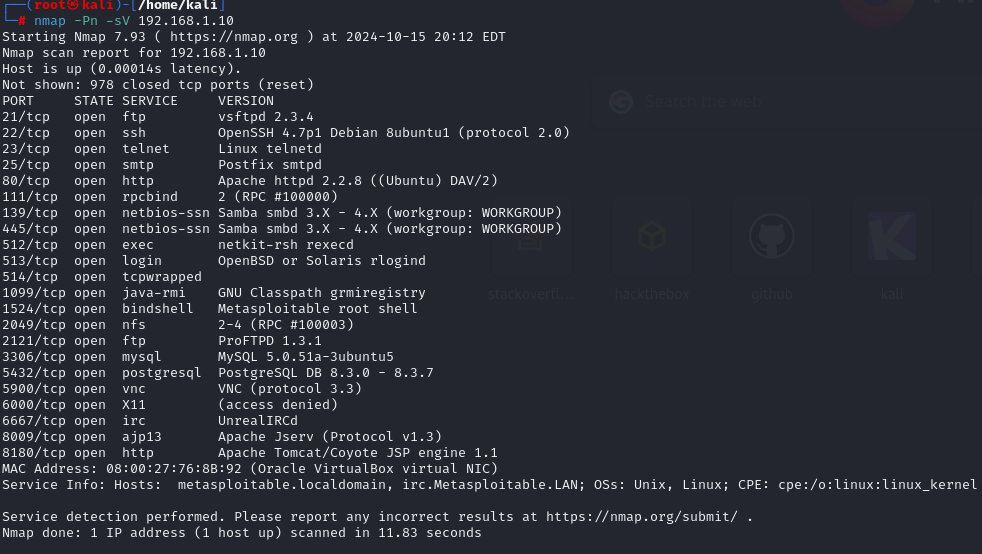
Metasploitable 2 Manual Vulnerability Assessment

# Port Scanning

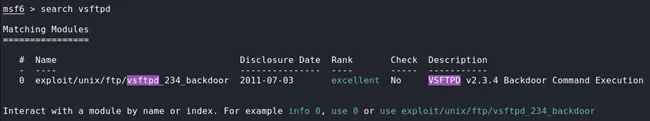


## Port 21 (FTP)

State: **Open**

Service: **FTP**

Version: **vsftpd 2.3.4**



Severity: Critical

Reason: Vulnerable to a backdoor exploit that allows unauthorized users to gain root access, especially with anonymous login enabled.

## Port 22 (SSH)

State: **Open**

Service: **SSH**

Version: **OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)**

**Severity: High**

**Reason:** Exposes sensitive information, and CVEs like CVE-2008-1657 allow bypassing security controls, compromising confidentiality and integrity.

**Other CVEs that could apply:**

* **CVE-2008–3844**: As signed in August 2008 with a valid Red Hat GPG key, some Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH contain an externally inserted change (Trojan Horse) that gives the package authors unexpected power.

**References:**

<https://nvd.nist.gov/vuln/detail/CVE-2008-3844>

<https://nvd.nist.gov/vuln/detail/CVE-2008-1657>

## Port 23 (Telnet)

State: **Open**

Service: **Telnet**

Version: **Linux telnetd**

**Severity: Critical**

**Reason:** Telnet transmits credentials in clear text, making it highly vulnerable to man-in-the-middle attacks and credential theft.

## Port 25 (SMTP)

State: **Open**

Service: **SMTP**

Version: **Postfix smtpd**

**Severity: High**

**Reason:** Weak authentication methods could allow attackers to send malicious emails or bypass security mechanisms like SPF.

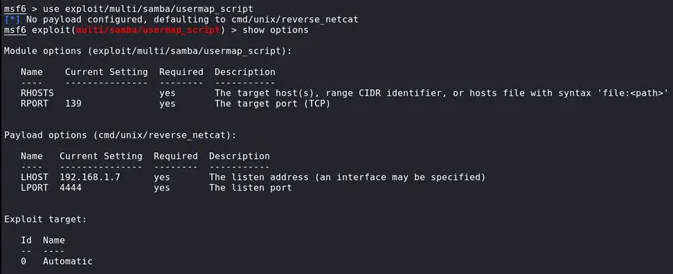
## Port 139 & 445 (Samba)

Samba is running on both port 139 and 445, we will be exploiting it using Metasploit. The default port for this exploit is set to port 139 but it can be changed to port 445 as well.

Severity: Critical

Reason: Vulnerable to remote code execution exploits using the "username map script" configuration option in Samba versions 3.X to 4.X

msf > use exploit/multi/samba/usermap\_script



## Port 5900 (VNC)

State: **Open**

Service: **VNC**

Version: **3.3**

**Severity: High**

**Reason:** Brute-force login attacks can gain unauthorized access due to weak or no credentials.

## Ports 512/513/514(Services « R »)

State: **Open**

Service: **Services « R »**

**Severity: High**

**Reason:** These "r" services are insecure, allowing unauthorized access if improperly configured, and they transmit data in clear text.

Type: rlogin -l root -p 513 192.168.1.10. The -l switch specifies the account to login as, the -p switch specifies the port, and 192.168.1.10 is the IP address of the remote system

TCP ports 512, 513 and 514 are known as "r" services which can allow an attacker to enter the system if they are incorrectly configured. RSH Remote Shell services (rsh, rexec, and rlogin) are active.

## Port 1524 (Netcat bindshell – Metasploitable root shell)

State: **Open**

Service: Netcat bindshell – Metasploitable root shell

**Severity: Critical**

**Reason:** A superuser shell is available, allowing full system control to attackers.

## Port 2049 (**NFS)**

State: **Open**

Service: NFS

**Severity: Critical**

**Reason:** No authentication is required to mount NFS shares, making it easy for attackers to perform sensitive actions and escalate privileges. Add our ssh key in the authorized keys. Log in as root.

## Port 6667 (**UnrealIRC Backdoor)**

State: **Open**

Service: **UnrealIRC Backdoor**

**Severity: Critical**

**Reason:** UnrealIRCd contains a backdoor that allows remote attackers to execute arbitrary commands, which is a severe security risk.

## Port 139/445 (**Samba smbd 3.X – 4.X)**

State: **Open**

Service: Samba smbd 3.X – 4.X

**Is it vulnerable?**

This flaw is related to a command execution vulnerability in Samba versions 3.0.20 to 3.0.25rc3 when using the "username map script" configuration option other than the default. Exploit present on Metasploit and log in as root.

## Port 1099 (**Java-rmi)**

State: **Open**

Service: **Java-rmi**

**Severity: High**

**Reason:** Default RMI registry configuration allows classes to be loaded from any remote URL, making it vulnerable to remote code execution.

## Port 3306 (**MYSQL)**

State: **Open**

Service: **MYSQL**

**Severity: Medium**

**Reason:** MySQL is installed with a default root password, allowing unauthorized database access.

## Port 5432 (**PostgreSQL DB 8.3.0 - 8.3.7)**

State: **Open**

Service: **PostgreSQL DB 8.3.0 - 8.3.7**

**Severity: Medium**

**Reason:** PostgreSQL uses a default password, leaving the database vulnerable to unauthorized access.

## Port 80 (**HTTP)**

State: **Open**

Service: **HTTP**

**Severity: Medium**

**Reason:** The presence of phpinfo.php exposes detailed information about the server environment, which can be exploited to gain shell access via a Metasploit exploit, which allows to get a shell as www-data.