Visualnet Media Inc.

HIPAA Assessment

External Vulnerability Scan Detail Report

Scan Date: 4/1/2014

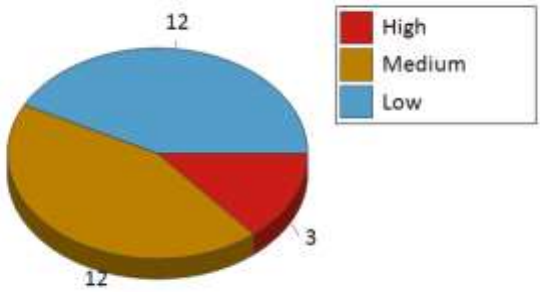
Prepared for:
Customer Name Here!
Prepared by:
YourIT! Company, Inc.

Table of Contents

1 - Summary
2 - Details
    2.1 - 42.62.65.25
    2.2 - 46.38.236.232 (fbnhffmnn.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)

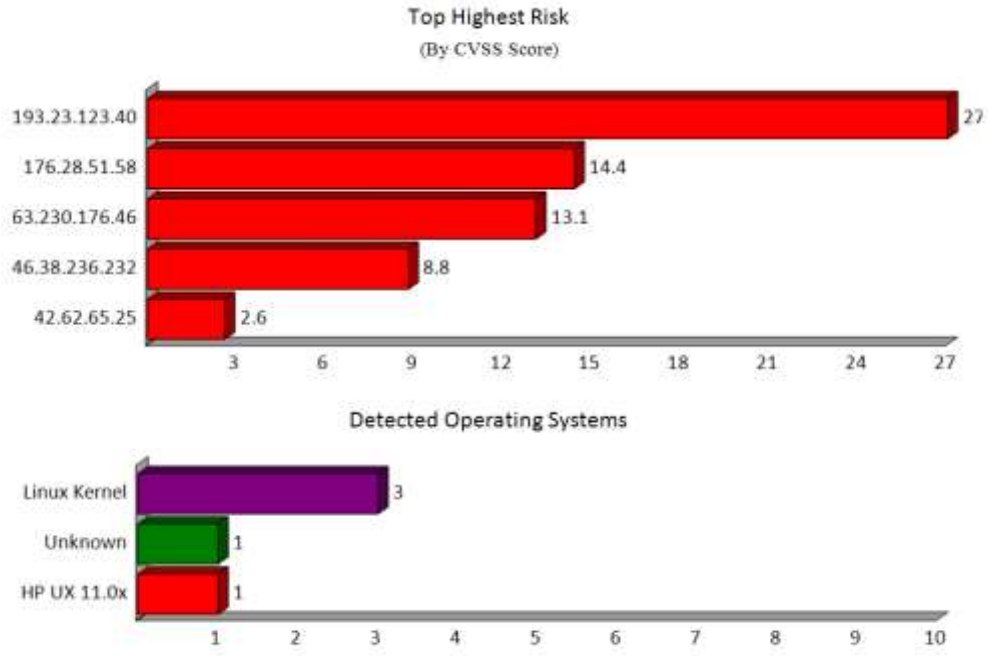
1 - Summary

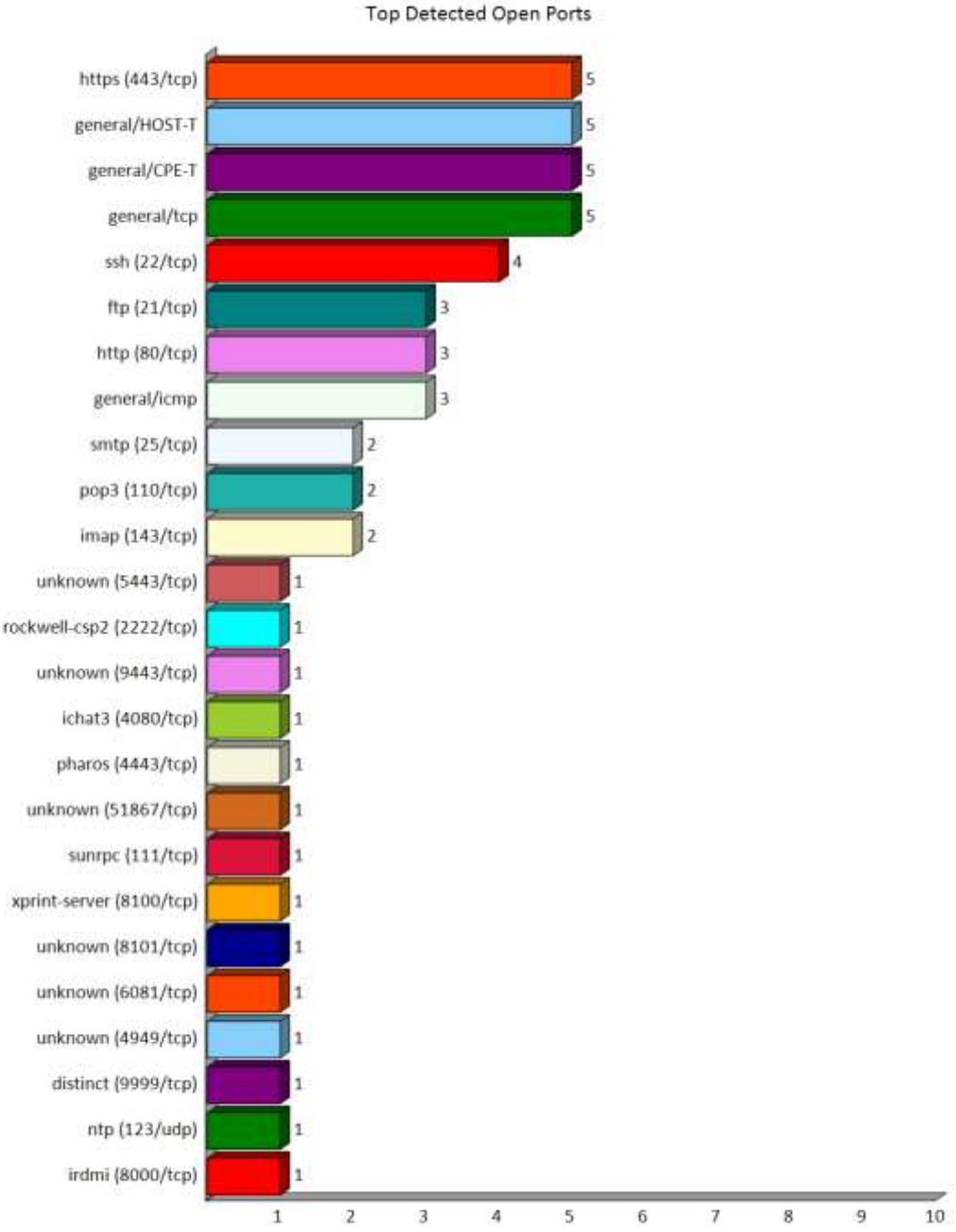
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.



