

Analysis Date	Monday - May 02, 2011
Type of Analysis	Full Report - report1
Overall Security Posture	Poor (100%)
Threats Discovered	46 (Risk: 5=2, 4=5, 3=6, 2=0, 1=33)
Total Hosts Scanned	1 (1 risk level 3, 4, 5)
Scan Date(s)	- Monday - May 02, 2011
Scanners Used	- EXTERNAL (165.212.169.136, 165.212.169.135, 165.212.169.200, 140.99.20.86, 140.99.20.85)
Scan Options Used	<ul style="list-style-type: none">- Port Scan: 1,000 most common using syn packets- Scan Speed: Medium- Safe Tests Only- Paranoid Threat Reporting- Scan Dead Hosts- Tools: Nessus, Nikto- Scan Depth: Heavy

Executive Summary

This document provides the results of the vulnerability assessment performed by gpremp S.A. de C.v. for gpremp S.A. de C.V.. The information contained within this document is considered extremely confidential and should be treated as such.

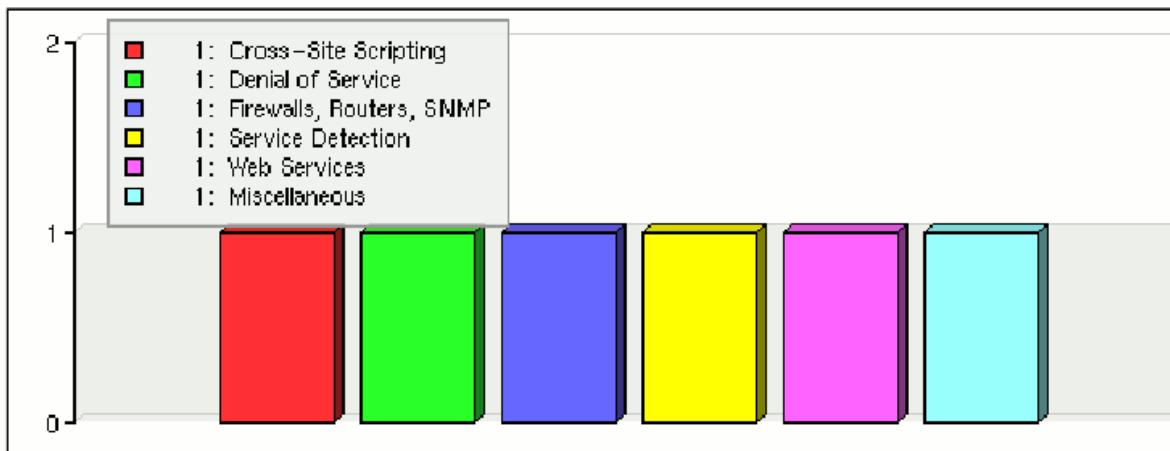
The scope of this analysis was to remotely audit and analyze the system and/or resources of each host in this assessment. This provides a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack.

Risk 5	2	4.35%
Risk 4	5	10.87%
Risk 3	6	13.04%
Risk 2	0	0.00%
Risk 1	33	71.74%

The pie chart to the right represents the number of vulnerabilities detected during the scan, categorized by level of risk. This analysis scanned 1 total IP addresses. Of those, 1 hosts were found with outstanding vulnerabilities. Risk factor definitions are included at the end of the this report.



The chart below shows how the potential security threats are spread across different families of threat classifications. The number of hosts with a vulnerability in that threat family is shown.



Number of Hosts vs. Threat Family Classifications






The graph below represents the seriousness of the security threats found during the assessment. The higher the percentage, the higher the priority should be for resolving the discovered security threats.



Scope of Assessment

All of the hosts part of this assessment are listed in this section. 0 hosts were not scanned because they were inactive and the Ignore Dead Hosts option was set. 0 hosts were scanned but not selected for inclusion in this report. 1 hosts are listed in the table below along with some information to help determine if there were any issues during the scan that may have affected the results.

Of note are the Scan Time, Packet Loss, and Flags. The flags are described in the legend below. A non-zero packet loss is a sign that there was some kind of congestion between the scanner and that host. 100% packet loss usually means the host was not active, heavily firewalled to not allow any incoming traffic, or blacklisted by an Intrusion Prevention System (IPS). The scans are configured to not be stealthy intentionally. Scan times can vary considerably. The primary factor affecting how long a scan takes is the network between the scanner and target, specifically latency and packet filtering. The scan times are shown in hours and minutes (HH:MM). A legend for the various flags used is provided below:

Flag	Description
	Is Latest: This flag indicates that the scan results being viewed for the host are the most recent.
	Is Dead or Blacklisted: This flag is set when it looks like the host was already dead or died during the scan. For hosts returning no open ports or vulnerabilities, a stealthy probe will be performed to determine if the scanner appeared to have been blacklisted.
	Timed Out: Abnormally long-running scans will be aborted automatically. If the port scan or any of the vulnerability-finding tools times out, then those long-running processes will be aborted and the scan will be flagged as timed out. Partial results will still be reported, but the completeness of the results cannot be guaranteed.
	Unusual Number of Open Ports: Some targets will show an obnoxious amount of ports as open, probably intentionally as a protection against port scanning. When 200 or more ports are returned as open, all port scan results will be automatically removed.
	Is Current Baseline: Any previous scan can be defined as the baseline to use in the differential analysis. If a baseline has not been explicitly set, then the next latest scan will be used automatically.

SCANNER: EXTERNAL

Host and Operating System	Risk	Scan Time	Packet Loss	Flags
www.domain.com (127.0.0.1)	5	00:39	0%	

Vulnerable Hosts

This analysis scanned 1 total IP addresses. Of those, 1 host was found active with outstanding vulnerabilities or open ports. The following table provides a brief summary about each of these active hosts and their analysis data.

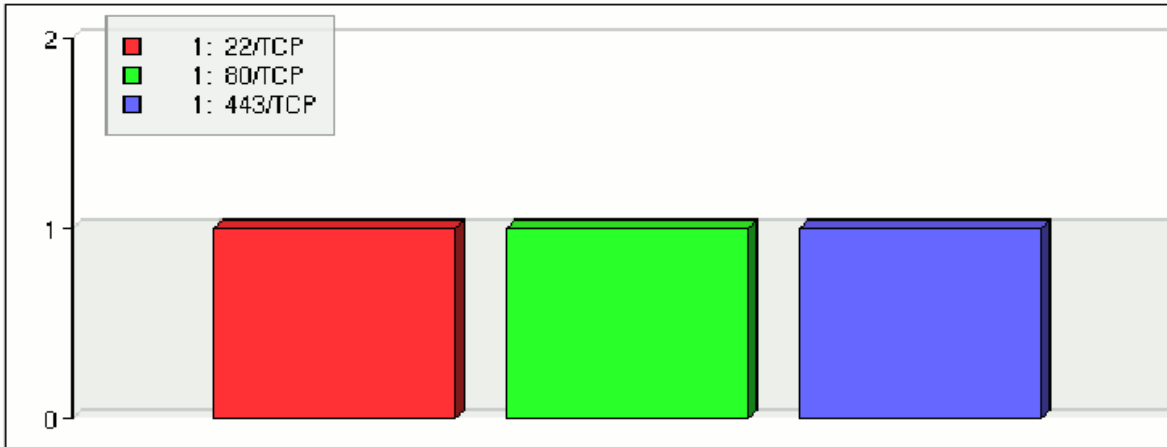
SCANNER: EXTERNAL

Host	Ports	5	4	3	2	1	Threats	
www.domain.com	5	2	5	6	0	33	46	
	Totals:	5	2	5	6	0	33	46

Discovered Open Ports (Nmap)

This assessment discovered a total of 5 distinct open network ports on the hosts in this report. This does not mean each open port is a security threat, but it does show some possible points of entry to your network that an attacker could potentially leverage. It is generally considered good practice to keep the number of open ports to a minimum. Sometimes hackers will target computers with a large number of open network ports because they may be more susceptible to attack. Minimizing the number of open network ports will help to minimize this risk and make your network less "attractive" to hackers and attacks.

