**Prueba técnica supervisada – Consultor Ciberseguridad Junior**

Para realizar esta prueba:

1. Deberá hacerse en sitio, sin acceso a internet.
2. Tiempo máximo: 1.5 horas.
3. Si se hace remoto:
   1. Deberá hacerse mediante teams, compartiendo su pantalla con personal de RRHH para supervisor la prueba.
   2. Validar que la cámara esté encendida.
   3. Validar que el aspirante esté compartiendo su pantalla.
   4. Validar que el aspirante no esté hacienda uso de un monitor extendido (Click derecho sobre el escritorio, “configuración de pantalla”).

La siguiente prueba tiene como objetivo identificar tus conocimientos sobre tecnología y seguridad informática. ¡Si esto te apasiona, será pan comido 😊 Happy Hacking!

1. **¿qué es kali linux?**

Sistema operativo UNIX normalmente utilizado para hacking ético y Pentester

1. **¿Qué es nmap?**

Programa que nos permite realizar escaneos análisis de red en las cuales podemos obtener mucha información de cada computadora, una de las principales herramientas para un pentester

1. **¿qué hace esto?: nmap -sv 192.168.1.1**

Comando de nmap el cual nos ayudara a conocer los servicios y puertos abiertos con sus respectivas versiones de la dirección IP 192.168.1.1

1. **¿qué es sudo?**

Palabra clave para permisos de administrador para ejecutar aplicaciones o hacer tareas como si fuese el usuario root

1. **¿Cuáles son las fases de una prueba de intrusión?**

Bueno, depende de la metodología que se utilice pero normalmente es: Identificación y Reconocimiento, Escaneo y Enumeración, Análisis de Vulnerabilidades, Explotación, Mantener Accesos, Borrado de huellas, Informe, agrego un paso extra que es Planeación como fase 1 y otra fase como Análisis y Evaluación de riesgos

1. **¿qué es burpsuite y para qué se usa?**

Es un programa que utilizamos para análisis de vulnerabilidades a aplicaciones web el cual nos permite leer los headers de las páginas, obtener información importante como directorios, cookies realizar ataques de intrusión, fuerza bruta, spider, es el más recomendado.

1. **¿Qué es owasp zap y para qué se usa?**

Lo mismo que burpsuite, solo que owasp zap ya es un proyecto propio de OWASP, junto con burpsuite son los más recomendados para el análisis de vulnerabilidades a aplicaciones web

1. **¿Qué es owasp?**

Es un proyecto para mejorar la seguridad del software mas enfocado para las aplicaciones web.

1. **¿Qué es owasp top 10?**

Es un proyecto abierto por OWASP el cual nos mencionan las 10 vulnerabilidades mas comunes en la actualidad y la cual se esta actualizando en un periodo de tiempo.

1. **Explique qué es inyección SQL y cómo puede corregirlo**

Es uno de los principales ataques siempre ha estado liderando el top 10 de OWASP la cual se pueden realizar a plataformas o aplicaciones web si estas no cuentan con los mecanismos de seguridad apropiados en sus entradas o salidas, el cual consiste en comandos SQL para engañar al interprete y asi obtener información de una base de datos.

1. **¿Qué es hack the box o try hack me?**

Son plataformas de entrenamiento para realizar pentesting, hacking ético y análisis de vulnerabilidades y practicas de capture de flag, además de afianzar los conceptos teóricos.

1. **¿Qué es Nessus?**

Es una aplicación para análisis de vulnerabilidades de Tenable, el cual nos permite escanear por dirección Ip las computadoras de una red y de manera automática nos da como resultado las vulnerabilidades a las que esta expuesta la computadora organizando cada uno de ellos con una valoración de riesgo y un puntaje (Critico, Alto, Medio, Bajo, Info) el cual también nos da una descripción de cada vulnerabilidad, la respectiva solución la vulnerabilidad, el puerto o ouput a la cual esta ligada la vulnerabilidad, referencias e información de si puede ser explotada con metasploit u otra vía.

