

Forum:[Hack Forums](#)

Thread: [How to fix these security vulnerability?](#)

N00b_n00b - July 18, 2020, 10:36 am

Hello,

I scanned my server with Greenbone and it showed me below vulnerabilities:

[Image 1](#)

[Image 2](#)

What is my server problem and how can I fix it?

Thank you.

CyberStrike - July 18, 2020, 12:12 pm

The "Log" appears that those services are leaking the service and version number, you can edit the source code and recompile services to show anything. Also you should be protecting (make the folders) when indexing of the site, you probably also want to deny access if someone say just puts in the URI. Search on Google for each of these, OpenVAS should have remediation steps or recommendations for you there, but search each vulnerability. Also search each product/service you are using and how to prevent it from disclosing version's, plugins all that jazz.

<http://www.securityspace.com/smysecure/catdescr.html?cat=Web+application+abuses>

N00b_n00b - July 22, 2020, 9:57 am

(Jul 18, 2020 12:12 PM)CyberStrike Wrote: [\[CITE\]](#) The "Log" appears that those services are leaking the service and version number, you can edit the source code and recompile services to show anything. Also you should be protecting (make the folders) when indexing of the site, you probably also want to deny access if someone say just puts in the URI. Search on Google for each of these, OpenVAS should have remediation steps or recommendations for you there, but search each vulnerability. Also search each product/service you are using and how to prevent it from disclosing version's, plugins all that jazz.

<http://www.securityspace.com/smysecure/catdescr.html?cat=Web+application+abuses>Edit the source code for what? I installed services by "yum" command and not from source code!!!

VolcanHacking - July 22, 2020, 10:30 am

(Jul 22, 2020 09:57 AM)N00b_n00b Wrote: [\[CITE\]](#) Edit the source code for what? I installed services by "yum" command and not from source code!!!

SSH weak algorithms supported : this need to be disabled and you are fine just disable "arcfour,arcfour128,arcfour256"

unprotected web app installers (http): i need more information from your scanner but most likely you need to disable directory listing in a browser

Untrusted certificate authorite :

Install an intermediate certificate on your web server.

Generate a new Certificate Signing Request. Upgrade to a dedicated IP address.

Get a wildcard SSL certificate. Change all URLS to HTTPS.

Renew your SSL certificate

N00b_n00b - July 23, 2020, 1:17 am

(Jul 22, 2020 10:30 AM)VolcanHacking Wrote: [\[CITE\]](#) SSH weak algorithms supported : this need to be disabled and you are fine just disable "arcfour,arcfour128,arcfour256"

unprotected web app installers (http): i need more information from your scanner but most likely you need to disable directory listing in a browser

Untrusted certificate authorite :

Install an intermediate certificate on your web server.

Generate a new Certificate Signing Request. Upgrade to a dedicated IP address.

Get a wildcard SSL certificate. Change all URLS to HTTPS.

Renew your SSL certificateHow can I disable "arcfour,arcfour128,arcfour256" ?

The directory listing is not disabled by default in Apache config file?

How can I "Install an intermediate certificate on your web server" , "Generate a new Certificate Signing Request" and "Get a wildcard SSL certificate" ?

VolcanHacking - July 23, 2020, 1:38 am

(Jul 23, 2020 01:17 AM)N00b_n00b Wrote: [\[CITE\]](#) How can I disable "arcfour,arcfour128,arcfour256" ?

The directory listing is not disabled by default in Apache config file?

How can I "Install an intermediate certificate on your web server" , "Generate a new Certificate Signing Request" and "Get a wildcard SSL certificate" ?

i give you the key and you should use google to help you with that if you want to hire me or anyone to do this work for you just say it

N00b_n00b - August 1, 2020, 6:52 am

(Jul 23, 2020 01:38 AM)VolcanHacking Wrote: [\[CITE\]](#) i give you the key and you should use google to help you with that if you want to hire me or anyone to do this work for you just say it

Thank you.

Can you see anything wrong in my Apache config?

Code \$ sudo cat /etc/httpd/conf/httpd.conf

least PidFile.

#

ServerRoot "/etc/httpd"

#Listen 12.34.56.78:80

Listen 80

Example:

LoadModule foo_module modules/mod_foo.so

#

Include conf.modules.d/*.conf

#

User apache

Group apache

#

ServerAdmin root@localhost

#

```
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
```

AllowOverride None

```
#
# Controls who can get stuff from this server.
#
Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>
```

```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
```

```
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn
```

```
<IfModule log_config_module>
#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common

<IfModule logio_module>
# You need to enable mod_logio.c to use %l and %O
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %l %O" combinedio
</IfModule>
```

```
#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog "logs/access_log" common

#
# If you prefer a logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
#
CustomLog "logs/access_log" combined
</IfModule>

<IfModule alias_module>
    ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"

</IfModule>

<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>

<IfModule mime_module>
    TypesConfig /etc/mime.types

    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
    AddType text/html .shtml
    AddOutputFilter INCLUDES .shtml
</IfModule>

#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default. To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8

<IfModule mime_magic_module>
#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
MIMEMagicFile conf/magic
</IfModule>
```

```
#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
```

```
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on
```

```
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
```

```
#Security
TraceEnable off
ServerSignature Off
ServerTokens Prod
SSLProtocol -ALL +TLSv1.2
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
TimeOut 60
```

```
# Modules
LoadModule reqtimeout_module modules/mod_reqtimeout.so
RequestReadTimeout header=10-30,MinRate=500
```

Elijah - August 1, 2020, 7:07 am

try re-installing the services and might fix this.

N00b_n00b - August 4, 2020, 9:03 am

(Aug 1, 2020 07:07 AM)Elijah Wrote: [\[CITE\]](#) try re-installing the services and might fix this.
Reinstalling the services!?