98-367
Fundamentos de seguridad

Dominio de objetivos

1. Comprender las Capas de Seguridad

1.1. Comprender los principios centrales de seguridad.
Este objetivo puede incluir más no se limita a: confidencialidad; integridad; disponibilidad; cómo la amenaza y el riesgo impactan los principios; el principio de contar con menos privilegios; ingeniería social; superficie de ataque

1.2. Comprender la seguridad física.
Este objetivo puede incluir más no se limita a: seguridad del site; seguridad de la computadora; dispositivos y unidades de disco removibles; control de acceso; seguridad de dispositivo móvil; desactivar Inicio de Sesión de forma local; keyloggers

1.3. Comprender la seguridad de Internet.
Este objetivo puede incluir más no se limita a: configuración del navegador; zonas; sitios Web seguros

1.4. Comprender la seguridad inalámbrica.
Este objetivo puede incluir más no se limita a: ventajas y desventajas de tipos específicos de seguridad; claves; SSID; filtros MAC

2. Comprender la Seguridad de un Sistema Operativo

2.1. Comprender la autenticación de usuario.
Este objetivo puede incluir más no se limita a: multifactor; tarjetas inteligentes; RADIUS; Infraestructura de Clave Publica (PKI); entender la cadena de certificación; biométricas; Kerberos y sesgo de reloj; utilizar Ejecutar Como para llevar a cabo tareas administrativas; procedimientos para restaurar contraseñas

2.2. Comprender los permisos.
Este objetivo puede incluir más no se limita a: archivo; compartir; registro; Directorio Activo; NTFS vs. FAT; activar o desactivar herencia; comportamiento cuando se mueven o copian archivos dentro del mismo disco o a otro disco; grupos múltiples con diferentes permisos; permisos básicos y permisos avanzados; tomar propiedad; delegación

2.3. Comprender las políticas de contraseñas.

Este objetivo puede incluir más no se limita a: complejidad de contraseñas; cuentas bloqueadas; longitud de contraseñas; historial de contraseñas; tiempo entre cambios de contraseñas; aplicación de políticas de grupo; métodos de ataque comunes

2.4. Comprender las políticas de auditoría.
Este objetivo puede incluir más no se limita a: tipos de auditoría; aspectos que son auditables; habilitar auditoria; que auditor para propósitos específicos; donde guardar la información auditada; como mantener segura la información de una auditoria

2.5. Comprender el cifrado.
Este objetivo puede incluir más no se limita a: EFS; como las carpetas cifradas en EFS impactan al mover y copiar archivos; BitLocker (To Go); Modulo de Plataforma Segura (TPM); software de encriptación; cifrado de MAIL, firmas y otros usos; VPN; claves públicas y privadas; algoritmos de encriptación; servicios de certificado; PKI/infraestructura de servicios de certificado; dispositivos de seguridad

2.6. Comprender el malware.
Este objetivo puede incluir más no se limita a: desbordamiento de buffer; gusanos; troyanos; spyware

3. Comprender la seguridad de la red

3.1. Comprender los cortafuegos dedicados.
Este objetivo puede incluir más no se limita a: tipos de cortafuegos hardware y sus características; cuando utilizar un cortafuegos hardware en lugar de un cortafuegos software; inspección stateful vs. stateless

3.2. Comprender la Protección de Acceso a Redes (NAP).
Este objetivo puede incluir más no se limita a: propósito de NAP; requerimientos para NAP

3.3. Comprender el aislamiento de redes.
Este objetivo puede incluir más no se limita a: VLANs; enrutamiento; honeypot; DMZ; NAT; VPN; IPsec; aislamiento de servidor y dominio

3.4. Comprender la seguridad de protocolos.
Este objetivo puede incluir más no se limita a: protocolo spoofing; IPsec; tunneling; DNSsec; sniffing en redes; métodos de ataque comunes

4. Comprender el Software de Seguridad

4.1. Comprender la protección del cliente.
Este objetivo puede incluir más no se limita a: anti-virus; Control de Cuenta de Usuario Control de Cuenta de Usuario (UAC); mantener el sistema operativo y el software del cliente actualizado; cifrar carpetas offline; políticas de restricción de software

4.2. Comprender la protección de correo electrónico.
Este objetivo puede incluir más no se limita a: anti-spam; anti-virus; spoofing, phishing, y pharming; cliente vs. protección del servidor; registros SPF; registros PTR

4.3. Comprender la protección del servidor.
Este objetivo puede incluir más no se limita a: separación de servicios; hardening; mantener

el software actualizado; actualizaciones de seguridad dinámica DNS; desactivar protocolos de autenticación inseguros; Controladores de Dominio de Solo-lectura; gestión VLAN; Microsoft Baseline Security Analyzer (MBSA)