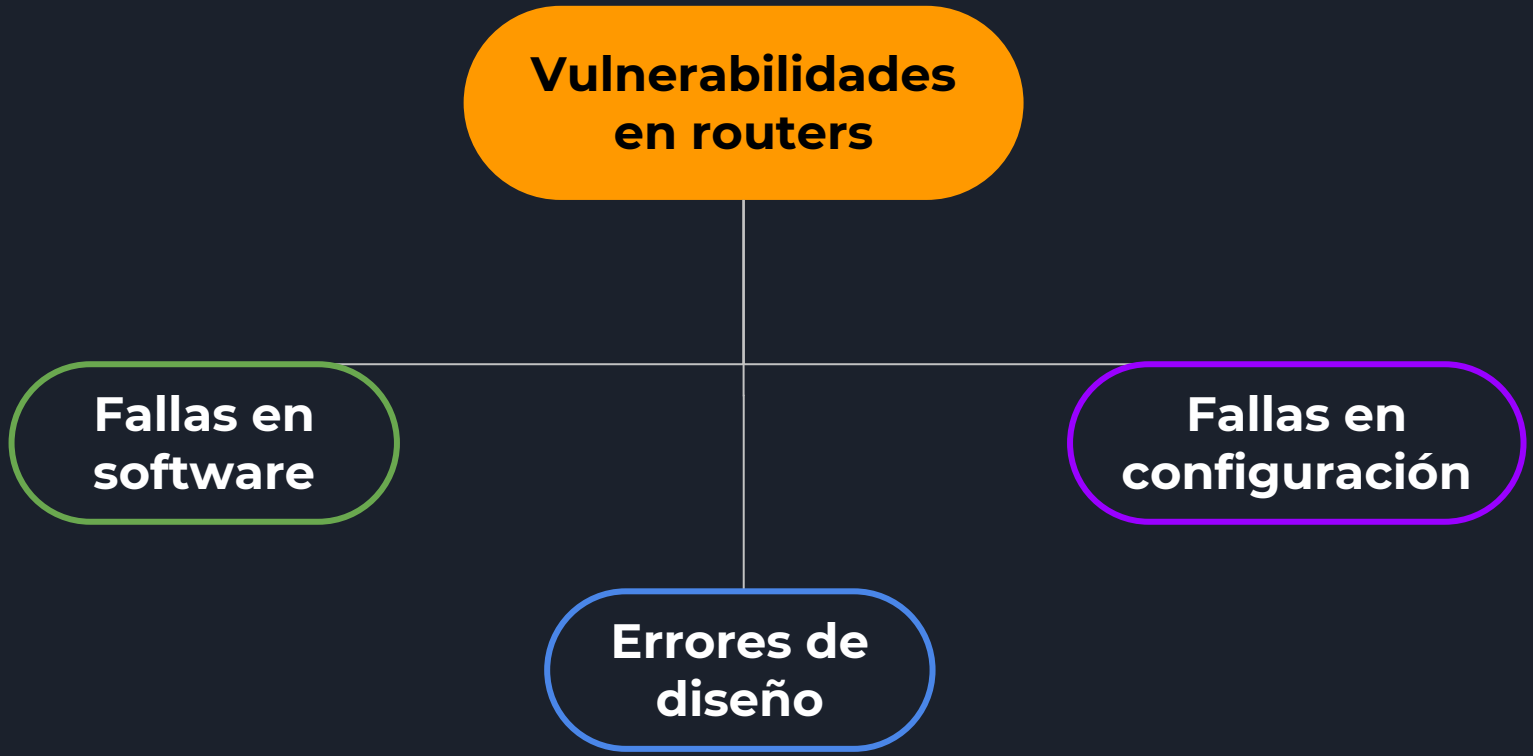
Enfoque de seguridad

Tener en cuenta elementos más allá de los servidores y los firewalls, como los **routers**.

APRENDER - EXPLOTAR VULNERABILIDADES - ENCONTRAR RIESGOS - ACTUAR



Tomado de: https://www.offensive-security.com/offensive-security-solutions/virtual-penetration-testing-labs/


Vulnerabilidades en routers
Fallas en software
Fallas en configuración
Errores de diseño

Fallas en software

¿Qué son?

Errores alocados en el **sistema operativo** de los routers encargados del enrutar de forma óptima los paquetes.

Fallas comunes

Desbordamiento de buffer: acceso remoto al router.

Más común en los últimos diez años

Complejidad

Alto riesgo en función de los **permisos concedidos** a atacantes. Diferentes SO en el mercado de los enrutadores..