A cross-reference of all discovered security threats by port number and risk factor is provided below. This analysis will help to determine which port represents the greatest overall risk to the target system. The most vulnerable port has been highlighted.



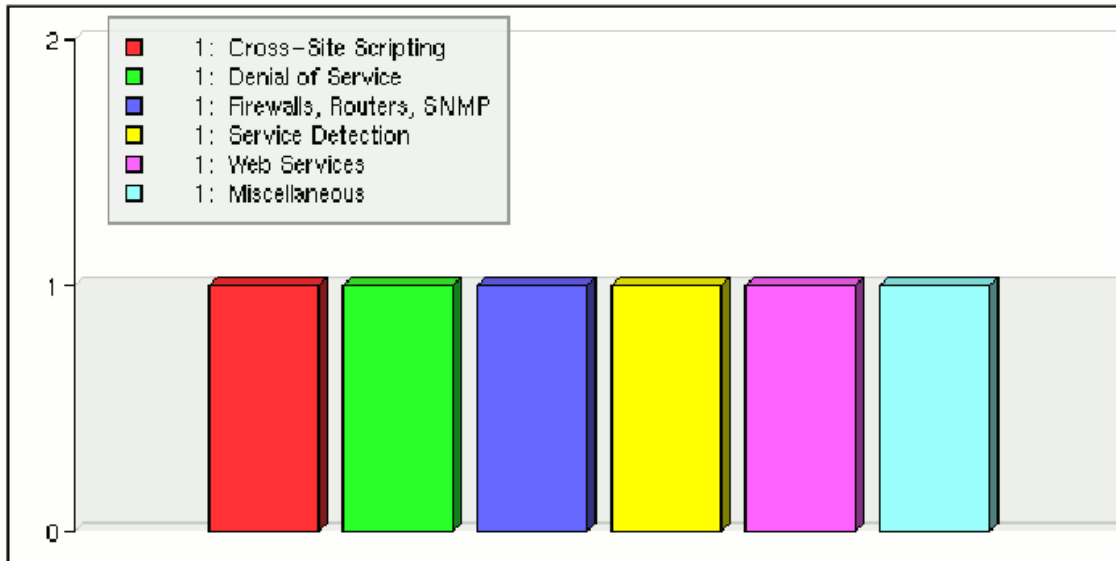
Number of Hosts vs. Open Ports

HOST: **www.domain.com**

Port	Service Type (estimated)	5	4	3	2	1	Total
ICMP		0	0	0	0	1	1
TCP		0	0	2	0	2	4
TCP:22	OPENSSSH 5.1P1 DEBIAN 6UBUNTU2 (PROTOCOL 2.0)	0	0	0	0	2	2
TCP:80	APACHE HTTPD 2.2.12 ((UBUNTU))	1	4	4	0	24	33
TCP:443	APACHE HTTPD 2.2.12 ((UBUNTU))	1	1	0	0	4	6

Vulnerable Threat Families

The 46 total discovered vulnerabilities are spread across 6 families of threat classifications. The graph below shows the most frequently occurring threat families discovered on this network. Also, a complete list of every threat classification along with the number of vulnerabilities discovered is in the table below. The most vulnerable family has been highlighted.



Number of Discovered Threats vs. Family Classifications

Family	5	4	3	2	1	Total
Cross-Site Scripting	0	0	2	0	0	2
Denial of Service	0	0	1	0	0	1
Firewalls, Routers, SNMP	0	0	1	0	0	1
Miscellaneous	0	0	0	0	3	3
Service Detection	0	0	0	0	1	1
Web Services	2	5	2	0	29	38

Discovered Security Threats Summary

This section provides a simple one-line summary of each discovered potential security threat on each host in this network. These summaries are grouped by host and sorted by risk factor. The full analysis report for each host is linked to the IP address.

HOST: www.domain.com

Risk	Port	ID	Summary
5	TCP:80	145004	Multiple Vulnerabilities in Apache < 2.2.15
5	TCP:443	145004	Multiple Vulnerabilities in Apache < 2.2.15
4	TCP:80	142052	Apache 2.2 < 2.2.14 Multiple Vulnerabilities
4	TCP:80	142055	CGI Generic Format String Vulnerability
4	TCP:443	142052	Apache 2.2 < 2.2.14 Multiple Vulnerabilities
4	TCP:80	143351	PHP < 5.2.12 Multiple Vulnerabilities
4	TCP:80	144921	The Remote Web Server Uses A Version Of PHP That Is Affected By\nmultiple Flaws.
3	TCP	111618	TCP/IP SYN+FIN Packet Filtering Weakness
3	TCP	112213	TCP/IP Sequence Prediction Blind Reset Spoofing DoS
3	TCP:80	141014	PHP < 5.2.11 Multiple Vulnerabilities
3	TCP:80	139466	CGI Generic Cross-Site Scripting Vulnerability
3	TCP:80	142425	CGI Generic Persistent Cross-Site Scripting Vulnerability
3	TCP:80	144136	Web Server Prone to Cookie Injection Attacks
1	ICMP	110114	ICMP Timestamp Request Remote Date Disclosure
1	TCP	118261	Apache Banner Linux Distribution Disclosure
1	TCP	125220	TCP/IP Timestamps Supported
1	TCP:22	110267	SSH Server Type And Version Information
1	TCP:22	110881	SSH Protocol Versions Supported
1	TCP:80	110107	HTTP Server Type And Version
1	TCP:80	110302	Web Server Robots.txt Information Disclosure
1	TCP:80	110386	Web Server No 404 Error Code Check
1	TCP:80	111419	Web Server Office File Inventory
1	TCP:80	124260	HyperText Transfer Protocol (HTTP) Information
1	TCP:80	133817	Web Application Tests : Load Estimation
1	TCP:80	135974	AWStats Detection
1	TCP:80	400000	Potentially Sensitive Resource Discovered
1	TCP:80	400000	Potentially Sensitive Resource Discovered
1	TCP:80	403092	Interesting Web Document Found
1	TCP:80	403092	Interesting Web Document Found
1	TCP:80	403092	Interesting Web Document Found
1	TCP:80	403092	Interesting Web Document Found

Threat Differential

This section lists all of the differences in discovered threats for all hosts in this assessment. Differences are derived based on the results obtained during the baseline scan.

This table shows the relative risks that exist on the hosts in this assessment and the remediation trends of said risks for the period of 2011-05-02 - 2011-05-02.

	5	4	3	2	1
Threats resolved since the baseline scan:	0	0	0	0	0
Threats discovered since the baseline scan:	0	0	0	0	0
Current outstanding threats:	2	5	6	0	33

There are no differences to report among all active hosts.

