Network Security

Código: CIS-021

Propuesta de Valor: CISCO

Duración: 70 Horas

Las organizaciones de hoy en día enfrentan el desafío de responder rápidamente a las amenazas de seguridad de red emergentes. El personal de seguridad configura y supervisa diversas medidas de mitigación de amenazas a la seguridad de la red, como el refuerzo de dispositivos, los sistemas de prevención de intrusiones y los cortafuegos, para proteger los activos de datos y los sistemas de red de los ataques.

El propósito de este curso es proporcionar habilidades y conocimientos en el campo de la seguridad de la red.

Más información: AQUÍ

Reserve su plaza: AQUÍ

AUDIENCIA

- Los estudiantes objetivo incluyen personas inscritas en programas de licenciatura en tecnología en instituciones de educación superior y profesionales de TI que desean seguir una carrera en el campo de la seguridad de redes.

PRE REQUISITOS

- Comprensión básica de las redes informáticas (CCNA: Introducción a las redes y CCNA: Conmutación, enrutamiento y fundamentos inalámbricos, o equivalente)
- Habilidades de navegación por PC e Internet.
- Familiaridad con Cisco Packet Tracer
- Comprensión básica de las redes informáticas (nivel CCNA ITN y SRWE)

OBJETIVOS

- Proporcionar una comprensión teórica profunda de la seguridad de la red.
- Proporcionar a los estudiantes los conocimientos y habilidades necesarios para diseñar y respaldar la seguridad de la red.
- Proporcionar un curso orientado a la experiencia que emplee enfoques de instrucción relevantes para la industria a fin de preparar a los estudiantes para trabajos de nivel inicial en la industria.
- Permita que los estudiantes tengan una interacción práctica significativa con el equipo de TI para prepararlos para los exámenes y las oportunidades profesionales.

CERTIFICACIÓN DISPONIBLE

- Certificado oficial de **CISCO Network Academy**.

CONTENIDO

1. PROTECCIÓN DE REDES

1.1. INTRODUCCIÓN
1.2. DESCRIPCIÓN GENERAL DE LA TOPOLOGÍA DE LA RED
1.3. RESUMEN DE REDES SEGURAS

2. AMENAZAS DE RED

2.1. INTRODUCCIÓN
2.2. ¿QUIÉN ESTÁ ATACANDO NUESTRA RED?
2.3. HERRAMIENTAS DE ACTORES DE AMENAZAS
2.4. MALWARE
2.5. ATAQUES DE RED COMUNES: RECONOCIMIENTO, ACCESO E INGENIERÍA SOCIAL
2.6. ATAQUES DE RED: DENEGACIÓN DE SERVICIO, BÚFER DESBORDAMIENTOS Y EVASIÓN
2.7. RESUMEN DE AMENAZAS DE RED

3. MITIGACIÓN DE AMENAZAS

3.1. INTRODUCCIÓN
3.2. DEFENSA DE LA RED
3.3. POLÍTICAS DE SEGURIDAD DE LA RED
3.4. HERRAMIENTAS, PLATAFORMAS Y SERVICIOS DE SEGURIDAD
3.5. MITIGACIÓN DE ATAQUES COMUNES A LA RED
3.6. PROTECCIÓN DE LA BASE DE RED DE CISCO FRAMEWORK
3.7. MITIGACIÓN DE AMENAZAS

4. ACCESO SEGURO A DISPOSITIVOS

4.1. INTRODUCCIÓN
4.2. PROTEGER EL ENRUTADOR PERIMETRAL
4.3. CONFIGURAR EL ACCESO ADMINISTRATIVO SEGURO
4.4. CONFIGURAR SEGURIDAD MEJORADA PARA INICIOS DE SESIÓN VIRTUALES
4.5. CONFIGURAR SSH
4.6. RESUMEN DE ACCESO SEGURO A DISPOSITIVOS

5. ASIGNACIÓN DE FUNCIONES ADMINISTRATIVAS

5.1. INTRODUCCIÓN
5.2. CONFIGURAR NIVELES DE PRIVILEGIOS
5.3. CONFIGURAR LA CLI BASADA EN FUNCIONES

6. MONITORIZACIÓN Y GESTIÓN DE DISPOSITIVOS

6.1. INTRODUCCIÓN
6.2. IMAGEN Y CONFIGURACIÓN SEGURAS DE CISCO IOS ARCHIVOS
6.3. BLOQUEAR UN ENRUTADOR USANDO AUTOSECURE
6.4. AUTENTICACIÓN DEL PROTOCOLO DE ENRUTAMIENTO
6.5. GESTIÓN E INFORMES SEGUROS
6.6. SEGURIDAD DE RED USANDO SYSLOG
6.7. CONFIGURACIÓN DE NTP
6.8. CONFIGURACIÓN DE SNMP
6.9. MONITOREO Y ADMINISTRACIÓN DE DISPOSITIVOS

7. AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD (AAA)

7.1. INTRODUCCIÓN
7.2. CARACTERÍSTICAS AAA
7.3. CONFIGURAR LA AUTENTICACIÓN AAA LOCAL
7.4. CARACTERÍSTICAS AAA BASADAS EN SERVIDOR Y PROTOCOLOS
7.5. CONFIGURAR LA AUTENTICACIÓN BASADA EN SERVIDOR
7.6. CONFIGURAR AUTORIZACIÓN BASADA EN SERVIDOR Y CONTABILIDAD
7.7. RESUMEN DE AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD (AAA)

