IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

ANEXO

HACKING ÉTICO INTRODUCCIÓN

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

- **DEFINICIONES Y CONCEPTOS BÁSICOS**
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

DEFINICIONES Y CONCEPTOS BÁSICOS

"LOS MALES, CUANDO SE LOS DESCUBRE A TIEMPO, SE LOS CURA PRONTO; PERO YA NO TIENEN REMEDIO CUANDO, POR NO HABERLOS ADVERTIDO, SE LOS DEJA CRECER HASTA EL PUNTO DE QUE TODO EL MUNDO LOS VE."

NICOLÁS MAQUIAVELO

DEFINICIONES Y CONCEPTOS BÁSICOS

DIARIAMENTE SE PRODUCEN NUMEROSOS CIBERATAQUES; CUANDO ALGUNO DE ELLOS ES DETECTADO **SURGEN VARIAS PREGUNTAS**:

¿QUIÉN HA SIDO?

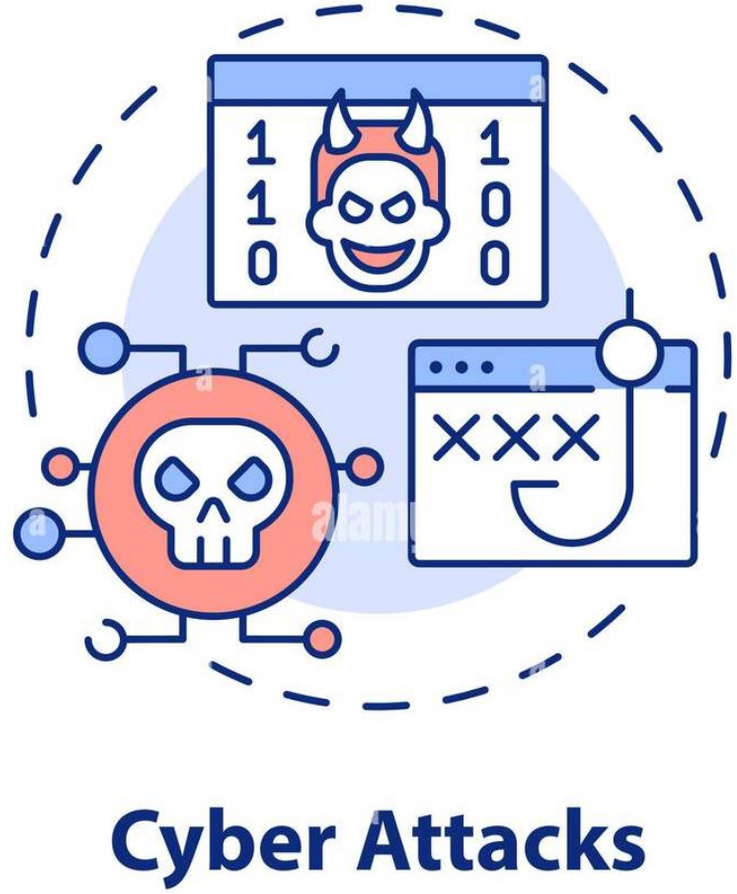
¿ CUÁNDO ENTRÓ EN LOS SISTEMAS?

¿QUÉ HA HECHO Y QUÉ SE HA LLEVADO?

¿CUÁNTO TIEMPO HA ESTADO DENTRO Y CÓMO CONSIGUIÓ ACCEDER?

DEFINICIONES Y CONCEPTOS BÁSICOS

ES PROBABLE QUE NUNCA SE PUEDA IDENTIFICAR AL ATACANTE, Y AVERIGUAR LO QUE HA HECHO EN EL SISTEMA PUEDE REQUERIR UN PROCESO LARGO Y COSTOSO, PERO LO QUE ES AÚN **MÁS PREOCUPANTE PARA MUCHAS ORGANIZACIONES ES SI PODRÁ RECUPERARSE DE LOS DAÑOS Y RECUPERAR LA INFORMACIÓN PERDIDA.**



DEFINICIONES Y CONCEPTOS BÁSICOS

SIN EMBARGO, **SI LA ORGANIZACIÓN HUBIERA IDENTIFICADO PREVIAMENTE EL CÓMO Y EL QUÉ, HABRÍA PODIDO PROTEGERSE** DE UNA MANERA MÁS ADECUADA Y EVITAR EL ATAQUE O, AL MENOS, APRENDER DE SUS VULNERABILIDADES PARA MINIMIZAR LOS DAÑOS.

DEFINICIONES Y CONCEPTOS BÁSICOS

EL OBJETIVO DE LA CIBERSEGURIDAD ES MINIMIZAR LOS RIESGOS, REDUCIENDO LAS VULNERABILIDADES Y BLOQUEANDO LAS AMENAZAS.

ES UN PROCESO CONTINUO QUE VA DESDE LA DETECCIÓN DE LAS VULNERABILIDADES HASTA EL ANÁLISIS DE LOS ATAQUES RECIBIDOS, PASANDO POR LA MONITORIZACIÓN EN TIEMPO REAL DE LO QUE SUCEDE EN LOS SISTEMAS.

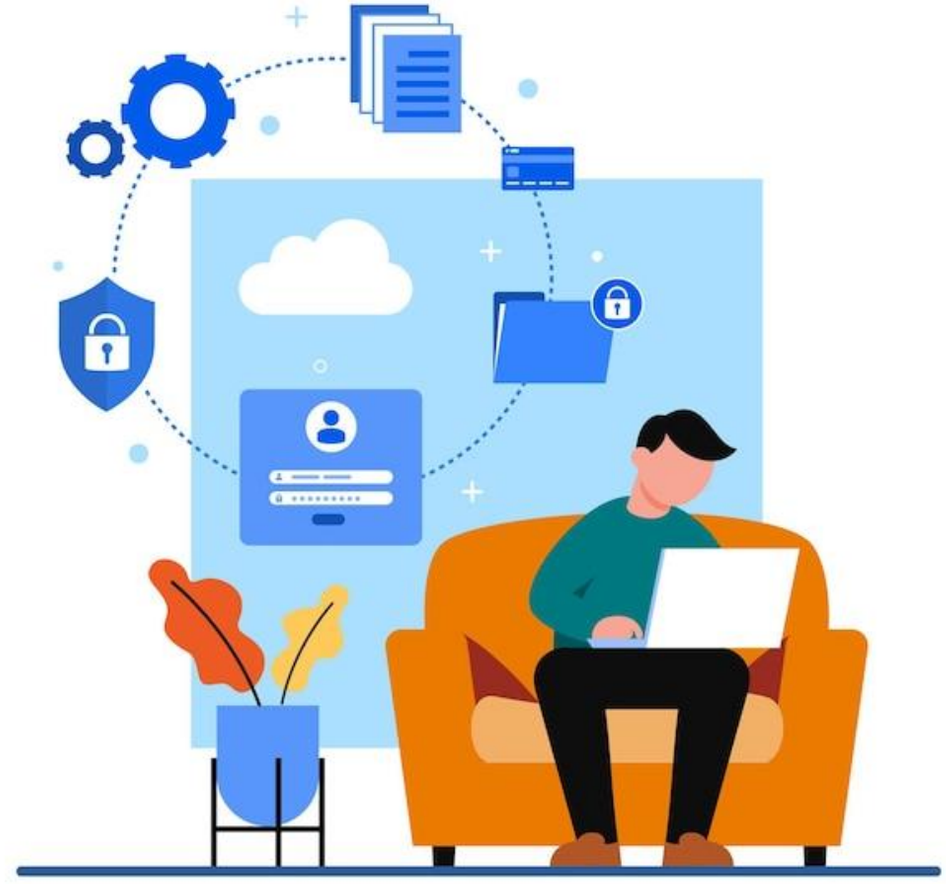
CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- **PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN**
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

CUANDO HABLAMOS DE LA **SEGURIDAD DE LA INFORMACIÓN** NOS REFERIMOS A LAS **MEDIDAS PARA PROTEGER LA INFORMACIÓN SENSIBLE** DE UNA ORGANIZACIÓN O PERSONA.

AUNQUE ABARCA TAMBIÉN LA INFORMACIÓN PROCESADA O ALMACENADA EN SISTEMAS NO INFORMÁTICOS, **ES UN CONCEPTO ÍNTIMAMENTE RELACIONADO CON LA CIBERSEGURIDAD**, PUESTO QUE, HOY EN DÍA, LA MAYOR PARTE DE LA INFORMACIÓN SE PROCESA O ALMACENA EN SISTEMAS INFORMÁTICOS.



PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

INDEPENDIENTEMENTE DEL PROPÓSITO FINAL DEL ATACANTE, TODOS **LOS ATAQUES BUSCARÁN AFECTAR AL MENOS A UNA DE LAS DIMENSIONES BÁSICAS DE LA SEGURIDAD DE LA INFORMACIÓN** O DE LOS SISTEMAS.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

UNA CORRECTA SEGURIDAD DE LA INFORMACIÓN CONSISTE ADOPTAR LAS MEDIDAS ADECUADAS PARA PROTEGER ESTAS DIMENSIONES, LO QUE SE TRADUCE EN UN PROCESO CONTINUO DE ACTUALIZACIÓN Y MEJORA DE LAS MEDIDAS DE SEGURIDAD, BASADO EN NUEVAS VULNERABILIDADES Y AMENAZAS.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

CONFIDENCIALIDAD

EL PRINCIPIO DE CONFIDENCIALIDAD SE BASA EN **PROTEGER LA INFORMACIÓN DEL ACCESO POR PARTE DE PERSONAS O SISTEMAS NO AUTORIZADOS**. POR EXTENSIÓN, SE DEBEN PROTEGER TAMBIÉN LOS SISTEMAS Y REDES QUE TRANSMITEN, PROCESAN O ALMACENAN DICHA INFORMACIÓN.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

CONFIDENCIALIDAD

UN ATACANTE PUEDE COMPROMETER LA INFORMACIÓN DE FORMAS SENCILLAS: HACIENDO SHOULDER SURFING CUANDO UN ADMINISTRADOR INTRODUCE SU CONTRASEÑA, O A TRAVÉS DE LO QUE SE HA DADO EN DENOMINAR DUMPSTER DIVING PARA BUSCAR PAPELES CON INFORMACIÓN SENSIBLE.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

INTEGRIDAD

ESTE PRINCIPIO SE BASA EN **EVITAR QUE SE PRODUZCAN CAMBIOS NO AUTORIZADOS EN LA INFORMACIÓN** NI EN LOS SISTEMAS.