These hosts from this assessment are considered new since only scanned once: www.domain.com

Network Characteristics

This section is not specific to security threats or vulnerabilities. Rather, the Network Characteristics section provides general information about how each host in this assessment responded to some standard basic network testing. The information in this section may be useful to gain an understanding of the characteristics of the hosts as seen from a remote network across the Internet.

Response Times and Packet Loss

Although ping is sometimes considered a valuable network diagnostic tool, it can also sometimes be used for certain denial of service (DoS) attacks. You should consider the possible impact this may, or may not, have on your network resources.

The table below lists the packet loss and round-trip times (ms) for each host in this assessment. Non-zero packet loss is a sign of too much network traffic. A significant amount of packet loss may skew the results of the entire assessment. Please note, however, that hosts that have no open ports and are rejecting ICMP Echo requests will report 100% packet loss.

Host	Packet Loss	Min	Avg	Max
www.domain.com	0%	112.7	115.9	118.2

Reverse DNS Information

Reverse DNS records are necessary for some network protocols and/or applications to function correctly. It is always a good idea to give an IP address a valid reverse DNS record, even if it is just a generic name within your domain. The results from attempting to resolve each host in this assessment are shown below.

IP Address	Reverse DNS	Resolved By	Authoritative Server
www.domain.com	static.	clients.you	

Traceroute Response

The information below shows the round-trip times for each responsive hop between the scanner and target host in this assessment. This traceroute was performed using a maximum TTL value of 30, one UDP query per TTL, and a starting TTL of 5.

HOST: www.domain.com

Hop	IP Address	Hostname	Time (ms)
5	4.69.134.153	ae-82-82.ebr2.Washington1	47.44
6	4.69.137.57	ae-43-43.ebr2.Frankfurt1	133.98
7	4.69.140.18	ae-62-62.csw1.Frankfurt1	134.53
8	4.68.23.11	ae-1-69.edge3.Frankfurt1	133.13
9	212.162.40.206	Frankfurt1.Level3.net	154.90
10	213.239.240.243	hos-bb1.juniper2.fs.	146.52
11	213.239.227.239	hos-tr4.ex3k14.rz10.h	144.48
12	55.200.200.7	static.	144.24

Online Public Database Search

There are various public databases, accessible via the Internet, which may contain information about your network, systems, and company. Under normal circumstances, this information is not confidential and does not contain any errors. However, it is also possible for these public databases to contain sensitive and/or incorrect data. If this is the case, the potential impact could vary widely. It may be a simple typo, it may allow your network to be hijacked by hackers, or it may expose proprietary information to the Internet.

In the sections Whois Domain and Whois Arin, online public databases were queried for information about each host in this assessment. Because this information is specific to your network, `www.domain.com` can not automatically determine if this information is correct or not. Please review the results listed in those sections for each of these queries to ensure that the information is both correct and non-confidential.

IP Address Registries

The ARIN IP Address registry was queried for each host in this assessment. The results of this query should show the owner (and associated contacts) for each host. This should probably be your company directly, your ISP, or maybe even your hosting provider (if applicable). The entity listed below is considered the authoritative owner of the host.

HOST(s): www.domain.com

```
#
# Query terms are ambiguous. The query is assumed to be:
# "n"
#
# Use "?" to get help.
#
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=
#
NetRange          78.0.0.0 - 78.255.255.255
CIDR              78.0.0.0/8
OriginAS
NetName          78-RIPE
NetHandle        NET-78-0-0-0-1
Parent
NetType          Allocated to RIPE NCC
Comment          These addresses have been further assigned to users in
Comment          the RIPE NCC region. Contact information can be found in
Comment          the RIPE database at http://www.ripe.net/whois
RegDate          2006-08-29
Updated          2009-05-18
Ref              http://whois.arin.net/rest/net/NET-78-0-0-0-1

OrgName          RIPE Network Coordination Centre
OrgId            RIPE
Address          P.O. Box 10096
City             Amsterdam
StateProv
PostalCode       1001EB
Country          NL
RegDate
Updated          2011-03-15
Ref              http://whois.arin.net/rest/org/RIPE

ReferralServer   whois://whois.ripe.net:43

OrgTechHandle    RNO29-ARIN
OrgTechName      RIPE NCC Operations
OrgTechPhone     +31 20 535 4444
OrgTechEmail     do_not_email@ripe.invalid
OrgTechRef       http://whois.arin.net/rest/poc/RNO29-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at   https://www.arin.net/whois_tou.html
#
```

Domain Name Registries

This section attempted to resolve the domain name for each host in this assessment. Then, that domain name, if any, was searched in the Internic and domain name registry databases. The results of this query should report the owner (and associated contacts) for the domain name, if any, associated the host. This should probably be your company directly, your ISP, or maybe even your hosting provider (if applicable). The entity listed below is considered the authoritative owner of the domain name, if any, associated with the host.

HOST(s): www.domain.com

```
% Copyright (c) 2010 by DENIC
% Version: 2.0
%
% Restricted rights.
%
% Terms and Conditions of Use
%
% The data in this record is provided by DENIC for informational purposes only.
% DENIC does not guarantee its accuracy and cannot, under any circumstances,
% be held liable in case the stored information would prove to be wrong,
% incomplete or not accurate in any sense.
%
% All the domain data that is visible in the whois service is protected by law.
% It is not permitted to use it for any purpose other than technical or
% administrative requirements associated with the operation of the Internet.
% It is explicitly forbidden to extract, copy and/or use or re-utilise in any
% form and by any means (electronically or not) the whole or a quantitatively
% or qualitatively substantial part of the contents of the whois database
% without prior and explicit written permission by DENIC.
% It is prohibited, in particular, to use it for transmission of unsolicited
% and/or commercial and/or advertising by phone, fax, e-mail or for any similar
% purposes.
%
% By maintaining the connection you assure that you have a legitimate interest
% in the data and that you will only use it for the stated purposes. You are
% aware that DENIC maintains the right to initiate legal proceedings against
% you in the event of any breach of this assurance and to bar you from using
% its whois service.
%
% The DENIC whois service on port 43 never discloses any information concerning
% the domain holder/administrative contact. Information concerning the domain
% holder/administrative contact can be obtained through use of our web-based
% whois service available at the DENIC website:
% http://www.denic.de/en/background/whois-service/webwhois.html
%
Domain: your-server.
Nserver: ns.second-ns.
Nserver: ns1.your-server
Nserver: ns3.second-ns.de
Status: connect
Changed: 2008-12-02T15:05:12+01:00

[Tech-C]
Type: PERSON
Name: Martin Hetzner
Address: Hetzner Online AG
Address: Industriestr. 6
PostalCode: 91710
City: Gunzenhausen
CountryCode: DE
Phone: +49-9831-610061
Fax: +49-9831-610062
Email: info@hetzner.de
Changed: 2003-01-28T08:12:09+01:00

[Zone-C]
```

Type: PERSON
Name: Martin Hetzner
Address: Hetzner Online AG
Address: Industriestr. 6
PostalCode: 91710
City: Gunzenhausen
CountryCode: DE
Phone: +49-9831-610061
Fax: +49-9831-610062
Email: info@hetzner.de
Changed: 2003-01-28T08:12:09+01:00

Discovered Security Threats by Host

This section provides all the details about each discovered potential security threat for all of the hosts in this assessment. These details are grouped by host and ordered by risk factor.

HOST: www.domain.com

Multiple Vulnerabilities in Apache < 2.2.15	ID	Port	Risk
Web Services :: Nessus	145004	TCP:80	5

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

- A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)
- The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)
- The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave call-backs in an undefined state. (CVE-2010-0425)
- A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)

Solution:

Upgrade to Apache version 2.2.15 or later.

