Network Security

Este examen valida que un candidato tiene conocimientos y habilidades fundamentales en seguridad.
Se espera que los candidatos tengan experiencia práctica con sistemas operativos de clientes, aplicaciones de seguridad, firewalls, dispositivos y puertos de red. Los candidatos deben tener al menos 150 horas de instrucción o experiencia práctica en seguridad de redes.

Para aprobar el examen, también se espera que el candidato tenga los siguientes conocimientos y habilidades previos:

- Habilidades de lectura de octavo grado
- Conocimiento práctico de sistemas operativos y redes.
- Pensamiento crítico y habilidades para resolver problemas.

1. Defensa en profundidad

1.1 Identificar los principios básicos de seguridad

- Confidencialidad, integridad, disponibilidad, no repudio, amenaza, riesgo, vulnerabilidad, principio de privilegio mínimo, superficies de ataque, incluido IoT

1.2 Definir y hacer cumplir la seguridad física

- Seguridad del sitio, seguridad informática, dispositivos y unidades extraíbles, trampas de mano

1.3 Identificar tipos de políticas de seguridad

- Controles administrativos, controles técnicos.

1.4 Identificar tipos de ataques

- Desbordamiento de búfer, virus, virus polimórficos, gusanos, caballos de Troya, spyware, ransomware, adware, rootkits, puertas traseras, ataques de día cero/ vulnerabilidades, ataques de denegación de servicio (DoS), métodos de ataque comunes, tipos de vulnerabilidad, secuencias de comandos entre sitios (XSS), inyección SQL, ataque de fuerza bruta, hombre en el medio (MITM) y hombre en el navegador (MITB), ingeniería social, keyloggers (software y hardware), bombas lógicas

1.5 Identificar tipos de copia de seguridad y restauración

- Completo, incremental, diferencial

2. Seguridad del sistema operativo

2.1 Identificar la protección del cliente y del servidor

- Separación de servicios, refuerzo, gestión de parches, reducción de la superficie de ataque, política de grupo (gpupdate y gpresult), dominio dinámico seguro Actualizaciones del sistema de nombres (DNS), control de cuentas de usuario (UAC), mantener actualizado el sistema operativo y el software del cliente, cifrar carpetas sin conexión, políticas de restricción de software

2.2 Configurar la autenticación de usuario

- Autenticación multifactor, aplicación de políticas de contraseñas, acceso remoto, uso de inicio de sesión secundario para realizar tareas administrativas (Ejecutar como, sudo), creación de dominios y usuarios y grupos locales, Kerberos

2.3 Administrar permisos en Windows y Linux

- Permisos de archivos y carpetas, permisos para compartir, herencia, movimiento o copiar archivos dentro del mismo disco o en otro disco, múltiples grupos con diferentes permisos, tomar propiedad, delegación

2.4 Facilitar el no repudio utilizando políticas de auditoría y archivos de registro

- Tipos de auditoría, qué se puede auditar, habilitación de la auditoría, qué auditar para propósitos específicos, dónde guardar la información de auditoría, revisión de archivos de registro

2.5 Demostrar conocimientos de cifrado

- Cifrado de archivos y carpetas, cómo el cifrado afecta el movimiento/copia de archivos y carpetas, cifrado de unidades, TPM, procesos de comunicación seguros (correo electrónico, mensajes de texto, chat, redes sociales), métodos de cifrado de red privada virtual (VPN), clave pública/clave privada, propiedades y servicios de certificados, Bitlocker

3. Seguridad del dispositivo de red

3.1 Implementar seguridad inalámbrica

- Tipos de seguridad inalámbrica (fuerza del cifrado), identificadores de conjuntos de servicios (SSID), filtrado MAC, configuración predeterminada (OOBE)

3.2 Identificar el papel de los dispositivos de protección de red.

- Propósito de los firewalls, firewalls de hardware versus software, firewalls de red versus host, inspección de firewall con estado versus sin estado, líneas de base de seguridad, sistema de detección de intrusiones (IDS), sistema de prevención de intrusiones (IPS), administrador de eventos e información de seguridad (SIEM), filtrado de contenidos, listas negras/ lista blanca

3.3 Identificar métodos de aislamiento de red

- Enrutamiento, Honeynet, redes perimetrales (DMZ), NAT/PAT, VPN, IPsec, red Air Gap, DirectAccess, LAN virtual (VLAN)

3.4 Identificar conceptos de seguridad de protocolo

- Túneles, DNSSEC, rastreo de redes, puertos conocidos (FTP, HTTP, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LDAPS, SNMP, SMTP, IMAP, SFTP)

4. Computación segura

4.1 Implementar protección de correo electrónico

- Antispam, spoofing, phishing y pharming, protección al cliente, formación de usuarios

4.2 Administrar la seguridad del navegador

- Configuración del navegador, gestión de caché, navegación privada

4.3 Instalar y configurar software antimalware y antivirus

- Instalar, desinstalar, reinstalar y actualizar; remediación, programación exploraciones, investigando alertas