Errores de diseño

¿Cuándo ocurren?

Se presentan en la etapa de desarrollo de hardware debido a la aplicación de arquitecturas incorrectas o tecnología obsoleta.

Dificultades

Detección más difícil de llevar a cabo debido a la naturaleza del problema y por lo tanto más costosa.

Fallas en configuración

¿Dónde están?

Son errores de origen humano que se generan a la hora de configurar el router. Las fallas pueden originarse en la **configuración de fábrica** o del **usuario**.

Explotación

Son el blanco más codiciado por atacantes remotos, lo que está ligado a su abundancia. Telnet, SSH y SNMP permiten la explotación.

Errores típicos

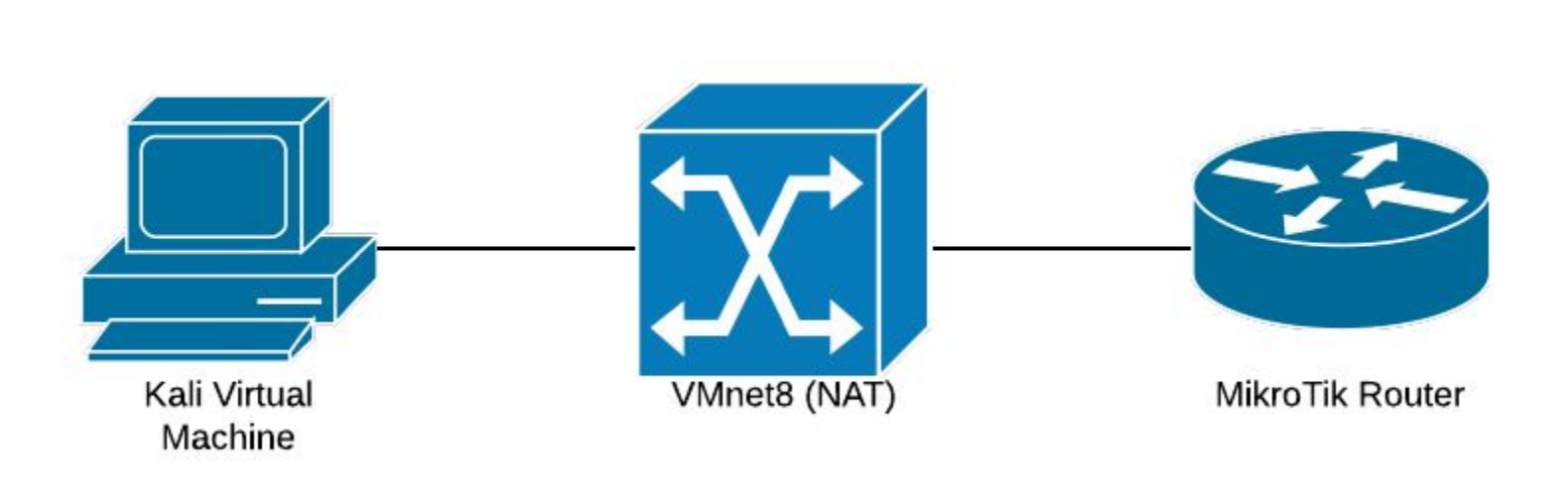
Puertos abiertos permanentemente, **contraseñas dejadas por defecto** o activación de protocolos que plantean una amenaza.

Objetivos

Proponer un entorno de pruebas basado en el **establecimiento de máquinas virtuales** para llevar a cabo el test.

Describir mecanismos de prueba basados en el uso de SSH, Telnet y SNMP para hallar fallas en la configuración de RouterOS versión 6.42.

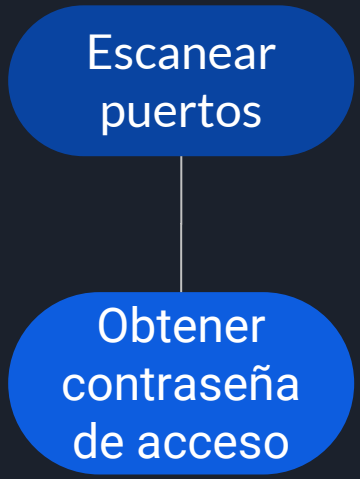
Configuración de entorno



Prueba con el protocolo SSH

Puertos abiertos	Creación de claves	Ataque de fuerza bruta
Nmap nmap -sV –n <<VMnet8 IP>> Respuesta esperada: puertos abiertos donde sea posible usar SSH para iniciar una comunicación	Crunch crunch 5 5 <<cadena>> > wordlist Resultado: archivo con todas las posibles cadenas del tamaño de la cadena ingresada	Metasploit Método: usar el módulo SSH_login. Resultado: SSH_login se detiene cuando logra conectarse al router e indica la clave correcta.

