# scanme.nmap.org Website

Report generated by Nessus™ Tue, 22 Aug 2023 11:44:39 EDT

TABLE OF CONTENTS

## Vulnerabilities by Host

# Vulnerabilities by Host

# 45.33.32.156

| 0 | 0 | 1 | 0 | 12 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

## Host Information

| | |
|---|---|
| DNS Name: | scanme.nmap.org |
| IP: | 45.33.32.156 |
| OS: | Linux Kernel 3.13 on Ubuntu 14.04 (trusty) |

## Vulnerabilities

### 40984 - Browsable Web Directories

#### Synopsis

Some directories on the remote web server are browsable.

#### Description

Multiple Nessus plugins identified directories on the web server that are browsable.

#### See Also

http://www.nessus.org/u?0a35179e

#### Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

#### Risk Factor

Medium

#### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

#### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

## Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

## Plugin Output

tcp/80

```
The following directories are browsable :

http://scanme.nmap.org/images/
```

## 18261 - Apache Banner Linux Distribution Disclosure

### Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

### Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

### Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

### Risk Factor

None

### Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

### Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 14.04 (trusty)
```

## 48204 - Apache HTTP Server Version

### Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

### Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

### See Also

https://httpd.apache.org/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0030 |
| XREF | IAVT:0001-T-0530 |

### Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

### Plugin Output

tcp/80

```
URL        : http://scanme.nmap.org/
Version    : 2.4.99
Source     : Server: Apache/2.4.7 (Ubuntu)
backported : 1
os         : ConvertedUbuntu
```

## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/80

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution (time based) : S=6          SP=6         AP=6         SC=6         AC=6

format string                            : S=2          SP=2         AP=2         SC=2         AC=2

cross-site scripting (comprehensive test): S=4          SP=4         AP=4         SC=4         AC=4

injectable parameter                     : S=2          SP=2         AP=2         SC=2         AC=2

arbitrary command execution              : S=16         SP=16        AP=16        SC=16        AC=16

local file inclusion                     : S=1          SP=1         AP=1         SC=1         AC=1

directory traversal                      : S=25         SP=25        AP=25        SC=25        AC=25

web code injection                       : S=1          SP=1         AP=1         SC=1         AC=1

blind SQL injection (4 requests)         : S=4          SP=4         AP=4         SC=4         AC=4
```

```
persistent XSS                          : S=4          SP=4          AP=4          SC=4          AC=4
directory traversal (write access)      : S=2          SP=2          AP=2          SC=2          AC=2
XML injection                           : S=1          SP=1          AP=1          SC=1          AC=1
blind SQL injection                     : S=12         SP=12         AP=12         SC=12         AC=12
SQL injection                           : S=24         SP=24         AP=24         SC=24         AC=24
directory traversal (extended test)     : S=51         SP=51         AP=51         SC=51         AC=51
SSI injection                           : S=3          SP=3          AP=3          SC=3          AC=3
unseen parameters                       : S=35         SP=35         AP=35         SC=35         AC=35
SQL injection (2nd order)              [...]
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/80

```
35 external URLs were gathered on this web server :
URL...                                  - Seen on...


https://facebook.com/nmap               - /
https://github.com/nmap/                - /
https://insecure.org/                   - /
https://insecure.org/advertising.html   - /
https://insecure.org/fyodor             - /
https://insecure.org/fyodor/            - /
https://insecure.org/privacy.html       - /
https://nmap.org                        - /
https://nmap.org/                       - /
https://nmap.org/book/install.html      - /
https://nmap.org/book/man.html          - /
https://nmap.org/docs.html              - /
https://nmap.org/download.html          - /
https://nmap.org/npsl/                  - /
https://nmap.org/oem/                   - /
https://npcap.com/                      - /
https://npcap.com/#download             - /
https://npcap.com/guide/                - /
https://npcap.com/guide/npcap-devguide.html#npcap-api - /
https://npcap.com/oem/                  - /
https://reddit.com/r/nmap/              - /
https://seclists.org/                   - /
https://seclists.org/dataloss/          - /
https://seclists.org/fulldisclosure/    - /
https://seclists.org/nmap-announce/     - /
https://seclists.org/nmap-dev/          - /
https://seclists.org/oss-sec/           - /
```

```
https://sectools.org                    - /
https://sectools.org/tag/pass-audit/    - /
https://sectools.org/tag/sploits/       - /
https://sectools.org/tag/vuln-scanners/ - /
https://sectools.org/tag/web-scanners/  - /
https://sectools.org/tag/wireless/      - /
https://twitter.com/nmap                - /
https://www.google-analytics.com/analytics.js - /
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /icons
    /images
    /shared
    /shared/css
    /shared/images


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /icons
    /images
    /shared
    /shared/css
    /shared/images
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/80

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

### Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 22 Aug 2023 15:36:27 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Accept-Ranges: bytes
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
<title>Go ahead and ScanMe!</title>
<meta name="viewport" content="width=device-width,initial-scale=1">
<meta name="theme-color" content="#2A0D45">
<link rel="preload" as="image" href="/images/sitelogo.png" imagesizes="168px" imagesrcset="/images/
sitelogo.png, /images/sitelogo-2x.png 2x">
```

```
<link rel="preload" as="image" href="/shared/images/nst-icons.svg">
<link rel="stylesheet" href="/shared/css/nst.css?v=2">
<script async src="/shared/js/nst.js?v=2"></script>
<link rel="stylesheet" href="/shared/css/nst-foot.css?v=2" media="print" onload="this.media='all'">
<link rel="stylesheet" href="/site.css">
<!--Google Analytics Code-->
<link rel="preload" href="https://www.google-analytics.com/analytics.js" as="script">
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','//www.google-analytics.com/analytics.js','ga');
ga('create', 'UA-11009417-1', 'auto');
ga('send', 'pageview');
</script>
<!--END Google Analytics Code-->
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
<link rel="shortcut icon" href="/shared/images/tiny-eyeicon.png" type="image/png">
</head>
<body><div id="nst-wrapper">

<div id="menu">
 <div class="blur">
  <header id="nst-head">

    <a id="menu-open" href="#menu" aria-label="Open menu">
     <img width="44" height="44" alt="" aria-hidden="true"
      src="/shared/images/nst-icons.svg#menu">
    </a>
    <a id="menu-close" href="#" aria-label="Close menu">
     <img width="44 [...]
```

## 11219 - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

### Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

## 11219 - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

### Plugin Output

tcp/80

```
Port 80/tcp was found to be open
```

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202308211809
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : scanme.nmap.org Website
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 302.716 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/22 11:17 EDT
Scan duration : 1601 sec
Scan for malware : no
```

## 11032 - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

### See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

### Solution

n/a

### Risk Factor

None

### References

XREF OWASP:OWASP-CM-006

### Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

### Plugin Output

tcp/80

```
The following directories were discovered:
/icons, /images, /shared

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

## 10662 - Web mirroring

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2023/07/17

### Plugin Output

tcp/80

```
Webmirror performed 18 queries in 16s (1.0125 queries per second)

The following CGIs have been discovered :


+ CGI : /search/
  Methods : GET
  Argument : q

Directory index found at /images/
```