1. **¿Qué técnicas de ingeniería social conoces? Detallar.**

Wifiphisher

Airgeddon

Hubo una tarea en la maestría donde se realizó la duplicación del login de redes sociales para engañar al objetivo creo que la herramienta se llama setTool (se me escapa el nombre)

1. **¿Has hackeado algo? Explica**

Tareas de la maestría con máquinas virtuales como BADSTORE, DVWA con inyecciones SQL y curso de auditor y Pentester en redes wifi el cual realizamos auditorias para obtener las credenciales de la red mediante phishing, desautenticar clientes, y también en Auditoria de una empresa de Servicios informáticos para trabajo de investigación de tesis, el cual consiste en realizar una auditoria a las computadoras del área de servicios secretariales, administración, caja e identificar las vulnerabilidades a las que están expuestas y logramos explotar una vulnerabilidad tomando control de ella aprovechando la vulnerabilidad si no mal recuerdo con nombre pexec a una maquina con Sistema Operativo Windows 7. Y también hemos realizado practicas con máquinas virtuales con HackTheBox y también practicas de un curso gratuito de RED TEAM

1. **¿qué es un hacker?**

Es una persona con grandes conocimientos de informática, cuyo rol es realizar pruebas de seguridad haciendo pruebas de penetración para encontrar vulnerabilidades, esto con el permiso de la empresa que lo contrate, realizando todo ello de forma ética y legal, éticamente correcto, normalmente este concepto mediáticamente lo confunden con los crackers que vienen haciendo lo mismo pero con intensiones maliciosas e ilegales por ello se utiliza el concepto Ethical Hacking para diferenciar los buenos con los malos.

1. **Menciona y da ejemplos de 5 comandos linux.**

**Sudo apt-get install nombre\_de\_programa:** Sirve para instalar programas

**Sudo nano /etc/network/interfaces:** Sirve para configurar dirección IP de la máquina, Gateway.

**Sudo msfconsole:** para ingresar al metasploit para realizar ataques con exploits y payloads

**Cd /angel/Desktop/:** CD Sirve para desplazar al directorio

**ls:** para listar los archivos en el directorio que nos encontramos

**lsusb:** listar dispositivos usb conectados al equipo.

**ifconfig:** para ver configuraciones IP y más información

**iwconfig:** ver configuraciones inalámbricas

**iv dev:** Configuración inalámbricas

1. **¿qué es y para qué se utiliza Metasploit?**

Viene siendo la navaja suiza para un Pentester el cual nos permite realizar los ataques mediante los exploit y payload que esta herramienta contiene

1. **Menciona tu película hacker favoritas**

No recuerdo los nombres, recuerdo una que es un robo a un banco y contratan a un muchacho el cual este no había aceptado una oferta de trabajo de una gran empresa ya que quería metas y desafíos grandes.

1. **¿cómo capturarías tráfico HTTP de una aplicación móvil hacia su backend?**

Intentaría primero con wireshark, segudo Burpsuite, si no investigaría en internet.

1. **¿qué es un apk?**

Extensión de una aplicación móvil

1. **¿qué es un ipa?**

No tengo conocimiento

1. **¿cuál es la diferencia entre análisis de caja blanca y negra? ¿Existen otros?**

Que en la blanca tenemos información de la empresa y con la negra tenemos que realizar desde cero realizando ataques para obtención de la información, Si existe caja Gris.

1. **¿qué es un DoS y un DDoS?**

Denegación de Servicios a un solo host y Denegación de servicios a múltiples hosts

1. **¿cómo categorizarías una vulnerabilidad? Explicar impacto o nivel de riesgo, por ejemplo.**

Critico: 9.0 a 10.0

Alto: 7.0. a 8.9

Medio: 5.0 a 6.9

Bajo: 0 a 4.9

1. **Explique qué es un CVE**

Viene siendo como un estándar de valoración de una vulnerabilidad, lo confundo con CWE o algo parecido que se refiere al nombre que se le coloca a una vulnerabilidad una vez descubierta

1. **¿Cómo haces reversing de un apk?**

En aplicaciones móviles, aun no tengo muchos conocimientos, pero interesado en investigar en ello. Pero me imagino a que se refiere en tomar un apk de una aplicación modificarlo e incrustar un exploit para que cuando la app sea instalada pida al usuario permisos de cámara, contactos entre otros y así tener acceso al dispositivo móvil.

