IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

RESUMEN

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA
3. RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA EN EL MARCO DE LOS SISTEMAS DE LA INFORMACIÓN
4. CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR
5. TIPOS DE PRUEBAS A REALIZAR EN EL MARCO DE LA AUDITORÍA. PRUEBAS SUSTANTIVAS Y PRUEBAS DE CUMPLIMIENTO
6. TIPOS DE MUESTREO A APLICAR DURANTE EL PROCESO DE AUDITORÍA
7. UTILIZACIÓN DE HERRAMIENTAS TIPO CAAT (COMPUTER ASSISTED AUDIT TOOLS)
8. EXPLICACIÓN DE LOS REQUERIMIENTOS QUE DEBEN CUMPLIR LOS HALLAZGOS DE AUDITORÍA
9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES
10. RELACIÓN DE LAS NORMATIVAS Y METODOLOGÍAS RELACIONADAS CON LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMÚNMENTE ACEPTADAS

RESUMEN

LA **AUDITORÍA INFORMÁTICA** CONSISTE EN *EL **ANÁLISIS EXHAUSTIVO DE LOS SISTEMAS DE INFORMACIÓN DE UNA ORGANIZACIÓN CON LA FINALIDAD DE DETECTAR, IDENTIFICAR Y DESCRIBIR LAS DISTINTAS VULNERABILIDADES QUE PUEDAN PRESENTARSE*.**

PARA QUE LA AUDITORÍA SE LLEVE A CABO SATISFACTORIAMENTE, **ES DE VITAL IMPORTANCIA LA FIGURA DEL AUDITOR**, QUE DEBE ACTUAR CONFORME A UN *CÓDIGO DEONTOLÓGICO Y UN CÓDIGO ÉTICO* PARA QUE LAS ACTIVIDADES SE DESARROLLEN CON OBJETIVIDAD E INDEPENDENCIA.

NO ES NECESARIO QUE EL AUDITOR SEA UNA SOLA PERSONA, TODO LO CONTRARIO, **SE RECOMIENDA QUE EXISTA UN EQUIPO AUDITOR** EN EL QUE *CADA UNO DE LOS MIEMBROS ESTÉ ESPECIALIZADO EN ÁREAS DISTINTAS DE LA AUDITORÍA* PARA QUE EJECUTEN SUS TAREAS DE UN MODO COMPLEMENTARIO Y ASÍ AUMENTAR LA CALIDAD DEL INFORME ELABORADO.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RESUMEN

UN **RIESGO** ES CUALQUIER TIPO DE *EVENTO O CONJUNTO DE EVENTOS QUE PUEDE PONER EN RIESGO UN PROYECTO DE LA ORGANIZACIÓN O IMPEDIR EL CUMPLIMIENTO DE SUS OBJETIVOS*.

A PESAR DE EXISTIR VARIOS TIPOS DE RIESGO, LA **GESTIÓN DE RIESGOS** *ES UN CONJUNTO DE PROCESOS CON LA FINALIDAD DE DISMINUIR LA PROBABILIDAD DE AMENAZAS Y ATAQUES SOBRE LOS ACTIVOS* MÁS IMPORTANTES DE LA ORGANIZACIÓN.

EL PROCEDIMIENTO DE GESTIÓN DE RIESGOS SIGUE UNAS FASES BIEN MARCADAS.

EN PRIMER LUGAR, **SE IDENTIFICAN Y VALORAN LOS ACTIVOS** DE LA **ORGANIZACIÓN Y LA DEGRADACIÓN** QUE PUEDEN SUFRIR EN CASO DE MATERIALIZARSE UNA AMENAZA (**IMPACTO**).

UNA VEZ IDENTIFICADOS LOS ACTIVOS Y LOS IMPACTOS SE DEBEN **IDENTIFICAR Y ANALIZAR LAS VULNERABILIDADES** DE ESTOS CON EL FIN DE **ESTIMAR LA FRECUENCIA Y PROBABILIDAD** DE MATERIALIZACIÓN DE AMENAZAS Y CÓMO PODER REDUCIRLAS.

RESUMEN

CON EL IMPACTO Y LAS PROBABILIDADES ESTIMADAS, SE PUEDE PROCEDER A **CALCULAR EL RIESGO POTENCIAL DE CADA ACTIVO Y**, CONJUNTAMENTE, **EL RIESGO POTENCIAL** GLOBAL DE LA ORGANIZACIÓN.