Host Issue Summary

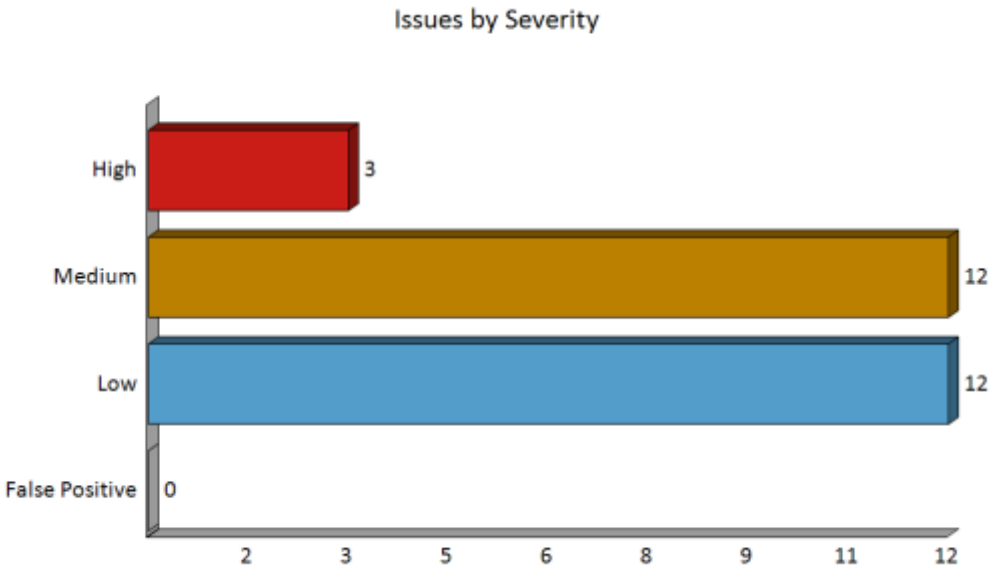
Host	Analysis	Open Ports	High	Med	Low	False	CVSS
42.62.65.25	Medium risk	14	0	1	3	0	2.6
46.38.236.232 (fbnhffmnn.de)	Medium risk	13	0	2	4	0	8.8
63.230.176.46 (etsio-prod.cnf.com)	Medium risk	11	0	3	3	0	13.1
176.28.51.58 (rs208305.rs.hosteurope.de)	**High risk**	7	**1**	2	2	0	14.4
193.23.123.40 (rev-040.snrm.fr)	**High risk**	9	**2**	4	0	0	27.0
Total: 5	**High risk**	54	**3**	**12**	12	0	65.9



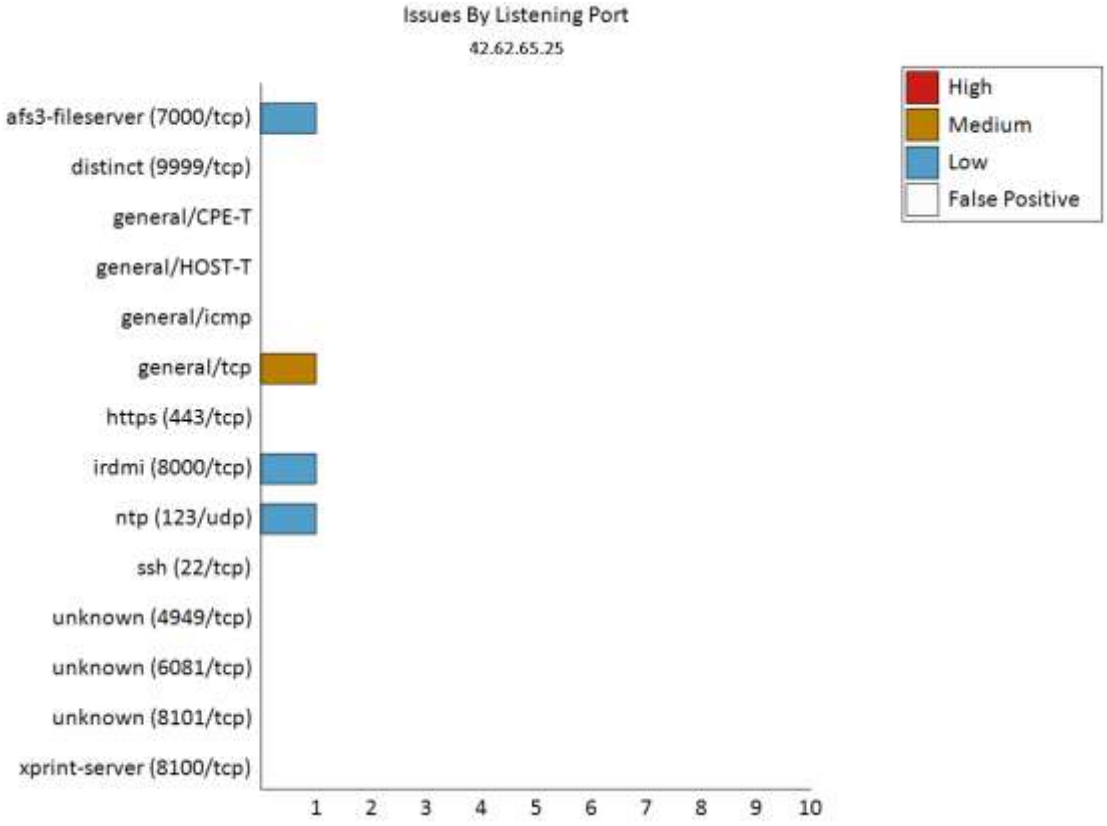

Top Detected Open Ports
https (443/tcp) 5
general/HOST-T 5
general/CPE-T 5
general/tcp 5
ssh (22/tcp) 4
ftp (21/tcp) 3
http (80/tcp) 3
general/icmp 3
smtp (25/tcp) 2
pop3 (110/tcp) 2
imap (143/tcp) 2
unknown (5443/tcp) 1
rockwell-csp2 (2222/tcp) 1
unknown (9443/tcp) 1
ichat3 (4080/tcp) 1
pharos (4443/tcp) 1
unknown (51867/tcp) 1
sunrpc (111/tcp) 1
xprint-server (8100/tcp) 1
unknown (8101/tcp) 1
unknown (6081/tcp) 1
unknown (4949/tcp) 1
distinct (9999/tcp) 1
ntp (123/udp) 1
irdmi (8000/tcp) 1
1 2 3 4 5 6 7 8 9 10


