CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 12/1/2014

Prepared for: Prospect Or Customer
Prepared by: Your Company Name
12/3/2014
# Table of Contents

1 - Summary
2 - Details
  2.1 - 42.62.65.25
  2.2 - 46.38.236.232 (fbnhffimnn.de)
  2.3 - 63.230.176.46 (etsio-prod.cnf.com)
  2.4 - 176.28.51.58 (rs208305.rs.hosteurope.de)
  2.5 - 193.23.123.40 (rev-040.snrm.fr)
1 - Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Analysis</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.62.65.25</td>
<td>Medium risk</td>
<td>14</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>46.38.236.232 (fbnhffmnn.de)</td>
<td>Medium risk</td>
<td>13</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>8.8</td>
</tr>
<tr>
<td>63.230.176.46 (etsio-prod.cnf.com)</td>
<td>Medium risk</td>
<td>11</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>13.1</td>
</tr>
<tr>
<td>176.28.51.58 (rs208305.rs.hosteurope.de)</td>
<td>High risk</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>14.4</td>
</tr>
<tr>
<td>193.23.123.40 (rev-040.snrm.fr)</td>
<td>High risk</td>
<td>9</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>27.0</td>
</tr>
<tr>
<td>Total: 5</td>
<td></td>
<td></td>
<td>54</td>
<td>3</td>
<td>12</td>
<td>12</td>
<td>0</td>
</tr>
</tbody>
</table>

Top Highest Risk
(By CVSS Score)

Detected Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Kernel</td>
<td>3</td>
</tr>
<tr>
<td>Unknown</td>
<td>1</td>
</tr>
<tr>
<td>HP UX 11.0x</td>
<td>1</td>
</tr>
</tbody>
</table>
## 2 - Scan Details

### Issues by Severity

<table>
<thead>
<tr>
<th>Severity</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>12</td>
</tr>
<tr>
<td>Low</td>
<td>12</td>
</tr>
<tr>
<td>False Positive</td>
<td>0</td>
</tr>
</tbody>
</table>
2.1 - 42.62.65.25

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Analysis</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.62.65.25</td>
<td>Medium risk</td>
<td>14</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Open Listening Ports

<table>
<thead>
<tr>
<th>Service (Port)</th>
<th>Analysis</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>afs3-fileserver (7000/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>irdmi (8000/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>ntp (123/udp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/tcp</td>
<td>Log risk</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>distinct (9999/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/CPE-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/HOST-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/icmp</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>https (443/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>ssh (22/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>unknown (4949/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>unknown (6081/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>unknown (8101/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>xprint-server (8100/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
## Security Issues

<table>
<thead>
<tr>
<th>Severity</th>
<th>CVSS Score</th>
<th>NVT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>2.6</td>
<td>afs3-fileserver (7000/tcp)</td>
<td>Variations --------- Variation 1: URL: <a href="http://42.62.65.25:7000/">http://42.62.65.25:7000/</a> Element: server Method: OPTIONS Tags: interesting, response, server Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification? false References: w3.org - <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html%5B%5E1">http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[^1</a>] Variation 2: URL: <a href="http://42.62.65.25:7000/">http://42.62.65.25:7000/</a> ID: Code: 405 Regular expression: Generates a simple list of safe/unsafe URLs. Legend:</td>
</tr>
<tr>
<td>Low</td>
<td>0.0</td>
<td>irdmi (8000/tcp)</td>
<td>Description: Generates a simple list of safe/unsafe URLs. Legend:</td>
</tr>
</tbody>
</table>

---

[^1]: [CVSS: 0.0] [Variations: 2] [URL: http://42.62.65.25:7000/] [Element: server] [Method: OPTIONS] [Tags: interesting, response, server] [Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.] [Requires manual verification? false] [References: w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html] [Variation 1: URL: http://42.62.65.25:7000/] [ID: Code: 405] [Regular expression: Generates a simple list of safe/unsafe URLs. Legend: |  |

---

The following timestamps were retrieved with a delay of 1 second between: Paket 1: 1609483043 Paket 2: 1609483387

It was detected that the host implements RFC1323.