UN ATAQUE QUE MODIFIQUE LA INTEGRIDAD DE LA INFORMACIÓN PUEDE TENER CONSECUENCIAS DE TODO TIPO PARA UNA ORGANIZACIÓN:

SE PUEDEN HACER FRAUDES ECONÓMICOS MODIFICANDO NÚMEROS DE CUENTA BANCARIA, DAR ACCESOS A PERSONAS NO AUTORIZADAS MODIFICAR MENSAJES TRANSMITIDOS, ETC.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

DISPONIBILIDAD

PERMITE QUE LA INFORMACIÓN Y LOS SISTEMAS SEAN ACCESIBLES POR LAS PERSONAS O SISTEMAS QUE DEBEN ACCEDER A LOS MISMOS**, EN EL MOMENTO QUE SEA REQUERIDO**.

EJEMPLOS TÍPICOS DE ATAQUES CONTRA LA DISPONIBILIDAD SON LOS DE DENEGACIÓN DE SERVICIO (DOS).

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

AUTENTICIDAD

CONSISTE EN QUE UNA ENTIDAD ES QUIEN DICE SER, DE MODO QUE SE GARANTICE LA FUENTE DE LA QUE PROCEDE LA INFORMACIÓN.

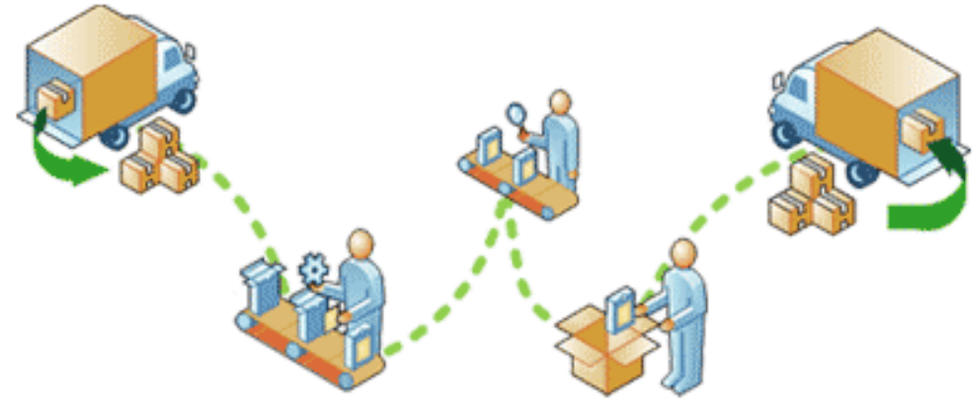
ES DECIR, QUE NO SE HA PRODUCIDO UNA SUPLANTACIÓN DE IDENTIDAD.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

TRAZABILIDAD

CONSISTE EN QUE SE PUEDAN IDENTIFICAR LAS ACCIONES REALIZADAS SOBRE LA INFORMACIÓN Y LOS SISTEMAS, DE MODO QUE SE PUEDA DETERMINAR QUIÉN Y CUÁNDO HA ACCEDIDO Y HA REALIZADO LAS MODIFICACIONES.

ESTE PRINCIPIO TAMBIÉN SE PUEDE DENOMINAR **AUDITORÍA**.



CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- **DEFINICIONES BÁSICAS**
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

DEFINICIONES BÁSICAS

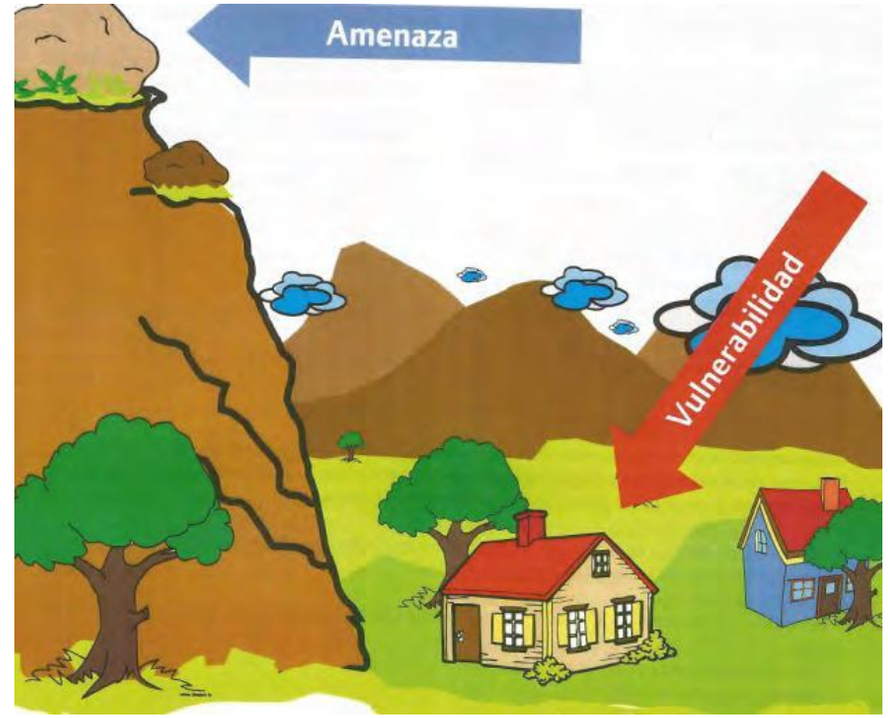
RIESGO, VULNERABILIDAD Y AMENAZA

UNA AMENAZA ES **UN AGENTE QUE PUEDE CAUSAR UN DAÑO**.

ALGUNAS AMENAZAS SON **NATURALES,** COMO INUNDACIONES, INCENDIOS O TERREMOTOS.

OTRAS TIENEN UN ORIGEN MÁS HUMANO Y PUEDEN SER **INTENCIONADAS O NO INTENCIONADAS**.

DE MANERA RESUMIDA, **LA AMENAZA SERÁ EL ATACANTE.**

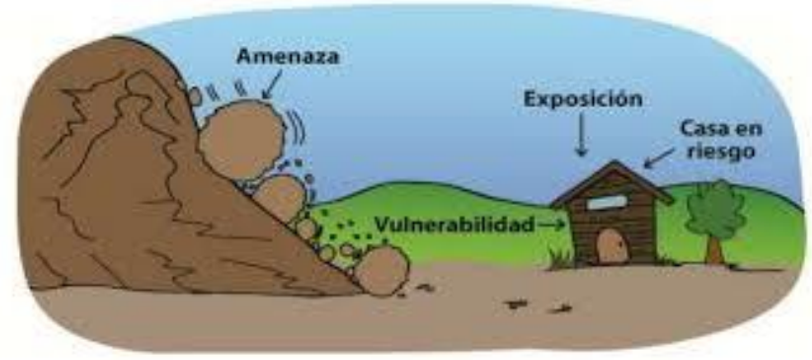


DEFINICIONES BÁSICAS

RIESGO, VULNERABILIDAD Y AMENAZA

UNA **VULNERABILIDAD ES UNA DEBILIDAD O UN FALLO QUE SE PUEDE UTILIZAR PARA CAUSAR UN DAÑO** DE MANERA VOLUNTARIA O INVOLUNTARIA.

ALGUNOS TIPOS DE VULNERABILIDADES SON FALLOS EN EL DESARROLLO DEL SOFTWARE O EN EL DISEÑO DEL HARDWARE, UN MAL DISEÑO DE LA ARQUITECTURA DE LOS SISTEMAS O MALAS CONFIGURACIONES.



DEFINICIONES BÁSICAS

RIESGO, VULNERABILIDAD Y AMENAZA

EL **RIESGO** ES **LA POSIBILIDAD DE QUE UNA AMENAZA EXPLOTE UNA VULNERABILIDAD**.

UNA AMENAZA INTENTARÁ MATERIALIZAR EL RIESGO MEDIANTE UN ATAQUE, PARA LO QUE UTILIZARÁ UN **VECTOR DE ATAQUE**, QUE ES EL CAMINO QUE SIGUE UNA AMENAZA PARA LOGRAR SUS FINES.

DEFINICIONES BÁSICAS

CUANDO SE REALIZA UN **ANÁLISIS DE SEGURIDAD** SURGEN LOS CONCEPTOS DE **CAJA NEGRA, GRIS O BLANCA, REFERIDOS AL GRADO DE CONOCIMIENTO QUE SE TENDRÁ PREVIAMENTE A LA REALIZACIÓN DEL MISMO**.

DEFINICIONES BÁSICAS

ESTE **CONOCIMIENTO** PUEDE VARIAR DESDE SER **NULO** (**CAJA NEGRA**) HASTA **CONOCER TODA LA INFORMACIÓN** DE LOS SISTEMAS (**BLANCA**), LO QUE INCLUYE EL ESQUEMA DE RED Y, TAL VEZ, DISPONER DE UN USUARIO INTERNO CON PRIVILEGIOS ELEVADOS.

ENTRE MEDIAS ESTÁ LA **CAJA GRIS**, QUE ES UN **CONOCIMIENTO PARCIAL** QUE PUEDE IRSE AMPLIANDO POR PARTE DE LA ORGANIZACIÓN SEGÚN SE HAYA ACORDADO PREVIAMENTE.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- **VULNERABILIDADES**
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

VULNERABILIDADES

RESULTA COMPLICADO HACER UNA CLASIFICACIÓN DE TIPOS DE VULNERABILIDADES, DADO QUE ESTAS SE PUEDEN AGRUPAR DE DISTINTAS MANERAS, SEGÚN EL PROPÓSITO DE LA PERSONA U ORGANIZACIÓN QUE ESTABLEZCA LA CLASIFICACIÓN.

