FASE FINAL DEL HACKEO ÉTICO

AUTOR: WALTER MADRIGAL CHAVES

NOVIEMBRE: 2020

San Marcos

Contenido

INTRODUCCIÓN

A lo largo de nuestro proceso de aprendizaje hemos podido aprehender el hackeo ético desde diferentes enfoques. En el primer eje conocimos qué es el hackeo y su historia, seguidamente exploramos las fases y herramientas de hackeo usadas en cada una de ellas. En el tercer eje, nos enfocamos en cómo utilizar lo aprendido llevando a cabo las fases y utilizando las herramientas correspondientes para obtener acceso y control del sistema que para nuestro ejemplo práctico fue una máquina Windows.

Con todo esto tenemos claro el qué, los cuáles y el cómo del hackeo; sin embargo, hay que aclarar que pese a tener metodologías, estas no son camisa de fuerza, ya que a la hora de efectuar un hackeo ético o malicioso lo importante es el ingenio, las habilidades y la creatividad que se puedan emplear en función de vulnerar la seguridad de un usuario, un servidor, una red o una infraestructura tecnológica.

En este último capítulo el estudiante podrá proponer su forma de planear su hackeo a un servidor de prueba del que se conoce que tiene múltiples vulnerabilidades explotables, aquí el estudiante podrá aplicar su ingenio, sus conocimientos y sus destrezas para lograr el objetivo.

ETHICAL HACKING SISTEMAS A SISTEMAS LINUX

La importancia de tener claros los conceptos nos permite en parte poder dimensionar la situación en la que necesitamos hacer un hackeo ético. Esto se resume en qué técnica o herramientas usar para lograr una efectividad a la hora de hacer el proceso. Por tal razón, a continuación, expondremos un caso que nos permitirá proponer la solución que más efectiva nos parezca.

Para lo anteriormente mencionado es importante saber analizar, investigar, conocer y determinar las vulnerabilidades encontradas en un sistema, ya que esto permite ahorrar tiempo en falsas vulnerabilidades, que en muchas ocasiones los escáneres establecen como críticas cuando en realidad no lo son, o leves cuando en realidad son críticas.

Es por lo que una constante investigación permite discernir a los hackers de sombrero blanco, gris o negro cuál es el camino óptimo para romper la seguridad, la cual puede ser vulnerada desde un servicio expuesto, una contraseña por defecto o simplemente una vulnerabilidad no remediada.

METASPLOITABLE (AMBIENTE PARA HACKEO)

Para tener un ambiente y hacer pruebas de hackeo de manera controlada, una opción es usar el proyecto Metasploitable: un sistema de entrenamiento en seguridad informática, en una plataforma Linux, que es vulnerable en su configuración y aplicaciones web con servicios no asegurados, desactualizados o configurados por defecto. Estos problemas en la seguridad nos aproximan a efectuar pruebas de hackeo aplicando los conocimientos adquiridos sin necesidad de incurrir en problemas legales.

Metasploitable
Máquina virtual preparada con vulnerabilidades en servicios y configuraciones inadecuadas que por lo general se presentan en una infraestructura sin aseguramiento o sin políticas de actualización de sistemas operativos, bases de datos o aplicaciones.

Esta plataforma está soportada sobre un sistema Linux y contiene un sistema Ubuntu 8.04 con más de 15 servicios vulnerables, los cuales pueden ser explotados usando diferentes herramientas explicadas en los ejes anteriores.

