Hack The Box Tier 0

Houssain Ezzaoua

MEOW

Preguntas ¿?	Respuestas¡!
¿Qué significan las siglas VM?	Virtual Machine
¿Qué herramienta utilizamos para interactuar con el sistema operativo con el fin de emitir comandos a través de la línea de comandos, como el de iniciar nuestra conexión VPN? También se conoce como consola o shell.	Terminal
¿Qué servicio utilizamos para formar nuestra conexión VPN en los laboratorios HTB?	OpenVPN
¿Qué herramienta utilizamos para probar nuestra conexión al objetivo con una solicitud de eco ICMP?	ping
¿Cómo se llama la herramienta más común para encontrar puertos abiertos en un objetivo?	nmap
¿Qué servicio identificamos en el puerto 23/tcp durante nuestras exploraciones?	telnet
¿Qué nombre de usuario es capaz de iniciar sesión en el objetivo a través de telnet con una contraseña en blanco?	root

FAWN

Preguntas ¿?	Respuestas¡!
¿Qué significa la sigla de 3 letras FTP?	File Transfer Protocol
¿En qué puerto escucha habitualmente el servicio FTP?	21
¿Qué acrónimo se utiliza para la versión segura de FTP?	SFTP
¿Cuál es el comando que podemos utilizar para enviar una solicitud de eco ICMP para probar nuestra conexión con el objetivo?	*ping*
Según tus análisis, ¿qué versión de FTP se está ejecutando en el objetivo?	vsftpd lhua 3.0.3(normalmente, depende de la vpn)
Según tus escaneos, ¿qué tipo de sistema operativo se está ejecutando en el objetivo?	Unix (normalmente)
¿Cuál es el comando que debemos ejecutar para mostrar el menú de ayuda del cliente 'ftp'?	*ftp -h*
¿Cuál es el nombre de usuario que se utiliza a través de FTP cuando se desea iniciar sesión sin tener una cuenta?	anonymous
¿Cual es el comando para listar archivos en un sistema Linux.	*ls*
¿Cuál es el código de respuesta que obtenemos para el mensaje FTP "Inicio de sesión correcto"?	230
¿Cuál es el comando utilizado para descargar el archivo que encontramos en el servidor FTP?	*get*

DANCING

Preguntas ¿?	Respuestas¡!
¿Qué significan las siglas SMB?	server message block
¿En qué puerto opera SMB?	445
¿Cuál es el nombre del servicio para el puerto 445 que apareció en el escaneo Nmap?	Microsoft-ds (puede ser otro)
¿Cuál es el 'flag' o 'switch' que podemos utilizar con la utilidad smbclient para 'listar' los recursos compartidos disponibles en Dancing (o otro)?	*-L*
¿Como ver el número de shares?	*server* --no-pass //ipMV
What is the name of the share we are able to access in the end with a blank password?	WorkShares
¿Cuál es el comando que podemos utilizar de SMB (o otros) para descargar los archivos que encontremos?	*get*

REDEEMER

Preguntas ¿?	Respuestas¡!
¿Qué tipo de base de datos es Redis?	In-memory Database
¿Como saber que puerto esta abierto en una maquina?	nmap -sV *ipVM* zaml -p-
¿Qué comando de utilidad de linea se utiliza para interactuar con el servidor Redis?	*redis-cli*
¿Qué bandera se utiliza con la utilidad de línea de comandos Redis para especificar el nombre de host?	*-h*
Una vez conectado a un servidor Redis, ¿qué comando se utiliza para obtener la información y las estadísticas sobre el servidor Redis?	*info*
¿Qué comando se utiliza para seleccionar la base de datos deseada en Redis?	*select*
¿Qué comando se utiliza para obtener todas las claves de una base de datos?	*keys **

COMANDES

Per obrir la VPN

sudo openvpn *nombre de la vpn*

Para ver puertos *nmap*

Nmap -sS *ip de la MV*
Nmap -sV *ip de la MV*
-p es cuando quieres especificar un puerto
-p- para encontrar muchos puertos

Comandas per accedir a un server

telnet *ip de la MV*
smbclient //*ipMV*/*nombreServer*
ftp *ipMV*
redis-cli -h

Para tener el root flag

Dentro del servidor:
Para instalar: get flag.txt
Para ver: cat/more flag.txt

Para obtener ayuda

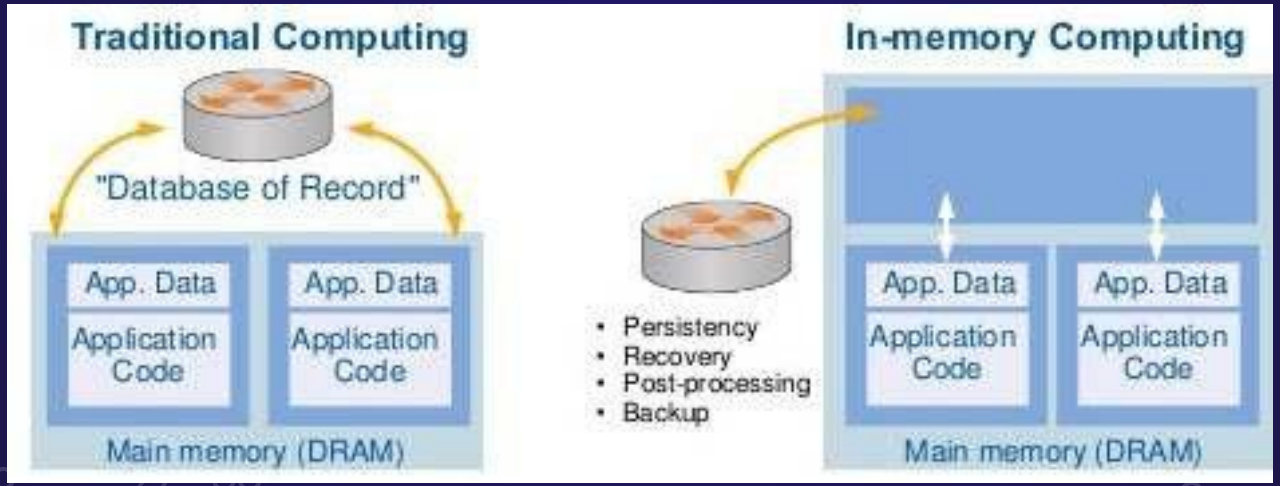
help o *-help*

Cuando no sabes ni el usuario ni la contraseña

--no-pass

In-Memory DB & Traditional DB

Una base de datos en memoria guarda todos los datos en la memoria principal o RAM de un ordenador. Una base de datos tradicional recupera los datos de las unidades de disco. Las bases de datos en memoria son más rápidas que las tradicionales porque requieren menos instrucciones de la CPU. También eliminan el tiempo que se tarda en acceder a los datos desde un disco.



Video para repasar

ESPERO QUE OS HAYA GUSTADO