# Comprehensive Vulnerability Analysis and Remediation on Metasploitable

Tawsif Chowdhury
Information Systems Security
Concordia University
Montreal, QC, Canada
tawsifulhye@gmail.com

## Executive Summary

This report documents the results of a vulnerability assessment conducted on a Metasploitable2 machine using OpenVAS and Nikto. The objective was to identify high-risk vulnerabilities and propose actionable remediation steps. The scan revealed several critical security flaws, including remote code execution vulnerabilities, backdoors, and misconfigurations in web services. Immediate remediation is recommended to prevent exploitation.

**Test Environment**: Kali Linux 2025.1(Scanner Host), Metasploitable2(Target Host).
**Tools Used**: Nmap, OpenVAS, Nikto.

## Network Reconnaissance

At first, we need to find out the network of the scanner host connected.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.77  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1dfd:e084:1d12:d927  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:67:29:8c  txqueuelen 1000  (Ethernet)
        RX packets 519618  bytes 765652680 (730.1 MiB)
        RX errors 0  dropped 52  overruns 0  frame 0
        TX packets 59303  bytes 12573931 (11.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.188.128  netmask 255.255.255.0  broadcast 192.168.188.255
        inet6 fe80::a7ed:2bd0:b86d:8640  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:67:29:96  txqueuelen 1000  (Ethernet)
        RX packets 177811  bytes 78944126 (75.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 168147  bytes 33851177 (32.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 53478  bytes 49363276 (47.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 53478  bytes 49363276 (47.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Use Nmap to discover open ports and services.

```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap 192.168.188.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-22 11:11 EDT
Nmap scan report for 192.168.188.128
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.188.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.188.129
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 256 IP addresses (2 hosts up) scanned in 19.52 seconds
```

From the scan, it can be found that Metasploitable has the IP address **192.168.188.129.** Now let's run another command to scan for versions of the open ports.

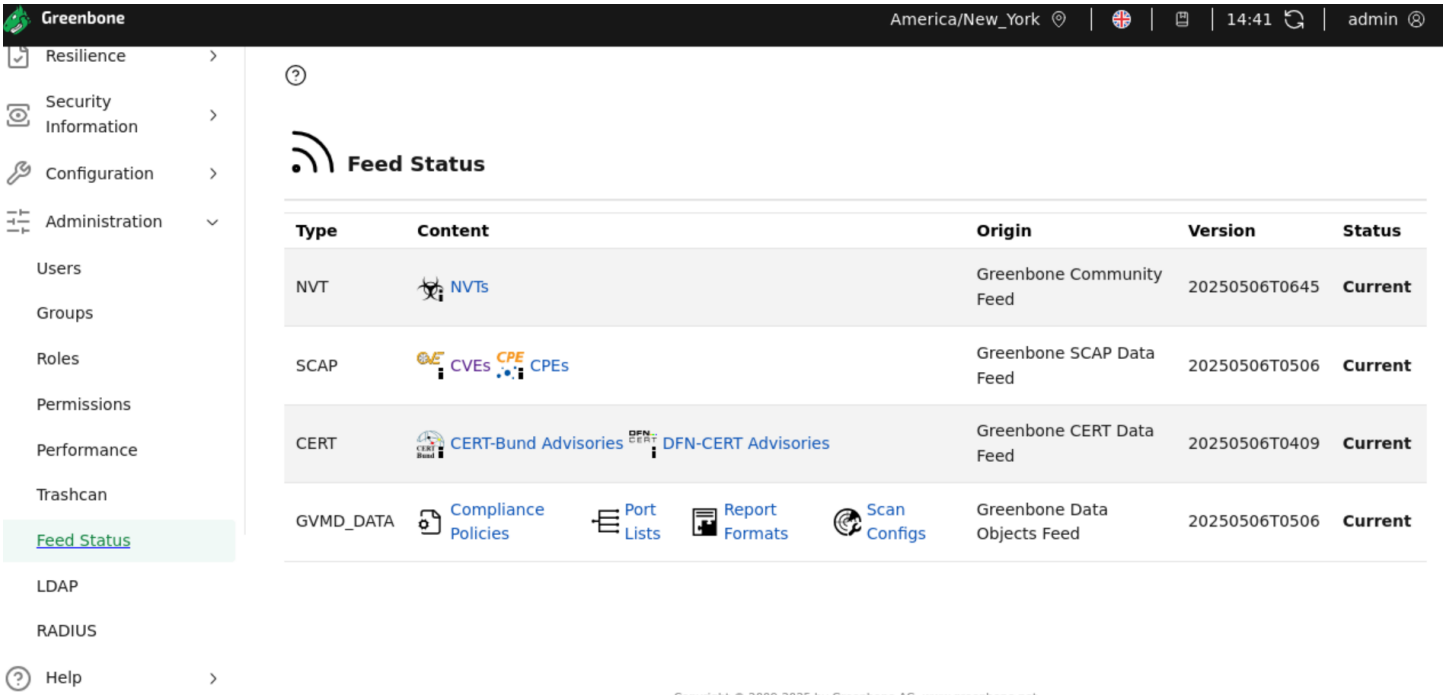
```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap -sV 192.168.188.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-22 11:14 EDT
Nmap scan report for 192.168.188.129
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.83 seconds
```