Esta es la oportunidad para que el estudiante pueda afianzar los conocimientos adquiridos de manera controlada en el ambiente virtualizado. Para comprender un poco de lo que contiene el proyecto Metasploitable

podemos resumir sus servicios de la siguiente manera:

Imagen 1 Servicios y puertos

ftp	21/tcp
ssh	22/tcp
telnet	23/tcp
smtp	25/tcp
dns	53/tcp
dns	53/udp
http	80/tcp
netbios	137/udp
smb	139/tcp
smb	445/tcp
mysql	3306/tcp
distccd	3632/tcp
postgres	5432/tcp
http	8180/tcp

Fuente: Elaboración propia

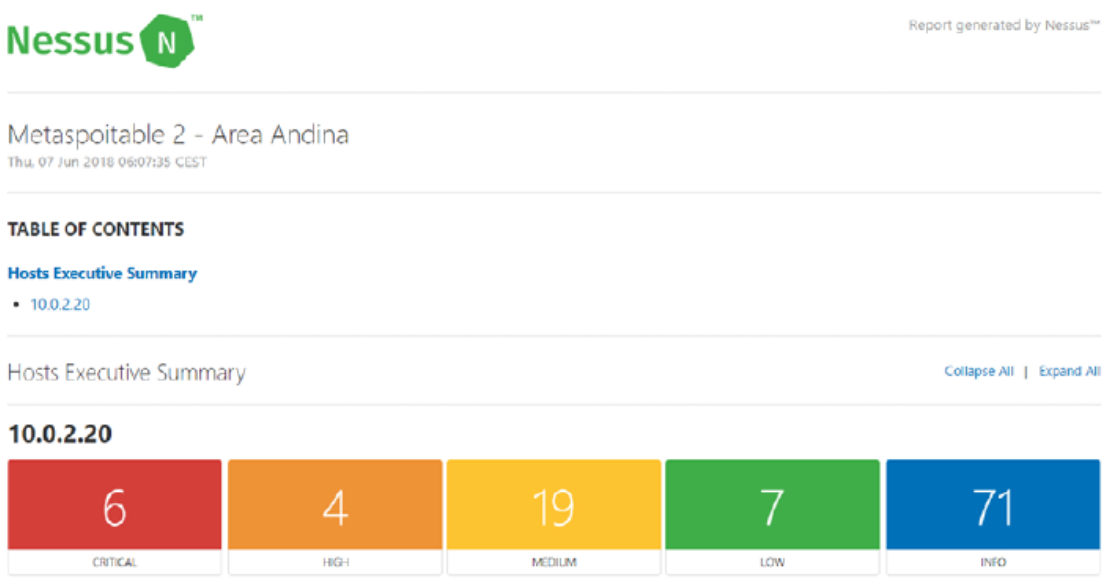
Sitio de descarga:

Hay que descargar la ISO de Metasploitable y utilizarla mediante VirtualBox o VMWare. El uso de Metasploitable es fácil y no es necesario instalarlo, solamente con arrancar la máquina virtual es suficiente. La máquina virtual de Metasploitable se debe descargar desde la siguiente dirección:
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

ESCANEO DE VULNERABILIDADES NESSUS

Una vez que la importación de la máquina virtual fue exitosa, está lista para un proceso de análisis de vulnerabilidades que comprende la fase de escaneo vista en los ejes anteriores con el fin de identificar, listar e inventariar todas las vulnerabilidades detectadas en Metasploitable, de esta manera se puede ayudar al análisis de las fases siguientes del hackeo. Para efectos de agilidad en el proceso de escaneo se presenta en las siguientes figuras el resumen de este, efectuado a nuestra máquina a vulnerar. Lo que nos ubicaría en la fase dos de las generales de un hackeo ya sea ético o malicioso.

Imagen 2 Resumen de vulnerabilidades Metasploitable



Fuente: Elaboración propia

En la figura 2, la herramienta Nessus presenta el resumen cuantificado de vulnerabilidades encontradas en la máquina analizada, que maneja 5 categorías de riesgo: críticas, altas, medias, bajas e informacionales.

A continuación, en la figura 3 se visualiza la forma de presentar las vulnerabilidades críticas (las más graves), resultado del escaneo con Nessus, donde se pueden identificar temas de SSH, versión de sistema operativo sin soporte e incluso contraseña detectada por el escáner Nessus.

Imagen 3 Resumen de vulnerabilidades críticas

Severity	CVSS	Plugin	Name
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	61708	VNC Server 'password' Password

Fuente: Elaboración propia

A continuación, en la figura 4 se visualizan las vulnerabilidades categorizadas como altas que al igual que las críticas vistas en la figura anterior tienen grave riesgo por vulnerabilidades de DNS, login y versión de servicio web sin soporte (descontinuado).