Top Detected Open Ports (continued)
afs3-fileserver (7000/tcp) 1
1 2 3 4 5 6 7 8 9 10

2 - Scan Details



2.1 - 42.62.65.25



Host Issue Summary

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
42.62.65.25	Medium risk	14	0	1	3	0	2.6

Open Listening Ports

Service (Port)	Analysis	High	Med	Low	False	Total CVSS
afs3-fileserver (7000/tcp)	Low risk	0	0	1	0	0.0
irdmi (8000/tcp)	Low risk	0	0	1	0	0.0
ntp (123/udp)	Low risk	0	0	1	0	0.0
general/tcp	Log risk	0	1	0	0	2.6
distinct (9999/tcp)	Log risk	0	0	0	0	0.0
general/CPE-T	Log risk	0	0	0	0	0.0
general/HOST-T	Log risk	0	0	0	0	0.0
general/icmp	Log risk	0	0	0	0	0.0
https (443/tcp)	Log risk	0	0	0	0	0.0
ssh (22/tcp)	Log risk	0	0	0	0	0.0
unknown (4949/tcp)	Log risk	0	0	0	0	0.0
unknown (6081/tcp)	Log risk	0	0	0	0	0.0
unknown (8101/tcp)	Log risk	0	0	0	0	0.0
xprint-server (8100/tcp)	Log risk	0	0	0	0	0.0

Security Issues

Medium (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

It was detected that the host implements RFC1323.The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1609483043 Paket 2: 1609483387

Low (CVSS: 0.0) afs3-fileserver (7000/tcp)
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[~] Report generated on: 2014-09-25 16:33:26 +0000 [~] Report false positives at: http://github.com/Arachni/arachni/issues[+] System settings: [~] ---------- [~] Version: 0.4.7 [~] Revision: 0.2.8 [~] Audit started on: Thu Sep 25 16:32:54 2014 [~] Audit finished on: Thu Sep 25 16:33:23 2014 [~] Runtime: 00:00:28[~] URL: http://42.62.65.25:7000/ [~] User agent: arachni[*] Audited elements: [~] * Links [~] * Forms [~] * Cookies[*] Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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[~] ==========[+] 1 issues were detected.[+] [1] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 6a3d62951e1128033852bef201ea5cb581a6f92e79c30ac35e9d693f61da7342 [~] Severity: Informational [~] 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[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://42.62.65.25:7000/ [~] ID: Code: 405 [~] Regular expression: [+] Plugin data: [~] ---------- [*] Resolver [~] ~~~~~~~~~~~~~~~ [~] Description: Resolves vulnerable hostnames to IP addresses.[~] 42.62.65.25: 42.62.65.25[*] Health map [~] ~~~~~~~~~~~~~~~ [~] Description: Generates a simple list of safe/unsafe URLs.[~] Legend: [+] No issues [-] Has issues[-] http://42.62.65.25:7000/[~] Total: 1 [+] Without issues: 0 [-] With issues: 1 (100%)

Low (CVSS: 0.0) irdmi (8000/tcp)
NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

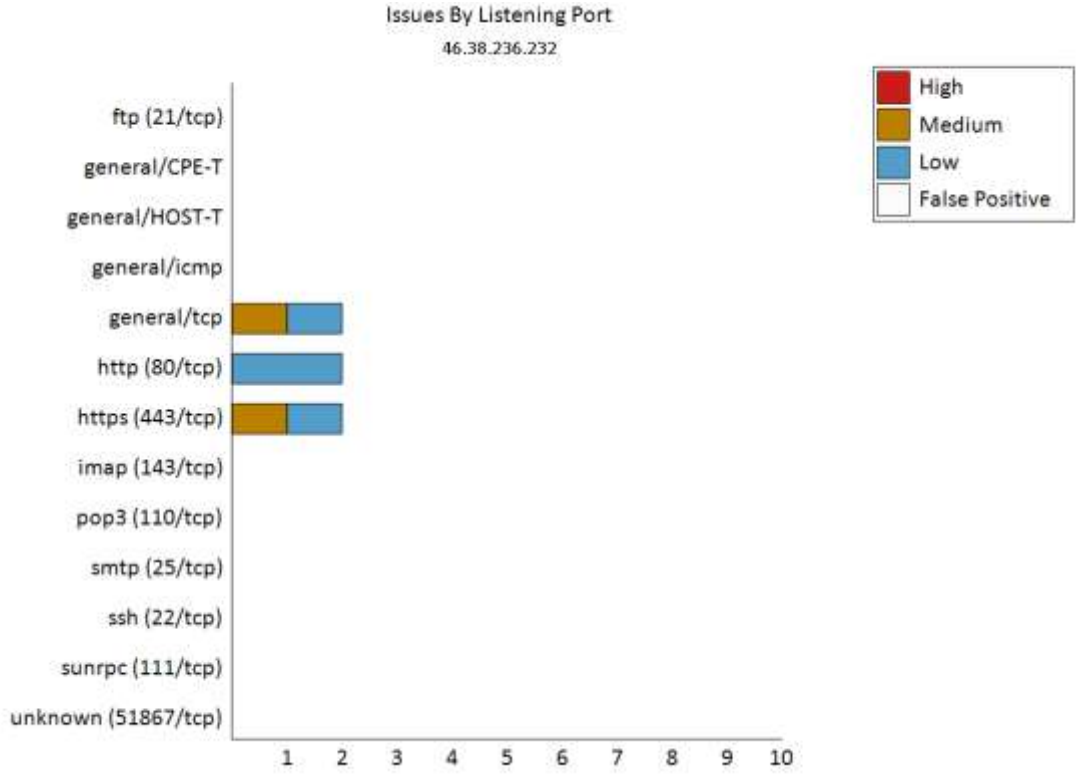
Here is the arachni report: == [+] Web Application Security Report - Arachni Framework[~] Report generated on: 2014-09-25 16:35:08 +0000 [~] Report false positives at: http://github.com/Arachni/arachni/issues[+] System settings: [~] ---------- [~] Version: 0.4.7 [~] Revision: 0.2.8 [~] Audit started on: Thu Sep 25 16:34:47 2014 [~] Audit finished on: Thu Sep 25 16:35:05 2014 [~] Runtime: 00:00:18[~] URL: http://42.62.65.25:8000/ [~] User agent: arachni[*] Audited elements: [~] * Links [~] * Forms [~] * Cookies[*] Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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[~] ==========[+] 2 issues were detected.[+] [1] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 0a297e1aecbb0835aa1e92a5100a1d7aefca4c0f18ac75ddfcfb0239fe50faab [~] Severity: Informational [~] URL: http://42.62.65.25:8000/%3Cmy_tag_7dddfff9e894138cd0d314d9091443aea30b51a7051eb3d32b20d60676ebf19a/%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://42.62.65.25:8000/%3Cmy_tag_7dddfff9e894138cd0d314d9091443aea30b51a7051eb3d32b20d60676ebf19a/%3E [~] ID: Code: 400 [~] Regular expression: [+] [2] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~ [~] ID Hash: db2c372bc9865bfb3da31ef719acf953a7191de47e593b3b1e8d51d87db43685 [~] 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.[~] Requires manual verification?: false[~] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] 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[*] Health map [~] ~~~~~~~~~~~~~~~ [~] 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_7dddfff9e894138cd0d314d9091443aea30b51a7051eb3d32b20d60676ebf19a/%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.