So from the output of the scan, it can be seen that the target system is vulnerable with several open ports. To get detailed overview

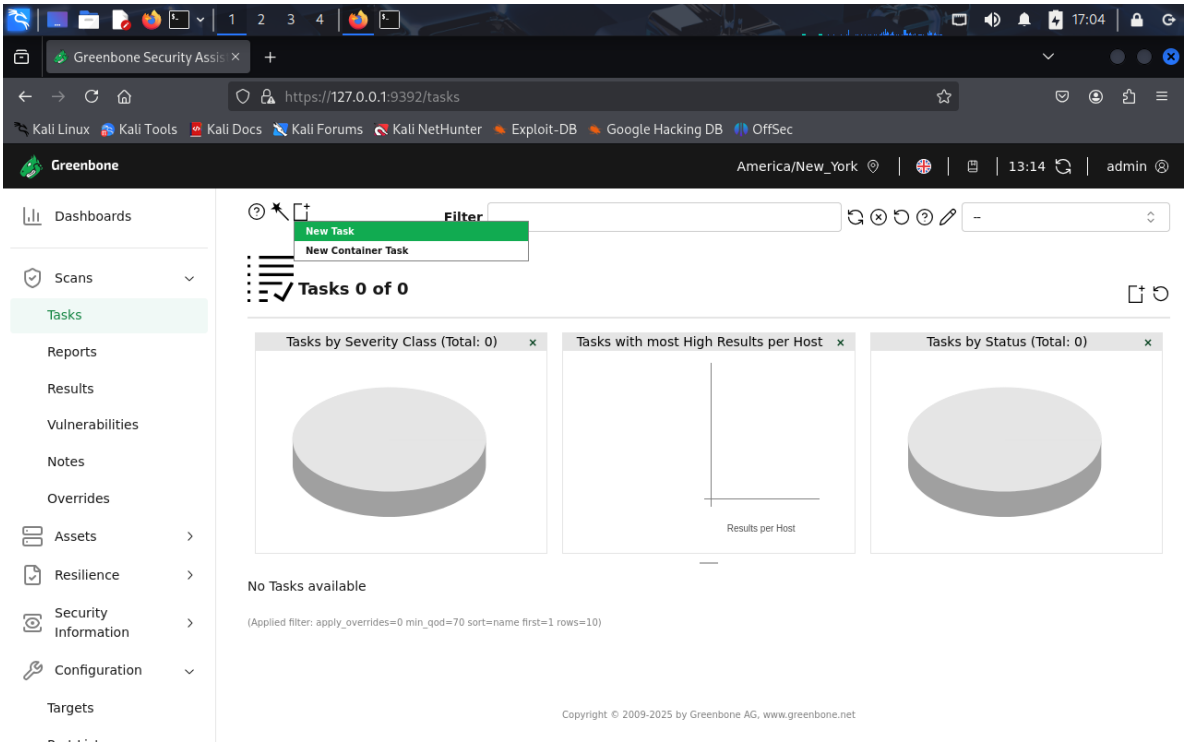
**OpenVAS Scan Workflow**

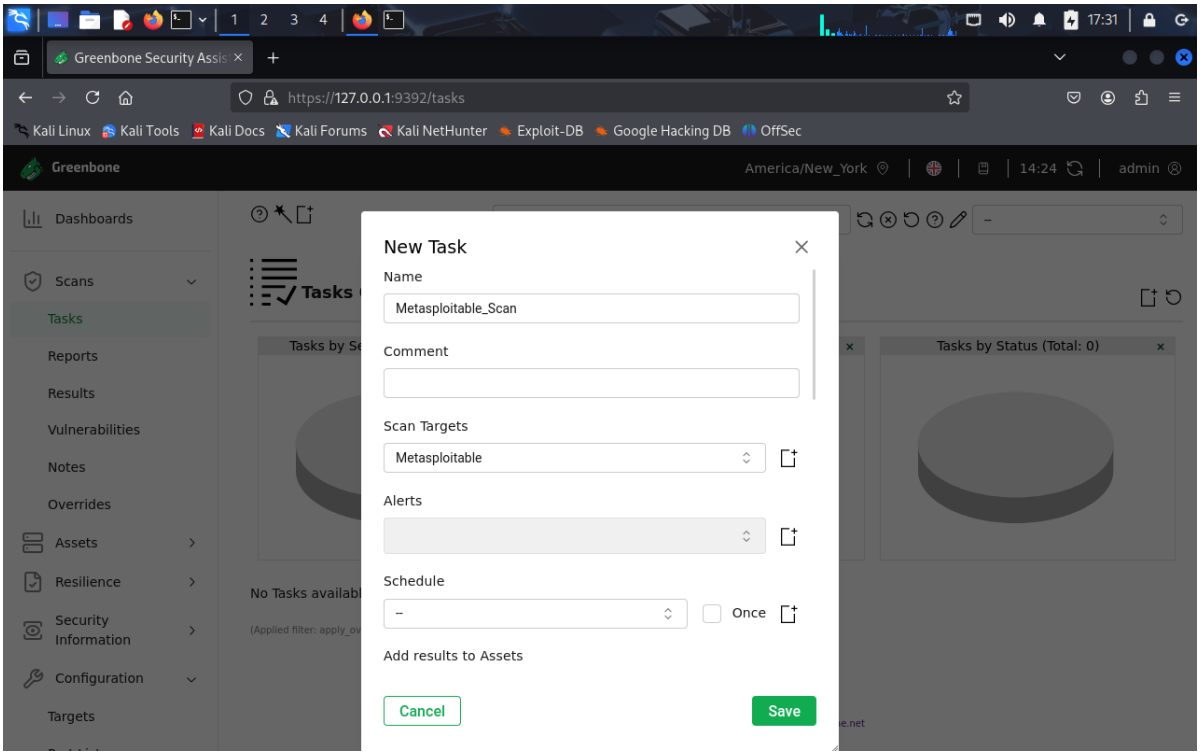
OpenVAS (Open Vulnerability Assessment System) is a powerful, free, and open-source framework used for scanning and assessing network vulnerabilities. It is part of the Greenbone Vulnerability Management (GVM) platform, which provides comprehensive solutions for identifying, classifying, and managing vulnerabilities in IT systems.

Before starting with OpenVAS, it is necessary to update the feed to. To update use the following command *sudo greenbone-feed-sync,* it takes time to update, by this time OpenVAS scan cannot be run. Run *sudo gvm-start* to start the OpenVAS in browser. To check update go to *Feed Status* under *Administration.* You can see all the status are current.