Imagen 4 Resumen de vulnerabilidades altas

HIGH	9.4	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
HIGH	7.5	10205	rlogin Service Detection
HIGH	7.5	10245	rsh Service Detection
HIGH	7.5	34460	Unsupported Web Server Detection

Fuente: Elaboración propia

En la siguiente figura (5) se identifica el inventario de las vulnerabilidades medias que, si bien no son tan fáciles de explotar como los dos grupos anteriores (críticas y altas), tendrán un grado de más dificultad para explotar. Las más relevantes en este grupo de vulnerabilidades medias son temas de cifrado débil, configuraciones por defecto y detección de servicios inseguros.

Imagen 5 Resumen de vulnerabilidades me

MEDIUM	6.8	12085	Apache Tomcat Default Files
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	5.0	42256	NFS Shares World Readable
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.0	52611	SMTP Service STARTTLS Plaintext Command Injection

Fuente: Elaboración propia

A continuación, en la figura 6 se muestran las vulnerabilidades definidas como bajas. Sin embargo, esto no quiere decir que no sean explotables, se han conocido casos de explotación de vulnerabilidades que pese a ser calificadas como bajas han podido vulnerar sistemas. Para este grupo de vulnerabilidades

se detectaron temas de versiones de cifrado y SSH.

Imagen 6 Resumen de vulnerabilidades bajas

LOW	2.6	10407	X Server Detection
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Fuente: Elaboración propia

Teniendo en cuenta que los escáneres de vulnerabilidades en ocasiones presentan algunas debilidades de nivel bajo, para este caso se omitirán las categorizadas como informacionales indicadas en la figura 2, identificadas con color azul. Ahora bien, si estas vulnerabilidades son encontradas en unas pruebas de hackeo ético en una organización lo primero que se debería preguntar es

- ¿Son explotables las vulnerabilidades listadas en las imágenes del escaneo?
- ¿Cómo podría explotarse cada una de ellas?
- ¿Qué herramientas serán efectivas para explotación?
- ¿Hasta qué punto me permiten las vulnerabilidades hackear el sistema?

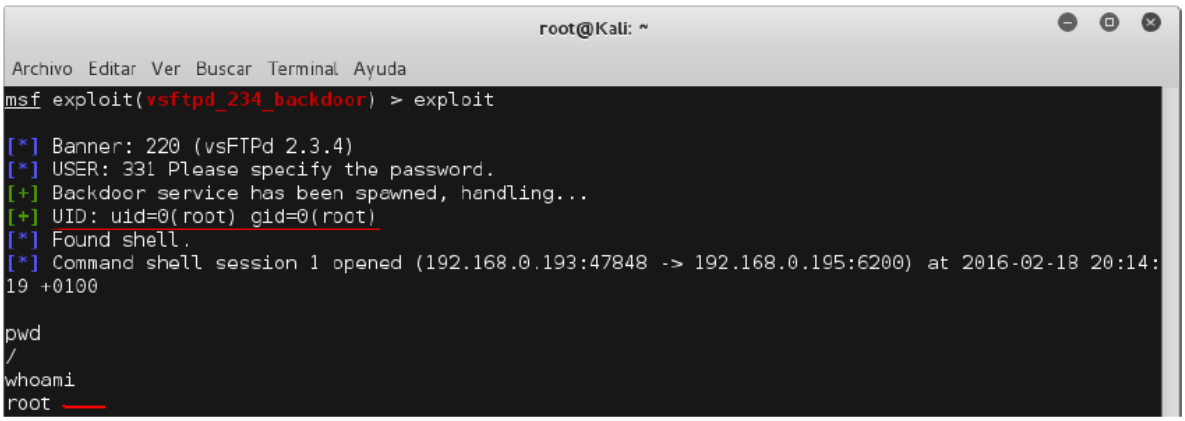
En este punto es donde la creatividad y la investigación del hacker ético deben hacer su función, es importante aclarar que los escáneres de vulnerabilidades ayudan mucho a dar puntos de partida en la documentación de cada una de las vulnerabilidades detectadas; sin embargo, no debe ser la única fuente de información para documentar las vulnerabilidades por el simple hecho que cada motor de detección de los escáneres puede detectar cosas que otros no, por eso no es recomendable determinar cómo verdad absoluta, lo que resume una sola herramienta.

