


Using OpenVAS to discover vulnerabilities








 **Greenbone**
Security Assistant

Logged in as Admin **admin** | Logout
Sun Oct 12 13:17:19 2014 UTC

Scan ManagementAsset ManagementSecInfo ManagementConfigurationExtrasAdministrationHelp

Tasks 1 - 1 of 1 (total: 1) ✓Refresh every 10 Sec.

Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=nam

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 10.0.1.101	<div><div></div>56%</div>	0 (1)				      

(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name)

1 - 1 of 1 (total: 1)

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