IpTables: Teoría y Práctica para Montar un Firewall Linux

Código: IPT-001

Propuesta de Valor: SOFTWARE LIBRE

Duración: 24 Horas

La seguridad es punto muy importante a tener en cuenta en cualquier organización de ahí que sea fundamental hacer uso de aquellos mecanismos que tengamos a nuestro alcance para poner el mayor número de barreras posibles a los atacantes. En una estructura de servidores, el firewall ocupa un papel fundamental para salvaguardar la información que se almacena en su interior. Esta herramienta, totalmente configurable, suele tener dos funciones básicas:

AUDIENCIA

- Administradores de red que quieran optimizar sus redes y gestionar filtrado y NAT de tráfico.
- Sysadmins Unix/Linux en general.
- Proveedores de servicios de Internet.
- Administradores de seguridad informática.
- Especialistas en seguridad en redes.

PRE REQUISITOS

- Conceptos de redes TCP/IP
- Administración básica de sistemas GNU/Linux
- Administración de la línea de comandos
- Conocimientos de routing en redes TCP/IP
- Conocimientos básicos de redes LAN
- Conocimientos básicos de arquitectura de Internet

OBJETIVOS

- Mejorar las habilidades técnicas en la gestión de filtrado y reenvío de tráfico de red en redes TCP/IP locales y de banda

ancha.

- Implementar un firewall completo y optimizado para la gestión de tráfico en redes locales.
- Entender y configurar firewalls stateless/statefull basados en iptables.

CERTIFICACIÓN DISPONIBLE

- Certificado emitido por **COGNOS.**

CONTENIDO

4.6. STATEFUL Y LAS CONEXIONES RELATED
4.7. OTROS EJEMPLOS DE STATEFUL IPTABLES

5. ¿SERVIDORES EN LA LAN? USANDO DNAT

5.1. DNAT: INTRODUCCIÓN Y CONCEPTOS
5.2. DNAT: MANOS A LA OBRA CON IPTABLES!

6. UN EJEMPLO COMPLETO

6.1. INTRODUCIENDO EL ENTORNO DE LABORATORIO
6.2. CONFIGURACIÓN BÁSICA DEL FIREWALL IPTABLES
6.3. AGREGANDO REGLAS: FILTER Y SNAT/MASQUERADE
6.4. PROBANDO EL FIREWALL! Y AGREGANDO MAS REGLAS
6.5. MONTANDO NUESTRO SERVIDOR EN LA LAN: DNAT
6.6. NOTAS FINALES: CERRANDO EL EJEMPLO

7. BONUS Y CLASES ADICIONALES (NUEVOS CONTENIDOS SEGUN REQUERIMIENTO DE ALUMNOS)

7.1. GNS3 + VIRTUALBOX - INTRO
7.2. GNS3 + VIRTUALBOX - PARTE 1
7.3. GNS3 + VIRTUALBOX - PARTE 2
7.4. GNS3 + VIRTUALBOX - PARTE 3
7.5. GNS3 + VIRTUALBOX - PARTE 4
7.6. NUEVO: CONFIGURACIÓN DE RED EN GNS3+VIRTUALBOX - PARTE 1
7.7. NUEVO: CONFIGURACIÓN DE RED EN GNS3+VIRTUALBOX - PARTE 2
7.8. NUEVO: CONFIGURACIÓN DE RED EN GNS3+VIRTUALBOX - PARTE 3
7.9. NUEVO: CONFIGURACIÓN DE RED EN GNS3+VIRTUALBOX - PARTE 4
7.10. NUEVO: CONFIGURACIÓN DE RED EN GNS3+VIRTUALBOX - PARTE 5
7.11. MITIGANDO ATAQUES DE DDOS CON IPTABLES
7.12. NOCIONES DEL STACK DE PROTOCOLOS TCP/IP

BENEFICIOS

- Comprender el funcionamiento de los firewalls de red en general, y de iptables en particular.