**SEGURIDAD INFORMÁTICA**

**PRÁCTICA I - ATAQUES A SERVIDOR**

Los objetivos de esta práctica son los siguientes:

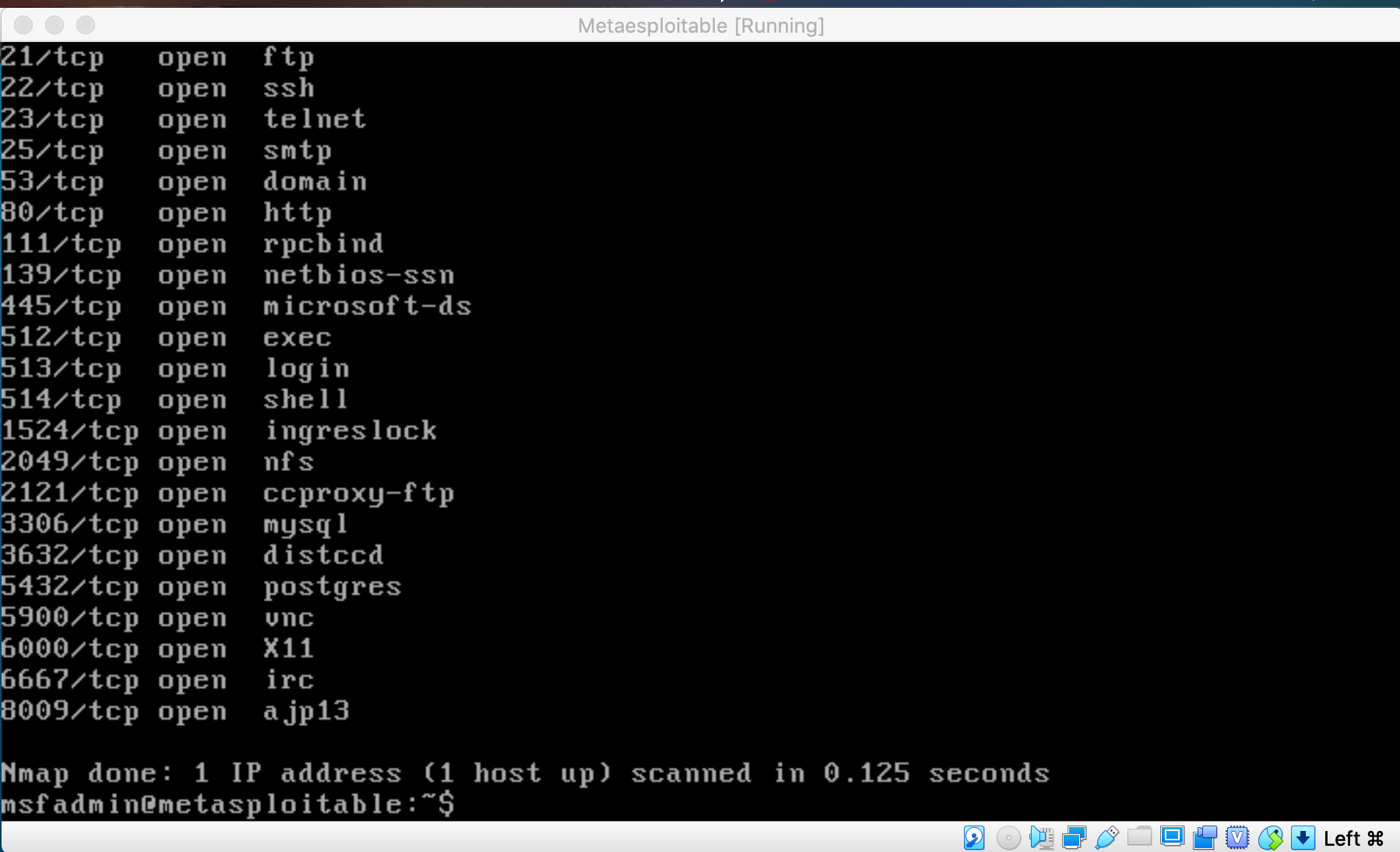
**I. APRENDER A HACER ESCANEOS A POSIBLES EQUIPOS VÍCTIMA**

**II. USO DE METASPLOIT PARA APROVECHARSE DE UNA VILNERABILIDAD**

**FASE I: EL USO DEL ESCANER DE VULNERABILIDADES NESSUS**

1. Realizar un escaneo mediante nmap para ver los puertos abiertos que tiene la máquina Metasploitable. En la salida de este escaneo de puertos debe aparecer la versión de cada servicio instalado.