ADEMÁS, **CON EL ANÁLISIS DE LAS SALVAGUARDAS SE PODRÁ CONOCER EL RIESGO RESIDUAL** Y EVALUAR SI ESTAS ESTÁN CUMPLIENDO CON SU COMETIDO O SI, POR EL CONTRARIO, NECESITAN TAREAS DE REVISIÓN.

EL ANÁLISIS Y GESTIÓN DE RIESGOS PERMITE A LAS ORGANIZACIONES DEFINIR ESTRATEGIAS PARA REDUCIR LA PROBABILIDAD DE OCURRENCIA DE AMENAZAS Y EL DAÑO QUE ESTAS PUEDEN CAUSAR EN CASO DE MATERIALIZARSE.

POR ELLO, NO SON POCOS LOS ORGANISMOS ENCARGADOS DE DISEÑAR HERRAMIENTAS Y METODOLOGÍAS QUE SIRVAN DE GUÍA A LAS ORGANIZACIONES PARA QUE ESTAS ELABOREN POLÍTICAS PROPIAS DE GESTIÓN DE RIESGOS; A DESTACAR LA METODOLOGÍA **MAGERIT** (DE CARÁCTER NACIONAL) Y LA METODOLOGÍA **NIST** SP 800-30 (DE CARÁCTER INTERNACIONAL).

CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

RESUMEN

EN LA AUDITORÍA DE SISTEMAS, FRECUENTEMENTE SE UTILIZAN HERRAMIENTAS QUE AYUDEN EN LA DETECCIÓN DE FALLOS Y VULNERABILIDADES QUE PERMITAN ESTIMAR EL RIESGO DEL SISTEMA DE INFORMACIÓN Y FORMULAR MEDIDAS CORRECTIVAS Y CONTROLES.

POR UNA PARTE, DENTRO DEL MISMO SISTEMA OPERATIVO DE LOS EQUIPOS SE ENCUENTRAN VARIAS HERRAMIENTAS DE AUDITORÍA, COMO **PING** O **TRACEROUTE**, QUE PERMITEN DETECTAR FALLOS Y ANOMALÍAS EN SU RED.

ADEMÁS, SE RECOMIENDA QUE EL AUDITOR DISPONGA DE HERRAMIENTAS QUE **ANALICEN LA RED, LOS PUERTOS Y LOS SERVICIOS** CONFIGURADOS EN ESTA PARA DETECTAR POSIBLES VÍAS DE ENTRADA DE INTRUSOS Y TRÁFICO DE RED INUSUAL QUE OFREZCA INDICIOS DE AMENAZA. EJEMPLOS DE ESTAS HERRAMIENTAS SON **NETCAT, NMAP Y NBTSCAN**.

RESUMEN

TAMBIÉN SIRVEN PARA EVALUAR LA SEGURIDAD DE UNA RED **LOS ANALIZADORES DE PROTOCOLOS**, QUE ANALIZAN PAQUETES DE DATOS QUE SE TRANSMITEN EN LA RED PARA DETECTAR ERRORES DE CONFIGURACIÓN, DE CONEXIÓN, ETC.

OTRA HERRAMIENTA FUNDAMENTAL Y DE GRAN UTILIDAD PARA EL AUDITOR ES **UN ANALIZADOR DE VULNERABILIDADES** CAPAZ DE IDENTIFICARLAS, EMITIR INFORMES CON LOS RESULTADOS OBTENIDOS Y FORMULAR PROPUESTAS DE SOLUCIÓN.

POR OTRA PARTE Y A NIVEL EXTERNO, EXISTEN LOS **ANALIZADORES DE PÁGINAS WEB**, CUYA FUNCIÓN PRINCIPAL ES CONOCER LA ESTRUCTURA DE LOS SITIOS WEB Y DETECTAR SUS VULNERABILIDADES PARA EVITAR QUE SUFRAN ATAQUES DE SEGURIDAD.

ESTAS HERRAMIENTAS, JUNTO CON LAS **HERRAMIENTAS DE ATAQUES DE DICCIONARIO Y FUERZA BRUTA,** SIRVEN PARA QUE EL AUDITOR DETECTE VÍAS DE ATAQUE E INTRUSIONES, QUE DEBERÁN SER SOLUCIONADAS PARA DISMINUIR EL RIESGO DEL SISTEMA DE INFORMACIÓN Y DE LA ORGANIZACIÓN EN GENERAL.