8. LISTAS DE CONTROL DE ACCESO

8.1. INTRODUCCIÓN
8.2. INTRODUCCIÓN A LAS LISTAS DE CONTROL DE ACCESO
8.3. ENMASCARAMIENTO COMODÍN
8.4. CONFIGURAR ACL
8.5. MODIFICAR ACL
8.6. IMPLEMENTAR ACL
8.7. MITIGAR ATAQUES CON ACL
8.8. ACL DE IPV6
8.9. RESUMEN DE LISTAS DE CONTROL DE ACCESO

9. TECNOLOGÍAS DE CORTAFUEGOS

9.1. INTRODUCCIÓN
9.2. REDES SEGURAS CON CORTAFUEGOS
9.3. CORTAFUEGOS EN EL DISEÑO DE REDES
9.4. RESUMEN DE TECNOLOGÍAS DE CORTAFUEGOS

10. FIREWALLS DE POLÍTICA BASADOS EN ZONAS

10.1. INTRODUCCIÓN
10.2. DESCRIPCIÓN GENERAL DE ZPF
10.3. FUNCIONAMIENTO DE ZPF

10.5. RESUMEN DE FIREWALLS DE POLÍTICA BASADOS ??EN ZONAS

11. TECNOLOGÍAS IPS

11.1. INTRODUCCIÓN
11.2. CARACTERÍSTICAS DE IDS E IPS
11.3. IMPLEMENTACIONES DE IPS
11.4. IPS EN CISCO ISR
11.5. ANALIZADOR DE PUERTOS CONMUTADOS DE CISCO
11.6. RESUMEN DE TECNOLOGÍAS IPS

12. OPERACIÓN E IMPLEMENTACIÓN DE IPS

12.1. INTRODUCCIÓN
12.2. FIRMAS IPS
12.3. CISCO SNORT IPS
12.4. CONFIGURAR SNORT IPS
12.5. RESUMEN DE OPERACIÓN E IMPLEMENTACIÓN DE IPS

13. SEGURIDAD DE PUNTO FINAL

13.1. INTRODUCCIÓN
13.2. DESCRIPCIÓN GENERAL DE LA SEGURIDAD DE LOS PUNTOS FINALES
13.3. AUTENTICACIÓN 802.1X
13.4. RESUMEN DE SEGURIDAD DE PUNTOS FINALES

14. CONSIDERACIONES DE SEGURIDAD DE CAPA 2

14.1. INTRODUCCIÓN
14.2. AMENAZAS A LA SEGURIDAD DE LA CAPA 2
14.3. ATAQUES DE TABLAS MAC
14.4. MITIGAR LOS ATAQUES A LA TABLA MAC
14.5. MITIGAR LOS ATAQUES DE VLAN
14.6. MITIGAR ATAQUES DHCP
14.7. MITIGAR ATAQUES ARP
14.8. MITIGAR ATAQUES DE SUPLANTACIÓN DE DIRECCIONES
14.9. PROTOCOLO DE ÁRBOL DE EXPANSIÓN
14.10. MITIGAR ATAQUES STP
14.11. RESUMEN DE LAS CONSIDERACIONES DE SEGURIDAD DE LA CAPA 2

15. SERVICIOS CRIPTOGRÁFICOS

15.1. INTRODUCCIÓN
15.2. COMUNICACIONES SEGURAS
15.3. CRIPTOGRAFÍA
15.4. CRIPTOANÁLISIS
15.5. CRIPTOLOGÍA

16. INTEGRIDAD Y AUTENTICIDAD BÁSICA

16.1. INTRODUCCIÓN
16.2. INTEGRIDAD Y AUTENTICIDAD
16.3. GESTIÓN DE CLAVES
16.4. CONFIDENCIALIDAD
16.5. RESUMEN DE INTEGRIDAD Y AUTENTICIDAD BÁSICA

17. CRIPTOGRAFÍA DE CLAVE PÚBLICA

17.1. INTRODUCCIÓN
17.2. CRIPTOGRAFÍA DE CLAVE PÚBLICA CON FIRMAS DIGITAL
17.3. AUTORIDADES Y EL SISTEMA DE CONFIANZA DE PKI
17.4. APLICACIONES E IMPACTOS DE LA CRIPTOGRAFÍA
17.5. RESUMEN DE CRIPTOGRAFÍA DE CLAVE PÚBLICA

18. VPN

18.1. INTRODUCCIÓN
18.2. DESCRIPCIÓN GENERAL DE VPN
18.3. TOPOLOGÍAS DE VPN
18.4. DESCRIPCIÓN GENERAL DE IPSEC
18.5. PROTOCOLOS IPSEC
18.6. INTERCAMBIO DE CLAVES DE INTERNET
18.7. RESUMEN DE VPN

19. IMPLEMENTAR VPN IPSEC DE SITIO A SITIO CON CLI

19.1. INTRODUCCIÓN
19.2. CONFIGURAR UNA VPN DE IPSEC DE SITIO A SITIO
19.3. POLÍTICA ISAKMP
19.4. POLÍTICA IPSEC
19.5. CRYPTO MAP
19.6.
19.7. RESUMEN DE IMPLEMENTAR VPN IPSEC DE SITIO A SITIO CON CLI

20. INTRODUCCIÓN AL ASA

20.1. INTRODUCCIÓN
20.2. SOLUCIONES ASA
20.3. EL ASA 5506-X CON SERVICIOS FIREPOWER
20.4. INTRODUCCIÓN AL RESUMEN ASA

21. CONFIGURACIÓN DEL CORTAFUEGOS ASA

21.1. INTRODUCCIÓN

BENEFICIOS

- Al finalizar el curso, los participantes Obtendrán habilidades prácticas para diseñar, implementar y administrar sistemas de seguridad de red y garantizar su integridad.