Para el caso práctico, se usará Nessus para dar continuidad al proceso adelantado en el eje anterior; no obstante, se puede usar cualquier otro escáner de vulnerabilidades en un sistema de pruebas como OpenVas. Para unas pruebas de hackeo ético, los resultados del escáner es importante incluirlos en el informe a presentar a la organización ya que puede tomarse como línea base de vulnerabilidades del activo tecnológico analizado en las pruebas. Es importante tener en cuenta que el escaneó Nessus a la máquina vulnerable pudo identificar puertos con servicios expuestos tales como:

- Puerto 21 VSFTPD
- Puerto 22 SSH
- Puerto 23 TELNET
- Puerto 25 SMTP

La explotación del puerto 21 correspondiente a un servicio FTP se identifica como vulnerable ya que contiene una versión vsftpd 2.3.4. Este tipo de explotación se puede lograr aprovechando la existencia de un exploit (VSFTPD_234_BACKDOOR) contenido en la base de datos de la herramienta Metasploit, que le permite al hacker la búsqueda específica del exploit relacionada a la versión del servicio. En la figura 7 se visualiza el resultado final de la explotación donde el comando whoami indica que se ha obtenido acceso como super usuario root.

Imagen 7 Resultado final de explotación puerto 21



Fuente: https://www.fwhibbit.es/guia-metasploitable-2-parte-1

En el marco de estar efectuando pruebas de hackeo para alguna empresa y que uno de los servidores analizados en nuestras pruebas sea una máquina Metasploitable, lo conveniente es que una vez se explote la vulnerabilidad se tomen las evidencias de la infiltración lo más detalladamente posible, explicando el procedimiento. Es en este punto es donde el hackeo ético hace la diferencia con respecto a los otros tipos de hackeo, ya que por medio de la documentación se ayuda a la organización a replantear la situación actual de las vulnerabilidades y con ello puede hacerse un plan de solución.

PRESENTACIÓN DE INFORMES

Teniendo en cuenta que es la fase final del hackeo ético, no se puede dejar este curso sin hablar de ella: esta fase es la que da valor, por ser la que pone al descubierto los agujeros de seguridad existentes en el activo tecnológico de la organización o empresa.

La presentación de informes es pertinente manejarla en dos frentes: informe ejecutivo e informe técnico. El primero que se menciona debe ser un informe corto, conciso y con el resumen de la actividad efectuada, indicando si se logró el objetivo y la cantidad de vulnerabilidades asociadas al riesgo.