CONTENIDOS

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

RESUMEN

UN **CORTAFUEGOS** ES UN SISTEMA COMPUESTO POR UNO O VARIOS DISPOSITIVOS CUYA FUNCIÓN PRINCIPAL ES LA SEPARACIÓN ENTRE LA RED LOCAL DE UN SISTEMA DE INFORMACIÓN Y LA RED EXTERIOR, DE MODO QUE SE IMPIDA LA ENTRADA DE ATAQUES Y SE INCREMENTE LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN.

EL **PERÍMETRO DE SEGURIDAD** ES EL ESPACIO PROTEGIDO POR EL CORTAFUEGOS, MIENTRAS QUE **LA ZONA DE RIESGO** ES LA RED FRENTE A LA QUE SE PROTEGE DICHO PERÍMETRO DE SEGURIDAD.

PARA DETERMINAR LA CONFIGURACIÓN DE UN CORTAFUEGOS, DEBEN TENERSE EN CUENTA TRES CARACTERÍSTICAS FUNDAMENTALES: **LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN, LA MONITORIZACIÓN DEL CORTAFUEGOS Y LA ECONOMÍA** Y PRESUPUESTO QUE SE ESTÁ DISPUESTO A ASUMIR.

RESUMEN

ATENDIENDO A ESTAS CARACTERÍSTICAS, SE PUEDEN IMPLANTAR DISTINTOS TIPOS DE CORTAFUEGOS SEGÚN SU UBICACIÓN Y FUNCIONALIDAD.

LOS **ROUTERS CON FILTRADO DE PAQUETES** SON CORTAFUEGOS QUE FILTRAN LOS PAQUETES DE DATOS ENTRANTES ATENDIENDO A UNA SERIE DE REGLAS PREDEFINIDAS. LOS **GATEWAYS O PASARELAS A NIVEL DE APLICACIÓN** ANALIZAN EL TRÁFICO ATENDIENDO A LOS SERVICIOS SOLICITADOS (PERMITIENDO EL ACCESO SOLO A DETERMINADAS APLICACIONES) Y **LOS GATEWAYS O PASARELAS A NIVEL DE CIRCUITO** REDIRIGEN LOS PAQUETES DE DATOS UNA VEZ VALIDADA LA CONEXIÓN.

LA ELECCIÓN DE IMPLANTAR UN TIPO DE CORTAFUEGOS U OTRO DEPENDERÁ DE LAS PREFERENCIAS DE SEGURIDAD DE LA ORGANIZACIÓN, ADEMÁS DEL VALOR DE LOS ACTIVOS Y DE LA INFORMACIÓN QUE SE DESEA PROTEGER.

RESUMEN

SI ENTRE ESTOS TIPOS DE CORTAFUEGOS NO HAY NINGUNO QUE SE ADAPTE LOS SUFICIENTE A LOS OBJETIVOS DE LA ORGANIZACIÓN, SE PUEDEN IMPLANTAR CORTAFUEGOS CON ARQUITECTURAS MÁS COMPLEJAS, COMO LOS CORTAFUEGOS **DUAL-HOMED HOST**, LOS CORTAFUEGOS **SCREENED HOST** Y LAS ARQUITECTURAS **SCREENED SUBNET** (QUE UTILIZAN ZONA DESMILITARIZADA COMO MEDIDA ADICIONAL DE PROTECCIÓN).

CONTENIDOS

1. INTRODUCCIÓN
2. GUÍA PARA LA AUDITORÍA DE LA DOCUMENTACIÓN Y NORMATIVA DE SEGURIDAD EXISTENTE EN LA ORGANIZACIÓN AUDITADA
3. GUÍA PARA LA ELABORACIÓN DEL PLAN DE AUDITORÍA
4. GUÍA PARA LAS PRUEBAS DE AUDITORÍA
5. GUÍA PARA LA ELABORACIÓN DEL INFORME DE AUDITORÍA

RESUMEN

LA REALIZACIÓN DE LAS TAREAS DE AUDITORÍA DE UN SISTEMA DE INFORMACIÓN SE DIVIDE EN VARIAS FASES.

- EN PRIMER LUGAR, **SE AUDITAN LA DOCUMENTACIÓN Y LA NORMATIVA** DE SEGURIDAD QUE PUEDAN VERSE RELACIONADOS CON EL SISTEMA A AUDITAR. LO MÁS FRECUENTE ES LA REVISIÓN Y COMPROBACIÓN DE LAS NORMAS DE AUDITORÍA Y DE LAS NORMAS REFERENTES A LA PROTECCIÓN DE DATOS PERSONALES.