Variations

---------- Variation 1: URL: http://42.62.65.25:8000/%3Cmy_tag_7dddf9f9e894138cd0d314d9091443aea30b51a7051eb3d32b20d60676ebf19a/%3E ID: 400 Regular expression: [+] [2] Trusted -- Interesting response [+] ~~~~~~~~~~~~~ ID Hash: db2c372bc9865bf3da31e719ac9f53a7191de47e593b3b1e8d51d87db43685 [+] Severity: Informational [+] URL: http://42.62.65.25:8000/ [+] Element: server [+] Method: TRACE [+] Tags: interesting, response, server [+] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

Variations

---------- Variation 1: URL: http://42.62.65.25:8000/ [+] ID: Code: 405 Regular expression: Plugin data: [+] Resolver [+] Description: Resolves vulnerable hostnames to IP addresses. 42.62.65.25: 42.62.65.25

---------- Variation 1: [+] Description: Generates a simple list of safe/unsafe URLs. Legend: [+] No issues [-] Has issues

http://42.62.65.25:8000/ [+] [+] http://42.62.65.25:8000/%3Cmy_tag_7dddf9f9e894138cd0d314d9091443aea30b51a7051eb3d32b20d60676ebf19a/%3E [+] Total: 2 [+] Without issues: 0 [+] With issues: 2 (100%)

Low (CVSS: 0.0) ntp (123/udp)

NVT: NTP read variables (OID: 1.3.6.1.4.1.25623.1.0.10884)

Summary: A NTP (Network Time Protocol) server is listening on this port.
Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Analysis</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.38.236.232 (fbnhffmnn.de)</td>
<td>Medium risk</td>
<td>13</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>8.8</td>
</tr>
</tbody>
</table>

Open Listening Ports

<table>
<thead>
<tr>
<th>Service (Port)</th>
<th>Analysis</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Total CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>https (443/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4.3</td>
</tr>
<tr>
<td>general/tcp</td>
<td>Low risk</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>http (80/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>ftp (21/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.9</td>
</tr>
<tr>
<td>general/CPE-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/HOST-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/icmp</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>imap (143/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>pop3 (110/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>smtp (25/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>ssh (22/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>sunrpc (111/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>unknown (51867/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Security Issues
Summary: This routine search for weak SSL ciphers offered by a service. Vulnerability Insight: These rules are applied for the evaluation of the cryptographic strength:- Any SSL/TLS using no cipher is considered weak.- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.- RC4 is considered to be weak.- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks.- Any cipher considered to be secure for only the next 10 years is considered as medium- Any other cipher is considered as strong.

Solution: The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Weak ciphers offered by this service:

SSL3_RSA_RC4_128_SHA
SSL3_RSA_WITH_SEED_SHA
TLS1_RSA_RC4_128_SHA

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 second in-between: Paket 1: 43459307 Paket 2: 43459604

Summary: Remote web server does not reply with 404 error code. Vulnerability Insight: This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead. OpenVAS enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead. CGI scanning will be disabled for this host.

Here is the arachni report: 

Web Application Security Report - Arachni Framework
Report generated on: 2014-09-26 14:09:05 +0000
Report false positives at: http://github.com/Arachni/arachni/issues
System settings:
Version: 0.4.7
Revision: 0.2.8
Audit started on: Fri Sep 26 14:08:47 2014
Audit finished on: Fri Sep 26 14:09:02 2014
Runtime: 00:00:14
URL: http://fbnhffmnn.de/80
User agent: arachni*
Audited elements:
* Links
* Forms
* Cookies*
Modules:
xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sql, sql_blind_timing, file_inclusion, response_splitting, sql_blind_rdf, code_injection_php_input_wrapper, os_cmd_injection Timing, xss_tag, xpath, xss_path, session_fixation, xss_event, unvalidated_redirect, code_injection_timing, xss, ldap, rfi, csrf,
unencrypted_password_forms, cvs_svn_users, http_only_cookies, html_objects, form_upload, capTCHA, mixed_resource,
credit_card, private_ip, emails, insecure_cookies, ssn, password_autocomplete, localstart_asp, common_files, allowed_methods,
backup_files, http_put, backdoors, common_directories, directory_listing, webdav, interesting_responses,
x_forwarded_for_access_restriction_bypass, htaccess_limit, xst[*]

25 issues were detected.