2.2 - 46.38.236.232 (fbnhffmnn.de)



Host Issue Summary

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
46.38.236.232 (fbnhffmnn.de)	Medium risk	13	0	2	4	0	8.8

Open Listening Ports

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

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 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

Medium (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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

Low (CVSS: 0.0) general/tcp
NVT: ProFTPD Server Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900815)

ProFTPD version 1.3.4.a was detected on the host

Low (CVSS: 0.0) http (80/tcp)
NVT: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

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.

Low (CVSS: 0.0) http (80/tcp)
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[~] 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, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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: 01b12e85e60cb3fdd174b19a19c485895d9aa8e337404230a01b982c618e278f [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/%3E%22'%3E%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%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'%3E%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%3E [~] ID: Code: 301 [~] Regular expression: [+] [2] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash:

9e48cc7be737ecae2f6c8ba664beafc62c0acb3e99d3595ae21e37b8e18d8e55 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%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/%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%3E [~] ID: Code: 301 [~] Regular expression: [+] [3] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 7c3295cd1b9694e74b0b99118ca971793a44bc6598629bfa931202fcbdf7e136 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/?%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%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/?%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%3E= [~] ID: Code: 301 [~] Regular expression: [+] [4] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 93a8c7aac76b491a94a8331fb2707766ea76bf70fb20f9bf714f685915175771 [~] 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: Code: 301 [~] Regular expression: [+] [5] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 3897a9e075084bdee46273474b3d6cd380f1744fa1d23d1501e27aa6c7a553c6 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/sitemap.xml [~] 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/sitemap.xml [~] ID: Code: 301 [~] Regular expression: [+] [6] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 8bd64c28cbde59afdc63f7632358d5fb249144873e22b34b8097fd2efb8a9f96 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/.git/HEAD [~] 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/.git/HEAD [~] ID: Code: 301 [~] Regular expression: [+] [7] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: c7bd9b523c62a3ab632d63e8318cb8b7738a3eb9d1430f8ad493b9bd3deebddf [~] 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: Code: 301 [~] Regular expression: [+] [8] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 191b552ed98358994d1b182b4d71d5c63e6f41be12c120f6f771ca1576d8b01d [~] 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: Code: 301 [~] Regular expression: [+] [9] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 59ab60ab3aed67471f19ce7bbe81437fb716f83b1d796521b286e87698f8e0a1 [~] 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.[~] Requires manual verification?: false[~] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/c99shell.php [~] ID: Code: 301 [~] Regular expression: [+] [10] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: db66d5e2adfcad2206157641bcf7c2a8cd53f1b0c43853f9c0e49cbc3ce400fd [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/c99.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/c99.php [~] ID: Code: 301 [~] Regular expression: [+] [11] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 9c777caccaf195e579f3a0ea5d18d6e1000f177193cb17cf9fdb774fcad92d68 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/nstview.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/nstview.php [~] ID: Code: 301 [~] Regular expression: [+] [12] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: a14571190f2387ec650f28ee9328280195836b3003f2dc87e5364c7dc81b66b9 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/zehir.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/zehir.php [~] ID: Code: 301 [~] Regular expression: [+] [13] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 1bc4c1545b21a06cb2f1e252e52a8b79f6df413a5abfcccdf412d42519a2d3b8 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/c-h.v2.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/c-h.v2.php [~] ID: Code: 301 [~] Regular expression: [+] [14] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 6b4f79798019d873d32637755b314cd2f5cd6acf97996a875e1cdac589379a2d [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/nst.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/nst.php [~] ID: Code: 301 [~] Regular expression: [+] [15] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 4bf3e6968a764a1a1346ba7c155beb845ed7fa5bb145c22afce2210481989e19 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/rst.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/rst.php [~] ID: Code: 301 [~] Regular expression: [+] [16] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: fd338afe71b1e2358c1a44dcdc00e8cd36ca640227270729e2e1e2441a13920f [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/r57eng.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/r57eng.php [~] ID: Code: 301 [~] Regular expression: [+] [17] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 9f89c9969149010f96e1bf3b92974cd043970c4ffbe9485c24822366e207988b [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/shell.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/shell.php [~] ID: Code: 301 [~] Regular expression: [+] [18] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 84e9c085bc304802277f8864c66c1f4ee93257a7b51d041465776bfd09d9fde2 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/r.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/r.php [~] ID: Code: 301 [~] Regular expression: [+] [19] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 5481cf79e34410338807df8608c741155993b1d95d50155f6590ccc2aaabdbd6 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/lol.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/lol.php [~] ID: Code: 301 [~] Regular expression: [+] [20] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 81c3cd61a418458e7f2494f7e961a78513f8c6a438f18aa2e0278fec654976f7 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/php-backdoor.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/php-backdoor.php [~] ID: Code: 301 [~] Regular expression: [+] [21] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: d05ad15fd347d7278976ec2acce7e1ea17e7089a30c8470f916f57402c605083 [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/cmdasp.asp [~] 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/cmdasp.asp [~] ID: Code: 301 [~] Regular expression: [+] [22] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 7d2b600dfbe3c93f902045cffabeba9b4de47487286bb0167cc5ee256dbf70da [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/simple-backdoor.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/simple-backdoor.php [~] ID: Code: 301 [~] Regular expression: [+] [23] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: dc413594cf47a20800434c8c4d225825b7b815860fe40ab6e2976799ee1fb3fd [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/_private/ [~] 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/_private/ [~] ID: Code: 301 [~] Regular expression: [+] [24] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 40004a9461201c4e6952d38ec87d036b6925380b9efaa0618f024d163441667c [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/_vti_bin/ [~] 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/_vti_bin/ [~] ID: Code: 301 [~] Regular expression: [+] [25] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 03206ca2039692d6fedc5c82d19de69b180929d8b3c6f7d7ae5fb642c6a7737b [~] Severity: Informational [~] URL: http://fbnhffmnn.de/80/cgi-bin/ [~] 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