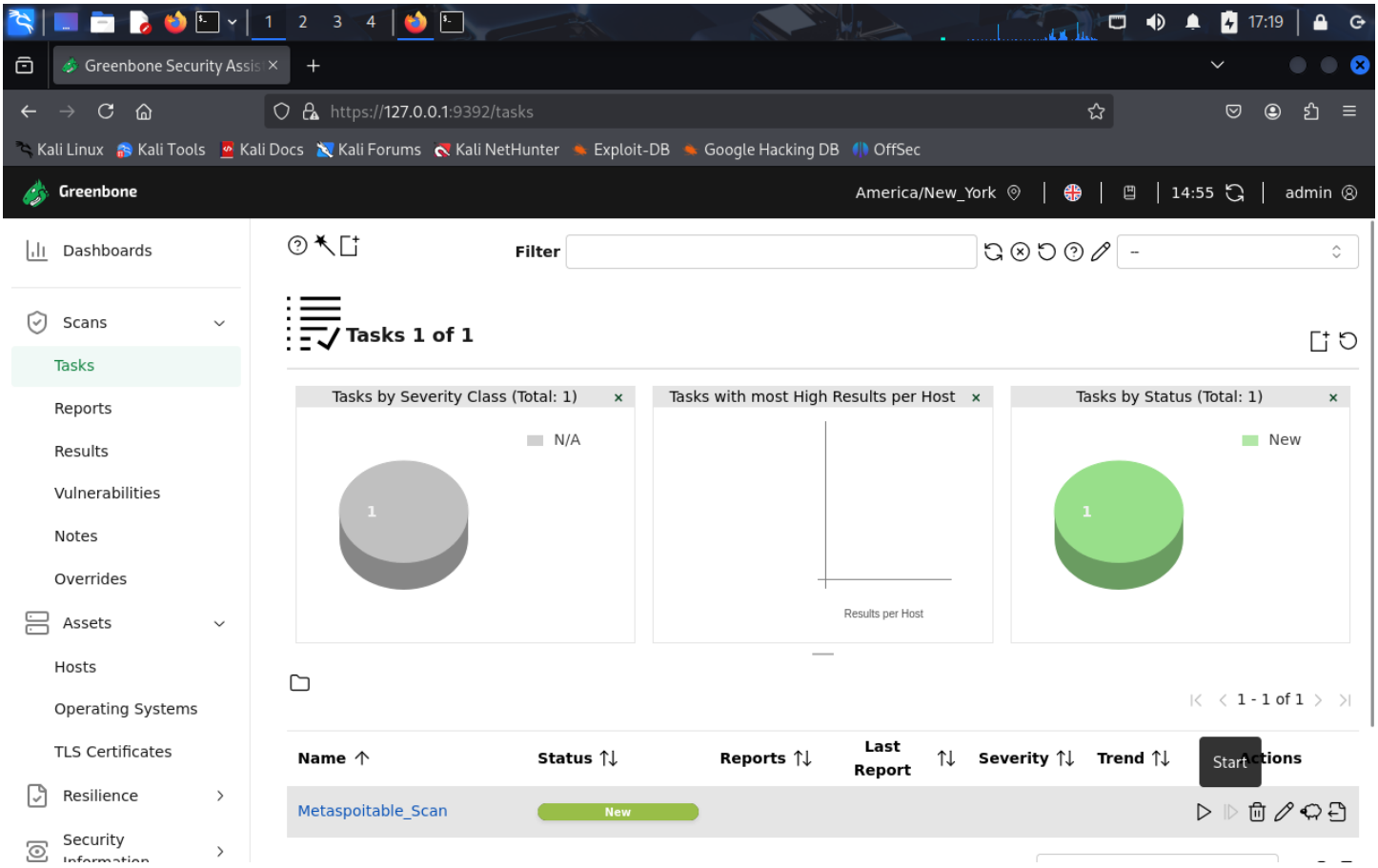



Now let's run the scan. First, we have to create a task following the attached workflow.