LA PRIMERA CLASIFICACIÓN GENERAL QUE SE PUEDE HACER CONSISTE EN CLASIFICAR LAS VULNERABILIDADES **SEGÚN CUAL SEA LA FUENTE** DE LA MISMA, DE MODO QUE SE PODRÍAN IDENTIFICAR:

- ***EN EL HARDWARE***
- ***EN EL DISEÑO E IMPLEMENTACIÓN DE LAS ARQUITECTURAS***
- ***EN EL DESARROLLO DEL SOFTWARE***
- ***EN LA IMPLEMENTACIÓN DEL SOFTWARE***
- ***EN LA OPERACIÓN DEL USUARIO***

VULNERABILIDADES

TIPOS DE VULNERABILIDADES

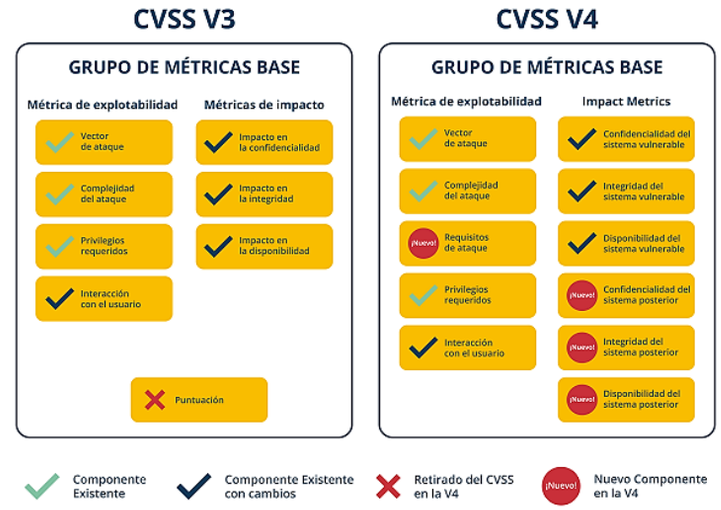
EL **COMMON VULNERABILITY SCORING SYSTEM (CVSS)** ES UN **ESTÁNDAR ABIERTO** DE EVALUACIÓN DE LA GRAVEDAD DE VULNERABILIDADES CONOCIDAS, PARA LO QUE SE **UTILIZAN UNAS MÉTRICAS PARA ASIGNAR UNA PUNTUACIÓN FINAL Y**, A PARTIR DE ELLA, **ESTABLECER LA SEVERIDAD DE LA VULNERABILIDAD** CORRESPONDIENTE.

VULNERABILIDADES

TIPOS DE VULNERABILIDADES

LOS **ASPECTOS** QUE SE VALORAN SON:

- *EL VECTOR DE ACCESO*
- *LA COMPLEJIDAD DE LA EXPLOTACIÓN*
- *EL NIVEL DE AUTENTICACIÓN QUE TIENE QUE TENER EL ATACANTE EN EL SISTEMA*
- *EL IMPACTO SOBRE LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD*



VULNERABILIDADES

TIPOS DE VULNERABILIDADES

UNA VEZ EVALUADOS TODOS ESOS ASPECTOS Y ASIGNADA LA PUNTUACIÓN CORRESPONDIENTE A CADA UNO, ESTAS PUNTUACIONES SE SUMAN PARA DAR LUGAR A UN NÚMERO ENTRE 0 Y 10, QUE SIRVE PARA REFLEJAR LOS SIGUIENTES GRADOS DE SEVERIDAD:

NULA: 0
BAJA: DE 0,1 A 3,9
MEDIA: DE 4,0 A 6,9
ALTA: DE 7,0 A 8,9
CRÍTICA: DE 9 A 10

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

VULNERABILIDADES

TIPOS DE VULNERABILIDADES SEGÚN EL TIEMPO DESDE SU DESCUBRIMIENTO

VULNERABILIDADES DE DÍA CERO (ZERO-DAY)

SE TRATA DE VULNERABILIDADES PARA LAS QUE **NO EXISTEN PARCHES** QUE LAS PUEDAN SOLUCIONAR.

DESDE QUE UN ATACANTE DESCUBRE LA EXISTENCIA DE ESTE TIPO DE VULNERABILIDADES HASTA QUE EL FABRICANTE PUBLICA EL PARCHE PUEDE TRANSCURRIR MUCHO TIEMPO, AÑOS INCLUSO, EN EL QUE EL SISTEMA ESTÁ COMPROMETIDO.

ES POSIBLE QUE LA VULNERABILIDAD SE HAGA PÚBLICA **PERO EL FABRICANTE NO HAYA PODIDO DESARROLLAR AÚN EL PARCHE** CORRESPONDIENTE, DE MODO QUE EL NÚMERO DE POTENCIALES ATACANTES SE INCREMENTA EXPONENCIALMENTE.

VULNERABILIDADES

TIPOS DE VULNERABILIDADES SEGÚN EL TIEMPO DESDE SU DESCUBRIMIENTO

VULNERABILIDADES DE DÍA UNO (ONE-DAY)

LA VULNERABILIDAD ES PÚBLICA Y HA SIDO RECONOCIDA POR EL DESARROLLADOR, QUE PUBLICA LOS PARCHES.

LOS PARCHES NO SE APLICAN INSTANTÁNEAMENTE, PUESTO QUE REQUIEREN DE UN **PROCESO DE PRUEBAS** ACORDE CON LAS POLÍTICAS DE LA ORGANIZACIÓN.

EL PERIODO DE TIEMPO DESDE QUE ESTOS PARCHES SE PUBLICAN HASTA QUE SE APLICAN EN TODOS LOS SISTEMAS **PUEDE SER UTILIZADO POR POTENCIALES ATACANTES**, QUE CONOCERÁN LA EXISTENCIA DE LA VULNERABILIDAD, PODRÁN ESTUDIAR LOS PARCHES PARA VER LA FORMA DE EXPLOTARLA, Y TENDRÁN TIEMPO DE BUSCAR SISTEMAS QUE NO ESTÉN PARCHEADOS.

VULNERABILIDADES

TIPOS DE VULNERABILIDADES SEGÚN EL TIEMPO DESDE SU DESCUBRIMIENTO

VULNERABILIDADES ANTIGUAS

SE TRATA DE VULNERABILIDADES **QUE SE CONOCEN DESDE HACE MÁS TIEMPO**, PARA LAS QUE SUELEN EXISTIR PARCHES O NUEVAS VERSIONES Y TAMBIÉN EXISTEN EXPLOITS PÚBLICOS PARA APROVECHAR LAS MISMAS.

AUN ASÍ, **EN OCASIONES LOS SISTEMAS ESTARÁN SIN PARCHEAR POR DIVERSOS MOTIVOS**, POR LO QUE UN ATACANTE PODRÍA UTILIZAR LAS MISMAS PARA COMPROMETER LOS SISTEMAS.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- **TIPOS DE AMENAZAS**
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

TIPOS DE AMENAZAS

DEJANDO A UN LADO LAS AMENAZAS NATURALES, CONTRA LAS QUE POCO SE PUEDE HACER APARTE DE TENER REDUNDANCIA DE LOS SISTEMAS Y UNAS BUENAS POLÍTICAS DE BACKUP, LAS AMENAZAS SE PUEDEN **CLASIFICAR SEGÚN SU NIVEL DE ORGANIZACIÓN**:

- **POCO ESTRUCTURADAS**
- **ESTRUCTURADAS**
- **MUY ESTRUCTURADAS**

TIPOS DE AMENAZAS

POCO ESTRUCTURADAS

SON **PERSONAS QUE ACTÚAN DE MANERA INDIVIDUAL O GRUPOS PEQUEÑOS**, QUE NO PERTENECEN A NINGUNA ORGANIZACIÓN NI TIENEN FINANCIACIÓN EXTERNA. NORMALMENTE, **LA EXPLOTACIÓN SE BASARÁ EN VULNERABILIDADES CONOCIDAS Y DOCUMENTADAS Y USARÁN TÉCNICAS POCO SOFISTICADAS**.

SUS PROPÓSITOS PUEDEN SER POR **SIMPLE CURIOSIDAD**, PARA **DEMOSTRAR SUS CAPACIDADES**, REALIZAR **ACCIONES DE HACKTIVISMO** O INTENTAR **OBTENER BENEFICIOS ECONÓMICOS**.

LOS **OBJETIVOS** DE ESTAS AMENAZAS SERÁN **OBJETIVOS DE OPORTUNIDAD**, QUE SE PUEDAN DESCUBRIR DURANTE EL RECONOCIMIENTO AL UTILIZAR ALGUNA TÉCNICA O HERRAMIENTA.

TIPOS DE AMENAZAS

ESTRUCTURADAS

SON **GRUPOS ORGANIZADOS**, QUE **TIENEN TIEMPO Y CONOCIMIENTOS PARA PLANIFICAR ADECUADAMENTE SUS ATAQUES** Y PUEDEN TENER ALGÚN MECANISMO DE FINANCIACIÓN.

GENERALMENTE REALIZARÁN **ATAQUES ESPECÍFICOS CONTRA OBJETIVOS CONCRETOS Y ESTABLECIDOS PREVIAMENTE**.

DEDICARÁN MÁS TIEMPO PARA OBTENER TODA LA INFORMACIÓN POSIBLE DEL OBJETIVO Y NORMALMENTE UTILIZARÁN VULNERABILIDADES NO DOCUMENTADAS PARA REALIZAR LA EXPLOTACIÓN.

UN ATAQUE DE RAMSOMWARE CONTRA UNA EMPRESA ENTRARÁ DENTRO DE ESTA CATEGORÍA, AL IGUAL QUE GRUPOS HACKTIVISTAS.

TIPOS DE AMENAZAS

MUY ESTRUCTURADAS

LOS **OBJETIVOS** SON **MUY ESPECÍFICOS**, GENERALMENTE **EMPRESAS ESTRATÉGICAS, OBJETIVOS GUBERNAMENTALES** O PERSONAS PERTENECIENTES A CIERTOS **COLECTIVOS NO AFINES**.

