



eJPT V2

Carta de compromiso - V1.0

Configuración del examen

El entorno del examen eJPT V2 es un entorno de laboratorio dentro del navegador que le proporciona acceso a un sistema Kali Linux preconfigurado con todas las herramientas, scripts y listas de palabras necesarias para responder y completar con éxito las preguntas/retos asociados al examen.

La arquitectura de laboratorio en navegador garantiza que pueda comenzar, avanzar y completar el examen desde cualquier dispositivo y desde cualquier lugar con una conexión a Internet estable y sin necesidad de configurar sus propias máquinas virtuales.

El sistema Kali Linux que se le proporciona durante el examen no tiene conexión a Internet, por lo que puede utilizar el navegador de su sistema operativo anfitrión para investigar.

Además, todos los módulos de explotación necesarios y el código de explotación son accesibles en el sistema Kali Linux a través del Metasploit Framework y la Exploit Database (Exploit-DB).

NOTA: No necesita descargar ni instalar ningún script o herramienta personalizada en el sistema Kali Linux integrado en el navegador al que se le ha proporcionado acceso. El sistema Kali Linux tiene todo lo necesario para completar con éxito el examen.

Alcance del compromiso

Usted ha sido contratado para realizar una Prueba de Penetración de Caja Negra in situ contra los hosts, aplicaciones web y redes de una organización llamada **Syntex**.

Dynamics.

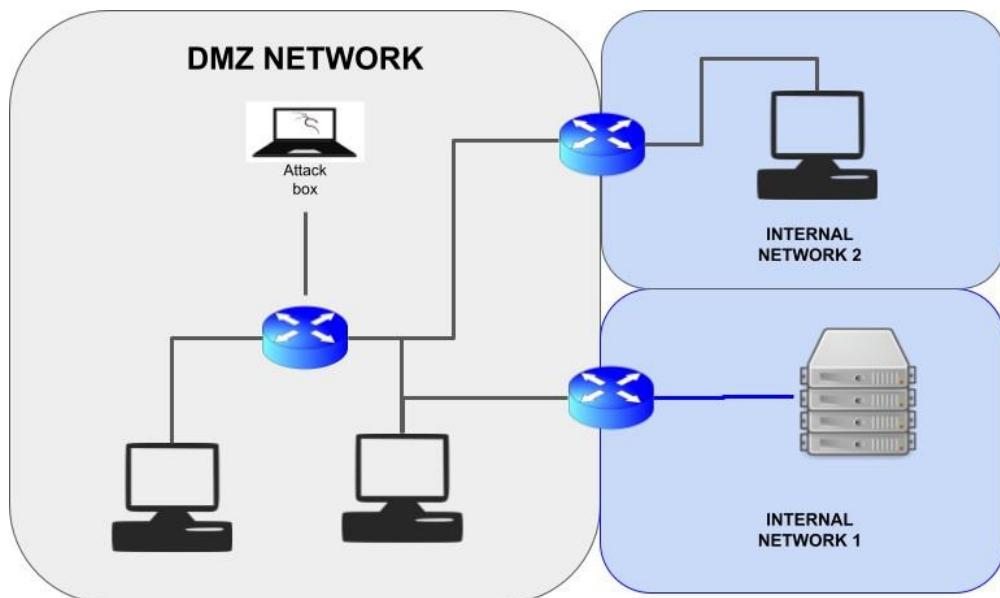
Esto es lo que la organización cliente ha definido como el alcance de las pruebas:

- La red DMZ a la que se conectará.
- Cualquier otra red interna a la que pueda acceder.

Cuando inicie por primera vez su entorno de laboratorio de examen, se conectará automáticamente a la red DMZ, esta red contiene servidores de producción y aplicaciones web a las que potencialmente puede obtener acceso a través de ataques de fuerza bruta y a través de la explotación de configuraciones erróneas o vulnerabilidades.

También se requiere que identifique cualquier red interna, pírote en ellas, identifique hosts dentro de esta red/redes internas y obtenga acceso a estos sistemas.

Tenga en cuenta que el siguiente diagrama es orientativo y no refleja la configuración de red real del examen.



Desde la red DMZ es posible llegar a algunas otras redes/redes internas. Todas las redes son redes /24. Hay que encontrar la información de enrutamiento y las direcciones de red identificando un punto pivote que interconecte las dos redes.

El sistema Kali Linux contiene todos los diccionarios de nombres de usuario y contraseñas comunes, por si tienes que realizar un ataque de fuerza bruta.

Objetivos del examen

Tenga en cuenta que debe realizar una prueba de penetración en todos los hosts incluidos.

Las preguntas de la zona de pruebas cubrirán la mayoría de sus finiciones del eJPT V2.

Puede elegir libremente cómo y en qué orden desea responder a las preguntas durante la prueba de penetración.

Tenga en cuenta que tanto el área del cuestionario como el entorno del laboratorio de examen serán accesibles simultáneamente durante todo el periodo del examen (48 Horas).

Herramientas recomendadas

Usted es libre de utilizar cualquier entorno para realizar su prueba de penetración.

A continuación se sugiere una lista de herramientas que pueden ser útiles durante el examen:

- Nmap
- Dirbuster
- Nikto
- WPScan
- CrackMapExec
- El marco Metasploit
- Searchsploit

- Hydra

Tenga en cuenta que todas las herramientas mencionadas vienen preinstaladas en el sistema Kali Linux que se le proporciona.

Consejos para una prueba de penetración con éxito

- No pienses en el examen como un "Atrapa la bandera". No lo es.
- Consulte el documento Directrices del laboratorio que se le proporciona junto con este documento para obtener información sobre el funcionamiento del laboratorio en el navegador.
- Tome notas y guarde sus hallazgos en una aplicación externa de toma de notas en su sistema operativo anfitrión. (Esto se debe a que cualquier dato que almacene en el sistema Kali Linux se borrará si reinicia su entorno de laboratorio).
- Otra gran idea es responder a las preguntas mientras realizas tu Prueba de Penetración. (Lea atentamente la pregunta y, a continuación, realice sus pruebas en el laboratorio).
- Cualquier ataque, herramienta o técnica, de acuerdo con las reglas de enfrentamiento, está permitido durante el examen.