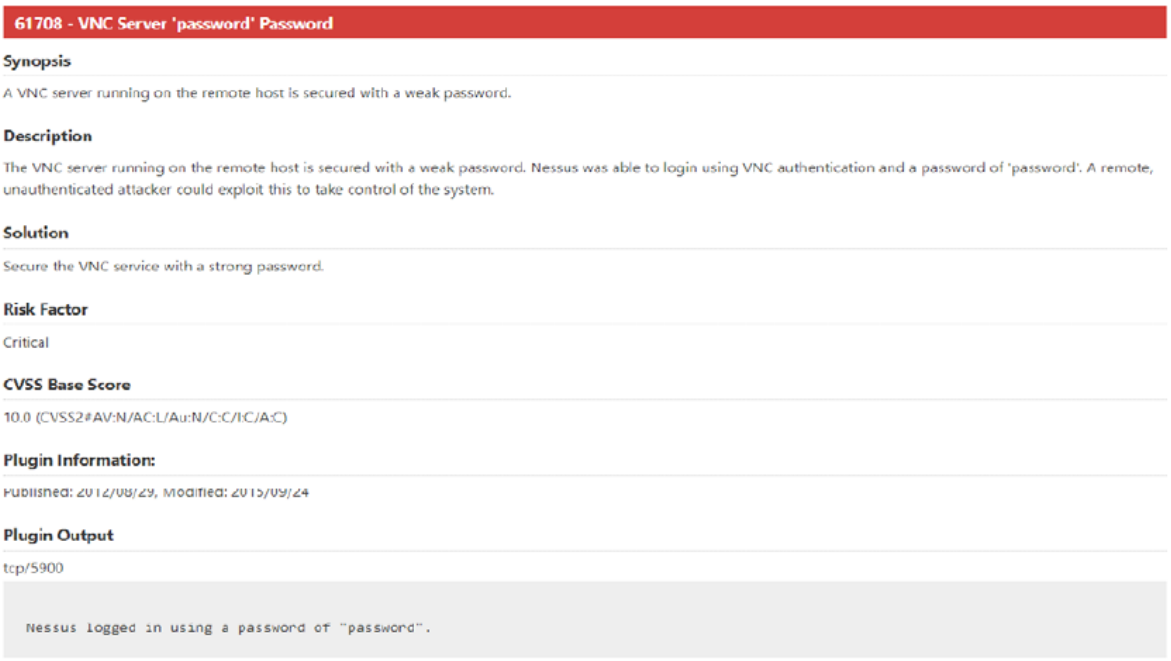
Por ser un informe que se dirige a la alta gerencia de las organizaciones, es recomendable ilustrarlo en términos de riesgo, ya que por medio de este se toman decisiones en función de minimizar vulnerabilidades y efectuar planes de solución que permitan endurecer la seguridad física y lógica de los activos tecnológicos.

Por otra parte, el informe técnico debe ser detallado y contener una serie de recomendaciones a los interesados o responsables de la plataforma tecnológica donde se encuentran los activos vulnerables. No hay una norma establecida de cómo presentar un informe técnico, pero es recomendable que el listado de vulnerabilidades halladas en la fase de escaneo sea la línea base para brindar

la información de explotabilidad, criticidad, recomendaciones y algún comentario adicional que se quiera aportar.

Para esta tarea, la información que brindan los escáneres de vulnerabilidades es de gran importancia, ya que dichos escáneres detallan la vulnerabilidad encontrada de manera que con ello se tiene en gran parte adelantado el informe. En la siguiente figura se puede apreciar un ejemplo sobre una vulnerabilidad específica de la máquina Metasploitable.

Imagen 8 Detalle de vulnerabilidad críticas



En la figura 8 podemos identificar lo siguiente de la vulnerabilidad: se ha encontrado un servidor VNC (Virtual Network Computing) el cual es un programa de software libre basado en una arquitectura cliente-servidor, que permite tener control del servidor remotamente a través de un computador cliente. Desde el punto de vista del hackeo ya nos da una ventaja al saber que hay un servicio que permite acceder a la máquina sin estar presentes físicamente.

Sin embargo, el detalle no termina ahí, el escáner indica que la vulnerabilidad consiste en estar protegido con una contraseña débil lo cual amplía el umbral de aprovechamiento de este fallo.

En la descripción se dice un poco más acerca del servidor VNC que se ejecuta en el host, pero lo más importante es que informa que en el escaneo se logró iniciar sesión utilizando la autenticación VNC con una contraseña para este caso “password”, que indica que un atacante remoto podría explotar esto para tomar el control del sistema.

Solución

Para analizar un poco el caso de esta vulnerabilidad, cabe aclarar que esta no es del servicio sino de la contraseña débil que pudo ser encontrada en el proceso, seguramente por un ataque de fuerza bruta o ataque de diccionario según el algoritmo empleado por el escáner. Es claro que la recomendación es asegurarse de que el servicio VNC tenga una contraseña segura lo cual se resume en longitud y complejidad en los caracteres.