LOS **PROPÓSITOS** DE ESTAS AMENAZAS EXCEDERÁN NORMALMENTE A LOS ECONÓMICOS, ESTANDO MÁS BIEN **ENCAMINADOS A BUSCAR A UNA SUPERIORIDAD ESTRATÉGICA U OPERACIONAL**.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- **TIPOS DE ATAQUES**
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

TIPOS DE ATAQUES

ALGUNOS DE LOS **CRITERIOS MÁS HABITUALES** PARA CLASIFICAR LOS CIBERATAQUES SON **EL PROPÓSITO O EL VECTOR DE ATAQUE UTILIZADO**.

OTRA POSIBLE CLASIFICACIÓN SERÍA **SEGÚN EL PRINCIPIO ATACADO** (*CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD O AUTENTICIDAD*).

TAMBIÉN PODRÍAN DIVIDIRSE EN **ACTIVOS O PASIVOS**, O **CLASIFICARSE SEGÚN EL OBJETIVO ATACADO** (RED, WIFI, CLIENTE, PERSONA…).

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU PROPÓSITO

CIBERESPIONAJE

ESTOS ATAQUES CONSISTEN EN REALIZAR **ACCIONES DE ESPIONAJES EN EL CIBERESPACIO**, O UTILIZANDO EL CIBERESPACIO COMO MEDIO, DE MODO QUE SE OBTENGA INFORMACIÓN PERTENECIENTE A **EMPRESAS, ORGANIZACIONES GUBERNAMENTALES O PERSONAS** PERTENECIENTES A **ORGANIZACIONES NO ALINEADAS CON EL ATACANTE.**

ESTE TIPO DE ATAQUES **NORMALMENTE SE LLEVARÁ A CABO POR ESTADOS O POR EMPRESAS** QUE TIENEN EL FIN DE OBTENER INFORMACIÓN SOBRE EMPRESAS RIVALES.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU PROPÓSITO

CIBERCRIMEN/CIBERDELITO

ACCIONES DELICTIVAS QUE **EMPLEAN EL CIBERESPACIO COMO HERRAMIENTA O COMO OBJETIVO**

ABARCA TANTO **ACTIVIDADES DELICTIVAS TRADICIONALES** (TIMOS, SUPLANTACIONES DE IDENTIDAD, VENTA DE DROGAS O DE ARMAS), COMO **DELITOS ESPECÍFICOS DE LOS SISTEMAS DE INFORMACIÓN** (DENEGACIONES DE SERVICIO, DEGRADACIÓN DE SISTEMAS).

EL **PROPÓSITO** SERÁ **ECONÓMICO**. ESTE TIPO DE ATAQUES **SE DIRIGEN CONTRA EMPRESAS, PERSONAS INDIVIDUALES O CONTRA ORGANISMOS PÚBLICOS**, Y SE LLEVARÁ A CABO POR **ORGANIZACIONES CRIMINALES** O POR INDIVIDUOS A SUELDO.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU PROPÓSITO

HACKTIVISMO

BUSCAN **CONTROLAR O DAÑAR EQUIPOS Y SISTEMAS CON EL FIN DE DAR VISIBILIDAD A UNA CAUSA**. LAS MOTIVACIONES PUEDEN SER POLÍTICAS, IDEOLÓGICAS, BÚSQUEDA DE VENGANZA,ETC.

EJEMPLOS DE ATAQUES SON LAS ACCIONES EN LAS QUE LOS ATACANTES PUBLICAN BASES DE DATOS TRAS ATACAR A UNA EMPRESA, O LOS DEFACEMENT DE SITIOS WEB PARA MOSTRAR UN MENSAJE CONTRARIO A LA EMPRESA PROPIETARIA DEL MISMO.

ESTE TIPO DE ATAQUES NORMALMENTE **SE LLEVARÁ A CABO POR GRUPOS ACTIVISTAS CONTRA EMPRESAS Y GOBIERNOS**.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU PROPÓSITO

CIBERTERRORISMO

TIENE EL PROPÓSITO FINAL DE **CREAR MIEDO GENERALIZADO EN LA POBLACIÓN E INFLUIR EN LA MISMA Y EN EL GOBIERNO.**

COMO CONSECUENCIA DE LA EJECUCIÓN DE **ACCIONES EN EL CIBERESPACIO PARA DESTRUIR O INTERRUMPIR SERVICIOS ESENCIALES.**

ESTE TIPO DE ATAQUES NORMALMENTE **SE LLEVARÁ A CABO POR GRUPOS TERRORISTAS**, BIEN SEA DE MANERA INDEPENDIENTE O COMO PANTALLA DE GOBIERNOS.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU PROPÓSITO

CIBERGUERRA

ES LA UTILIZACIÓN DEL CIBERESPACIO PARA **ALCANZAR UNA SUPERIORIDAD MILITAR, DEBILITANDO O DESTRUYENDO OBJETIVOS ESTRATÉGICOS U OPERACIONALES DE UNA NACIÓN ENEMIGA EN EL MARCO DE UN CONFLICTO ARMADO.**

DENTRO DE LA DEFINICIÓN ANTERIOR SE INCLUYEN ACCIONES QUE ABARCAN **DESDE ACCIONES DE PROPAGANDA Y ESPIONAJE HASTA ATAQUES CONTRA INFRAESTRUCTURAS CRÍTICAS.**

ESTOS ATAQUES **SÓLO SE PUEDEN LLEVAR A CABO POR ORGANIZACIONES MILITARES EN EL MARCO DE UN CONFLICTO BÉLICO**, E IRÁN DIRIGIDOS CONTRA OBJETIVOS CONFORME A LO REGULADO EN LOS TRATADOS INTERNACIONALES.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU VECTOR DE ATAQUE

EL CONCEPTO **VECTOR DE ATAQUE** PROVIENE DEL ÁMBITO MILITAR Y **ES EL MÉTODO QUE UTILIZA LA AMENAZA PARA APROVECHAR UNA VULNERABILIDAD Y ATACAR EL SISTEMA.**

UNA VEZ QUE UN ATACANTE HA OBTENIDO SUFICIENTE INFORMACIÓN DEL OBJETIVO, INCLUIDOS SISTEMAS Y DATOS PERSONALES DE LOS EMPLEADOS DE LA ORGANIZACIÓN, ESTARÁ EN CONDICIONES DE ELEGIR LA MEJOR FORMA DE ATACARLO CON GARANTÍAS DE ÉXITO.

EN MUCHAS OCASIONES, SE USA UNA COMBINACIÓN DE VARIOS PARA MATERIALIZAR UN ATAQUE.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU VECTOR DE ATAQUE

MALWARE

SON AQUELLOS PROGRAMAS QUE EJECUTAN ACCIONES MALICIOSAS EN UN EQUIPO. EL TÉRMINO MALWARE ABARCA NUMEROSOS TIPOS DE PROGRAMAS, COMO VIRUS, GUSANOS, TROYANOS, KEYLOGGERS, RAMSOMWARE, ADWARE O SPYWARE.

E-MAIL

SE PUEDE UTILIZAR PARA ENVIAR SPAM, PARA REALIZAR PHISHING O PARA ENVIAR MALWARE. EN MUCHAS OCASIONES, EL CORREO ELECTRÓNICO SIRVE COMO VECTOR DE ATAQUE INICIAL PARA QUE LA PERSONA DESCARGUE Y EJECUTE EL MALWARE EN EL SISTEMA.

TIPOS DE ATAQUES

TIPOS DE ATAQUES SEGÚN SU VECTOR DE ATAQUE

NAVEGACIÓN POR INTERNET

EN MUCHAS OCASIONES ASOCIADO A LOS DOS ANTERIORES, INTERNET SE PUDE UTILIZAR PARA ROBAR INFORMACIÓN O PARA DESCARGAR MALWARE EN LA VÍCTIMA.

APLICACIONES Y PÁGINAS WEB

LAS PÁGINAS WEB DE LAS EMPRESAS SON APLICACIONES. UN ATACANTE LAS PUEDE UTILIZAR PARA LLEVAR A CABO ATAQUES A LAS APLICACIONES CON EL FIN DE LOGRAR ACCESO O EXTRAER INFORMACIÓN DE LAS MISMAS Y DE SUS BASES DE DATOS RELACIONADAS. ALGUNOS TIPOS DE ATAQUES WEB CONOCIDOS SON LAS INYECCIONES SQL O LOS ATAQUES DE CROSS SITE SCRIPTING (XSS), ENTRE OTROS MUCHOS.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- **TIPOS DE ANÁLISIS DE SEGURIDAD**
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

TIPOS DE ANÁLISIS DE SEGURIDAD

EN PRIMER LUGAR, ES NECESARIO COMPRENDER ADECUADAMENTE EL TÉRMINO **HACKING**.

EL TÉRMINO **HACKER** SE UTILIZÓ DESDE SU ORIGEN PARA DEFINIR A *AQUELLA PERSONA QUE ESTUDIABA EN PROFUNDIDAD UNA TECNOLOGÍA, CON EL FIN DE CONOCERLA DE MODO QUE PUDIERA MODIFICARLA Y REALIZAR TAREAS PARA LAS QUE NO ESTABA PENSADA ORIGINALMENTE*.