RESUMEN

- A CONTINUACIÓN, UNA VEZ OBTENIDA Y REVISADA TODA LA DOCUMENTACIÓN NECESARIA Y LA NORMATIVA IMPLICADA, **SE DEBE REALIZAR UN PLAN DE AUDITORÍA**, EN EL QUE SE DESCRIBEN LOS OBJETIVOS, LAS PARTES IMPLICADAS Y LAS TAREAS A DESARROLLAR DURANTE TODO EL PROCESO AUDITOR.
- EN TERCER LUGAR, CUANDO YA SE TIENE DEFINIDA LA PLANIFICACIÓN DE LAS TAREAS AUDITORAS, SE PUEDE PROCEDER A LA **REALIZACIÓN DE LAS PRUEBAS DE AUDITORÍA**. LA ELECCIÓN DE LAS PRUEBAS A EJECUTAR DEPENDERÁ DE LAS CARACTERÍSTICAS DE LA ORGANIZACIÓN, DE LAS DEL SISTEMA DE ORGANIZACIÓN Y DE LOS ASPECTOS PRINCIPALES QUE SE DESEAN AUDITAR, ENTRE OTROS FACTORES.

RESUMEN

- POR ÚLTIMO, CON LOS RESULTADOS OBTENIDOS CON LAS PRUEBAS DE AUDITORÍA SE REALIZA UNO DE LOS DOCUMENTOS MÁS RELEVANTES DE LA AUDITORÍA: **EL INFORME DE AUDITORÍA**. ESTE ESTARÁ FORMADO POR VARIOS DOCUMENTOS Y DEBERÁ SER REDACTADO DE MODO QUE SE REFLEJEN A LA PERFECCIÓN LA SITUACIÓN REAL DEL SISTEMA DE UN MODO COMPRENSIBLE PARA LA ORGANIZACIÓN Y LAS SUGERENCIAS Y RECOMENDACIONES FORMULADAS POR EL PROFESIONAL AUDITOR.

ACTIVIDADES

- ACTIVIDAD 01. INSTALACIÓN DE KALI LINUX
- ACTIVIDAD 02. SEGURIDAD EN CONEXIONES INALÁMBRICAS
- ACTIVIDAD 03. GIT Y GITHUB
- ACTIVIDAD 04. BASTIONADO, DEFENSA EN PROFUNDIDAD , CIBER RESILIENCIA Y ZERO TRUST
- ACTIVIDAD 05. SOFTWARE DE VIRTUALIZACIÓN
- ACTIVIDAD 06. INSTALACION DE METASPLOITABLE 2
- ACTIVIDAD 07. HERRAMIENTAS BÁSICAS DE RED
- ACTIVIDAD 08. USO DE HERRAMIENTA NMAP (E1)
- ACTIVIDAD 09. LA AUDITORÍA INFORMÁTICA. EL AUDITOR
- ACTIVIDAD 10. USO DE HERRAMIENTA METASPLOIT

ACTIVIDADES

- ACTIVIDAD 11. INSTALACION DE METASPLOITABLE 3
- ACTIVIDAD 12. MATRIZ DE RIESGOS
- ACTIVIDAD 13. PRUEBA DE PENTESTING (E2)
- ACTIVIDAD 14. SEGURIDAD EN NAVEGADORES Y NAVEGACIÓN SEGURA
- ACTIVIDAD 15. USO DE HERRAMIENTAS DE RECONOCIMIENTO
- ACTIVIDAD 16. USO DE WIRESHARK (E3)
- ACTIVIDAD 17. SERVICIOS EN WINDOWS Y LINUX
- ACTIVIDAD 18. USO DE FIREWALL

ANEXOS

- COMANDOS DE GIT BÁSICOS
- HACKING ÉTICO-01-INTRODUCIÓN
- NORMA ISO 31000-2018. GESTIÓN DEL RIESGO
- SOFTWARE DE VIRTUALIZACIÓN EN SEGURIDAD INFORMÁTICA
- HERRAMIENTAS DE RED LINUX Y WINDOWS
- NMAP
- HACKING ÉTICO-02-RECONOCIMIENTO
- PRUEBA DE PENTESTING
- GUÍAS DE AUDITORIA INFORMÁTICA
- SEGURIDAD EN NAVEGADORES
- AUDITORÍA DE LA SEGURIDAD INFORMÁTICA
- WIRESHARK

ESTO ES TODO