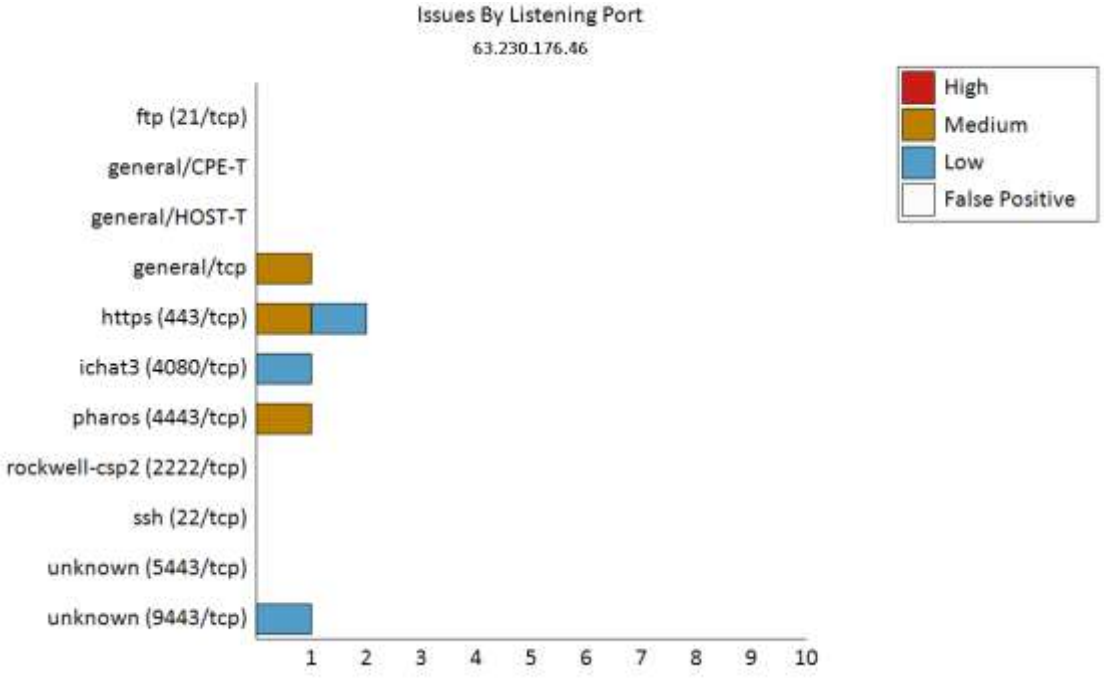
and assist with the penetration test.[~] Requires manual verification?: false[~] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://fbnhffmnn.de/80/cgi-bin/ [~] ID: Code: 301 [~] Regular expression: [+] Plugin data: [~] ---------- [*] Resolver [~] ~~~~~~~~~~~~~~~ [~] 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[+] http://fbnhffmnn.de/80 [+] https://fbnhffmnn.de/80 [-] http://fbnhffmnn.de/80/%3E%22'%3E%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%3E [-] http://fbnhffmnn.de/80/%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%3E [-] http://fbnhffmnn.de/80/?%3Cmy_tag_15fe8696070fc1bc16ab11f89b6d81e26a15bc2c52dd349ccef321ec4682fb54/%3E= [-] http://fbnhffmnn.de/80/robots.txt [-] http://fbnhffmnn.de/80/sitemap.xml [-] http://fbnhffmnn.de/80/.git/HEAD [-] http://fbnhffmnn.de/80/error_log [-] http://fbnhffmnn.de/80/80.OLD [-] http://fbnhffmnn.de/80/c99shell.php [-] http://fbnhffmnn.de/80/c99.php [-] http://fbnhffmnn.de/80/nstview.php [-] http://fbnhffmnn.de/80/zehir.php [-] http://fbnhffmnn.de/80/c-h.v2.php [-] http://fbnhffmnn.de/80/nst.php [-] http://fbnhffmnn.de/80/rst.php [-] http://fbnhffmnn.de/80/r57eng.php [-] http://fbnhffmnn.de/80/shell.php [-] http://fbnhffmnn.de/80/r.php [-] http://fbnhffmnn.de/80/lol.php [-] http://fbnhffmnn.de/80/php-backdoor.php [-] http://fbnhffmnn.de/80/cmdasp.asp [-] http://fbnhffmnn.de/80/simple-backdoor.php [-] http://fbnhffmnn.de/80/_private/ [-] http://fbnhffmnn.de/80/_vti_bin/ [-] http://fbnhffmnn.de/80/cgi-bin/[~] Total: 27 [+] Without issues: 2 [-] With issues: 25 (93%)

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: ========== [+] Web Application Security Report - Arachni Framework[~] Report generated on: 2014-09-26 14:09:34 +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 14:09:18 2014 [~] Audit finished on: Fri Sep 26 14:09:32 2014 [~] Runtime: 00:00:14[~] URL: https://46.38.236.232:443/ [~] User agent: arachni[*] Audited elements: [~] * Links [~] * Forms [~] * Cookies[*] Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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[~] ==========[+] 5 issues were detected.[+] [1] Trusted -- E-mail address disclosure [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 4b8d77af6b1afa0ba0754a201b0c053d7ce45bbcd0c7d3b73ac59f0a4c65c001 [~] 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: (?i-mx:[A-Z0-9._%+-]+@[A-Z0-9.-]+\\.[A-Z]{2,4}) [~] Matched string: info@fbnhffmnn.de[+] [2] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: ecff07aaacfffe2867992dbc6cac85140de4ba3f406c4136e3e4310b65f5ccfd [~] 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: [+] [3] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: b363f47965c9303c8036e3b2be47ca5c40f341a59db82f3372a7fe4fa91ac116 [~] 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: Code: 405 [~] Regular expression: [+] [4] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: fa32e5efc9dc994951919aa4d74e7df421f7dabe74a664a6bd1dff6139587c4f [~] 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 [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: cc7c00d5a5593555f99820ffca79e1af2178923a5d7fadfa095934a8251aac60 [~] Severity: Informational [~] URL: https://46.38.236.232:443/protect/index_p.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: https://46.38.236.232:443/protect/index_p.php [~] ID: Code: 401 [~] Regular expression: [+] Plugin data: [~] ---------- [*] Resolver [~] ~~~~~~~~~~~~~~ [~] Description: Resolves vulnerable hostnames to IP addresses.[~] 46.38.236.232: 46.38.236.232[*] Health map [~] ~~~~~~~~~~~~~~ [~] Description: Generates a simple list of safe/unsafe URLs.[~] Legend: [+] No issues [-] Has issues[-] https://46.38.236.232:443/ [+] https://46.38.236.232:443/biographie.php [+] https://46.38.236.232:443/css/layout.css [+] https://46.38.236.232:443/impressum.php [+] https://46.38.236.232:443/index.php [+] https://46.38.236.232:443/informatik.php [+] https://46.38.236.232:443/music.php [-] https://46.38.236.232:443/protect/index_p.php [+] https://46.38.236.232:443/server.php [+] https://46.38.236.232:443/sport.php [+] https://46.38.236.232:443/technik.php [+] https://46.38.236.232:443/wetter.php [-] https://46.38.236.232:443/Arachni-98e04 [-] https://46.38.236.232:443/css/Arachni-98e04[~] Total: 14 [+] Without issues: 10 [-] With issues: 4 (29%)