ESTA DEFINICIÓN **SE ADOPTÓ EN EL ÁMBITO INFORMÁTICO, PERO SU SIGNIFICADO HA IDO VARIANDO**, DE TAL MANERA QUE, ACTUALMENTE, SE SUELE UTILIZAR EL TÉRMINO HACKING **PARA DEFINIR EL ACCESO NO AUTORIZADO A SISTEMAS AJENOS CON EL PROPÓSITO DE OCASIONAR DAÑOS.**

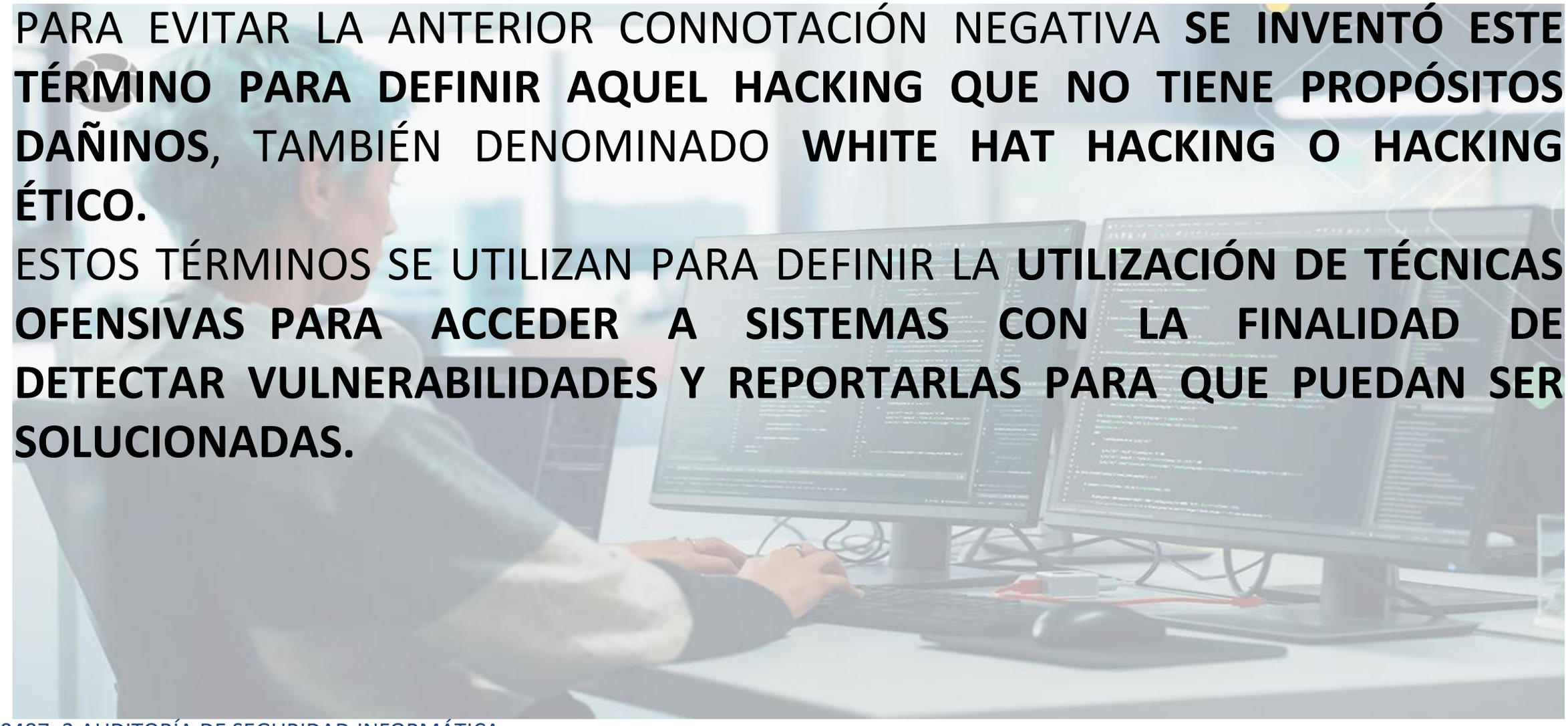
TIPOS DE ANÁLISIS DE SEGURIDAD

LA **RAE** RECONOCE EL **TÉRMINO HACKER** EN SUS **DOS ACEPCIONES**:

- PIRATA INFORMÁTICO
- PERSONA CON GRANDES HABILIDADES EN EL MANEJO DE COMPUTADORAS QUE INVESTIGA UN SISTEMA INFORMÁTICO PARA AVISAR DE LOS FALLOS Y DESARROLLAR TÉCNICAS DE MEJORA.

TIPOS DE ANÁLISIS DE SEGURIDAD

ETHICAL HACKING



PARA EVITAR LA ANTERIOR CONNOTACIÓN NEGATIVA **SE INVENTÓ ESTE TÉRMINO PARA DEFINIR AQUEL HACKING QUE NO TIENE PROPÓSITOS DAÑINOS**, TAMBIÉN DENOMINADO **WHITE HAT HACKING O HACKING ÉTICO.**

ESTOS TÉRMINOS SE UTILIZAN PARA DEFINIR LA **UTILIZACIÓN DE TÉCNICAS OFENSIVAS PARA ACCEDER A SISTEMAS CON LA FINALIDAD DE DETECTAR VULNERABILIDADES Y REPORTARLAS PARA QUE PUEDAN SER SOLUCIONADAS.**

TIPOS DE ANÁLISIS DE SEGURIDAD

PENETRATION TESTING

TAMBIÉN **PENTESTING**, **PENTEST O TEST DE PENETRACIÓN**.

ES **UN SUBCONJUNTO DEL ETHICAL HACKING**, EN QUE **UTILIZA LAS MISMAS TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTP) EMPLEADAS POR ATACANTES REALES PARA ENCONTRAR VULNERABILIDADES Y EXPLOTARLAS PARA ACCEDER Y TOMAR CONTROL DE LOS SISTEMAS**, SEGÚN LO QUE SE HAYA ACORDADO AL DEFINIR EL ALCANCE DE LAS PRUEBAS Y CONFORME A LAS REGLAS DE ENFRENTAMIENTO (**ROE**).

UN TEST DE PENETRACIÓN SERVIRÁ PARA IDENTIFICAR LAS AMENAZAS Y LOS RIESGOS, ASÍ COMO PARA DETERMINAR EL IMPACTO QUE TENDRÍAN SOBRE LOS SISTEMAS.

TIPOS DE ANÁLISIS DE SEGURIDAD

PENETRATION TESTING

TIPOS DE ANÁLISIS DE SEGURIDAD

TEAMING

SE TRATA DEL **PROCESO DE REALIZAR UNA SIMULACIÓN DE ATAQUE CON EL FIN DE VALORAR Y MEJORAR LOS PROCEDIMIENTOS DE UNA ORGANIZACIÓN, ASÍ COMO SUS TECNOLOGÍAS Y LAS CAPACIDADES DE DETECCIÓN Y RESPUESTA ANTE INCIDENTES.**

CUANDO SE REALIZAN ACCIONES DE **RED TEAM** EXISTE UN **BLUE TEAM DEFENSIVO Y EQUIPOS** DENOMINADOS **CON OTROS COLORES**, COMO EL **PURPLE TEAM**, PARA INTEGRAR LAS MEDIDAS DEFENSIVAS DEL **BLUE TEAM** CON LAS VULNERABILIDADES DETECTADAS Y LOS ATAQUES REALIZADOS POR EL **RED TEAM**.

EL **PURPLE TEAM** **DEBERÍA SER, MÁS QUE UN EQUIPO, UNA DINÁMICA DE COOPERACIÓN ENTRE EL RED TEAM Y EL BLUE TEAM**.

TIPOS DE ANÁLISIS DE SEGURIDAD

TEAMING

TIPOS DE ANÁLISIS DE SEGURIDAD

ANÁLISIS DE VULNERABILIDADES

LOS ANÁLISIS DE VULNERABILIDADES **TIENEN EL PROPÓSITO DE IDENTIFICAR TODAS LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS, PERO SIN LLEGAR A EXPLOTARLAS.**

UN ANÁLISIS DE VULNERABILIDADES TAMBIÉN **DEBERÍA COMPRENDER ASPECTOS** QUE NO SE REALIZAN EN UN TEST DE PENETRACIÓN, **COMO LA REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA ORGANIZACIÓN Y DE LA DOCUMENTACIÓN DE SEGURIDAD.**

Análisis de vulnerabilidades

TIPOS DE ANÁLISIS DE SEGURIDAD

AUDITORÍA DE SEGURIDAD

LAS AUDITORÍAS DE SEGURIDAD **IMPLICAN COMPROBAR EL ESTADO DE LA SEGURIDAD DE UNA ORGANIZACIÓN CONFORME A UNOS ESTÁNDARES DE SEGURIDAD DETERMINADOS**, PARA LO QUE SE SUELEN EMPLEAR CHECKLISTS EN LOS QUE EL AUDITOR REFLEJA MÚLTIPLES ASPECTOS.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- **TIPOS DE HACKERS**
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

TIPOS DE HACKERS

ES COMÚN IDENTIFICAR LOS DISTINTOS TIPOS DE HACKERS SEGÚN **COLORES DE SOMBREROS.**

AL HABLAR DEL **ETHICAL HACKING** SE INTRODUJO EL TÉRMINO **WHITE HAT HACKING**. COMO SE PUEDE DEDUCIR, **UN WHITE HAT HACKER** ES AQUEL QUE LLEVA A CABO **ACCIONES DE HACKING** DEBIDAMENTE **AUTORIZADAS** CON EL **PROPÓSITO DE IDENTIFICAR VULNERABILIDADES.**

POR EL CONTRARIO, UN **BLACK HAT HACKER** ES AQUEL QUE TIENE **PROPÓSITOS MALICIOSOS**, CUYOS FINES CONSISTEN **EN OBTENER UN BENEFICIO PERSONAL O ECONÓMICO, O CAUSAR DAÑOS** A UNA ORGANIZACIÓN O PERSONA.

