Elaborar Cuadro Comparativo

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@June 27, 2024
Wochentage	Donnerstag
Deadline	@June 27, 2024
Status	Sended
Attached files	Unidad_23_GuiaActividad_Elaborar Cuadro Comparativo VPN^J Malwaare^J Análisis de Riesgo.pdf

Descripción e Instrucciones

Descripción:

Elabora cuadros comparativos del Material de lectura “Unidad_21 VPN_CD_CERT_Malware_AnalisisRiesgo_Material_Lectura.pdf” para cada uno de los temas siguientes, destacando las características más relevantes y sus diferencias.
Asegúrate de incluir detalles específicos y ejemplos donde sea aplicable. Utiliza la información proporcionada en el material de lectura.

Temas:

1. Red Privada Virtual (VPN)

2. Modelos de VPN (Acceso Remoto, Site-to-Site, Host-to-Host, Extranet Access)
3. Modos de Cifrado en VPN (Túnel vs. Transporte)
4. Certificados Digitales
5. Autoridades de Certificación
6. CERTs (Computer Emergency Response Team)
7. Software Malicioso (Malware)
8. Análisis de Riesgos

Requisitos:

1. Formato: Utiliza un formato de tabla para cada tema, comparando las características más relevantes y las diferencias entre ellas.
2. Contenido: Asegúrate de incluir:
   o Definición de cada concepto.
   o Características principales.
   o Ventajas y desventajas (si aplican).
   o Ejemplos específicos.
   o Comparaciones directas entre subcategorías o modelos (por ejemplo, VPN de acceso remoto vs. VPN de sitio a sitio).
3. Extensión: Cada cuadro comparativo debe tener al menos 5 filas y 3 columnas.

Instrucciones:

1. Leer el material: Asegúrate de leer y comprender la información proporcionada en el material de lectura sobre cada tema.
2. Investigación adicional: Si es necesario, realiza una investigación adicional para obtener más detalles y ejemplos específicos.
3. Elaborar cuadros: Crea cuadros comparativos claros y bien organizados, destacando las diferencias y similitudes más importantes.

Desarrollo

1. Red Privada Virtual (VPN)

Característica	VPN de Confianza	VPN Segura	VPN Híbrida
Definición	Utiliza infraestructura propia o alquilada	Utiliza cifrado para garantizar privacidad	Combina VPN de confianza y segura
Propiedad de Infraestructura	Propiedad exclusiva o alquilada	Puede utilizar infraestructura pública	Puede utilizar ambas
Costo	Alto	Medio a bajo	Varía
Seguridad	Depende de la confianza en la infraestructura	Alta, debido al uso de cifrado	Alta, combina ventajas de ambos tipos
Ejemplos	Redes privadas empresariales grandes	VPNs comerciales como NordVPN	VPNs empresariales complejas

2. Modelos de VPN

Característica	Acceso Remoto	Site-to-Site	Host-to-Host	Extranet Access
Definición	Permite a usuarios conectarse a una red	Conecta dos redes completas a través de	Conecta dos hosts individuales	Permite a socios externos acceder a una

	remota a través de internet	internet		parte de la red
Uso Común	Teletrabajo, acceso móvil	Conexión de oficinas o sucursales	Conexión segura entre dos dispositivos	Colaboración entre empresas
Seguridad	Alta, depende del cifrado	Alta, con uso de túneles cifrados	Alta, generalmente usa IPsec	Alta, con políticas de acceso estrictas
Costo	Bajo a medio	Medio a alto	Medio	Medio a alto
Ejemplos	VPNs comerciales para trabajadores	Conexión entre sedes corporativas	Conexión segura entre servidores	Acceso a aplicaciones compartidas

3. Modos de Cifrado en VPN

Característica	Modo Túnel	Modo Transporte
Definición	Encapsula todo el paquete IP	Solo el payload del paquete IP es cifrado
Uso Común	VPN de sitio a sitio, VPN de acceso remoto	Comunicación entre hosts o aplicaciones específicas
Seguridad	Alta, cifra todo el paquete	Alta, pero más eficiente en términos de rendimiento
Costo	Varía dependiendo del proveedor y la infraestructura	Generalmente más bajo debido a menor carga de procesamiento
Ejemplos	Conexión entre oficinas, acceso remoto seguro	Aplicaciones específicas, VPNs ligeras