CVSS Information:

Low Attack Complexity, Complete Confidentiality Impact, Complete Integrity Impact, Complete Availability Impact

Additional References:

CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434, Bugtraq-36935, Bugtraq-38491, Bugtraq-38494, Bugtraq-38580, OSVDB-59969, OSVDB-62674, OSVDB-62675, OSVDB-62676, Secunia-38776, http://httpd.apache.org/security/vulnerabilities_22.html, https://issues.apache.org/bugzilla/show_bug.cgi?id=48359, http://www.apache.org/dist/httpd/CHANGES_2.2.15

Information from Target:

Apache version 2.2.12 appears to be running on the remote host based on the following Server response header :

```
Server: Apache/2.2.12 (Ubuntu)
```

Multiple Vulnerabilities in Apache < 2.2.15	ID	Port	Risk
Web Services :: Nessus	145004	TCP:443	5

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

- A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)
- The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)
- The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave call-backs in an undefined state. (CVE-2010-0425)
- A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)

Solution:

Upgrade to Apache version 2.2.15 or later.

CVSS Information:

Low Attack Complexity, Complete Confidentiality Impact, Complete Integrity Impact, Complete Availability Impact

Additional References:

CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434, Bugtraq-36935, Bugtraq-38491, Bugtraq-38494, Bugtraq-38580, OSVDB-59969, OSVDB-62674, OSVDB-62675, OSVDB-62676, Secunia-38776, http://httpd.apache.org/security/vulnerabilities_22.html, https://issues.apache.org/bugzilla/show_bug.cgi?id=48359, http://www.apache.org/dist/httpd/CHANGES_2.2.15

Information from Target:

Apache version 2.2.12 appears to be running on the remote host based on the following Server response header :

```
Server: Apache/2.2.12 (Ubuntu)
```

Apache 2.2 < 2.2.14 Multiple Vulnerabilities	ID	Port	Risk
Web Services :: Nessus	142052	TCP:80	4

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)
- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)
- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial-of-service. (CVE-2009-3094)

Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves.

Solution:

Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

CVSS Information:

Low Attack Complexity, Partial Confidentiality Impact, Partial Integrity Impact, Partial Availability Impact

Additional References:

CVE-2009-2699, CVE-2009-3094, CVE-2009-3095, Bugtraq-36254, Bugtraq-36260, Bugtraq-36596, OSVDB-57851, OSVDB-58879, Secunia-36549, <http://www.securityfocus.com/advisories/17947>, <http://www.securityfocus.com/advisories/17959>, <http://www.intevydis.com/blog/?p=59>, https://issues.apache.org/bugzilla/show_bug.cgi?id=47645, http://www.apache.org/dist/httpd/CHANGES_2.2.14

Information from Target:

Apache version 2.2.12 appears to be running on the remote host based on the following Server response header :

```
Server: Apache/2.2.12 (Ubuntu)
```

CGI Generic Format String Vulnerability	ID	Port	Risk
Web Services :: Nessus	142055	TCP:80	4

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. They seem to be vulnerable to a 'format string' attack. By leveraging this issue, an attacker may be able to execute arbitrary code on the remote host subject to the privileges under which the web server operates.

Please inspect the results as this script is prone to false positives.

Solution:

Restrict access to the vulnerable application / scripts. And contact the vendor for a patch or upgrade.

Additional References:

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

Information from Target:

```

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to format string :

/systemas-de-software/?cat=%2508x

----- output -----
<script type="text/javascript">
//
var LANGUAGEID_ES = 16777216;
var LANGUAGEID_EN = 33554432;
var LANGUAGEID_DE = 67108864;
-----

Clicking directly on these URLs might expose the vulnerabilities :
(you will probably need to check the HTML source)

http://www.domain.com/?cat=%2508x
</pre>
</div>
<div data-bbox="118 449 879 496" data-label="Table">
<table border="1">
<tr>
<td><b>Apache 2.2 &lt; 2.2.14 Multiple Vulnerabilities</b></td>
<td>ID</td>
<td>Port</td>
<td><b>Risk</b></td>
</tr>
<tr>
<td>Web Services :: Nessus</td>
<td>142052</td>
<td>TCP:443</td>
<td><b>4</b></td>
</tr>
</table>
</div>
<div data-bbox="114 502 887 529" data-label="Text"><p>According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :</p></div>
<div data-bbox="129 538 887 612" data-label="List-Group">
<ul>
<li>- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)</li>
<li>- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)</li>
<li>- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial-of-service. (CVE-2009-3094)</li>
</ul>
</div>
<div data-bbox="114 625 887 652" data-label="Text"><p>Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves.</p></div>
<div data-bbox="114 674 181 688" data-label="Section-Header"><p><b>Solution:</b></p></div>
<div data-bbox="114 691 696 706" data-label="Text"><p>Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.</p></div>
<div data-bbox="114 716 242 730" data-label="Section-Header"><p><b>CVSS Information:</b></p></div>
<div data-bbox="114 733 746 749" data-label="Text"><p>Low Attack Complexity, Partial Confidentiality Impact, Partial Integrity Impact, Partial Availability Impact</p></div>
<div data-bbox="114 758 271 772" data-label="Section-Header"><p><b>Additional References:</b></p></div>
<div data-bbox="114 775 830 829" data-label="Text">
<p>CVE-2009-2699, CVE-2009-3094, CVE-2009-3095, Bugtraq-36254, Bugtraq-36260, Bugtraq-36596, OSVDB-57851, OSVDB-58879, Secunia-36549, <a href="http://www.securityfocus.com/advisories/17947">http://www.securityfocus.com/advisories/17947</a>, <a href="http://www.securityfocus.com/advisories/17959">http://www.securityfocus.com/advisories/17959</a>, <a href="http://www.intevydis.com/blog/?p=59">http://www.intevydis.com/blog/?p=59</a>, <a href="https://issues.apache.org/bugzilla/show_bug.cgi?id=47645">https://issues.apache.org/bugzilla/show_bug.cgi?id=47645</a>, <a href="http://www.apache.org/dist/httpd/CHANGES_2.2.14">http://www.apache.org/dist/httpd/CHANGES_2.2.14</a></p>
</div>
<div data-bbox="114 838 280 853" data-label="Section-Header"><p><b>Information from Target:</b></p></div>
<div data-bbox="114 856 754 884" data-label="Text"><p>Apache version 2.2.12 appears to be running on the remote host based on the following Server response header :</p></div>
<div data-bbox="132 894 380 908" data-label="Text"><pre>Server: Apache/2.2.12 (Ubuntu)</pre></div>
<div data-bbox="107 945 193 958" data-label="Page-Footer"><p>CONFIDENTIAL</p></div>
<div data-bbox="500 945 519 958" data-label="Page-Footer"><p>20</p></div>
<div data-bbox="805 945 897 958" data-label="Page-Footer"><p>CONFIDENTIAL</p></div>
```

PHP < 5.2.12 Multiple Vulnerabilities	ID	Port	Risk
Web Services :: Nessus	143351	TCP:80	4

According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues:

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)
- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)
- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, he may be able to cause the web server to stop responding while it processes the file list. (CVE-2009-4017)
- Missing protection for '\$_SESSION' from interrupt corruption and improved 'session.save_path' check. (CVE-2009-4143)
- Insufficient input string validation in the 'htmlspecialchars()' function. (CVE-2009-4142)

Solution:

Upgrade to PHP version 5.2.12 or later.