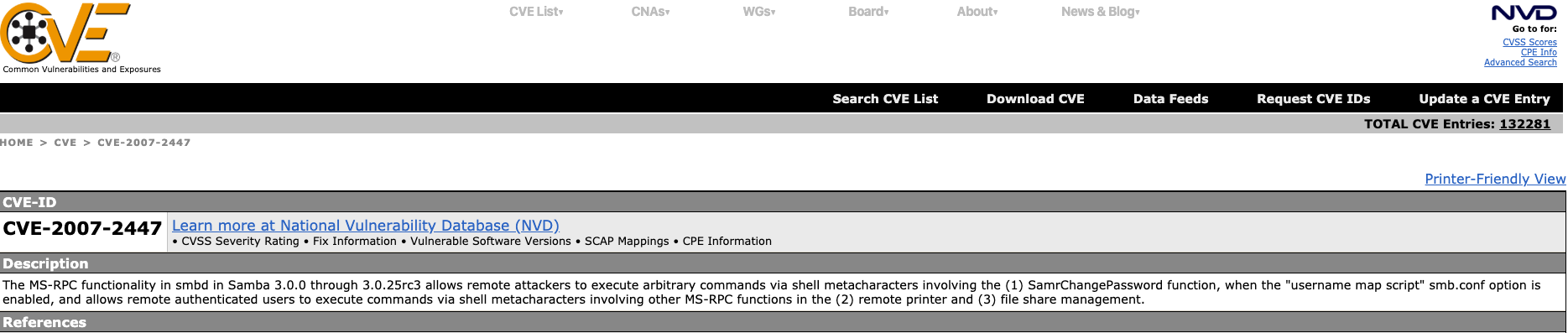
**NOTA: Esto se puede hacer desde Metasploit (puedo lanzar nmap dentro de Metasploit) o ejecutando la aplicación nmap.**

**Insertar pantallazo con el resultado del escaneo**.

1. Explicar qué es el servicio SAMBA en Linux (o SMB en Windows). Para ello responde a las siguientes preguntas:
   1. Los servicios SMB y Netbios se usan en Windows para. SMB es un protocolo para compartir archivos que se ejecuta en el puerto 445. Netbios fue un protocolo famoso desarrollado entre IBM y Sytek para redes entre computadoras
   2. Estos dos servicios utilizan los puertos 445 y 137,138,139 UDP
   3. El servicio SAMBA es la implementación en Linux del servicio SMB y Netbios de Windows. ¿Para qué se instala en equipos Linux?
2. ¿Cuál es la versión de SAMBA que está instalada en la máquina Metasploitable que ha sido escaneada?