2.3 - 63.230.176.46 (etsio-prod.cnf.com)



Host Issue Summary

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
63.230.176.46 (etsio-prod.cnf.com)	Medium risk	11	0	3	3	0	13.1

Open Listening Ports

Service (Port)	Analysis	High	Med	Low	False	Total CVSS
https (443/tcp)	Medium risk	0	1	1	0	4.3
pharos (4443/tcp)	Medium risk	0	1	0	0	4.3
ichat3 (4080/tcp)	Low risk	0	0	1	0	0.0
unknown (9443/tcp)	Low risk	0	0	1	0	0.0
general/tcp	Log risk	0	1	0	0	2.6
ftp (21/tcp)	Log risk	0	0	0	0	1.9
general/CPE-T	Log risk	0	0	0	0	0.0
general/HOST-T	Log risk	0	0	0	0	0.0
rockwell-csp2 (2222/tcp)	Log risk	0	0	0	0	0.0
ssh (22/tcp)	Log risk	0	0	0	0	0.0
unknown (5443/tcp)	Log risk	0	0	0	0	0.0

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 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_DES_40_CBC_SHA SSL3_RSA_DES_64_CBC_SHA SSL3_EDH_RSA_DES_40_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: 4.3) pharos (4443/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 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_DES_40_CBC_SHA SSL3_RSA_DES_64_CBC_SHA SSL3_EDH_RSA_DES_40_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
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

It was detected that the host implements RFC1323.The following timestamps were retrieved with a delay of 1 seconds 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: == [+] Web Application Security Report - Arachni Framework[~] Report generated on: 2014-07-25 18:12:50 +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 Jul 25 18:12:12 2014 [~] Audit finished on: Fri Jul 25 18:12:47 2014 [~] Runtime: 00:00:35[~] URL: https://63.230.176.46:443/ [~] User agent: arachni[*] Audited elements: [~] * Links [~] * Forms [~] * Cookies[*] Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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://63.230.176.46:443/[~] Total: 1 [+] Without issues: 1 [-] With issues: 0 (0%)

Low (CVSS: 0.0) ichat3 (4080/tcp)
NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

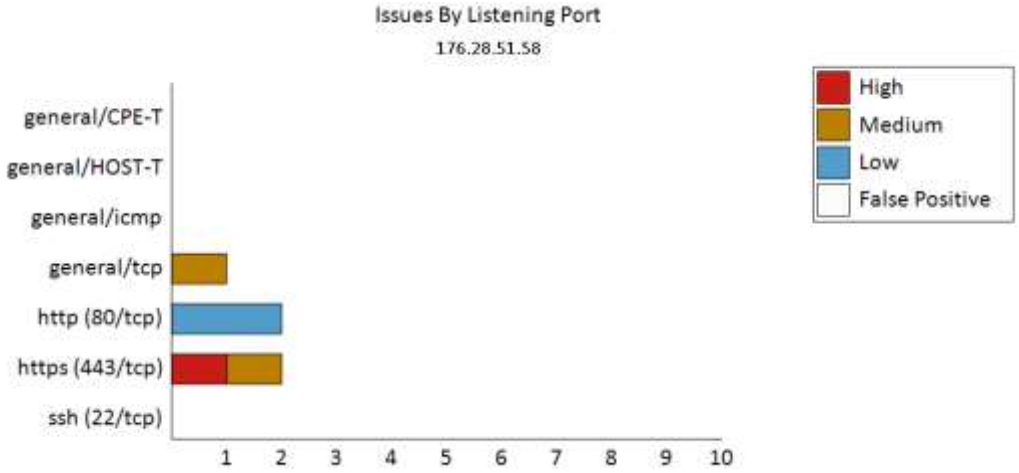
Here is the arachni report: == [+] Web Application Security Report - Arachni Framework[~] Report generated on: 2014-07-25 18:11:40 +0000 [~] Report false

positives at: http://github.com/Arachni/arachni/issues[+] System settings: [~] ---------- [~] Version: 0.4.7 [~] Revision: 0.2.8 [~] Audit started on: Fri Jul 25 18:11:28 2014 [~] Audit finished on: Fri Jul 25 18:11:37 2014 [~] Runtime: 00:00:08[~] URL: http://63.230.176.46:4080/ [~] User agent: arachni[*] Audited elements: [~] * Links [~] * Forms [~] * Cookies[*] Modules: xss_script_tag, os_cmd_injection, path_traversal, code_injection, trainer, source_code_disclosure, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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) unknown (9443/tcp)
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[~] Report generated on: 2014-07-25 18:14:49 +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 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, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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%)

2.4 - 176.28.51.58 (rs208305.rs.hosteurope.de)



Host Issue Summary

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
176.28.51.58 (rs208305.rs.hosteurope.de)	**High risk**	7	**1**	2	2	0	14.4

Open Listening Ports

Service (Port)	Analysis	High	Med	Low	False	Total CVSS
https (443/tcp)	**High risk**	**1**	1	0	0	11.8
http (80/tcp)	Low risk	0	0	2	0	0.0
general/tcp	Log risk	0	1	0	0	2.6
general/CPE-T	Log risk	0	0	0	0	0.0
general/HOST-T	Log risk	0	0	0	0	0.0
general/icmp	Log risk	0	0	0	0	0.0
ssh (22/tcp)	Log risk	0	0	0	0	0.0

Security Issues

High (CVSS: 7.5) https (443/tcp)
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) 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 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_40_CBC_SHA SSL3_RSA_DES_64_CBC_SHA SSL3_EDH_RSA_DES_40_CBC_SHA SSL3_EDH_RSA_DES_64_CBC_SHA SSL3_RSA_WITH_SEED_SHA TLS1_RSA_RC4_40_MD5 TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC2_40_MD5 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