CVSS Information:

Partial Confidentiality Impact, Partial Integrity Impact, Partial Availability Impact

Additional References:

CVE-2009-3557, CVE-2009-3558, CVE-2009-4017, CVE-2009-4142, CVE-2009-4143, Bugtraq-37389, Bugtraq-37390, OSVDB-61208, OSVDB-61209, Secunia-37821, <http://www.nessus.org/u?57f2d08f>, http://www.php.net/releases/5_2_12.php, <http://www.php.net/ChangeLog-5.php#5.2.12>

Information from Target:

PHP version 5.2.10 appears to be running on the remote host based on the following X-Powered-By response header :

```
X-Powered-By: PHP/5.2.10-2ubuntu6.4\r
```

The Remote Web Server Uses A Version Of PHP That Is Affected By\nmultiple Flaws.	ID	Port	Risk
Web Services :: Nessus	144921	TCP:80	4

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.
- It may be possible to bypass the 'open_basedir/' 'safe_mode' configuration restrictions due to an error in session extensions.
- An unspecified vulnerability affects the LCG entropy.

Solution:

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

CVSS Information:

Low Attack Complexity, Partial Confidentiality Impact, Partial Integrity Impact

Additional References:

Bugtraq-38182, Bugtraq-38430, Bugtraq-38431, OSVDB-62582, OSVDB-62583, Secunia-38708, http://securityreason.com/achievement_securityalert/82, <http://securityreason.com/securityalert/7008>, <http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0209.htm>, http://www.php.net/releases/5_3_2.php, <http://www.php.net/ChangeLog-5.php#5.3.2>, http://www.php.net/releases/5_2_13.php, <http://www.php.net/ChangeLog-5.php#5.2.13>

Information from Target:

PHP version 5.2.10 appears to be running on the remote host based on the following X-Powered-By response header :

```
X-Powered-By: PHP/5.2.10-2ubuntu6.4\r
```

TCP/IP SYN+FIN Packet Filtering Weakness	ID	Port	Risk
Firewalls, Routers, SNMP :: Nessus	111618	TCP	3

The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

Solution:

Contact your vendor for a patch.

CVSS Information:

Low Attack Complexity, Partial Integrity Impact

Additional References:

Bugtraq-7487, OSVDB-2118, <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>, <http://www.kb.cert.org/vuls/id/464113>

TCP/IP Sequence Prediction Blind Reset Spoofing DoS	ID	Port	Risk
Denial of Service :: Nessus	112213	TCP	3

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution:

See <http://www.securityfocus.com/bid/10183/solution/>

Additional References:

CVE-2004-0230, Bugtraq-10183, OSVDB-4030, IAVA-2004-A-0007, <http://www.securityfocus.com/bid/10183/solution/>

PHP < 5.2.11 Multiple Vulnerabilities	ID	Port	Risk
Web Services :: Nessus	141014	TCP:80	3

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.
- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.
- An unspecified input validation vulnerability affects exif processing.
- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)

Solution:

Upgrade to PHP version 5.2.11 or later.

CVSS Information:

Low Attack Complexity, Partial Availability Impact

Additional References:

CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, Bugtraq-36449, OSVDB-58185, OSVDB-58186, OSVDB-58187, OSVDB-58188, Secunia-36791, http://www.php.net/releases/5_2_11.php, <http://news.php.net/php.internals/45597>, <http://www.php.net/ChangeLog-5.php#5.2.11>

Information from Target:

PHP version 5.2.10 appears to be running on the remote host based on the following X-Powered-By response header :

```
X-Powered-By: PHP/5.2.10-2ubuntu6.4\r
```

CGI Generic Cross-Site Scripting Vulnerability	ID	Port	Risk
Cross-Site Scripting :: Nessus	139466	TCP:80	3

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non persistent' or 'reflected'.

Solution:

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

CVSS Information:

Partial Integrity Impact

Additional References:

http://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent, <http://jeremiahgrossman.blogspot.com/2009/06/results-unicode-leftright>

Information from Target:

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (XSS) :

```
?lang=<IMG%20SRC="javascript:alert(42);">
```

----- output -----

```
PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="<IMG SRC="jav [... ]
<head>
<base href="http://www.domain.com /" />
```

CGI Generic Persistent Cross-Site Scripting Vulnerability	ID	Port	Risk
Cross-Site Scripting :: Nessus	142425	TCP:80	3

The remote web server hosts one or more CGI scripts that fail to adequately sanitize request strings containing malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These issues are likely to be 'persistent' or 'stored', but this aspect should be checked manually. Please note that persistent XSS can be triggered by any channel that provides information to the application. Nessus cannot test them all.

Or contact the vendor for a patch or upgrade.

Solution:

Restrict access to the vulnerable application

CVSS Information:

Partial Integrity Impact

Additional References:

http://en.wikipedia.org/wiki/Cross_site_scripting#Persistent

Information from Target:

```

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross site scripting :

?cat=&lang=<BODY ONLOAD=alert($URL$)>
Seen on :
          ?cat=&lang=<BODY%20ONLOAD=alert(G2f73697374656d617
32d64652d736f6674776172652f3f6361743d266c616e673d3c424f4459204f4e4c4f414
43d616c657274282455524c24293e)>
----- output -----
PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="<BODY ONLOAD= [...]
<head>
<base href="http://www.domain.com /" />
-----

```

Web Server Prone to Cookie Injection Attacks	ID	Port	Risk
Web Services :: Nessus	144136	TCP:80	3

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that :

- Nessus did not check if the session fixation attack is feasible.
- This is not the only vector of session fixation.

Solution:

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

CVSS Information:

Partial Integrity Impact

Additional References:

http://en.wikipedia.org/wiki/Session_fixation, http://www.owasp.org/index.php/Session_Fixation, http://www.acros.si/papers/session_fixation.pdf, <http://projects.webappsec.org/Session-Fixation>

Information from Target:

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cookie manipulation :

```
?lang=<script>document.cookie="testemep=9057;"</sc
ript>

----- output -----
PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="<script>docum [...]
<head>
<base href="http://          /" />
-----
```

ICMP Timestamp Request Remote Date Disclosure	ID	Port	Risk
Miscellaneous :: Nessus	110114	ICMP	1

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Solution:

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Additional References:

CVE-1999-0524, OSVDB-94

Information from Target:

The difference between the local and remote clocks is 306 seconds.

Apache Banner Linux Distribution Disclosure	ID	Port	Risk
Web Services :: Nessus	118261	TCP	1

This script extracts the banner of the Apache web server and attempts to 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.