****

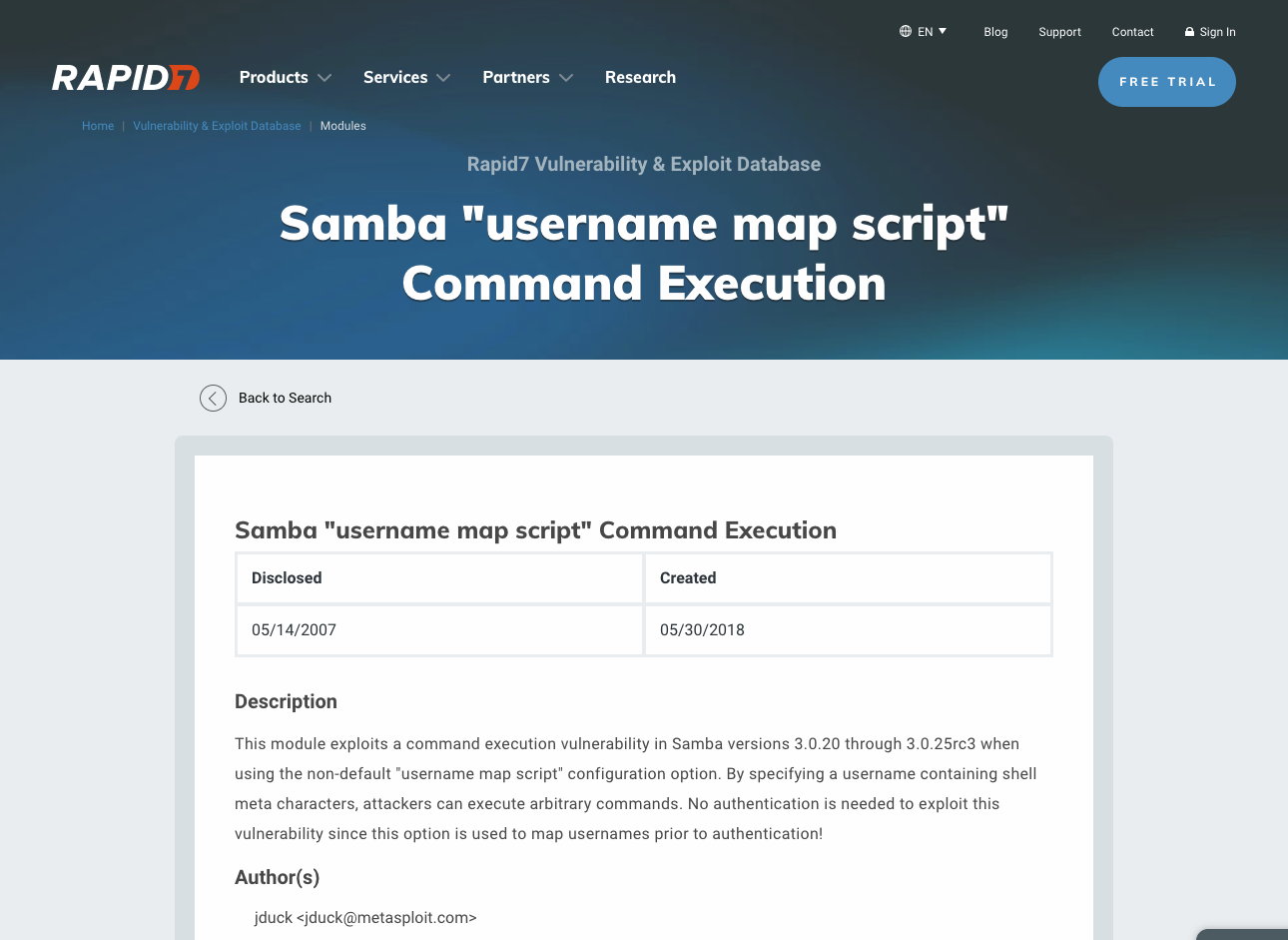
1. Buscar en <http://cve.mitre.org/> o en [www.cvdetails.com](http://www.cvdetails.com) las vulnerabilidades que tiene la versión de SAMBA encontrada en dicha máquina Metasploitable. ¿Cuántas has encontrado? **Insertar respuesta con el número encontrado y la referencia de la página consultada** <http://cve.mitre.org/> ——> 194 resultados. www.cvedetails.com ——-> 44 resultados.
2. Vamos a fijarnos en una de ellas, la que tiene que ver con la opción username map del fichero smb.conf. ¿Cómo se llama esa vulnerabilidad? Indicar el CVE correspondiente y su nivel de riesgo que se puede consultar en dicha base de datos. **Insertar respuesta**

****

1. En la misma base de datos se puede encontrar el nombre del exploit, cargado ya en Metasploit, que se puede usar para explotar esta vulnerabilidad. ¿Cómo se llama?