Factor de riesgo

Esta vulnerabilidad fue categorizada como crítica con toda razón, ya que es claro que un acceso con contraseña legítima a un sistema garantiza todos los privilegios que tenga el propietario de la cuenta de usuario comprometida, que en este caso es a quien se le pudo adivinar la contraseña.

PUNTUACIÓN BASE: COMMON VULNERABILITY SCORE SYSTEM (CVSS).

La puntuación de la vulnerabilidad está dada por una nomenclatura del CVSS separados por el carácter “:” haciendo que cada segmento de caracteres indique la calificación obtenida. Por ejemplo:

10.0 (CVSS#AV:N/AC:L/Au:N/C:C/I:C/A:C).

La puntuación CVSS es un puntaje creado para proveer un método abierto y estándar que permite estimar y valorar el impacto proveniente de las

vulnerabilidades identificadas en el campo de la tecnología, lo cual ayuda a cuantificar la severidad que pueden representar las vulnerabilidades valoradas. Actualmente existe la versión 3 del sistema de puntaje determinado por el marco de referencia de la CVSS.

La CVSS se encuentra regulado por el Forum of Incident Response and Security Teams (FIRST), un estándar abierto, que puede ser utilizado por cualquiera.

Para entender un poco a lo que se refiere la cadena de caracteres indicada en el puntaje CVSS, es necesario comprender los parámetros calculados por el sistema diseñado por el FIRST. Para ello podemos empezar conociendo cómo se calcula el impacto con CVSS.

Partamos del punto de que para determinar el impacto que representa una vulnerabilidad se utiliza una escala numérica con los rangos de 0 a 10. La severidad se considera baja (low) si el puntaje alcanzado después de aplicar la fórmula CVSS resulta entre 0.0 y 3.9. El impacto es medio si el resultado se ubica entre 4.0 y 6.9. Se considera alto cuando el puntaje cae dentro del rango: 7.0 y 10.0. - mismo tiempo un conjunto de otras métricas, como se verá a continuación.

Para calcular un puntaje de una vulnerabilidad, CVSS utiliza tres grupos o categorías de métricas:

- Base
- Temporal
- Entorno

Métricas base

Las métricas base son las características exclusivas de la vulnerabilidad, son constantes en el tiempo y en el entorno del usuario. Incluyen las métricas de vector de acceso, complejidad de acceso y autenticación, de manera que permiten definir cómo se puede acceder a una vulnerabilidad y si se cumplen

las condiciones para que sea explotada.

La severidad de las tres métricas mide la manera en la que una vulnerabilidad se explota y también la forma de afectación directa al hardware o software de la infraestructura tecnológica. Los impactos se determinan de manera individual, como el grado de pérdida de confidencialidad, integridad y disponibilidad, ya que una vulnerabilidad podría causar pérdida parcial solo en alguno de los pilares de la seguridad de la información como también en todos.

Métricas temporales

Este segundo grupo representa las características de una vulnerabilidad que puede cambiar en el tiempo, pero que es constante en el ambiente de un usuario. Se consideran tres factores que influyen en ello:

- Explotabilidad
- Nivel de solución
- Reporte de confianza

Estas métricas temporales hacen referencia a la disponibilidad del código o técnicas que permitan la explotación de la vulnerabilidad. Estas métricas son opcionales y no afectan la calificación, en caso de no calificarlas; es decir, no son un campo obligatorio, solo se contemplan en caso de tenerse la información en el contexto de detección de la vulnerabilidad.

Entorno

Representa las características de una vulnerabilidad que son influyentes y únicas para el entorno de un usuario. Se definen en función de los distintos ambientes que pueden implicar una gran influencia sobre el riesgo que representa la fragilidad para una organización. Este grupo de métricas se enfoca en las características de vulnerabilidad asociadas al entorno del usuario.

También como el grupo anterior son opcionales y no influyen en la puntuación.

La siguiente tabla resume el grupo de métricas con los posibles valores que pueden tomar en el momento de calificar y su obligatoriedad.