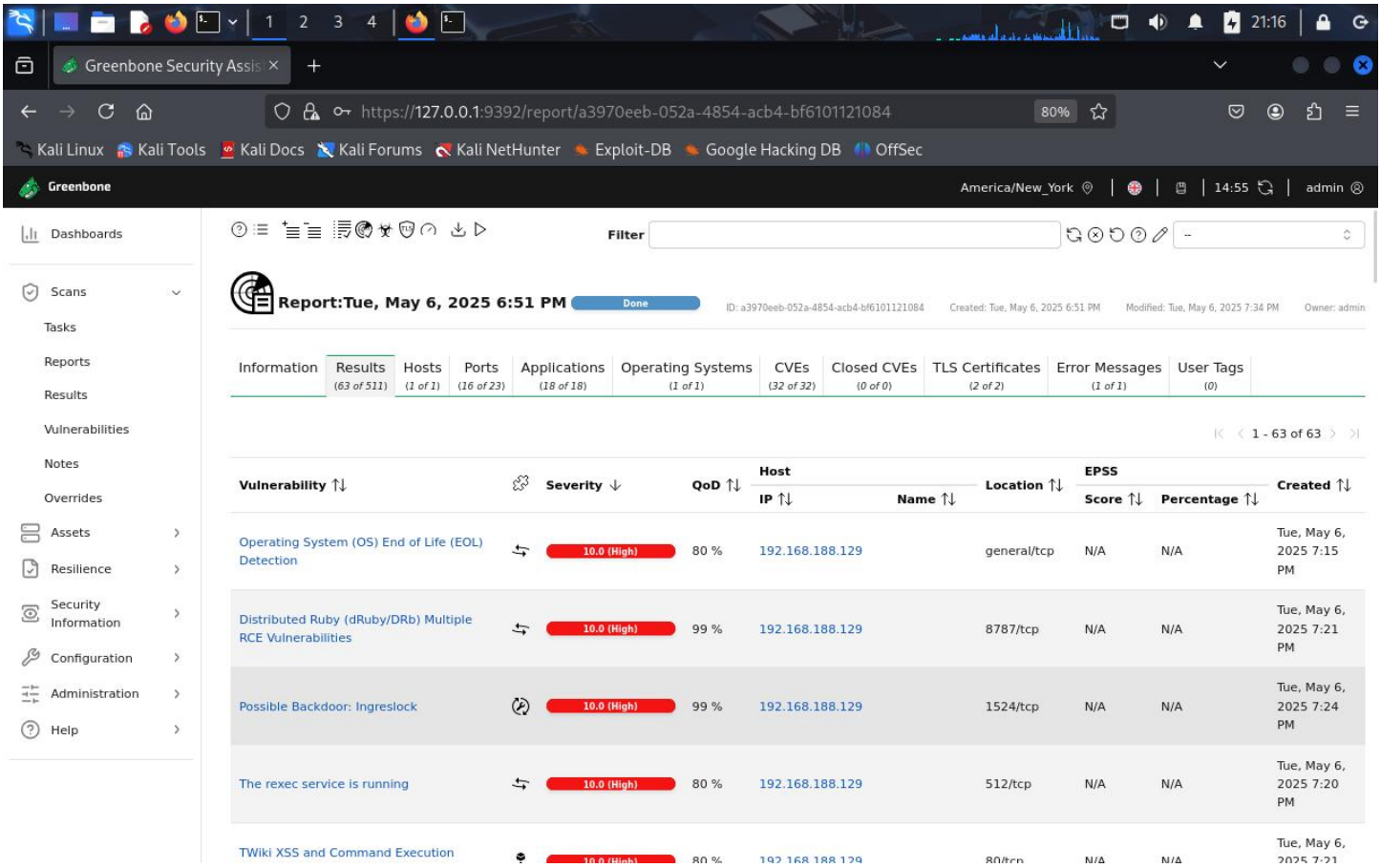





After adding the required configuration click on ‘Save’ to create a task. Click ‘Start’ button to start the scan.




After the scan is over the report shows the vulnerability found.




From the OpenVAS report, five high-severity vulnerabilities have been selected for analysis.

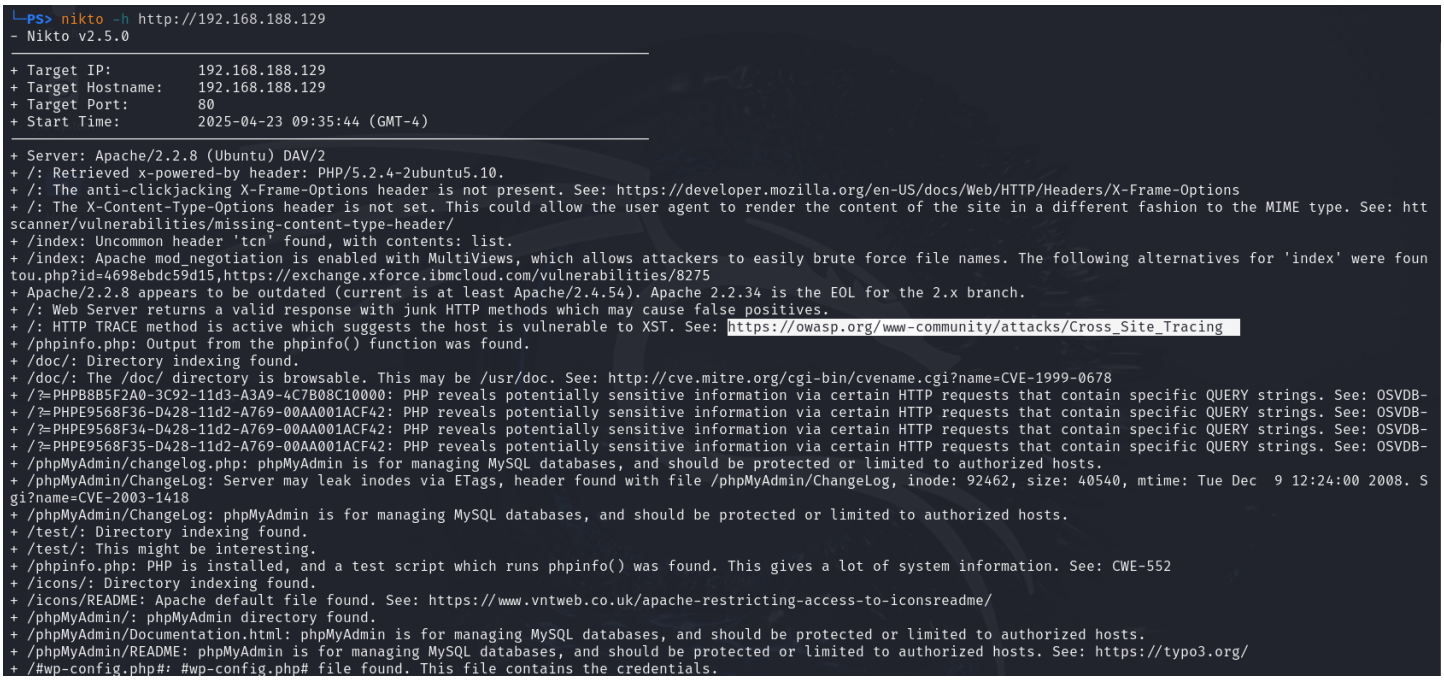
1. **vsftpd Compromised Source Packages Backdoor Vulnerability (CVE-2011-2523)**
    - **Severity:** High (CVSS 9.8).
    - **Description:** vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.
    - **Detection Tool:** OpenVAS (Scan Date: May 6, 2025).
    - **Evidence:** vsFTPd FTP Server Detection. OID: .3.6.1.4.1.25623.1.0.103185.
    - **Impact:** Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
    - **Remediation:**
        - Type: VendorFix.
        - The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
2. **DistCC RCE Vulnerability (CVE-2004-2687)**
    - **Severity:** High (CVSS 9.3)
    - **Description:** distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
    - **Detection Tool:** OpenVAS (Scan Date: May 6, 2025)
    - **Evidence:** Version used: 2022-07-07T10:16:06Z.
    - **Impact:** DistCC by default trusts its clients completely that in turn could allow a malicious client to
    - execute arbitrary commands on the server.
    - **Remediation:**
        - Type: VendorFix.