Medium (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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

Low (CVSS: 0.0) http (80/tcp)
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[~] Report generated on: 2014-09-25 18:30:26 +0000 [~] Report false positives at: http://github.com/Arachni/arachni/issues[+] System settings: [~] ---------- [~] Version: 0.4.7 [~] Revision: 0.2.8 [~] Audit started on: Thu Sep 25 18:29:19 2014 [~] Audit finished on: Thu Sep 25 18:30:17 2014 [~] Runtime: 00:00:57[~] URL: http://rs208305.rs.hosteurope.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, sqli, sqli_blind_timing, file_inclusion, response_splitting, sqli_blind_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, ldapi, 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: 766dfcbb1fa97389e356c4fc03846e9d121394dc5416ad2c7eb7654b2c7882f5 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%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://rs208305.rs.hosteurope.de/80/%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%3E [~] ID: Code: 301 [~] Regular expression: [+] [2] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 733d1fc9c7c53a3779025f17e1216b6bbcf9bf7d2e6937598b85ddb6ddf4f894 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/%3E%22'%3E%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%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://rs208305.rs.hosteurope.de/80/%3E%22'%3E%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%3E [~] ID: Code: 301 [~] Regular expression: [+] [3] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: b1d13370f23b8c0dc9cbb767d0381907eb70f914d0d4ae89a5a66c2fa1e66ecf [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/?%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%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://rs208305.rs.hosteurope.de/80/?%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%3E= [~] ID: Code: 301 [~] Regular expression: [+] [4] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: f387b6b2c98855c24cbd1de0fcdf7fbaf17e0c83a702ca6903d8a73b3bef741e [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6 [~] 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/80/7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6 [~] ID: Code: 301 [~] Regular expression: [+] [5] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 3e425c6b26b0ac788d0b7d3b150076303aac7f7209b305e824b9cd55ffd0ddb8 [~] Severity: Informational [~] 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/robots.txt [~] ID: Code: 301 [~] Regular expression: [+] [6] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: ad95c20934d19044171750b945fde94a1b3f044db51dbddaaa36784903f59738 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/sitemap.xml [~] 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: [+] [7] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: bdc9efe041c2d786779b27dfec627a3063aecf73e1975cc9e05c2aaebe46afb8 [~] 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: [+] [8] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 27e8318df858ac02207329b826fafca07dd656123fba0c83433217c0fac63368 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/phpinfo.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/phpinfo.php [~] ID: Code: 301 [~] Regular expression: [+] [9] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: e1d8637bdfa168b6b2c720df5f7e7d98cfa580cce23c038ad6e39361e53b5700 [~] 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: 3e2b54b21d5fca480db9eb17536c0369fc1a5eae7c10f19fa914c857ff8c60f1 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/CVS/Root [~] 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/Root [~] ID: Code: 301 [~] Regular expression: [+] [11] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: fe1478030854a1baa0691c8ab803050c4390316264ec1e29fa2f3f2887280fc6 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/CVS/Entries [~] 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/Entries [~] ID: Code: 301 [~] Regular expression: [+] [12] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: ae667c5cda6eb7dc8b9c84779ef1b8cde1637d7e50bb0b4cbd28be118d16a759 [~] 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: d003afa36687e27b1bf080ae5ee470bbe9fc462f7e1faf2de5986ec412172380 [~] Severity: Informational [~] URL:

http://rs208305.rs.hosteurope.de/80/.git/HEAD [~] 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/.git/HEAD [~] ID: Code: 301 [~] Regular expression: [+] [14] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: c56e517475e8cff9676d54c80ea18b58a05dbaea8f908ebed13ef99b67e35560 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/_mmServerScripts/MMHTTPDB.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/_mmServerScripts/MMHTTPDB.php [~] ID: Code: 301 [~] Regular expression: [+] [15] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 4f480fa90041a42fe1d458d1033dc5ae5d2314a1907b65ae5a7a8d22a58b910c [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/_mmServerScripts/MMHTTPDB.asp [~] 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/_mmServerScripts/MMHTTPDB.asp [~] ID: Code: 301 [~] Regular expression: [+] [16] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 6467e429f463d6112302258cb9df130140ec6ac81ba1d3a6530bac7435fa6193 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/_mmDBScripts/MMHTTPDB.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/_mmDBScripts/MMHTTPDB.php [~] ID: Code: 301 [~] Regular expression: [+] [17] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 5e0922a25cff47320c7ea69f19d934d983eefcf058b3ed869369a421ca3cefc3 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/_mmDBScripts/MMHTTPDB.asp [~] 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/_mmDBScripts/MMHTTPDB.asp [~] ID: Code: 301 [~] Regular expression: [+] [18] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 4cd79d17e444deeddc012cf50c16b45b772817b596b60986df406f9eb3c297ed [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/config/database.yml [~] 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/config/database.yml [~] ID: Code: 301 [~] Regular expression: [+] [19] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 220b62dec3998993c20da061acae4cea961be80656bdda770d82fb0670f3f0ab [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/install.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/install.php [~] ID: Code: 301 [~] Regular expression: [+] [20] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 126bed66332d3d23203b9436c39dc9ed403ed7308e2e0d701bcb681ef63601af [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/wp-admin/install.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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/wp-admin/install.php [~] ID: Code: 301 [~] Regular expression: [+] [21] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: a732854211c9dec5817f644dc8e37cafe352e9223d5730a046182ae0444b7704 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/wp-admin/setup-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,