[1] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 01b12e85e60cb3fdd3fd174b19a19c485895d9aa8e337404230a01b982c618e278f [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/%3E%22%3Cmy_tag_15fe8696070fci1c16ab11f89b6d81e26a15bc252dd349ceff321ec4682fb54/%3E Element: server [~] Method: GET [~] Tags: interesting, response, server [~] Description: [~] The server responded with a non-200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. [~] Requires manual verification?: false [~] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html [~] Variations [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/%3E%22%3Cmy_tag_15fe8696070fci1c16ab11f89b6d81e26a15bc252dd349ceff321ec4682fb54/%3E [~] ID: Code: 301 [~] Regular expression: [~] [2] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash:
The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification? false References: w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html Variations ------- Variation 1: URL: http://fbnhffmnn.de/80/sitemap.xml ID: 301 [Regular expression: [+] [9] Trusted -- Interesting response ~~~~~~~~~~~~~~~~~~~~ ID Hash: 93a8c7ac76b491a9a48331fb270776eaa76f70fb2f09fb714f685915175771 Severity: Informational URL: http://fbnhffmnn.de/80/robots.txt Element: server Method: GET Tags: interesting, response, server Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification? false References: w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html Variations ------- Variation 1: URL: http://fbnhffmnn.de/80/robots.txt ID: 301 [Regular expression: [+] [5] Trusted -- Interesting response ~~~~~~~~~~~~~~~~~~~~ ID Hash: 8bd64c28cbe59af0d63f7632358d5f0249144873e22b34b8097fd2e6b8a9f96 Severity: Informational URL: http://fbnhffmnn.de/80/error_log Element: server Method: GET Tags: interesting, response, server Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification? false References: w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html Variations ------- Variation 1: URL: http://fbnhffmnn.de/80/error_log ID: 301 [Regular expression: [+] [8] Trusted -- Interesting response ~~~~~~~~~~~~~~~~~~~~ ID Hash: 191b552ed9835994d1b182b4d71d5c63e6f41be12c120f6f771ca15767b8b01d Severity: Informational URL: http://fbnhffmnn.de/80/80.OLD Element: server Method: GET Tags: interesting, response, server Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification? false References: w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html Variations ------- Variation 1: URL: http://fbnhffmnn.de/80/80.OLD ID: 301 [Regular expression: [+] [9] Trusted -- Interesting response ~~~~~~~~~~~~~~~~~~~~ ID Hash: S9ab60ab3aee674717f197e1b2e81437b716f83b1d796521b28668767f8f8e0a1 Severity: Informational URL: http://fbnhffmnn.de/80/c99shell.php Element: server Method: GET Tags: interesting, response, server Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.
The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however each HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.
and assist with the penetration test. [*] Requires manual verification?: false [*] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html [*] Variations [*] ------- [*] Variation 1: [*] URL: http://fbnhffmnn.de/80/cgi-bin/ [*] ID: Code: 301 [*] Regular expression: [+] Plugin data: [+] Resolution: [*] Description: Resolves vulnerable hostnames to IP addresses. [*] fbnhffmnn.de: 46.38.236.232 [*] Health map [*] ~~~~~~~~~~~~~ [*] Description: Generates a simple list of safe/unsafe URLs. [*] Legend: [+] No issues [-] Has issues [+] 5 issues were detected [+] 1 [Trust] - E-mail address disclosure [*] ~~~~~~~~~~~~~ [*] ID Hash: 4b8d77a6b1a1f0ba0754a21019c0d537ce45bbcd07d3b73ac59f0a465c001 [*] Severity: Informational [*] URL: https://46.38.236.232:443/ [*] Element: body [*] Method: GET [*] Tags: [+] Description: [+] Email addresses are typically found on 'Contact us' pages, however they can also be found within scripts or code comments of the application. They are used to provide a legitimate means of contacting an organisation. As one of the initial steps in information gathering, cyber-criminals will spider a website and using automated methods collect as many email addresses as possible, that they may then use in a social engineering attack against that user. Using the same automated methods, Arachni was able to detect one or more email addresses that were stored within the affected page. [*] CWE: http://cwe.mitre.org/data/definitions/200.html [*] Requires manual verification?: false [*] References: [~] Variations [*] ------- [*] Variation 1: [*] URL: https://46.38.236.232:443/ [*] Regular expression: (?:[^\s.]+\s+)?@([A-Za-z0-9.-]+)\.[A-Za-z]{2,6}(?:\.[A-Za-z]{2,6})? [+] 5 issues were detected [+] [Trust] - Email address disclosure [*] ~~~~~~~~~~~~~ [*] ID Hash: eecff07a0aaffee2867992d8c6c8cb51404e4ba3f406c413e6e4310b5f51c9d [*] Severity: Informational [*] URL: https://46.38.236.232:443/Arachni-98e04[*] Element: server [*] Method: PUT [*] Tags: interesting, response, server [*] Description: [+] The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. [*] Requires manual verification?: false [*] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html [*] Variations [*] ------- [*] Variation 1: [*] URL: https://46.38.236.232:443/Arachni-98e04[*] ID: Code: 405 [*] Regular expression: [+] [Trust] - Interesting response [*] ~~~~~~~~~~~~~ [*] ID Hash: b363f47965c930c8036e3b2be47ca5c4034a159dbb2f3372a7e4f491a116 [*] Severity: Informational [*] URL: https://46.38.236.232:443/ [*] Element: server [*] Method: TRACE [*] Tags: interesting, response, server [*] Description: [+] The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. [*] Requires manual verification?: false [*] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html [*] Variations [*] ------- [*] Variation 1: [*] URL: https://46.38.236.232:443/