4. Certificados Digitales

Característica	Certificados SSL/TLS	Certificados de firma de correo electrónico	Certificados de código de software
Definición	Certificados utilizados para asegurar comunicaciones en línea y verificar la identidad de un sitio web.	Certificados utilizados para firmar electrónicamente correos electrónicos, garantizando su autenticidad y la integridad del contenido.	Certificados utilizados para firmar digitalmente código de software para asegurar su autenticidad e integridad.
Usos Principales	Autenticación del servidor web, cifrado de datos transmitidos.	Firmar correos electrónicos para verificar la autenticidad del remitente y la integridad del mensaje.	Firmar y proteger el código de software para evitar modificaciones no autorizadas y garantizar la seguridad.
Ventajas	Mejora la seguridad del sitio web, genera confianza entre los usuarios.	Asegura la autenticidad de los correos electrónicos y protege contra la falsificación de identidad.	Protección contra la modificación no autorizada del código, validación de la fuente del software.
Desventajas	Costos asociados, necesidad de renovación periódica y gestión de claves.	Requiere configuración y gestión adecuada de claves privadas, puede ser costoso en términos de implementación y mantenimiento.	Requiere procedimientos estrictos para la gestión de claves y certificados, costos de implementación y actualización.
Ejemplos	Let's Encrypt, VeriSign, Comodo	S/MIME (Secure/Multipurpose Internet Mail Extensions) certificates	Microsoft Authenticode, Apple Developer ID

5. Autoridades de Certificación (CA)

Característica	Autoridades de Certificación (CA)
Definición	Entidades que emiten y gestionan certificados digitales
Funciones Principales	Emisión, revocación y renovación de certificados
Ventajas	Establecen confianza, aseguran autenticidad
Desventajas	Puede ser costoso, centralización
Ejemplos	DigiCert, Let's Encrypt, Comodo

6. CERTs (Computer Emergency Response Team)

Característica	CERT-PY	US-CERT	CERT Privado
Definición	Equipo nacional que responde a incidentes de seguridad informática.	Equipo nacional de EE.UU. para la respuesta a incidentes de ciberseguridad.	Equipo privado dedicado a la respuesta a incidentes de seguridad informática.
Funciones Principales	Gestión de incidentes, coordinación de respuestas en Paraguay.	Coordinación y gestión de respuestas a nivel nacional en EE.UU.	Respuesta a incidentes específicos para organizaciones privadas.
Ventajas	Conocimiento profundo del entorno local y regulaciones.	Amplia experiencia y recursos a nivel nacional.	Enfoque personalizado y adaptado a las necesidades internas.
Desventajas	Dependencia de recursos limitados comparado con certificados más grandes.	Requiere coordinación con múltiples agencias y grandes volúmenes de incidentes.	Menos recursos comparado con los CERTs nacionales.

7. Software Malicioso (Malware)

Característica	Virus	Gusano	Troyano	Ransomware	Spyware
Definición	Programa que se replica a sí mismo	Se auto-replica sin necesidad de un archivo huésped	Se disfraza de software legítimo	Bloquea el acceso a datos hasta que se pague un rescate	Espía la actividad del usuario
Ejemplos	ILoveYou, Melissa	WannaCry, Blaster	Zeus, Trojan.Generic	CryptoLocker, WannaCry	Keyloggers, Adware
Impacto	Daño a archivos, pérdida de datos	Saturación de redes, daño a sistemas	Robo de información, control remoto	Pérdida de acceso a datos, demanda de pago	Robo de información, violación de privacidad

8. Análisis de Riesgos

Característica	Fase 1: Definir el Alcance	Fase 2: Identificar Activos	Fase 3: Identificar Amenazas	Fase 4: Identificar Vulnerabilidades	Fase 5: Evaluar el Riesgo	Fase 6: Tratar el Riesgo
Definición	Establece los límites del análisis	Inventario de recursos importantes	Evaluación de posibles amenazas	Evaluación de debilidades	Cálculo de riesgo	Gestión de riesgos identificados
Actividades Principales	Determina qué sistemas y procesos serán evaluados	Identifica los recursos críticos	Identifica las posibles amenazas a los activos	Identifica las debilidades de los activos	Estima probabilidad e impacto de amenazas	Implementar estrategias de mitigación
Resultados Esperados	Claridad en el alcance del análisis	Listado de activos relevantes	Listado de amenazas potenciales	Identificación de puntos débiles	Cálculo del riesgo total	Reducción del riesgo a niveles aceptables