1. **Describe qué servicios usualmente corren sobre los siguientes puertos:**
   1. 80: http
   2. 443: https
   3. 21:ftp
   4. 22: ssh
   5. 23
   6. 445 ftps
   7. 3389
   8. 3306: mysql
   9. 1443

Me falta practica para que se me queden los números de los puertos se que en esos números tiene que estar el SMTP

1. **¿Cuál es la diferencia entre un ataque de fuerza bruta y un ataque de diccionario?**

Fuerza bruta es tratar de ingresar a un login de manera brusca, violenta o a la fuerza de manera aleatoria.

Diccionario: mismo que la anterior solo que va realizando las combinaciones de crackeo de contraseñas mediante las palabras que contenga el diccionario de datos

1. **¿cómo hackearías el wifi del colegio?**

Primero analizaría si la contraseña la dan así por así a particulares o por ser alumno dan la contraseña, si no dan la contraseña a particulares, me centraría en realizar pruebas de desautenticación y capturar el handshake y crackear la contraseña con un diccionario de datos, si no se logra obtener la contraseña de esa manera la otra opción es realizar ataques de phishing con por cautivo duplicando la red para ver quien cae en la trampa

1. **Si tuvieras que elegir entre CEH y OSCP, ¿cuál elegirías y por qué?**

Se me olvido, pero si e visto esas abreviaturas

1. Escribir las contrapartes seguras de los siguientes protocolos inseguros:
   1. Telnet - ssh
   2. HTTP - https
   3. FTP - ftps
2. **¿Cómo garantizarías que una organización esté “100% segura”?**

En mi opinión el 100% nunca se daría por el factor humano, pero para tener altos índices de seguridad lo primero es capacitar al personal de la organización, realizar auditorias de los sistemas de información y a partir de los resultados tener una metodología de detección y mitigación de vulnerabilidades con sus respectivos controles de seguridad y tener plan de contingencias por cualquier desastre.

1. **¿por qué deberíamos contratarte para hackear el mundo?**

Una por mis conocimientos que he obtenido en este tiempo de la Maestría en Seguridad informática y las ganas de poner en practica esos conocimientos, otra porque me ha apasionado el área de la ciberseguridad, y hay temas que aun no conozco, pero me es un reto porque me gustan los desafíos ya que me gusta la retroalimentación investigar por mí mismo tema que aún no domino. Nunca me doy por vencido hasta lograr el objetivo.

1. **Estás evaluando un sitio hecho en wordpress. Realiza un pequeño checklist que describa qué verificar para tener lineamientos básicos de aseguramiento del sitio.**

Análisis de la página web/ Estructura

Diagramar Lógica de la página web

Revisar todas las entradas (inputs, links)

Revisar todas las salidas

1. **Si tuvieras que hacer un pentest interno, y debes elegir solamente 3 herramientas para utilizar, ¿cuáles usarías y por qué? (trick: ¡kali no te hace hacker!)**

Nmap

Nessus

Metasploit / msfconsole

**Valor agregado: the real thing** 😊

¿Qué parece esto?

**aG9sYSBtdW5kbw==** una clave encriptada el cual puede ser descifrada en crackstation.

No se si seria md5

¿qué parece esto otro?

**Administrador:500:42f29043y123fa9c74f23606c6g522b0:71759a1bb2web4da43e676d6b7190711:::** son las credenciales de una cuenta de usuario si no me equivoco de Windows el cual podemos decifrar con herramientas como hashcat o jhon de Ripper, si no mal recuerdo con hashcat se usa el modulo 2500 o 1500, creo que es NTLM el cifrado

¿Y esto?

**msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::**

Vendría siendo el mismo caso que el anterior pero en sistema de LINUX o MAC