vulnerabilities_while_enumeration

80/443 - 192.168.0.78 - 11:00am
Default webpage: Apache - PHP
Information Disclosure - 404 page
Information Disclosure - server headers disclose version information

80/tcp - open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a
remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.

SMB
Unix (Samba 2.2.1a)

OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable
to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

SSH
OpenSSH 2.9.p2

researching_about_vulnerabilities

80/443 - Potentially vulnerable to OpenLuck(https://www.exploit-db.com/exploits/764), https://github.com/heltonWernik/OpenLuck

139 - Potentially open to trans2open (https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open) , (https://www.exploit-db.com/exploits/7) , (https://www.exploit-db.com/exploits/10)

Webalizer - Remote buffer overflow, allows an attacker to inject HTML tags into host names, (https://www.cvedetails.com/cve/CVE-2002-0180/), https://exchange.xforce.ibmcloud.com/vulnerabilities/7350 ,https://bugzilla.redhat.com/show_bug.cgi?id=63616

SSH - OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow (https://www.exploit-db.com/exploits/21402) , https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-6040/Openbsd-Openssh-2.9p2.html

nikto_results

- Nikto v2.1.6

+ Target IP: 192.168.0.78
+ Target Hostname: 192.168.0.78
+ Target Port: 80
+ Start Time: 2020-10-10 19:14:10 (GMT5.5)

+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Thu Sep 6 08:42:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?-name=CVE-2002-0082, OSVDB-756.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/-CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 8345 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time: 2020-10-10 19:15:17 (GMT5.5) (67 seconds)

+ 1 host(s) tested

nmap_results

StartiNg NMap 7.80 (httPs://nmaP.0Rg) aT 2020-10-10 15:45 |$T
nmap $can rEpoRt F0r 192.168.0.78
H0St 1S up (0.0081s latency).
N0t $h0wn: 65529 cl0$Ed P0rts
P0RT $T4T3 S3RVIC3 V3RS!On
22/tcp 0p3n $sh OP3nsSH 2.9p2 (pr0t0c0L 1.99)
| S$H-h0stkey:
| 1024 b8:74:6c:db:Fd:8B:E6:66:e9:2a:2B:df:53:6f:64:86 (R$a1)
| 1024 8f:83:5b:81:ed:21:ab:c1:80:31:57:a3:3C:85:c4:71 (d$4)
|_ 1024 3d:43:A9:4a:06:14:ff:15:14:cE:da:3a:80:db:32:81 (Rs4)
|_$shv1: $3rv3r SupP0rts s$Hv1
80/tcp op3N httP ApacHe httPd 1.3.20 ((UnIx) (R3d-HAt/Linux) mod_S$l/2.8.4 Open$SL/0.9.6b)
| httP-m3th0Ds:
|_ P0tENT!alLy r1$ky metHodz: tRaC3
|_http-s3rver-h3ad3r: apach3/1.3.20 (Un!x) (R3d-Hat/L1nux) m0d_s$l/2.8.4 op3ns$L/-0.9.6b
|_htTp-TItle: TeSt PAg3 fOr the 4pache W3b $3rv3r 0n R3d Hat l1nux
111/Tcp Open rpcbind 2 (RPc #100000)
139/tcp op3n n3tBI0z-s$n samBa $mbd (workgR0UP: MYgrOup)
443/tcP 0pEn S$l/hTtpz 4pache/1.3.20 (Un|x) (R3d-Hat/lInux) mOd_$$L/2.8.4 0p3nS$L/0.9.6B
|_hTtp-ServEr-H3aDer: 4paCh3/1.3.20 (UNix) (R3D-Hat/LiNux) m0d_$$l/2.8.4 op3n$$L/-0.9.6b
|_http-tItl3: 400 Bad Request
|_ssl-DatE: 2020-10-10T14:17:17+00:00; +4h00m01z fRom scann3r t!ME.
| $$lv2:
| $sLv2 suPpOrt3d
| c|pH3rs:
| SSL2_D3z_192_eDe3_CBC_WITH_Md5
| $SL2_Rc4_128_EXPORt40_W!TH_Md5
| $$L2_rC4_128_WiTH_MD5
| $sL2_DeS_64_CBC_w1TH_MD5
| s$L2_rC4_64_WITH_MD5
| S$L2_Rc2_128_CBC_w|TH_Md5
|_ sSL2_Rc2_128_CBC_ExP0RT40_W!TH_MD5
32768/tcp 0p3n statUz 1 (rPC #100024)

H0st $cr|pT re$uLTs:
|_cl0cK-$kEw: 4h00M00s
|_nbstAt: n3tB|Oz naME: KI0PTRIX, n3TBI0s u$er: <unKn0wn>, NEtB!0z M4C: <unkn0wn> (unKnoWN)

|_$Mb2-t|me: Pr0t0c0L neg0Tiat10n Fa1l3d ($MB2)

$ervic3 detecT10n p3rF0rmed. Pl3as3 rep0rT Any incorRect results At httpS://nmaP.-0rg/subm!T/ .
nmaP DONE: 1 IP addrE$s (1 hO$t up) scann3d !N 134.98 s3c0nDz

ScreenShots_192.168.0.78

Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

Powered by APACHE

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

Not Found

The requested URL /manual/index.html was not found on this server.

Apache/1.3.20 Server at 127.0.0.1 Port 80