Imagen 9 Base, Temporal and Environmental Vectors

Metric Group	Metric Name	Possible Values	Mandatory?
Base	Attack Vector, AV	[N,A,L,P]	Yes
	Attack Complexity, AC	[L,H]	Yes
	Privileges Required, PR	[N,L,H]	Yes
	User Interaction, UI	[N,R]	Yes
	Scope, S	[U,C]	Yes
	Confidentiality, C	[H,L,N]	Yes
	Integrity, I	[H,L,N]	Yes
	Availability, A	[H,L,N]	Yes
Temporal	Exploit Code Maturity, E	[X,H,F,P,U]	No
	Remediation Level, RL	[X,U,W,T,O]	No
	Report Confidence, RC	[X,C,R,U]	No
Environmental	Confidentiality Req., CR	[X,H,M,L]	No
	Integrity Req., IR	[X,H,M,L]	No
	Availability Req., AR	[X,H,M,L]	No
	Modified Attack Vector, MAV	[X,N,A,L,P]	No
	Modified Attack Complexity, MAC	[X,L,H]	No
	Modified Privileges Required, MPR	[X,N,L,H]	No
	Modified User Interaction, MUI	[X,N,R]	No
	Modified Scope, MS	[X,U,C]	No
	Modified Confidentiality, MC	[X,N,L,H]	No
	Modified Integrity, MI	[X,N,L,H]	No
	Modified Availability, MA	[X,N,L,H]	No

Fuente: https://www.first.org/cvss/specification-document

Con todo lo expuesto se puede definir el nivel de riesgo y criticidad de las vulnerabilidades según su puntaje en el sistema CVSS teniendo en cuenta los criterios de calificación.

Recomendaciones de solución de vulnerabilidades

Las recomendaciones en el informe de un hackeo ético son el punto clave para endurecer la seguridad en los activos que fueron sometidos a pruebas, de tal modo que con dichas recomendaciones se disminuya el nivel de riesgo en las organizaciones.

Las sugerencias tienen que ser alcanzables y realistas, sin importar el tipo de organización. Si bien es claro que la solución de vulnerabilidades en muchos casos está ligada a la inversión de soluciones de seguridad costosas, así como

también a otras que son únicamente de parametrización y configuración del activo tecnológico, lo que se recomiende y concluya en el informe de hackeo ético ayudará a las organizaciones a enfrentarse a nuevos retos tecnológicos y compromisos desde la alta gerencia, ya que muchas veces al no identificarse como propios de la operación del negocio de las compañías, pueden no recibir la prioridad real necesaria.

CONCLUSIONES Y RECOMENDACIONES

- El hackeo ético es un medio para ayudar al mundo a ser más seguro a nivel tecnológico. Las organizaciones y personas hoy en día están reconociendo este tipo de hackeo para evitar intrusiones o daños en los activos tecnológicos que soportan su funcionamiento.
- Pese a que el concepto de hacker tiene una connotación ética, a veces puede malinterpretarse con aquel informático que tiene como único objetivo hacer daño tecnológico a personas o compañías. La ética o ausencia de ella en el hacker siempre definirá qué tan buenas o ilegales pueden ser las actividades que efectúe en el medio tecnológico.
- Como cultura del hackeo ético debe siempre prevalecer el ser un mecanismo para proteger la infraestructura tecnológica de las organizaciones o usuarios.
- Las habilidades, destrezas y conocimientos adquiridos en este curso deben ser siempre usadas para proteger y evitar ataques cibernéticos que estarán en función de encontrar fallos en la seguridad de plataformas tecnológicas para efectuar algún daño, robo, sabotaje o espionaje.

REFERENCIAS BIBLIOGRÁFICAS

FIRST. (s. f.). Common Vulnerability Scoring System v3.0: Specification Document. Recuperado de https://www.first.org/cvss/specification-document

Fernández, J. (2016)). Guia Metasploitable 2: Parte 1. Recuperado de https://www.fwhibbit.es/guia-metasploitable-2-parte-1

Rapid7user. (s. f.). Metasploitable2/. Recuperado de https://sourceforge.net/projects-/metasploitable/files/Metasploitable2/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica