Nessus Report

Nessus Scan Report

Tue, 13 Oct 2015 14:07:45 GMT-0500

Table Of Contents

Vulnerabilities By Host

192.168.1.254

Scan Information

Start time:	Tue Oct 13 14:08:01 2015
End time:	Tue Oct 13 14:19:22 2015

Host Information

IP:	192.168.1.254
OS:	Dell iDRAC Controller, KYOCERA Printer, Linux Kernel 2.6, Net Optics Switch (Director)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	2	1	12	15

Results Details

22/tcp

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:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/22

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

80/tcp

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header in all content responses. This could potentially expose the site to a clickjacking or UI Redress attack wherein an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.
Note that while the X-Frame-Options response header is not the only mitigation for clickjacking, it is currently the most reliable method to detect through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?1bced8d9

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

http://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF CWE:693

Plugin Information:

Publication date: 2015/08/22, Modification date: 2015/08/28

Ports

tcp/80

```
The following pages do not use an X-Frame-Options response header :

  - http://192.168.1.254/login.cgi
  - http://192.168.1.254/
```

33821 - .svn/entries Disclosed via Web Server

Synopsis

The remote web server discloses information due to a configuration weakness.

Description

The web server on the remote host allows read access to '.svn/entries'
files. This exposes all file names in your svn module on your website. This flaw can also be used to download the source code of the scripts (PHP, JSP, etc...) hosted on the remote server.

See Also

http://www.nessus.org/u?4cdb772a

Solution

Configure permissions for the affected web server to deny access to the '.svn' directory.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2008/08/05, Modification date: 2015/09/24

Ports

tcp/80

```
Nessus was able to retrieve the contents of '.svn/entries' using the
following URL :

  http://192.168.1.254/img/.svn/entries
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2007/09/28, Modification date: 2015/06/23

Ports

tcp/80

```
Page : /
Destination Page: /login.cgi

Page : /login.cgi
Destination Page: /login.cgi
```

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:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/80

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

11239 - Web Server Crafted Request Vendor/Version Information Disclosure

Synopsis

The remote host is running a web server that may be leaking information.

Description

The web server running on the remote host appears to be hiding its version or name, which is a good thing. However, using a specially crafted request, Nessus was able to discover the information.

Solution

No generic solution is known. Contact your vendor for a fix or a workaround.

Risk Factor

None

Plugin Information:

Publication date: 2003/02/19, Modification date: 2015/09/24

Ports

tcp/80

```
After sending this request :
HELP


Nessus was able to gather the following information from the web server :
thttpd/2.25b
```

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/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2013/04/02

Ports

tcp/80

```
The following directories were discovered:
/css, /html, /img, /js

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:

Publication date: 2001/05/04, Modification date: 2015/08/22

Ports
tcp/80

```
Webmirror performed 14 queries in 1s (14.000 queries per second)

The following CGIs have been discovered :


+ CGI : /login.cgi
  Methods : POST
  Argument : name
   Value: TELMEX
  Argument : pswd
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Ports
tcp/80

```
Page : /
Destination Page: /login.cgi

Page : /login.cgi
Destination Page: /login.cgi
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.
Note that this plugin detects all general cookies missing the 'secure'
cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2015/08/24, Modification date: 2015/08/24

Ports

tcp/80

```
The following cookie does not set the secure cookie flag :

Name : lang
Path : /
Value : spa
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it. Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

https://www.owasp.org/index.php/HttpOnly

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442

XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Publication date: 2015/08/24, Modification date: 2015/08/24

Ports

tcp/80

```
The following cookie does not set the HttpOnly cookie flag :

Name : lang
Path : /
Value : spa
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

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

Plugin Information:

Publication date: 2000/01/04, Modification date: 2014/08/01

Ports
tcp/80

```
The remote web server type is :

thttpd/2.25b 29dec2003
```

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.
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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports
tcp/80

```
Based on tests of each method :

  - HTTP methods GET HEAD POST are allowed on :

    /
    /css
    /html
    /img
    /js
```

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:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports
tcp/80

```
Protocol version : HTTP/1.0
SSL : no
```

```
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  enter update_user_session
  before get LOID
  after get LOID
  Content-type:text/html; charset=UTF-8
  Cache-Control:private,max-age=0;
  Set-Cookie: lang=spa; path=/;
```

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:

Publication date: 2009/10/26, Modification date: 2014/03/12

Ports

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]

format string                           : S=4          SP=6         AP=6         SC=6
 AC=6
arbitrary command execution (time based) : S=12         SP=18        AP=18        SC=18
 AC=18
cross-site scripting (comprehensive test): S=8          SP=12        AP=12        SC=12
 AC=12
injectable parameter                    : S=4          SP=6         AP=6         SC=6
 AC=6
directory traversal                     : S=50         SP=75        AP=75        SC=75
 AC=75
local file inclusion                    : S=2          SP=3         AP=3         SC=3
 AC=3
arbitrary command execution             : S=32         SP=48        AP=48        SC=48
 AC=48
web code injection                      : S=2          SP=3         AP=3         SC=3
 AC=3
blind SQL injection (4 requests)        : S=8          SP=12        AP=12        SC=12
 AC=12
directory traversal (write access)      : S=4          SP=6         AP=6         SC=6
 AC=6
persistent XSS                          : S=8          SP=12        AP=12        SC=12
 AC=12
XML injection                           : S=2          SP=3         AP=3         SC=3
 AC=3
blind SQL injection                     : S=24         SP=36        AP=36        SC=36
 AC=36
directory traversal (extended test)     : S=102        SP=153       AP=153       SC=153
 AC=153
SQL injection (2nd order)               : S=2          SP=3         AP=3         SC=3
 AC=3
SSI injection                           : S=6          SP=9         AP=9         SC=9
 AC=9
SQL injection                           : S=48         SP=72        AP=72        SC=72
 AC=72
```

```
unseen parameters                       [...]
```