Information from Target:

```
The linux distribution detected was :
- Ubuntu 9.10 (karmic)
```

TCP/IP Timestamps Supported	ID	Port	Risk
Miscellaneous :: Nessus	125220	TCP	1

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Additional References:

<http://www.ietf.org/rfc/rfc1323.txt>

SSH Server Type And Version Information	ID	Port	Risk
Service Detection :: Nessus	110267	TCP:22	1

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Information from Target:

```
SSH version : SSH-2.0-OpenSSH_5.1p1 Debian-6ubuntu2
SSH supported authentication : publickey,password
```

SSH Protocol Versions Supported	ID	Port	Risk
Miscellaneous :: Nessus	110881	TCP:22	1

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Information from Target:

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.99
- 2.0

```
SSHv2 host key fingerprint : 14:2f:be:ea:4c:67:ce:39:9a:7a:13:a5:59:05:54:fb
```

HTTP Server Type And Version	ID	Port	Risk
Web Services :: Nessus	110107	TCP:80	1

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

Information from Target:

```
The remote web server type is :
```

```
Apache/2.2.12 (Ubuntu)
```

```
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

Web Server Robots.txt Information Disclosure	ID	Port	Risk
Web Services :: Nessus	110302	TCP:80	1

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

Solution:

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Additional References:

OSVDB-238, <http://www.robotstxt.org/wc/exclusion.html>

Information from Target:

Contents of robots.txt :

```
User-agent: *
Disallow: /admin/
Disallow: /box/
Disallow: /cgi-bin/
Disallow: /include/
Disallow: /iot/
Disallow: /jsCalendar/
Disallow: /jsMenu/
Disallow: /lang/
# Disallow: /pics/
# Allow: /pics/content/
Disallow: /pics/logos/
Disallow: /pics/tree/
Disallow: /pics/wmarks/
Disallow: /pics/blank.gif
Disallow: /pics/trans.gif
Disallow: /pics/trans.png
Disallow: /pics/loading-bar.gif
Disallow: /pics/loading-circle.gif
Disallow: /pics/newsfeed.png
# Allow: /uploaded/
```

Web Server No 404 Error Code Check	ID	Port	Risk
Web Services :: Nessus	110386	TCP:80	1

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Information from Target:

The following title tag will be used :

Web Server Office File Inventory	ID	Port	Risk
Web Services :: Nessus	111419	TCP:80	1

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution:

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Information from Target:

The following office-related files are available on the remote server :

- Adobe Acrobat files (.pdf) :
/uploaded/content/article/998827006.pdf
/uploaded/content/article/1983748574.pdf

HyperText Transfer Protocol (HTTP) Information	ID	Port	Risk
Web Services :: Nessus	124260	TCP:80	1

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.

Information from Target:

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

Date: Mon, 02 May 2011 19:43:05 GMT\r
Server: Apache/2.2.12 (Ubuntu)\r
X-Powered-By: PHP/5.2.10-2ubuntu6.4\r
Set-Cookie: lang=es\r
Content-Language: es\r
Vary: Accept,Accept-Encoding\r
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r
Pragma: no-cache\r
Keep-Alive: timeout=15, max=100\r
Connection: Keep-Alive\r
Transfer-Encoding: chunked\r
Content-Type: text/html;charset=iso-8859-1\r
\r
```

Web Application Tests : Load Estimation	ID	Port	Risk
Web Services :: Nessus	133817	TCP:80	1

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 as it would depend upon external factors such as the network and web servers loads.

Information from Target:

Here are the estimated number of requests in miscellaneous modes for the GET method only :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution	: S=2944	SP=2944	AP=2944	SC=2944	AC=2944
format string	: S=128	SP=128	AP=128	SC=128	AC=128
header injection	: S=128	SP=128	AP=128	SC=128	AC=128
SSI injection	: S=384	SP=384	AP=384	SC=384	AC=384
unseen parameters	: S=4480	SP=4480	AP=4480	SC=4480	AC=4480
blind SQL injection	: S=3072	SP=3072	AP=3072	SC=3072	AC=3072
SQL injection	: S=3584	SP=3584	AP=3584	SC=3584	AC=3584
directory traversal	: S=3712	SP=3712	AP=3712	SC=3712	AC=3712
local file inclusion	: S=512	SP=512	AP=512	SC=512	AC=512
web code injection	: S=128	SP=128	AP=128	SC=128	AC=128
persistent XSS	: S=512	SP=512	AP=512	SC=512	AC=512
cross-site scripting (XSS)	: S=2176	SP=2176	AP=2176	SC=2176	AC=2176

Here are the estimated number of requests in miscellaneous modes for both methods (GET & POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution	: S=5888	SP=5888	AP=5888	SC=5888	AC=5888
format string	: S=256	SP=256	AP=256	SC=256	AC=256
header injection	: S=256	SP=256	AP=256	SC=256	AC=256
SSI injection	: S=768	SP=768	AP=768	SC=768	AC=768
unseen parameters	: S=8960	SP=8960	AP=8960	SC=8960	AC=8960
blind SQL injection	: S=6144	SP=6144	AP=6144	SC=6144	AC=6144
SQL injection	: S=7168	SP=7168	AP=7168	SC=7168	AC=7168
directory traversal	: S=7424	SP=7424	AP=7424	SC=7424	AC=7424
local file inclusion	: S=1024	SP=1024	AP=1024	SC=1024	AC=1024
web code injection	: S=256	SP=256	AP=256	SC=256	AC=256
persistent XSS	: S=1024	SP=1024	AP=1024	SC=1024	AC=1024
cross-site scripting (XSS)	: S=4352	SP=4352	AP=4352	SC=4352	AC=4352

AWStats Detection	ID	Port	Risk
Web Services :: Nessus	135974	TCP:80	1

The remote host is running AWStats, an open source log analysis tool written in Perl used to generate advanced graphic reports.

Additional References:

<http://awstats.sourceforge.net/>

Information from Target:

The following instance of AWStats was detected on the remote host :

Version : unknown
URL : <http://www.domain.com/awstats/awstats.pl>

Potentially Sensitive Resource Discovered	ID	Port	Risk
Web Services :: Nikto	400000	TCP:80	1

Path: /

The Nikto web application scanner found an interesting file/url. It is recommended to verify that this resource does not contain any sensitive information and is intended to be available to the public. If this is a legitimate resource, then this file/url can be marked to be ignored from future reporting.

Information from Target:

DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us>

Potentially Sensitive Resource Discovered	ID	Port	Risk
Web Services :: Nikto	400000	TCP:80	1

Path: /pccsmysqldm/incs/dbconnect.inc

The Nikto web application scanner found an interesting file/url. It is recommended to verify that this resource does not contain any sensitive information and is intended to be available to the public. If this is a legitimate resource, then this file/url can be marked to be ignored from future reporting.

Information from Target:

/pccsmysqldm/incs/dbconnect.inc: This file should not be accessible, as it contains data

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /css

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /swf

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /pics/

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /not

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /lib/

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /js

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /img/

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /cliente/

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /ad

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /sitemap.xml

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

Potentially Dangerous Web Document Found	ID	Port	Risk
Web Services :: Nikto	403093	TCP:80	1

Path: /bugtest+/?

A potentially dangerous file was found on the web server. While there is no known vulnerability or exploit associated with this file, it has been found in logs after web servers have come under attack from unknown sources and software. This may indicate the presence of an undisclosed vulnerability that is being exploited in the wild.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them. If CGI programs contain exploits, remove the files or correct the vulnerability.

Additional References:

OSVDB-3093

Potentially Dangerous Web Document Found	ID	Port	Risk
Web Services :: Nikto	403093	TCP:80	1

Path: /adi

A potentially dangerous file was found on the web server. While there is no known vulnerability or exploit associated with this file, it has been found in logs after web servers have come under attack from unknown sources and software. This may indicate the presence of an undisclosed vulnerability that is being exploited in the wild.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them. If CGI programs contain exploits, remove the files or correct the vulnerability.