    - Restrict network access.
    - Configure distcc for greater security.

3. **Apache Tomcat AJP RCE Vulnerability (Ghostcat) (CVE-2020-1938)**
    - **Severity:** High (CVSS 9.5)
    - **Description:** Apache Tomcat is prone to a remote code execution (RCE) vulnerability (dubbed 'Ghostcat') in the AJP connector. Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.
    - **Detection Tool:** OpenVAS (Scan Date: May 6, 2025)
    - **Evidence:** It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
    - **Impact:** Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.
    - **Remediation:**
        - Type: VendorFix.
        - Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later.
4. **Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check (CVE-2011-3556)**
    - **Severity:** High (CVSS 7.5)
    - **Description:** Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code (remote code execution/RCE) on a targeted system with elevated privileges.
    - **Detection Tool:** OpenVAS (Scan Date: May 6, 2025)
    - **Evidence:** By doing an RMI request it was possible to trigger the vulnerability and make th e remote host sending a request back to the scanner host
    - **Impact:** An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.
    - **Remediation:**
        - Type: Workaround.
        - Disable class-loading.
5. **NVT: UnrealIRCd Authentication Spoofing Vulnerability (CVE-2016-7144)**
    - **Severity:** High (CVSS 8.1)
    - **Description:** UnrealIRCd is prone to authentication spoofing vulnerability.
    - **Detection Tool:** OpenVAS (Scan Date: May 6, 2025)
    - **Evidence:** The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
    - **Impact:** Successful exploitation of this vulnerability will allow remote attackers to spoof certificate fingerprints and consequently log in as another use.
    - **Remediation:**
        - Type: VendorFix.
        - Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

**Web Server Scanning Using Nikto**

Nikto is a free, open-source web server scanner that identifies vulnerabilities and misconfigurations on web servers. It's used to assess the security of websites and web applications by checking for dangerous files, outdated software, and other security risks.




Based on the Nikto scan results from your screenshot (http://192.168.188.129), here are the key findings:

| Issue | Description | CVE/Reference | Risk |
|---|---|---|---|
| Outdated Apache | Apache/2.2.8 is outdated | - | High |
| Missing Headers | Lacks X-Frame-Options, X-Content-Type-Options | OWASP | Medium |
| TRACE Method Enabled | Allows XST attacks | OWASP | Medium |
| Directory Indexing | /usr/doc exposed | CVE-1999-0678 | Medium |
| phpinfo.php | Full system disclosure | OSVDB-12184 | High |
| phpMyAdmin Directory | Accessible without auth | CVE-2003-1418 | High |

## Recommendations

1. **Apply all vendor-released patches** to close known CVEs.
2. **Restrict network services** such as FTP, RMI, and DistCC to internal, authenticated users.
3. **Harden Apache web server configuration**:
    - Disable TRACE.
    - Remove sensitive scripts (e.g., phpinfo.php).
    - Enforce security headers.
4. **Limit access to administrative directories** such as /phpMyAdmin/.

## Conclusion

This vulnerability assessment of the Metasploitable2 virtual machine demonstrates the importance of continuous security evaluation and prompt remediation. Utilizing tools such as OpenVAS and Nikto, several critical and high-severity vulnerabilities were uncovered, including remote code execution backdoors, misconfigured services, and web server weaknesses. If these vulnerabilities existed in a production environment, they would pose a significant threat to the confidentiality, integrity, and availability of systems and data.

To mitigate these risks, organizations should enforce strict network access controls, regularly update software, harden service configurations, and adopt a defense-in-depth approach. Timely patch management, combined with consistent vulnerability assessments, is essential to maintaining a strong security posture.