---

[^] ID Hash: fa32e5efc9dc994951919aa4d74e7df421f7dabe74a664a6bd1dfff6139587c4f[^] Severity: Informational[^] URL: https://46.38.236.232:443/css/Arachni-98e04[^] Element: server[^] Method: PUT[^] Tags: interesting, response, server[^] Description:[^] The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[^] Requires manual verification?: false[^] References: [^] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations[^] ---[^] Variation 1:[^] URL: https://46.38.236.232:443/css/Arachni-98e04[^] ID: Code: 405[^] Regular expression: [+] [5] Trusted -- Interesting response[^]

---

**Host Issue Summary**

<table>
<thead>
<tr>
<th>Host</th>
<th>Analysis</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>63.230.176.46 (etsio-prod.cnf.com)</td>
<td>Medium risk</td>
<td>11</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>13.1</td>
</tr>
</tbody>
</table>

**Open Listening Ports**

<table>
<thead>
<tr>
<th>Service (Port)</th>
<th>Analysis</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Total CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>https (443/tcp)</td>
<td>Medium risk</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4.3</td>
</tr>
<tr>
<td>pharos (4443/tcp)</td>
<td>Medium risk</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4.3</td>
</tr>
<tr>
<td>icht3 (4080/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>unknown (9443/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/tcp</td>
<td>Log risk</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>ftp (21/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.9</td>
</tr>
<tr>
<td>general/CPE-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/HOST-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>rockwell-csp2 (2222/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>ssh (22/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>unknown (5443/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

**Security Issues**

- **Medium (CVSS: 4.3)**
  - **https (443/tcp)**

  NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

  Summary: This routine search for weak SSL ciphers offered by a service. Vulnerability Insight: These rules are applied for the
evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks. - Any cipher considered to be secure for only the next 10 years is considered as medium. - Any other cipher is considered as strong.

Solution: The configuration of this service should be changed so that it does not support the listed weak ciphers anymore.

Weak ciphers offered by this service:
- SSL3_RSA_RC4_40_MD5
- SSL3_RSA_RC4_128_MD5
- SSL3_RSA_DES_40_CBC_SHA
- SSL3_RSA_DES_64_CBC_SHA
- SSL3_EDH_RSA_DES_64_CBC_SHA
- SSL3_ECDHE_RSA_WITH_RC4_128_SHA
- TLS1_RSA_RC4_40_MD5
- TLS1_RSA_RC4_128_MD5
- TLS1_RSA_RC4_128_SHA
- TLS1_RSA_DES_40_CBC_SHA
- TLS1_RSA_DES_64_CBC_SHA
- TLS1_EDH_RSA_DES_40_CBC_SHA
- TLS1_EDH_RSA_DES_64_CBC_SHA
- TLS1_ECDHE_RSA_WITH_RC4_128_SHA
- TLS1_RSA_RC4_40_MD5
- TLS1_RSA_RC4_128_MD5
- TLS1_RSA_RC4_128_SHA
- TLS1_RSA_DES_40_CBC_SHA
- TLS1_RSA_DES_64_CBC_SHA
- TLS1_EDH_RSA_DES_40_CBC_SHA
- TLS1_EDH_RSA_DES_64_CBC_SHA
- TLS1_ECDHE_RSA_WITH_RC4_128_SHA

Medium (CVSS: 4.3)

pharos (4443/tcp)

Summary: This routine search for weak SSL ciphers offered by a service. Vulnerability Insight: These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks. - Any cipher considered to be secure for only the next 10 years is considered as medium. - Any other cipher is considered as strong.

Solution: The configuration of this service should be changed so that it does not support the listed weak ciphers anymore.