Prueba con el protocolo Telnet



NMap
nmap –sS <<VMnet8 IP>> –n
Resultado: puertos abiertos para realizar una conexión a través de Telnet

CAT(Cisco Auditing Tool)
CAT -h <<VMnet IP>>
Resultado: contraseña de autenticación para conexión haciendo uso de Telnet

Alternativa

Obtener los datos de autenticación mediante un ataque man-in-the-middle

Prueba con el protocolo SNMP

Escanear puertos

nmap

nmap -sU -p 161 <<VMnet8 IP>>

Puertos en los que está activo el servicio SNMP.

Ataque de fuerza bruta

nmap

nmap –sU –Pn –n –p 161 –script SNMP-brute.nse <<VMnet8 IP>> –sV –O

Obtener los nombres de la comunidad dispuestos en el router.

Determinar permisos de cada nombre

SNMPcheck

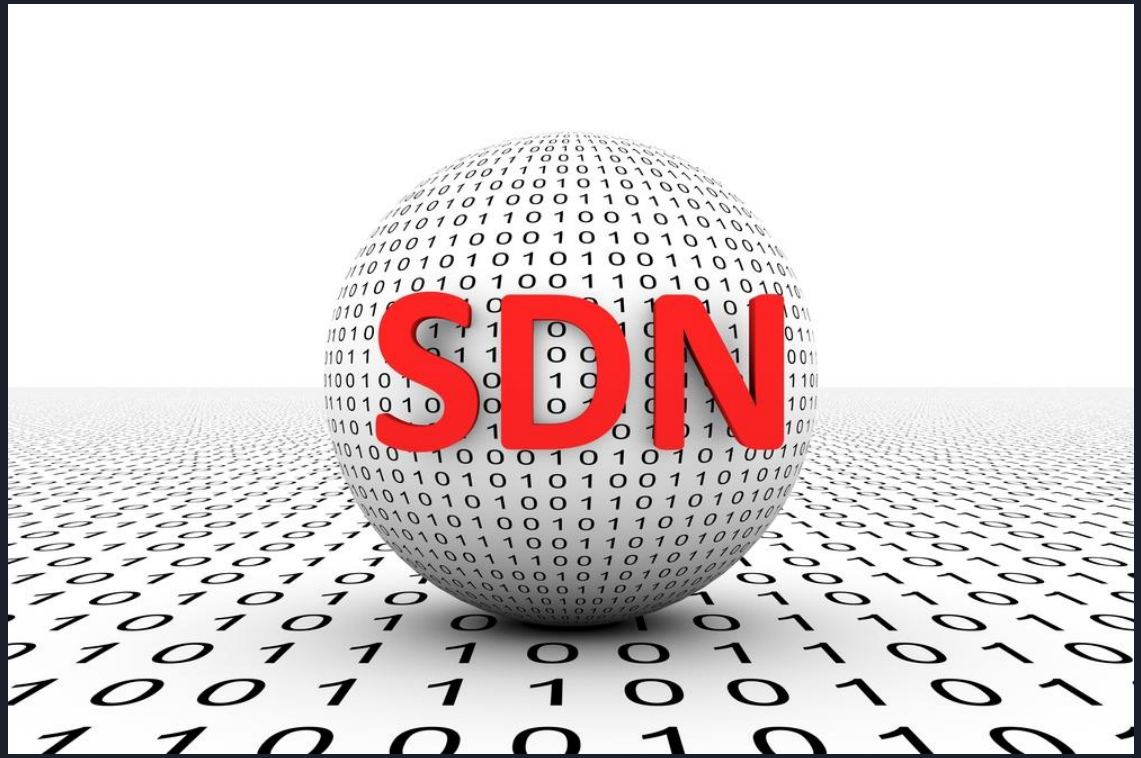
snmpcheck -c <<nombre>> -w -t <<VMnet8 IP>>

Permisos concedidos a cada nombre.

Propuesta a futuro

Poder trabajar verdaderas metodologías de **Pen testing** (*Penetration testing*) desde la academia, con un enfoque más real sobre la realidad en las vulnerabilidades a nivel de red.

INVESTIGACIÓN-REALIDAD


SDN

“Si tu empresa gasta más en café que en seguridad TI, serás hackeado. Es más, merecerás ser hackeado.”

Eric S. Raymond