

# Setting up OpenVAS (on Kali Linux)

1. Update\* signature database

```
$ openvas-setup
```

## 2. Start OpenVAS

```
$ openvas-start
```

3. Change\* admin password

```
$ openvasmd --create-user=admin
```

```
$ openvasmd --new-password=admin --user=admin
```

## 4. Open the web interface

```
https://localhost:9392
```

\* already done in the kali vagrant box provided for hw2

# Report

Greenbone

Security Assistant

Logged in as Admin **admin** | Logout

Sun Oct 12 13:33:23 2014 UTC

Scan Management

Asset Management

SecInfo Management

Configuration

Extras

Administration

Help

▼ Report: Results

1 - 100 of 124 (total: 124)

PDF

Done

Filter: sort-reverse=severity result\_hosts\_only=1 min\_cvss\_base= levels=hmlg

Vulnerability	Severity	Host	Location	Actions
PHP version smaller than 5.2.7	10.0 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	
PHP version smaller than 5.2.6	10.0 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	
NFS export	10.0 (High)	10.0.1.101 (METASPLOITABLE )	2049/udp	
X Server	10.0 (High)	10.0.1.101 (METASPLOITABLE )	6000/tcp	
PHP version smaller than 5.2.14	9.3 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	
PHP version smaller than 5.2.5	9.3 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	
PHP version smaller than 5.3.3	9.3 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	
MySQL 5.x Unspecified Buffer Overflow Vulnerability	9.3 (High)	10.0.1.101 (METASPLOITABLE )	3306/tcp	
distcc Remote Code Execution Vulnerability	9.3 (High)	10.0.1.101 (METASPLOITABLE )	3632/tcp	
SSH Brute Force Logins with default Credentials	9.0 (High)	10.0.1.101 (METASPLOITABLE )	22/tcp	
MySQL weak password	9.0 (High)	10.0.1.101 (METASPLOITABLE )	3306/tcp	
PostgreSQL weak password	9.0 (High)	10.0.1.101 (METASPLOITABLE )	5432/tcp	
MySQL 'sql_parse.cc' Multiple Format String Vulnerabilities	8.5 (High)	10.0.1.101 (METASPLOITABLE )	3306/tcp	
DistCC Detection	8.5 (High)	10.0.1.101 (METASPLOITABLE )	3632/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	10.0.1.101 (METASPLOITABLE )	5432/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	10.0.1.101 (METASPLOITABLE )	21/tcp	
ProFTPD Server SQL Injection Vulnerability	7.5 (High)	10.0.1.101 (METASPLOITABLE )	21/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	10.0.1.101 (METASPLOITABLE )	80/tcp	