Weak ciphers offered by this service:
- SSL3_RSA_RC4_40_MD5
- SSL3_RSA_RC4_128_MD5
- SSL3_RSA_DES_40_CBC_SHA
- SSL3_RSA_DES_64_CBC_SHA
- SSL3_EDH_RSA_DES_64_CBC_SHA
- SSL3_ECDHE_RSA_WITH_RC4_128_SHA
- TLS1_RSA_RC4_40_MD5
- TLS1_RSA_RC4_128_MD5
- TLS1_RSA_RC4_128_SHA
- TLS1_RSA_DES_40_CBC_SHA
- TLS1_RSA_DES_64_CBC_SHA
- TLS1_EDH_RSA_DES_40_CBC_SHA
- TLS1_EDH_RSA_DES_64_CBC_SHA
- TLS1_ECDHE_RSA_WITH_RC4_128_SHA

Medium (CVSS: 2.6)

general/tcp

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 second in-between: Paket 1: 1853447401 Paket 2: 1853448653

Low (CVSS: 0.0)

https (443/tcp)

NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

Here is the arachni report: https://63.230.176.46:443/[


Low (CVSS: 0.0)

ichat3 (4080/tcp)

NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

Here is the arachni report: https://63.230.176.46:443/[


PROPRIETARY & CONFIDENTIAL
Vulnerability Scan Detail Report

SECURITY ASSESSMENT

PROPRIETARY & CONFIDENTIAL

PAGE 18 of 26

positives at: http://github.com/Arachni/arachni/issues[

System settings: [ ] Version: 0.4.7 [ ] Revision: 0.2.8
Audit started on: Fri Jul 25 18:11:28 2014 [ ] Audit finished on: Fri Jul 25 18:11:37 2014 [ ] Runtime: 00:00:08
Audited elements: [ ] * Links [ ] * Forms [ ] * Cookies
Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sql, sql盲_injection_timing, file_inclusion, response_splitting, sql盲_rdiff, code_injection_php_input_wrapper, os_cmd_injection_timing, xss_tag, xpath, xss_path, session_fixation, xss_event, unvalidated_redirect, code_injection_timing, xss, ldap, rfi, csrf, unencrypted_password_forms, cvs_svn_users, http_only_cookies, html_objects, form_upload, captcha, mixed_resource, credit_card, private_ip, emails, insecure_cookies, ssn, password_autocomplete, localstart_asp, common_files, allowed_methods, backup_files, http_put, backdoors, common_directories, directory_listing, webdav, interesting_responses, x_forwarded_for_access_restriction_bypass, htaccess_limit, xst

0 issues were detected.

Plugin data: [ ] [ ] [ ] Health map [ ] [ ] [ ] Description: Generates a simple list of safe/unsafe URLs.
Legend: [ ] No issues [-] Has issues
http://63.230.176.46:4080/ Total: 1 [+] Without issues: 1 [-] With issues: 0 (0%)

Low (CVSS: 0.0)
NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

Here is the arachni report: 

Web Application Security Report - Arachni Framework
Audit started on: Fri Jul 25 18:14:07 2014
Audit finished on: Fri Jul 25 18:14:45 2014
Runtime: 00:00:38
URL: https://63.230.176.46:9443/
User agent: arachni
Audited elements: [ ] * Links [ ] * Forms [ ] * Cookies
Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sql, sql盲_injection_timing, file_inclusion, response_splitting, sql盲_rdiff, code_injection_php_input_wrapper, os_cmd_injection_timing, xss_tag, xpath, xss_path, session_fixation, xss_event, unvalidated_redirect, code_injection_timing, xss, ldap, rfi, csrf, unencrypted_password_forms, cvs_svn_users, http_only_cookies, html_objects, form_upload, captcha, mixed_resource, credit_card, private_ip, emails, insecure_cookies, ssn, password_autocomplete, localstart_asp, common_files, allowed_methods, backup_files, http_put, backdoors, common_directories, directory_listing, webdav, interesting_responses, x_forwarded_for_access_restriction_bypass, htaccess_limit, xst

0 issues were detected.

Plugin data: [ ] [ ] [ ] Health map [ ] [ ] [ ] Description: Generates a simple list of safe/unsafe URLs.
Legend: [ ] No issues [-] Has issues
https://63.230.176.46:9443/ Total: 1 [+] Without issues: 1 [-] With issues: 0 (0%)

unknown (9443/tcp)
2.4 - 176.28.51.58 (rs208305.rs.hosteurope.de)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Analysis</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.28.51.58 (rs208305.rs.hosteurope.de)</td>
<td>High risk</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>14.4</td>
</tr>
</tbody>
</table>