También se puede consultar en <https://www.rapid7.com/db/?type=metasploit>

**Insertar respuesta**

****

1. ¿Cuál es el parche que habría que instalar para solucionar esta vulnerabilidad? **Insertar respuesta con la url de samba.org donde viene información del parche y desde donde podría descargarlo.**

<https://www.samba.org/samba/security/CVE-2007-2447.html>

<https://download.samba.org/pub/samba/patches/security/samba-3.0.24-CVE-2007-2447_v2.patch>

**Después de recopilar la información de la vulnerabilidad vamos a hacer uso de ella para infiltrarnos en la víctima en la siguiente fase.**

**FASE II: USO DE METASPLOIT PARA APROVECHARSE DE UNA VILNERABILIDAD**

El objetivo es acceder a la máquina Metasploitable explotando la vulnerabilidad encontrada en el servicio SAMBA en la fase 1, haciendo uso del exploit descubierto en la misma fase 1.

Una vez dentro lo que queremos es acceder a la SAM del equipo, hacernos con los hashes de las contraseñas de dos usuarios y descifrarlos con John the Ripper.

Para ello:

1. Crear dos usuarios en la máquina Linux Metasploitable: usuariodic y usuariobrut

* El primero de ellos, **usuariodic** tendrá una contraseña que deberá ser obtenida mediante un ataque por diccionario (**por ejemplo, passw0rd, pero que no sea esta**). pass123
* El segundo usuario, **usuariobrut** tendrá una contraseña de tres caracteres (números y letras) y que deberá ser obtenida mediante un ataque por fuerza bruta (**por ejemplo pL5, pero que no sea esta**) rl2

1. Acceder mediante Metasploit a la máquina víctima, y conseguir abrir un shell remoto en dicho equipo.

A screenshot of a computer

Description automatically generated

1. Acceder a los ficheros donde están los usuarios y las contraseñas (SAM) y obtener los hashes

A screenshot of a computer screen

Description automatically generated



1. Descifrar dichos hashes (contraseñas) con John the Ripper.
   1. La contraseña del usuario usuariodic debe romperse con un ataque por diccionario. Para ello debéis descargar y usar el diccionario gratuito disponible en Openwall (<http://www.openwall.com/wordlists/>) o cualquier otro que descarguéis de Internet (en esta caso dar la referencia de donde lo habéis obtenido) Deberíais usar una contraseña que estuviera en este diccionario.

A close up of text on a black background

Description automatically generated

* 1. La contraseña del usuario usuariobrut debe descifrarse con un ataque de fuerza bruta

A screenshot of a cell phone

Description automatically generated

* 1. Ya que estamos dentro, intentar descifrar la contraseña de algún usuario que tenga permisos de administración.

A screenshot of a cell phone

Description automatically generated

Consultar el documento subido a Moodle donde se explica el uso de John the Ripper para los diferentes ataques

**Entregable: Pantallazos que muestren:**

1. **Ejecución con éxito del exploit de la guía. Insertar pantallazo**
2. **Demostrar que se está dentro ejecutando, una vez se ha lanzado el exploit, las órdenes:** 
   1. **date** (para ver el día y la fecha en la que se ha entrado)
   2. **whoami** (para ver con qué usuario he accedido a la máquina
   3. **pwd** (para ver en qué directorio de la máquina remota me encuentro)

**Insertar pantallazo**

1. **Obtención de las contraseñas mediante John the Ripper. Insertar pantallazo**

**INSTRUCCIONES**

* Entrega:
  + Un archivo **PDF** a partir de este documento de Word con las respuestas (las que están señaladas en rojo) y los pantallazos pedidos.
* Los ejercicios **SOLO** podrán realizarse en grupos de dos alumnos o tres alumnos como máximo. **No se permiten entregas de prácticas realizadas de forma individual o por grupos de más de tres alumnos.**

* El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
* **La fecha límite de entrega será el viernes 20 de marzo a las 23 horas (IMPRORROGABLE).**
* **No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.**