Additional References:

OSVDB-3093

Directory Indexing Enabled	ID	Port	Risk
Web Services :: Nikto	403268	TCP:80	1

Path: /icons/

Directory indexing has been found to be enabled on the web server. While there is no known vulnerability or exploit associated with this, it may reveal sensitive or "hidden" files or directories to remote users, or aid in more focused attacks.

Solution:

Disable directory indexing according to the web server's documentation.

Additional References:

OSVDB-3268

PHP Version And Information Disclosure	ID	Port	Risk
Web Services :: Nikto	412184	TCP:80	1

Path: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

PHP contains a flaw that may lead to an unauthorized information disclosure. The issue is triggered when a remote attacker makes certain HTTP requests with crafted arguments, which will disclose PHP version and another sensitive information resulting in a loss of confidentiality.

Solution:

No patches are necessary to correct this issue. Set the "expose_php" setting to "Off" in the php.ini file, which will disable this functionality.

Additional References:

OSVDB-12184

HTTP Server Type And Version	ID	Port	Risk
Web Services :: Nessus	110107	TCP:443	1

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

Information from Target:

```
The remote web server type is :
```

```
Apache/2.2.12 (Ubuntu)
```

```
Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
```

HyperText Transfer Protocol (HTTP) Information	ID	Port	Risk
Web Services :: Nessus	124260	TCP:443	1

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.

Information from Target:

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

Date: Mon, 02 May 2011 19:43:06 GMT\r
Server: Apache/2.2.12 (Ubuntu)\r
Vary: Accept-Encoding\r
Content-Length: 279\r
Keep-Alive: timeout=15, max=100\r
Connection: Keep-Alive\r
Content-Type: text/html; charset=iso-8859-1\r
\r
```

AWStats Detection	ID	Port	Risk
Web Services :: Nessus	135974	TCP:443	1

The remote host is running AWStats, an open source log analysis tool written in Perl used to generate advanced graphic reports.

Additional References:

<http://awstats.sourceforge.net/>

Information from Target:

The following instance of AWStats was detected on the remote host :

Version : unknown
URL : http://www.domain.com :443/awstats/awstats.pl

HTTP Methods Per Directory	ID	Port	Risk
Web Services :: Nessus	143111	TCP:443	1

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Information from Target:

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

External Advisories

Some of the security threats discovered have external advisory sources for additional cross-reference information. To view the external advisory information, click on the reference number in the table below. Other web resources listed for the threat will be linked to as well.

ID	Risk	Description and References
145004	5	Multiple Vulnerabilities in Apache < 2.2.15 CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434, Bugtraq-36935, Bugtraq-38491, Bugtraq-38494, Bugtraq-38580, OSVDB-59969, OSVDB-62674, OSVDB-62675, OSVDB-62676, Secunia-38776, http://httpd.apache.org/security/vulnerabilities_22.html , https://issues.apache.org/bugzilla/show_bug.cgi?id=48359 , http://www.apache.org/dist/httpd/CHANGES_2.2.15
142052	4	Apache 2.2 < 2.2.14 Multiple Vulnerabilities CVE-2009-2699, CVE-2009-3094, CVE-2009-3095, Bugtraq-36254, Bugtraq-36260, Bugtraq-36596, OSVDB-57851, OSVDB-58879, Secunia-36549, http://www.securityfocus.com/advisories/17947 , http://www.securityfocus.com/advisories/17959 , http://www.intevydis.com/blog/?p=59 , https://issues.apache.org/bugzilla/show_bug.cgi?id=47645 , http://www.apache.org/dist/httpd/CHANGES_2.2.14
143351	4	PHP < 5.2.12 Multiple Vulnerabilities CVE-2009-3557, CVE-2009-3558, CVE-2009-4017, CVE-2009-4142, CVE-2009-4143, Bugtraq-37389, Bugtraq-37390, OSVDB-61208, OSVDB-61209, Secunia-37821, http://www.nessus.org/u?57f2d08f , http://www.php.net/releases/5_2_12.php , http://www.php.net/ChangeLog-5.php#5.2.12
142055	4	CGI Generic Format String Vulnerability http://en.wikipedia.org/wiki/Format_string_attack
144921	4	The Remote Web Server Uses A Version Of PHP That Is Affected By\nmultiple Flaws. Bugtraq-38182, Bugtraq-38430, Bugtraq-38431, OSVDB-62582, OSVDB-62583, Secunia-38708, http://securityreason.com/achievement_securityalert/82 , http://securityreason.com/securityalert/7008 , http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0209.htm , http://www.php.net/releases/5_3_2.php , http://www.php.net/ChangeLog-5.php#5.3.2 , http://www.php.net/releases/5_2_13.php , http://www.php.net/ChangeLog-5.php#5.2.13
144136	3	Web Server Prone to Cookie Injection Attacks http://en.wikipedia.org/wiki/Session_fixation , http://www.owasp.org/index.php/Session_Fixation , http://www.acros.si/papers/session_fixation.pdf , http://projects.webappsec.org/Session-Fixation
112213	3	TCP/IP Sequence Prediction Blind Reset Spoofing DoS CVE-2004-0230, Bugtraq-10183, OSVDB-4030, IAVA-2004-A-0007, http://www.securityfocus.com/bid/10183/solution/
111618	3	TCP/IP SYN+FIN Packet Filtering Weakness Bugtraq-7487, OSVDB-2118, http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html , http://www.kb.cert.org/vuls/id/464113
139466	3	CGI Generic Cross-Site Scripting Vulnerability http://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent , http://jeremiahgrossman.blogspot.com/2009/06/results-unicode-leftright
141014	3	PHP < 5.2.11 Multiple Vulnerabilities CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, Bugtraq-36449, OSVDB-58185, OSVDB-58186, OSVDB-58187, OSVDB-58188, Secunia-36791, http://www.php.net/releases/5_2_11.php , http://news.php.net/php.internals/45597 , http://www.php.net/ChangeLog-5.php#5.2.11
142425	3	CGI Generic Persistent Cross-Site Scripting Vulnerability http://en.wikipedia.org/wiki/Cross_site_scripting#Persistent
110302	1	Web Server Robots.txt Information Disclosure OSVDB-238, http://www.robotstxt.org/wc/exclusion.html
403093	1	Potentially Dangerous Web Document Found OSVDB-3093

110114	1	ICMP Timestamp Request Remote Date Disclosure CVE-1999-0524, OSVDB-94
412184	1	PHP Version And Information Disclosure OSVDB-12184
403268	1	Directory Indexing Enabled OSVDB-3268
135974	1	AWStats Detection http://awstats.sourceforge.net/
403092	1	Interesting Web Document Found OSVDB-3092
125220	1	TCP/IP Timestamps Supported http://www.ietf.org/rfc/rfc1323.txt

Education

The Education report is written to provide a very high level explanation of network and information security. This report will also show some statistics about the need for security, dispel common myths about security, and define (in plain English) many of the terms used throughout this document.

This particular section is non-technical and is geared toward non-technical individuals, business management, and/or executives. For the stated audience, this report should be a prerequisite to the other reports in this document. If you are already familiar with gpremp S.A. de C.v. documents, or if you are a technical professional, you may wish to simply skim this Education report. However, if you are a non-technical person, it is strongly recommended that you read this report.

What is Network and/or Information Security

Before you can understand the concept of network security, you must decide what security means to you and your company. Perhaps to you, feeling secure means knowing that you are safe from any outsider gaining access to your confidential files and private company information. If this is the case, use this policy to evaluate what goes on with your network because the same private information is also stored in your computer systems.

Network security simply means preventing unauthorized use of your computer network. Taking the necessary precautions to protect your network will help to keep unauthorized users, or hackers, from gaining access to your computer system or network. Network security can also assist you in detecting whether or not a hacker tried breaking into your system, and what damage, if any, was done.

When it comes to network security, most companies fall somewhere between two boundaries: complete access and complete security. A completely secure computer is one that is not connected to the network, not plugged in, and physically unreachable by anyone. Obviously, a machine like this does not serve much of a purpose in your office. On the other hand, a computer with complete access is very easy to use, requiring no passwords or authorization to provide information. Unfortunately, having a machine with complete access means anyone could access it. This could spell disaster for you and your organization.

Risk Factor Definitions

gpremp S.A. de C.v. is a 100% impartial analysis company. The classifications shown below are therefore based on international and recognized industry standards.

Urgent Risk (Level 5)

Urgent Risk vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, remote execution of commands as a root or administrator user.

Critical Risk (Level 4)

Critical Risk vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as level 4 vulnerabilities.

High Risk (Level 3)

High Risk vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying).

Medium Risk (Level 2)

Medium Risk vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.

Low Risk (Level 1)

Low Risk vulnerabilities are informational, such as open ports.

Threat Family Definitions

AIX Local Checks

Local operating system and application level security checks for AIX.

Backdoors

Access to application files, system data, or confidential information.

Centos Local Checks

Local operating system and application level security checks for Centos.

CentOS Local Checks

CGI abuses

Cross-Site Scripting

Threats related to improper sanitation of untrusted input in web pages.

Database Services

Exploits in database servers, services, and configurations.

Debian Local Checks

Local operating system and application level security checks for Debian.

Denial of Service

Threats of DoS attacks exploits used to launch other DoS attacks.

DNS Services

Vulnerabilities with domain name servers and configurations.

Fedora Local Checks

Local operating system and application level security checks for Fedora.

Firewalls

Firewalls, Routers, SNMP

Threats or attack methods related to firewall and router devices and the SNMP protocol.

FreeBSD Local Checks

Local operating system and application level security checks for FreeBSD.

FTP Services

Vulnerabilities of FTP (file sharing) applications, servers, or services.

General

Gentoo Local Checks

Local operating system and application level security checks for Gentoo.

HP-UX Local Checks

Local operating system and application level security checks for HP-UX.

MacOS X Local Checks

Local operating system and application level security checks for MacOS X.

Mail Services

Threats dealing with e-mail server problems or exploits.

Mandriva Local Checks

Microsoft Bulletins

Local operating system and application level security checks for Microsoft Windows.

Miscellaneous

Various threats and attacks that do not fit into any other family.

Netware

Problems with Netware operating systems, applications, and services.

Peer-To-Peer Services

Threats of exposed private data through file sharing services.

Port scanners

Red Hat Local Checks

Local operating system and application level security checks for Red Hat.

Remote File Access

Unauthorized access to files or data on your systems.

Remote Shell Access

Vulnerability of user or service-level accounts and information.

Service Detection

Tests for services, ports, and versions.

Slackware Local Checks

Local operating system and application level security checks for Slackware.

Solaris Local Checks

Local operating system and application level security checks for Solaris.

SuSE Local Checks

Local operating system and application level security checks for SuSE.

Ubuntu Local Checks

Local operating system and application level security checks for Ubuntu.

Unix

Problems, exploits, or attack methods related to UNIX systems or common UNIX services.

VMWare ESX Local Checks

Web Services

Problems exposed by web servers, configurations, or CGI scripts.

Windows

Problems with Windows operating systems, applications, and services.

Definitions of Technical Terms

ARIN

American Registry of Internet Numbers. This is the primary governing body that regulates Internet IP addresses. Other similar registries include APNIC and RIPE.

CGI

Common Gateway Interface. A standard structure and protocol for running external programs from a web server. For example, a program to process e-commerce credit card purchases would likely use CGI.

CVE / CAN

Common Vulnerabilities and Exposures / CANDidate. A dictionary that tracks information about known network and information security vulnerabilities.

DoS

Denial of Service. DoS is a specific type of network attack which can make servers and/or routers crash and typically results in a network outage.

DNS

Domain Name System/Service. A protocol used on the Internet for translating hostnames into Internet addresses. For example, DNS is the service that would translate www.google.com into the IP address 216.239.57.104. DNS is basically a phone book for the Internet.

Domain Name

Strings of alphanumeric characters used to name/identify computers, networks, and organizations on the Internet.

Exploit

A vulnerability in software or computer configurations that can be used for breaking security or otherwise attacking an Internet host over the network.

Family

The classification system used to determine the general category or type of service affected by a particular security threat. For example, security threats specific to Microsoft Windows systems would be classified in the "Windows" family in the security threats database.

Fingerprint

To identify by means of a distinctive mark or characteristic. For example, fingerprints are used to remotely identify which services, servers, operating systems, etc... that are running on any network.

Firewall

Any of a number of security schemes that prevent unauthorized users from gaining access to a computer network. Generally, a firewall is a hardware device installed on a network to help protect the network from hackers and attacks.

Hacker

A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. Many times the term is also used to describe a person who breaks into computer systems and/or networks.

Host

See Server.

IP Address

A numerical representation of a computer's address on the Internet.

MTA

Mail Transport Agent. The program running on a server to perform email functions and protocols. For example, when you send an email, your ISP's mail server uses an MTA to process the message.

Nessus

Open source security scanning engine used by most security professionals world-wide.

Network

An interconnected group of computers and electronic systems. A LAN is an example of a network. The Internet is another (albeit much more complex) example of a network.

Port

A computer's network interface is divided into several channels - each channel is called a "port." A port is used by specific hardware or software components to service requests on a network. For example, web servers typically use port number 80 to accept connections from users' web browsers. Generally, each computer has 65,535 unique ports.

Port Scan

The process of examining a group of ports on a computer to determine which ones are active. A port scan does not identify which applications/services are running on a computer, what any active ports are used for, or any security threats on the computer. It only determines which ports are active.

Protocol

A standard procedure for regulating data transmission between computers. For example, an email server uses a specific set of protocols so that anyone on the Internet can send email to anyone else on the Internet - regardless of which software or ISP either party is using.

Risk Factor

The classification system used to determine the severity or potential impact of a particular security threat.

Security Scan

The process of using various information security methodologies and techniques to audit the level of security for a computer, application, service, and/or network.

Security Threat

See Exploit.

Server

A computer that provides some service(s) to other computers that are connected to it via a network. For example, a web server provides web pages to your computer via the Internet.

Service

Work performed, or offered by, a server. For example, a web server offers the service of providing web pages to a web browser.

SSL

Secure Sockets Layer. A protocol designed to provide encrypted secure communications on the Internet. SSL is very commonly used to secure the transmission of e-commerce transactions. However, SSL does not provide any security for data after the initial transmission of the transaction.

TCP/IP

Transmission Control Protocol / Internet Protocol. A suite of data networking and communications protocols for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

Virus

A rogue computer program that searches out other programs and infects them by embedding a copy of itself in them, so that they become Trojan horses. When these programs are executed, the embedded virus is executed too, thus propagating the infection. This normally happens invisibly to the user.

Vulnerability

See Exploit.

VPN

Virtual Private Network. The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

Whois

An Internet directory service for looking up information on a remote server. Whois is commonly used to lookup information about people, companies, IP addresses, computers, and domain names.