TIPOS DE HACKERS

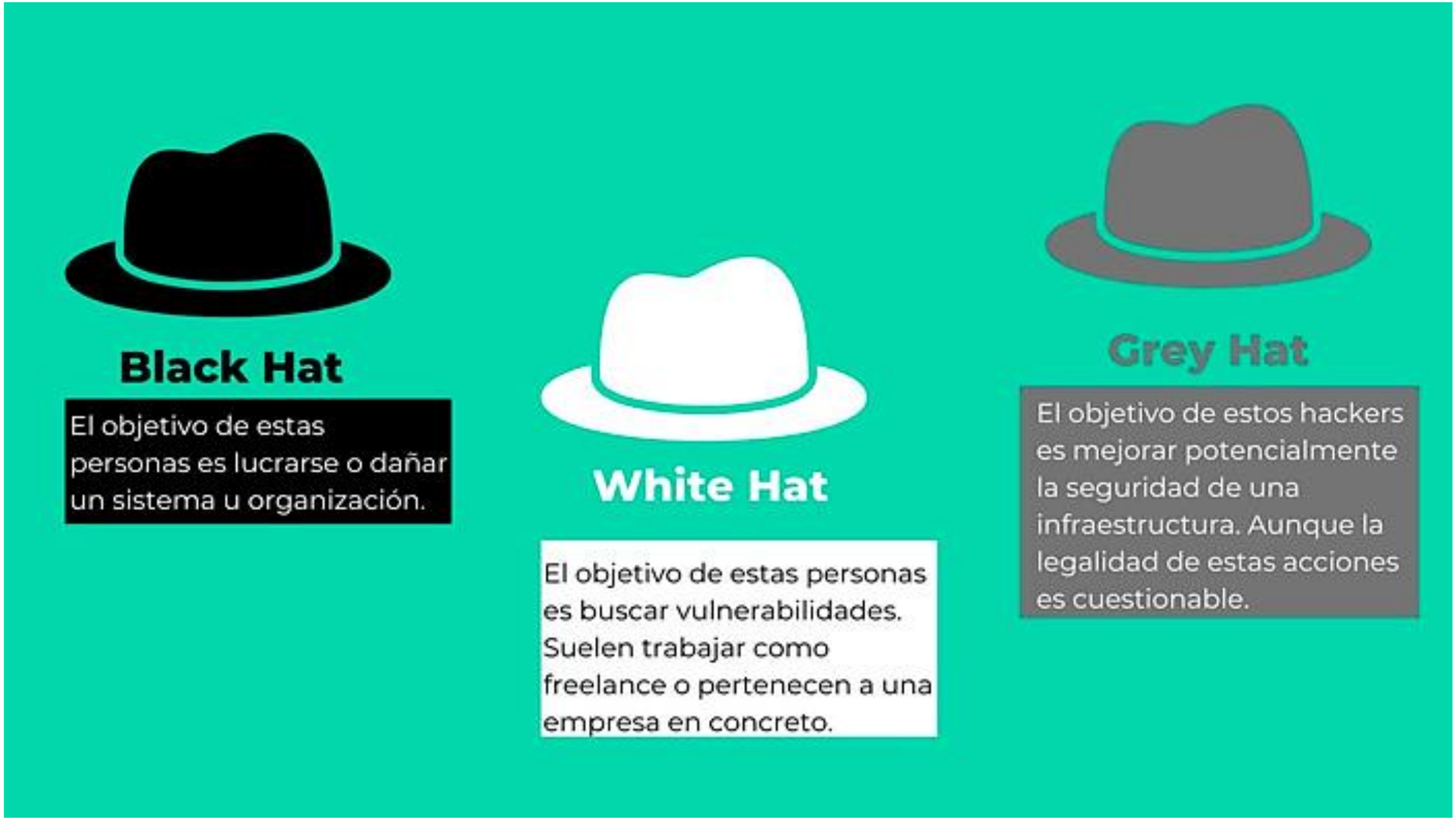
ENTRE MEDIAS SE ENCONTRARÍAN LOS DENOMINADOS **GREY HAT HACKERS.**

COMO CORRESPONDE AL COLOR, HAY MUCHOS TONOS DE GRIS Y BAJO ESTA DENOMINACIÓN CABEN UNOS CUANTOS TIPOS DE PERSONAS.

POR EJEMPLO, AQUÍ ENTRARÍAN AQUELLOS QUE ATACAN A UNA ORGANIZACIÓN PARA, A CONTINUACIÓN, PONERSE EN CONTACTO CON ELLA Y OFRECER SUS SERVICIOS.

TAMBIÉN PODRÍAN ENTRAR EN ESTE TIPO AQUELLOS QUE TRABAJAN PARA UN GOBIERNO CON EL FIN DE OBTENER INFORMACIÓN SOBRE OTROS PAÍSES.

TIPOS DE HACKERS



CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- **ASPECTOS ÉTICOS Y LEGALES**
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

ASPECTOS ÉTICOS Y LEGALES

SE HA UTILIZADO LA PALABRA **ÉTICO** PARA REFERIRSE A CIERTAS **ACCIONES REALIZADAS CON UN BUEN PROPÓSITO,** Y **SE HA IDENTIFICADO A LOS HACKERS POR COLORES** SEGÚN SUS INTENCIONES.

SE PODRÍA PENSAR QUE, SI LAS ACCIONES ESTÁN AUTORIZADAS Y EL HACKER ÉTICO SE CIÑE A LO ACORDADO Y NO REVELA LA INFORMACIÓN QUE PUEDA OBTENER A LO LARGO DE SUS ACCIONES, **SE ESTÁ CUMPLIENDO LA LEGALIDAD.**

SIN EMBARGO, EN MUCHAS OCASIONES **LA LÍNEA DE SEPARACIÓN ENTRE LO LEGAL Y LO ILEGAL PUEDE SER MUY FINA.**

ASPECTOS ÉTICOS Y LEGALES

PENSEMOS EN UNA ACCIÓN DE INGENIERÍA SOCIAL EN LA QUE EL HACKER ÉTICO ENGAÑA A UN EMPLEADO PARA QUE LE PROPORCIONE SUS CREDENCIALES Y LUEGO LAS UTILIZA PARA ACCEDER AL SISTEMA Y A LA INFORMACIÓN MANEJADA POR EL MISMO, COMO HARÍA UN ATACANTE REAL.

SI SE PIENSA BIEN, EN ESTE CASO SE ESTÁ PRODUCIENDO UNA SUPLANTACIÓN DE IDENTIDAD Y **PODRÍA TENER CONSECUENCIAS LEGALES TANTO PARA EL HACKER ÉTICO COMO PARA LA EMPRESA**.

ASPECTOS ÉTICOS Y LEGALES

PARA INTENTAR MINIMIZAR LOS PROBLEMAS LEGALES, **ES FUNDAMENTAL DEFINIR MUY BIEN LOS ASPECTOS** DE LA PREPARACIÓN DE UN TEST DE PENETRACIÓN.

LA ORGANIZACIÓN QUE ENCARGA UNA ACCIÓN DE HACKING ÉTICO O LA HACE CON SU PROPIO PERSONAL, **DEBE HABER ESTABLECIDO DE MANERA CLARA A TODOS SUS EMPLEADOS LA POLÍTICA QUE SEGUIRÁ EN CUANTO AL EMPLEO DE SUS SISTEMAS DE INFORMACIÓN**.

EN EL INFORME FINAL, SE DEBERÁN OMITIR LOS DATOS PERSONALES DE AQUELLOS EMPLEADOS SOBRE LOS QUE SE HAYAN REALIZADO ACCIONES O DE LOS QUE SE HAYA PODIDO OBTENER INFORMACIÓN.

ASPECTOS ÉTICOS Y LEGALES

SI, DURANTE UNA ACCIÓN DE HACKING ÉTICO, **SE ENCUENTRAN ELEMENTOS QUE REVELEN QUE LA ORGANIZACIÓN HA RECIBIDO O ESTÁ RECIBIENDO UN ATAQUE REAL**, EL PENTESTER PARARÍA LAS ACCIONES E **INFORMARÍA INMEDIATAMENTE AL PERSONAL DE CONTACTO EN LA ORGANIZACIÓN.**

A PARTIR DE AHÍ SE ABREN DOS VÍAS:

DENUNCIAR O IR POR LIBRE E INTENTAR AVERIGUAR QUÉ HA PASADO

UNA INVESTIGACIÓN DEL INCIDENTE PODRÍA LLEVAR A OBTENER INFORMACIÓN DEL POTENCIAL ATACANTE, ASÍ COMO DIRECCIONES IP DE EQUIPOS IMPLICADOS EN EL ATAQUE.

ASPECTOS ÉTICOS Y LEGALES

PUEDE SURGIR LA TENTACIÓN DE **ACCEDER A ESAS DIRECCIONES IP E, INCLUSO, HACER ACCIONES OFENSIVAS SOBRE LAS MISMAS,** COMO PODRÍAN SER DENEGACIONES DE SERVICIO O HACER TODO EL PROCESO DE HACKING PARA INTENTAR ACCEDER A LOS SISTEMAS.

DEJANDO AL MARGEN QUE ESOS SISTEMAS PUEDEN SER SISTEMAS LEGÍTIMOS QUE HAN SIDO PREVIAMENTE VULNERADOS POR EL ATACANTE PARA UTILIZARLOS COMO SALTO INTERMEDIO, SI NOS TRASLADAMOS AL MUNDO “FÍSICO” SERÍA EL EQUIVALENTE DE AGREDIR A UN CARTERISTA AL QUE HEMOS PILLADO IN FRAGANTI: PUEDE PARECER JUSTO Y RESULTAR SATISFACTORIO, PERO A EFECTOS LEGALES RESULTARÁ DE DIFÍCIL JUSTIFICACIÓN.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- **TIPOS DE PENTESTING**
- METODOLOGÍAS
- FASES DE UN PENTEST

TIPOS DE PENTESTING

EXISTEN **MÚLTIPLES ASPECTOS** QUE SE PUEDEN COMPROBAR **DURANTE LA REALIZACIÓN DE UN PENTESTING**, EN FUNCIÓN DE LAS NECESIDADES DE LA ORGANIZACIÓN, EL TIEMPO Y EL PRESUPUESTO.

PARA PODER DETERMINAR ADECUADAMENTE LAS ACCIONES QUE SE LLEVARÁN A CABO ES NECESARIO CONOCER, AL MENOS SOMERAMENTE, LOS **TIPOS DE PENTESTING** MÁS COMUNES.

- **NETWORK**
- **CLIENT-SIDE**
- **WEB**
- **WIRELESS**
- **INGENIERÍA SOCIAL**
- **FÍSICO**

TIPOS DE PENTESTING

NETWORK

CONSISTE EN **LOCALIZAR SISTEMAS Y SERVICIOS EN UNA RED Y BUSCAR VULNERABILIDADES** EN LOS SISTEMAS OPERATIVOS Y APLICACIONES DE SERVIDOR, MALAS CONFIGURACIONES O CUALQUIER COSA QUE PUDIERA PERMITIR A UN ATACANTE EXPLOTARLOS DE MANERA REMOTA.