Open Listening Ports

<table>
<thead>
<tr>
<th>Service (Port)</th>
<th>Analysis</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Total CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>https (443/tcp)</td>
<td>High risk</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>11.8</td>
</tr>
<tr>
<td>http (80/tcp)</td>
<td>Low risk</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/tcp</td>
<td>Log risk</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>general/CPE-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/HOST-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/icmp</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>ssh (22/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Security Issues

**High (CVSS: 7.5)**

NVT: phpinfo.php (OID: 1.3.6.1.4.1.25623.1.0.11229)

The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker:

```
/info.php Solution: Delete them or restrict access to them
```

**Medium (CVSS: 4.3)**

NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary: This routine search for weak SSL ciphers offered by a service. Vulnerability Insight: These rules are applied for the evaluation of the cryptographic strength:- Any SSL/TLS using no cipher is considered weak.- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.- RC4 is considered to be weak.- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.- 1024 bit RSA authentication is considered to be insecure and therefore as weak.- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks- Any cipher considered to be secure for only the next 10 years is considered as medium- Any other cipher is considered as strong
Solution: The configuration of this services should be changed so that it does not support the listed weak ciphers anymore. Weak ciphers offered by this service: SSL3_RSA_RC4_40_MD5 SSL3_RSA_RC4_128_MD5 SSL3_RSA_RC4_128_SHA SSL3_RSA_RC2_40_MD5 SSL3_RSA_DES_CBC_SHA SSL3_RSA_DES_64_CBC_SHA SSL3_RSA_DES_60_CBC_SHA SSL3_EDH_RSA_DES_64_CBC_SHA SSL_RSA_WITH_SEED_SHA TLS1_RSA_RC4_40_MD5 TLS1_RSA_RC4_40_SHA TLS1_RSA_RC4_128_SHA TLS1_RSA_DES_40_CBC_SHA TLS1_RSA_DES_40_CBC_SHA TLS1_RSA_DES_64_CBC_SHA TLS1_EDH_RSA_DES_40_CBC_SHA TLS1_EDH_RSA_DES_64_CBC_SHA

Vulnerability Scan Detail Report
SECURITY ASSESSMENT

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 629800840 Paket 2: 629801166

---

VARIATIONS

Variation 1:

- **URL:** http://rs208305.rs.hosteurope.de/80/?%3Cmy_tag_7bb8a2f05f74ee44ad7c6299b0ec7fd51ac94c94fabe6225752b6f5f35ce5e6/%3E=

  - **ID:** 766dfcbb1fa97398e356c4fc03846ed9121394dc5416ad2c7e67564b2c7882f5
  - **Severity:** Informational
  - **URL:** http://rs208305.rs.hosteurope.de/80/?%3Cmy_tag_7bb8a2f05f74ee44ad7c6299b0ec7fd51ac94c94fabe6225752b6f5f35ce5e6/%3E=
  - **Element:** server
  - **Method:** GET
  - **Tags:** interesting, response, server
  - **Description:** The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP responses status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification?: false
  - **References:**

Variation 2:

- **URL:** http://rs208305.rs.hosteurope.de/80/7bb8a2f05f74ee44ad7c6299b0ec7fd51ac94c94fabe6225752b6f5f35ce5e6

  - **ID:** ff387b6b2c98855c24b31de0efcd7b7fa17e0c83a707ca6930d8973b3b7f47a4
  - **Severity:** Informational
  - **URL:** http://rs208305.rs.hosteurope.de/80/7bb8a2f05f74ee44ad7c6299b0ec7fd51ac94c94fabe6225752b6f5f35ce5e6
  - **Element:** server
  - **Method:** GET
  - **Tags:** interesting, response, server
  - **Description:** The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification?: false
  - **References:**

---

Here is the arachni report:===============================================================================
NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

Low (CVSS: 0.0)
NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

Here is the arachni report:

```plaintext

<table>
<thead>
<tr>
<th>ID</th>
<th>Code</th>
<th>Regular expression</th>
<th>Type</th>
<th>severity</th>
<th>Details</th>
</tr>
</thead>
</table>
| 2  | 301   | (+) [2] Trusted -- Interesting response | (+) | Low |...