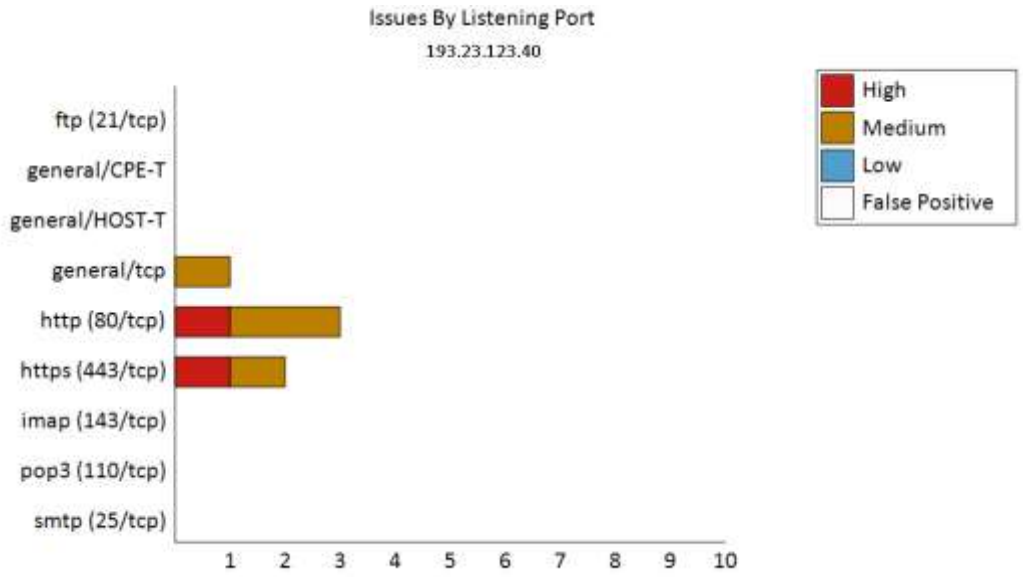
however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.[~] Requires manual verification?: false[~] References: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/wp-admin/setup-config.php [~] ID: Code: 301 [~] Regular expression: [+] [22] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: ced2f1bc35b181dbdcd58d62edc440c000d7abc26e1d5ffd29d99a0a952a109d [~] 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: [~] w3.org - http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html[*] Variations [~] ---------- [~] Variation 1: [~] URL: http://rs208305.rs.hosteurope.de/80/config.php [~] ID: Code: 301 [~] Regular expression: [+] [23] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 820e04ea416419e61b91db06c8ff4aaea7aaf4253db7e458ded1902c55280acb [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/php.ini [~] 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/php.ini [~] ID: Code: 301 [~] Regular expression: [+] [24] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 6379e02a8384ea44b64d4d212ffd59f384fe578f36037dc122ba8f53e8707dc9 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.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://rs208305.rs.hosteurope.de/80/error_log [~] ID: Code: 301 [~] Regular expression: [+] [25] Trusted -- Interesting response [~] ~~~~~~~~~~~~~~~~~~~~ [~] ID Hash: 6593df6cc64cee409b5c7b293f8b97441aea20992aab463e90afd0c221feb136 [~] Severity: Informational [~] URL: http://rs208305.rs.hosteurope.de/80/elmah.axd [~] 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/elmah.axd [~] ID: Code: 301 [~] Regular expression: [+] Plugin data: [~] ---------- [*] Resolver [~] ~~~~~~~~~~~~~~~ [~] Description: Resolves vulnerable hostnames to IP addresses.[~] rs208305.rs.hosteurope.de: 176.28.51.58[*] Health map [~] ~~~~~~~~~~~~~~~ [~] Description: Generates a simple list of safe/unsafe URLs.[~] Legend: [+] No issues [-] Has issues[+] http://rs208305.rs.hosteurope.de/80 [+] http://rs208305.rs.hosteurope.de/index.php [-] http://rs208305.rs.hosteurope.de/80/%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%3E [-] http://rs208305.rs.hosteurope.de/80/%3E%22'%3E%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%3E [-] http://rs208305.rs.hosteurope.de/80/?%3Cmy_tag_7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6/%3E= [-] http://rs208305.rs.hosteurope.de/80/7bb8a2f05f74ee44ad7c629d9b0ec7fd51a4c94fdabe6225752ba6f5f35ce5e6 [-] http://rs208305.rs.hosteurope.de/80/robots.txt [-] http://rs208305.rs.hosteurope.de/80/sitemap.xml [-] http://rs208305.rs.hosteurope.de/80/sitemap.xml.gz [-] http://rs208305.rs.hosteurope.de/80/phpinfo.php [-] http://rs208305.rs.hosteurope.de/80/CVS/Repository [-] http://rs208305.rs.hosteurope.de/80/CVS/Root [-] http://rs208305.rs.hosteurope.de/80/CVS/Entries [-] http://rs208305.rs.hosteurope.de/80/.svn/wc.db [-] http://rs208305.rs.hosteurope.de/80/.git/HEAD [-] http://rs208305.rs.hosteurope.de/80/_mmServerScripts/MMHTTPDB.php [-] http://rs208305.rs.hosteurope.de/80/_mmServerScripts/MMHTTPDB.asp [-] http://rs208305.rs.hosteurope.de/80/_mmDBScripts/MMHTTPDB.php [-] http://rs208305.rs.hosteurope.de/80/_mmDBScripts/MMHTTPDB.asp [-] http://rs208305.rs.hosteurope.de/80/config/database.yml [-] http://rs208305.rs.hosteurope.de/80/install.php [-] http://rs208305.rs.hosteurope.de/80/wp-admin/install.php [-] http://rs208305.rs.hosteurope.de/80/wp-admin/setup-config.php [-] http://rs208305.rs.hosteurope.de/80/config.php [-] http://rs208305.rs.hosteurope.de/80/php.ini [-] http://rs208305.rs.hosteurope.de/80/error_log [-] http://rs208305.rs.hosteurope.de/80/elmah.axd[~] Total: 27 [+] Without issues: 2 [-] With issues: 25 (93%)

Low (CVSS: 0.0) http (80/tcp)
NVT: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

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

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
193.23.123.40 (rev-040.snrm.fr)	**High risk**	9	**2**	4	0	0	27.0

Open Listening Ports

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

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

Medium (CVSS: 5.0) http (80/tcp)
NVT: Apache /server-status accessible (OID: 1.3.6.1.4.1.25623.1.0.10677)

Summary: Leak of information in Apache. Vulnerability Detection: Check if /server-status page exist. Vulnerability Insight: server-status is a built-in Apache HTTP Server handler used to retrieve the server's status report. Impact: Requesting the URI /server-status gives information about the currently running Apache. Affected Software/OS: All Apache version. Solution: 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.

High (CVSS: 5.0) https (443/tcp)
NVT: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103936)

Summary: OpenSSL is prone to an information disclosure vulnerability.Vulnerability Detection: Send a special crafted TLS request and check the response.Vulnerability Insight: The TLS and DTLS implementations do not properly handle Heartbeat Extension packets.Impact: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.Affected Software/OS: 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.Solution: Updates are available.

Medium (CVSS: 4.3) http (80/tcp)
NVT: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

Summary: 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.Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information. Solution: OpenBSD has released a patch to address 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.Information that was gathered: Inode: 139518 Size: 6421

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 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_40_CBC_SHA SSL3_RSA_DES_64_CBC_SHA SSL3_EDH_RSA_DES_40_CBC_SHA SSL3_EDH_RSA_DES_64_CBC_SHA SSL3_RSA_WITH_SEED_SHA TLS1_RSA_RC4_40_MD5 TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC2_40_MD5 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

Medium (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

It was detected that the host implements RFC1323.The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1274025501 Paket 2: 1274025623