CLIENT-SIDE

TIENE COMO PROPÓSITO **ENCONTRAR VULNERABILIDADES EN SOFTWARE** INSTALADO EN EQUIPOS DE USUARIO.

WEB

SU FINALIDAD ES **ENCONTRAR VULNERABILIDADES EN LAS APLICACIONES WEB** DE UNA ORGANIZACIÓN.

TIPOS DE PENTESTING

WIRELESS

CONSISTE EN **COMPROBAR LA SEGURIDAD DE LAS REDES WIRELESS** (GENERALMENTE WI-FI) EXISTENTES EN LAS INSTALACIONES DE UNA ORGANIZACIÓN.

INGENIERÍA SOCIAL

CONSISTE EN **ATACAR A LOS USUARIOS** PARA LOGAR QUE REVELEN INFORMACIÓN, EJECUTEN ALGUNA APLICACIÓN MALICIOSA, ACCEDAN A SITIOS WEB CONTROLADOS POR EL ATACANTE, O REALICEN OTRAS ACCIONES QUE PUDIERAN PERMITIR A UN ATACANTE OBTENER VENTAJA DE SUS ACCIONES.

TIPOS DE PENTESTING

FÍSICO

SE INTENTARÁ ACCEDER A LAS INSTALACIONES DEL CLIENTE CON EL FIN **DE ACCEDER A SUS EQUIPOS, ENCONTRAR DOCUMENTACIÓN, ROBAR DISPOSITIVOS DE ALMACENAMIENTO, DESPLEGAR DISPOSITIVOS** PARA REALIZAR POSTERIORES ACCIONES REMOTAS, Y CUALQUIER OTRA ACCIÓN QUE PUDIERA REALIZAR UN ATACANTE.

EL PENTESTER DEBERÁ PORTAR UN PERMISO DE EJECUCIÓN Y DISPONER DE UN PUNTO DE CONTACTO EN LA ORGANIZACIÓN QUE LE AVALE EN CASO DE QUE SEA DETECTADO POR LA SEGURIDAD.

GENERALMENTE UN PENTEST NO SERÁ DE UN ÚNICO TIPO, SINO QUE SE UTILIZARÁ UNA COMBINACIÓN DE VARIOS DE ELLOS. POR EJEMPLO, UN PENTEST CLIENT-SIDE SUELE LLEVAR APAREJADO, AL MENOS, LA REALIZACIÓN DE ACCIONES DE INGENIERÍA SOCIAL.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- **METODOLOGÍAS**
- FASES DE UN PENTEST

METODOLOGÍAS

PARA LLEVAR A CABO **UN TEST DE PENETRACIÓN** SE **DEBE SEGUIR UNA METODOLOGÍA.**

AUNQUE UN PENTESTER EXPERIMENTADO HABRÁ DESARROLLADO LA SUYA PROPIA, SIEMPRE RESULTA CONVENIENTE **CONOCER ALGUNAS METODOLOGÍAS** Y SEGUIRLAS, SIN PERJUICIO DE REALIZAR LAS ADAPTACIONES NECESARIAS PARA ADECUARLAS A LAS NECESIDADES Y GUSTOS PERSONALES.

ENTRE LAS MÁS CONOCIDAS SE ENCUENTRAN LAS SIGUIENTES:

- **PENETRATION TESTING FRAMEWORK**
- **PENETRATION TESTING EXECUTION STANDARD (PTES)**
- **OPEN WEB APPLICATION SECURITY PROJECT (OWASP) TESTING GUIDE**

METODOLOGÍAS

PENETRATION TESTING FRAMEWORK

SE ENFOCA PRINCIPALMENTE EN EL **NETWORK PENTESTING**.

PROPORCIONA UNA GUÍA PASO A PASO DE CADA ASPECTO A EVALUAR E INDICA LAS HERRAMIENTAS Y COMANDOS A UTILIZAR. INCLUYE SECCIONES DEDICADAS A VOIP, BLUETOOTH Y WIRELESS, ENTRE OTRAS SECCIONES. ESTÁ DISPONIBLE EN:

http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

METODOLOGÍAS

PENETRATION TESTING EXECUTION STANDARD (PTES)

DEFINE LAS ACTIVIDADES QUE SE DEBEN CONTEMPLAR EN UN PENTEST, CON EL PROPÓSITO DE QUE LAS ORGANIZACIONES A LAS QUE SE LES REALIZA RECIBAN UN PRODUCTO QUE PUEDAN ENTENDER Y QUE PROPORCIONE VALOR PARA EL NEGOCIO.

PROPORCIONA DATOS PARA LAS **DISTINTAS FASES DE UN PENTEST**: **INTERACCIONES PREVIAS**, COMO LA DEFINICIÓN DEL ÁMBITO Y LAS ROE; **ACTIVIDADES DE RECONOCIMIENTO**; **MODELADO DE LA AMENAZA; ANÁLISIS DE VULNERABILIDADES; EXPLOTACIÓN; POST EXPLOTACIÓN, Y ELABORACIÓN DEL INFORME**.

SE ENCUENTRA DISPONIBLE EN:

http://www.pentest-standard.org/index.php/main_page

METODOLOGÍAS

OPEN WEB APPLICATION SECURITY PROJECT (OWASP) TESTING GUIDE

A DIFERENCIA DE LAS ANTERIORES, ESTA **METODOLOGÍA SE CENTRA EXCLUSIVAMENTE EN LA SEGURIDAD DE APLICACIONES WEB** Y EN DESCRIBIR EN DETALLE LAS DIFERENTES COMPROBACIONES QUE SE DEBEN LLEVAR A CABO, ADEMÁS DE INDICAR LAS HERRAMIENTAS QUE SE PUEDEN USAR A LO LARGO DEL PROCESO.

SE ENCUENTRA DISPONIBLE EN:

https://owasp.org/www-project-web-security-testing-guide/

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- **FASES DE UN PENTEST**

FASES DE UN PENTEST

EL PROCESO DE UN TEST DE PENETRACIÓN **COMPRENDE VARIAS FASES** QUE SE PUEDEN AGRUPAR EN TRES BLOQUES PRINCIPALES:

- **PREPARACIÓN**
- **EJECUCIÓN**
- **PRESENTACIÓN DE RESULTADOS**

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN CON EL CLIENTE

EN ESTA FASE **PARTICIPAN EL RESPONSABLE DEL EQUIPO DE PENTESTING Y EL RESPONSABLE DESIGNADO POR LA ORGANIZACIÓN,** PARA DEFINIR VARIOS ASPECTOS DEL PENTESTING, ENTRE LOS CUALES SE INCLUYE EN QUÉ CONSISTIRÁ, LAS RESPONSABILIDADES DE AMBAS PARTES Y SU DURACIÓN.

ES MUY PROBABLE QUE SUS RESPONSABLES NO TENGAN CLARAS SUS NECESIDADES O NO LAS SEPAN EXPRESAR MÁS QUE DE UNA MANERA MUY GENÉRICA, POR LO QUE **ESTA FASE COMENZARÁ CON UNA REUNIÓN INICIAL** PARA PLANTEAR CUESTIONES QUE SIRVAN PARA GUIARLE.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN CON EL CLIENTE

SE PUEDEN **UTILIZAR CUESTIONARIOS** BASADOS EN LOS INCLUIDOS EN EL **PTES**, QUE SIRVAN PARA DELIMITAR EL TEST, LA DURACIÓN, QUÉ TIPO DE PENTESTING REALIZAR Y EL ALCANCE.

DURANTE ESTA REUNIÓN **SE PUEDEN TRATAR LOS ASPECTOS MÁS RELEVANTES PARA LA ORGANIZACIÓN**, ENTRE LOS QUE PUEDEN ESTAR **SUS SISTEMAS MÁS SENSIBLES, SUS PRINCIPALES PREOCUPACIONES Y LAS AMENAZAS IDENTIFICADAS.**

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN CON EL CLIENTE

ACUERDO DE CONFIDENCIALIDAD

TAMBIÉN CONOCIDO COMO **NDA (NON-DISCLOSURE AGREEMENT)**, CUYO **PROPÓSITO ES PROTEGER LA INFORMACIÓN DE LA ORGANIZACIÓN QUE SE PUEDA CONOCER DURANTE EL PENTESTING.**

OBLIGA A PROTEGER LAS COMUNICACIONES, EQUIPOS UTILIZADOS, SOPORTES DE ALMACENAMIENTO Y LOS RESULTADOS DEL PENTESTING.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN CON EL CLIENTE

ROE (RULES OF ENGAGEMENT)

REGLAS DE COMPROMISO. **DESCRIBEN LAS PRÁCTICAS QUE SE SEGUIRÁN**. ESTO INCLUYE ASPECTOS COMO **LA DURACIÓN DEL PENTESTING Y EL HORARIO**, SI SERÁ DE **CAJA BLANCA, NEGRA O GRIS**, LA **PERIODICIDAD DE LAS REUNIONES** ENTRE EL PERSONAL RESPONSABLE DE LA ORGANIZACIÓN Y EL EQUIPO DE PENTESTING, ASÍ COMO **INFORMACIÓN DE CONTACTO EN AMBOS SENTIDOS**, PARA IMPREVISTOS O COMUNICACIONES URGENTES, ENTRE OTROS ASPECTOS.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN CON EL CLIENTE

ALCANCE DEL TEST

DETERMINA **QUÉ RANGOS DE IP, NOMBRES DE DOMINIO, EQUIPOS O APLICACIONES** DEBEN **COMPROBARSE Y CUALES DEBEN EXCLUIRSE** EXPRESAMENTE.

TAMBIÉN LA PROFUNDIDAD, LO QUE CONDICIONARÁ LA POSIBILIDAD DE REALIZAR LA EXPLOTACIÓN Y POST-EXPLOTACIÓN.EL ALCANCE TAMBIÉN DEBE CONTEMPLAR LOS TIPOS DE TEST QUE SE LLEVARÁN A CABO.