```
http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/robots.txt [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] ----- ---- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/sitemap.xml [*] ID: Code: 301 [*] Regular expression: [*] [+] [5] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: e1d8637bfda16bb6b2c720df57e9d98fa580ce232c038a6e39361e5b5700 [*] Severity: Informational [*] URL: http://rs208305.rs.hosteurope.de/80/sitemap.xml.gz [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/sitemap.xml.gz [*] ID: Code: 301 [*] Regular expression: [*] [+] [7] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: fe1478030854a1baa0691c8ab803050c4390316264ec1e29fa2f3f2887280fc6 [*] Severity: Informational [*] URL: http://rs208305.rs.hosteurope.de/80/sitemap.xml.gz [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/sitemap.xml.gz [*] ID: Code: 301 [*] Regular expression: [*] [+] [9] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: e1d8637bfda16bb6b2c720df57e9d98fa580ce232c038a6e39361e5b5700 [*] Severity: Informational [*] URL: http://rs208305.rs.hosteurope.de/80/CVS/Repository [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/CVS/Repository [*] ID: Code: 301 [*] Regular expression: [*] [+] [10] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: 3e2b54b21d5fca480db9eb17536c0366fa1a5ea7e7c0ff19afa4c857ff8c6f01 [*] Severity: Informational [*] URL: http://rs208305.rs.hosteurope.de/80/CVS/Repository [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/CVS/Repository [*] ID: Code: 301 [*] Regular expression: [*] [+] [11] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: fe1478030854a1baa0691c8ab803050c4390316264ec1e29fa2f3f2887280fc6 [*] Severity: Informational [*] URL: http://rs208305.rs.hosteurope.de/80/CVS/Repository [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/CVS/Repository [*] ID: Code: 301 [*] Regular expression: [*] [+] [12] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: ae667c5da6e67d3b8b9c847779ef1b8cdce1637d7e50bb0b4cb028be118d1a759 [*] Severity: Informational [*] URL: http://rs208305.rs.hosteurope.de/80/svn/wc.db [*] Element: server [*] Method: GET [*] Tags: interesting, response, server [*] Description: The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[*] Requires manual verification?: false References: [*] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*] Variations [*] -------- [*] Variation 1: [*] URL: http://rs208305.rs.hosteurope.de/80/svn/wc.db [*] ID: Code: 301 [*] Regular expression: [*] [+] [13] Trusted -- Interesting response [*] ------------------------------- [*] ID Hash: d003afa36687e27b1bf080ae5e47obbe9fc462f7e1af2de5986ec412172380 [*] Severity: Informational [*] URL:
however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification?: false References: [~] Severity: Informational
Variations: [~] --- Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/phpinfo.php [~] ID: Code: 301 [~] Regular expression: [+] [22] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~ [~] ID Hash: ced2f1bc35b181d1bdcdd5b8d62964c060d7ab2c31d5f6f97d90a9a992a109d [~] Severity: Informational
URL: http://rs208305.rs.hosteurope.de/80/config.php [~] Element: server [~] Method: GET [~] Tags: interesting, response, server [~] Description: [~] The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification?: false References: [~] Severity: Informational
Variations: [~] --- Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/config.php [~] ID: Code: 301 [~] Regular expression: [+] [23] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~ [~] ID Hash: 820e04ea16419e61b91b06c8bf4aaea7afa4f253db7e458de1902c5250a8c [~] Severity: Informational
URL: http://rs208305.rs.hosteurope.de/80/7bb8a2f05f74e44ad7c629d9b0e76f5f35f5e6 [~] Element: server [~] Method: GET [~] Tags: interesting, response, server [~] Description: [~] The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test. Requires manual verification?: false References: [~] Severity: Informational
Variations: [~] --- Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/error_log [~] ID: Code: 301 [~] Regular expression: [+] [24] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~ [~] ID Hash: 820e04ea16419e61b91b06c8bf4aaea7afa4f253db7e458de1902c5250a8c [~] Severity: Informational
URL: http://rs208305.rs.hosteurope.de/80/config.php [~] ID: Code: 301 [~] Regular expression: [+] [25] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~ [~] ID Hash: 820e04ea16419e61b91b06c8bf4aaea7afa4f253db7e458de1902c5250a8c
Summary: Remote web server does not reply with 404 error code. Vulnerability Insight: This web server is [mis]configured in that it does not return ‘404 Not Found’ error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead. OpenVAS enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate This web server is [mis]configured in that it does not return ‘404 Not Found’ error codes when a non-existent file is requested, perhaps returning a site map,
search page or authentication page instead. CGI scanning will be disabled for this host.
2.5 - 193.23.123.40 (rev-040.snrm.fr)

Host Issue Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Analysis</th>
<th>Open Ports</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>193.23.123.40 (rev-040.snrm.fr)</td>
<td>High risk</td>
<td>9</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>27.0</td>
</tr>
</tbody>
</table>