EL ALCANCE DETERMINA QUÉ SE PUEDE HACER, MIENTRAS QUE LAS ROE DETERMINAN EL CÓMO HACERLO.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN CON EL CLIENTE

PERMISO DE EJECUCIÓN

SE TRATA DE UNA **AUTORIZACIÓN FIRMADA POR EL RESPONSABLE DE LA ORGANIZACIÓN PARA LLEVAR A CABO EL PENTEST.**

ES UN DOCUMENTO FUNDAMENTAL, SIN EL CUAL JAMÁS SE DEBERÍA INICIAR NINGUNA ACCIÓN, Y QUE DEBERÁ LLEVAR ENCIMA TODO EL PERSONAL QUE PARTICIPE EN EL TEST, SOBRE TODO EN EL CASO DE REALIZAR UN PENTEST FÍSICO.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

ANTES DE INICIAR CUALQUIER TIPO DE TEST DE PENETRACIÓN **ES NECESARIO CONFIGURAR LA INFRAESTRUCTURA, LO QUE IMPLICA UNA PLANIFICACIÓN** NO SÓLO DEL SOFTWARE Y HARDWARE NECESARIOS, SINO TAMBIÉN DE LA INFRAESTRUCTURA DE RED NECESARIA.

AL IGUAL QUE UN ATACANTE REAL, UN EQUIPO DE PENTESTING NECESITARÁ ORDENADORES DESDE LO QUE LANZAR SUS ATAQUES, ASÍ COMO MÁQUINAS DE APOYO Y, PROBABLEMENTE, UNA INFRAESTRUCTURA EN INTERNET QUE PERMITA OCULTAR EL ORIGEN DE LOS ATAQUES.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

ES IMPORTANTE TENER EN CUENTA QUE LA MISMA INFRAESTRUCTURA NO SERVIRÁ PARA TODOS LOS PENTEST QUE SE REALICEN, SERÁ NECESARIO ADAPTARLA O CREAR UNA INFRAESTRUCTURA NUEVA CADA VEZ.

TODOS **LOS EQUIPOS QUE SE UTILICEN DURANTE UN TEST DE PENETRACIÓN DEBEN ESTAR ACTUALIZADOS COMPLETAMENTE** (TANTO EL S.O. COMO LAS APLICACIONES**) Y NO TENER APLICACIONES NI SERVICIOS INNECESARIOS.**

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

EQUIPOS OFENSIVOS

AUNQUE PARA LAS ACCIONES OFENSIVAS **ES BASTANTE HABITUAL UTILIZAR EQUIPOS CON SISTEMA OPERATIVO LINUX**, NO HAY QUE DESCARTAR LA UTILIZACIÓN DE **WINDOWS**.

ES MÁS, **RESULTA CONVENIENTE DISPONER DE DISTINTOS EQUIPOS CON DISTINTOS SISTEMAS OPERATIVOS**, DADO QUE ES POSIBLE REALIZAR ACCIONES Y ENCONTRAR HERRAMIENTAS ESPECÍFICAS PARA UNO DE ELLOS, O QUE SIMPLEMENTE FUNCIONEN MEJOR EN UN SISTEMA QUE EN OTRO.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

EQUIPOS OFENSIVOS

LOS EQUIPOS QUE SE UTILICEN PARA LAS ACCIONES OFENSIVAS **DEBEN SER TOTALMENTE DIFERENTES DE LOS DE USO PERSONAL Y DE LOS EMPLEADOS EN EL TRABAJO DIARIO.**

LOS MOTIVOS PARA ELLO SON TANTO DE SEGURIDAD COMO DE PRIVACIDAD, PUESTO QUE SE PUEDE COMPROMETER TANTO LA INFORMACIÓN DE LA ORGANIZACIÓN COMO LA DEL PROPIO EQUIPO ATACANTE, AL EXPONERLO A LA RED INTERNA.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

EQUIPOS OFENSIVOS

EN MUCHAS **OCASIONES SERÁ NECESARIO MODIFICAR LAS CONFIGURACIONES DEL EQUIPO ATACANTE E INSTALAR APLICACIONES QUE NO SE EMPLEEN HABITUALMENTE**, POR LO QUE, ADEMÁS DE UTILIZAR UN EQUIPO ESPECÍFICO, ES CONVENIENTE CREAR UNA IMAGEN DEL EQUIPO ANTES DE INICIAR EL ANÁLISIS Y RESTAURARLA AL FINALIZAR EL MISMO.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

EQUIPOS OFENSIVOS

CUANDO SE VAYAN A CONFIGURAR LOS EQUIPOS OFENSIVOS **SE DEBEN DETERMINAR DOS ASPECTOS**:

- SI SE UTILIZARÁN EQUIPOS FÍSICOS O MÁQUINAS VIRTUALES
- SI SE INSTALARÁ UNA DISTRIBUCIÓN EXISTENTE O SI SE VA A UTILIZAR UN SISTEMA PROPIO EN EL QUE SE HAYAN INSTALADO HERRAMIENTAS.

FASES DE UN PENTEST

FASE DE PREPARACIÓN

PREPARACIÓN DE LA INFRAESTRUCTURA DE ATAQUE

EQUIPOS OFENSIVOS

LA MAYOR PARTE DE LAS D**ISTRIBUCIONES ESTÁN BASADAS EN LINUX**, ALGUNAS DE LAS MÁS POPULARES SON:

KALI LINUX: https://www.kali.org/

PARROT OS: https://www.parrotsec.org/

TAMBIÉN EXISTEN ALGUNAS BASADAS EN **WINDOWS**, COMO:

PENTESTBOX: https://pentestbox.org/

COMMANDO VM: https://github.com/fireeye/commando-vm

FASES DE UN PENTEST

FASE DE EJECUCIÓN

SE TRATA DE LA PARTE TÉCNICA DEL PENTEST QUE SE PUEDE DIVIDIR EN:

- **RECONOCIMIENTO**
- **ENUMERACIÓN**
- **EXPLOTACIÓN**
- **POST-EXPLOTACIÓN**

DURANTE ESTA FASE SE DEBEN DOCUMENTAR TODAS LAS ACCIONES REALIZADAS Y LOS RESULTADOS DE LAS MISMAS, LO QUE RESULTA ESENCIAL TANTO DE CARA AL INFORME FINAL COMO PARA DESHACER LAS MODIFICACIONES REALIZADAS EN LOS SISTEMAS A LO LARGO DEL PROCESO.

FASES DE UN PENTEST

FASE DE PRESENTACIÓN DE RESULTADOS

ESTA FASE RESULTA FUNDAMENTAL EN UN TEST DE PENETRACIÓN, DADO QUE SIRVE PARA EXPONER A LA ORGANIZACIÓN LAS ACCIONES REALIZADAS, LAS VULNERABILIDADES Y RIESGOS DE SUS SISTEMAS Y UNAS RECOMENDACIONES PARA MEJORAR LA SEGURIDAD.

SIN ENTRAR EN EXCESIVOS DETALLES DEL INFORME FINAL, ESTE DEBE CONTEMPLAR COMO MÍNIMO LOS SIGUIENTES APARTADOS:

1. **RESUMEN EJECUTIVO**
2. **INTRODUCCIÓN**
3. **METODOLOGÍA SEGUIDA**
4. **VULNERABILIDADES ENCONTRADAS**
5. **CONCLUSIONES**
6. **ANEXOS**

FASES DE UN PENTEST

FASE DE PRESENTACIÓN DE RESULTADOS

1. **RESUMEN EJECUTIVO**

   BREVE Y DIRIGIDO AL PERSONAL DE LA DIRECCIÓN CON ESCASOS O NULOS CONOCIMIENTOS TÉCNICOS Y QUE NO TENDRÁ TIEMPO PARA LEER EL INFORME COMPLETO.

2. **INTRODUCCIÓN**

   DESCRIPCIÓN A ALTO NIVEL, INDICACIÓN DE LA DURACIÓN, PARTICIPANTES Y RESUMEN DE LOS PRINCIPALES RIESGOS.

3. **METODOLOGÍA SEGUIDA**

   DESCRIPCIÓN TÉCNICA DE LAS ACCIONES REALIZADAS Y LOS RESULTADOS OBTENIDOS. NO DEBE SER UN COPIA-PEGA DE LOS RESULTADOS DE LAS HERRAMIENTAS NI DE LA SALIDA DE LA EJECUCIÓN DE LOS COMANDOS, QUE DEBERÁN IR EN LOS ANEXOS, SI SE QUIEREN INCLUIR.

FASES DE UN PENTEST

FASE DE PRESENTACIÓN DE RESULTADOS

4. VULNERABILIDADES ENCONTRADAS

DESCRIPCIÓN DETALLADA E INDIVIDUALIZADA DE LAS VULNERABILIDADES DETECTADAS, INDICANDO EL RIESGO, SISTEMAS AFECTADOS, CÓMO SE PODRÍA EXPLOTAR Y RECOMENDACIONES PARA CORREGIRLAS.

5. CONCLUSIONES

UN RESUMEN GENERAL DEL ESTADO DE LA SEGURIDAD Y DE LAS VULNERABILIDADES, ASÍ COMO UNAS RECOMENDACIONES PARA EL FUTURO.

6. ANEXO

DOCUMENTACIÓN ANEXA.

CONTENIDOS

- DEFINICIONES Y CONCEPTOS BÁSICOS
- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN
- DEFINICIONES BÁSICAS
- VULNERABILIDADES
- TIPOS DE AMENAZAS
- TIPOS DE ATAQUES
- TIPOS DE ANÁLISIS DE SEGURIDAD
- TIPOS DE HACKERS
- ASPECTOS ÉTICOS Y LEGALES
- TIPOS DE PENTESTING
- METODOLOGÍAS
- FASES DE UN PENTEST

ESTO ES TODO

Extraído de Hacking Ético. Luis Herrero Pérez. Editorial Ra-Ma