Open Listening Ports

<table>
<thead>
<tr>
<th>Service (Port)</th>
<th>Analysis</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>False</th>
<th>Total CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>http (80/tcp)</td>
<td>High risk</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>15.1</td>
</tr>
<tr>
<td>https (443/tcp)</td>
<td>High risk</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>9.3</td>
</tr>
<tr>
<td>ftp (21/tcp)</td>
<td>Medium</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>general/CPE-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>general/HOST-T</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>imap (143/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>pop3 (110/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>smtp (25/tcp)</td>
<td>Log risk</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

Security Issues

**High (CVSS: 5.8) - http (80/tcp)**

**NVT: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213)**

Summary: Debugging functions are enabled on the remote HTTP server. Description: The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution: Disable these methods. Plugin output: Solution: Add the following lines for each virtual host in your configuration file: `RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)$ RewriteRule .* - [F]` See also [http://httpd.apache.org/docs/current/de/mod/core.html#traceenable](http://httpd.apache.org/docs/current/de/mod/core.html#traceenable)
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVSS</th>
<th>Protocol</th>
<th>NVT Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Medium (CVSS: 5.0)</strong></td>
<td></td>
<td>http (80/tcp)</td>
<td><strong>Apache /server-status accessible (OID: 1.3.6.1.4.1.25623.1.0.10677)</strong></td>
</tr>
<tr>
<td><strong>Summary</strong>: Leak of information in Apache. <strong>Vulnerability Detection</strong>: Check if /server-status page exist. <strong>Vulnerability Insight</strong>: server-status is a built-in Apache HTTP Server handler used to retrieve the server's status report. <strong>Impact</strong>: Requesting the URI /server-status gives information about the currently running Apache. <strong>Affected Software/OS</strong>: All Apache version. <strong>Solution</strong>: If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>High (CVSS: 5.0)</strong></td>
<td></td>
<td>https (443/tcp)</td>
<td><strong>OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103936)</strong></td>
</tr>
<tr>
<td><strong>Summary</strong>: OpenSSL is prone to an information disclosure vulnerability. <strong>Vulnerability Detection</strong>: Send a special crafted TLS request and check the response. <strong>Vulnerability Insight</strong>: The TLS and DTLS implementations do not properly handle Heartbeat Extension packets. <strong>Impact</strong>: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks. <strong>Affected Software/OS</strong>: OpenSSL 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, and 1.0.1 are vulnerable. <strong>Solution</strong>: Updates are available.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Medium (CVSS: 4.3)</strong></td>
<td></td>
<td>http (80/tcp)</td>
<td><strong>Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)</strong></td>
</tr>
<tr>
<td><strong>Summary</strong>: A weakness has been discovered in Apache web servers that are configured to use the FileETag directive. Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number. <strong>Exploitation</strong>: Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information. <strong>Solution</strong>: OpenBSD has released a patch that addresses this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details. <strong>Information gathered</strong>: Inode: 139518 Size: 6421</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Medium (CVSS: 4.3)</strong></td>
<td></td>
<td>https (443/tcp)</td>
<td><strong>Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)</strong></td>
</tr>
<tr>
<td><strong>Summary</strong>: This routine search for weak SSL ciphers offered by a service. <strong>Vulnerability Insight</strong>: These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS &lt; 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks. Any cipher considered to be secure for only the next 10 years is considered as medium. Any other cipher is considered as strong. <strong>Solution</strong>: The configuration of this services should be changed so that it does not support the listed weak ciphers anymore. <strong>Weak ciphers offered by this service</strong>: SSL3_RSA_RC4_40_MD5 SSL3_RSA_RC4_128_MD5 SSL3_RSA_RC4_128_SHA SSL3_RSA_RC2_40_MDS SSL3_RSA_DES_40_CBC_SHA SSL3_RSA_DES_64_CBC_SHA SSL3_EDH_RSA_DES_64_CBC_SHA SSL3_RSA_WITH_SEED_SHA TLS1_RSA_RC4_40_MDS TLS1_RSA_RC4_128_MDS TLS1_RSA_RC4_128_SHA TLS1_RSA_RC2_40_MDS TLS1_RSA_DES_40_CBC_SHA TLS1_RSA_DES_64_CBC_SHA TLS1_EDH_RSA_DES_40_CBC_SHA TLS1_EDH_RSA_DES_64_CBC_SHA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Medium (CVSS: 2.6)</strong></td>
<td></td>
<td>general/tcp</td>
<td><strong>TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)</strong></td>
</tr>
<tr>
<td><strong>Summary</strong>: It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds between: Paket 1: 1274025501 Paket 2: 1274025623</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>