



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

PC Week Hack of 1999

Shawn Balestracci

February 26, 2001

In September of 1999, PC Week Magazine set up `securelinux.hackpcweek.com` and offered \$1000 to the first person who could successfully hack into it. Many people tried, and four days later someone broke into the machine. A CGI exploit allowed a hacker going by the name of Jfs to get his foot in the door.

PC Week installed Red Hat Linux 6.0 with the latest version of Apache Web Server. They also implemented commonly used security products to fend off certain high level attacks. Their firewall blocked all ports except for port 80 (as it was to be a web server) and they ran a popular commercial banner ad system. The sample CGI scripts that come with apache were also disabled. They also specified that the server would provide Server Side Includes and `mod_perl`, however they failed to do this. This seemed like a reasonable approach, lock down the server with a firewall, run a minimal set of applications, and use a commercial, popular banner ad system. In 1999, this site had more thorough security than many other sites on the net, a scary thought.

How did it happen?

This hack began like most hacks, with the gathering of information. A port scan showed that the only thing open was the http server. The hacker scanned through the HTML of the web pages. He then queried the server and was able to gather that it was an Apache 1.3.6 server on Redhat. The server had the directories `"/cgi-bin /photoads/ and /photoads/cgi-bin"` The hacker then tried some well known CGI exploits, `wwwboard`, `test-cgi`, `Count.cgi` which were not available. Those CGI exploits came preinstalled with many versions of apache.

The hacker then turned to the `/photoads/` directory. With a web search, he found out that it is a commercial CGI package selling for \$149. He found a friend that had a photoad installation, who then let Jfs take a look at the source.

The hacker then simply looked at the default installation files, and attempted to retrieve the ads database which was at `/photoads/ads_data.pl`. This attempt was successful; it allowed the hacker to see the user passwords for their ads.

Next the hacker was able to gather some more information with an `env.cgi` script that was included with photoads (which is similar to `test-cgi`) and found the document root of `/home/httpd/html`.

The hacker then tried to exploit SSI and `mod_perl`. He looked for an unfiltered HTML variable, and found one in the `post.cgi` script, `$ENV{'HTTP_REFERER'}`. However, the server wasn't running SSI or `mod_perl`.

PC Week also failed to evaluate the code of the Smart Photo Ad for vulnerabilities. They missed the lack of a filter on one of the user provided variables and didn't scrutinize the system calls: open() and rename(). There were also some file permission issues with these scripts as no file should be writable by user nobody, especially within the web tree.

PC Week did not install the latest security patches available at the time for Red Hat. These patches would have blocked the well known crontab exploit that the hacker used to get root access, as well as others. PC Week claimed that they wanted to show how a typical beginning administrator might act, and thus chose not to do these updates.

How can I protect against similar problems?

This hack, and ones similar to it, first involved a hole from the outside in, then another hole which allowed for a jump in access from limited to superuser. The recommendations below are by no means comprehensive, but are given to provide an area of emphasis to deter hacks of this type.

It is vitally important that a user keeps up to date with their distribution and applies security fixes as soon as possible. Most distributions of Linux have updates on their web site that are freely accessible. Never just set up an install from the CD and be done with it. Check for and apply the security updates. Also remove any applications from the server that aren't required. The crontab exploit that this hack used was well known at the time, and Red Hat had a patch available. Subscribe to your distributions mailing list, and they will even send you a message whenever security updates are available.

Scrutinize any CGI scripts that you plan to use. Eliminate any ones that aren't used, and any sample scripts. Check the file permissions on them to make sure they aren't writable.

Carefully look at the code involved in the CGI scripts, make sure any user changeable data has the appropriate checks on it. Anything based on HTTP variables, or dealing with user input should be considered suspect.

Make sure that the parameters for any calls to open() and system() are checked and stripped of undesired effects. Make sure that any spurious characters are eliminated from them before allowing the call to open, or system. People often neglect the backslash, and the NUL character. Without these checks, people can open files that they shouldn't be such as the /etc/passwd file, violating confidentiality. Or they could make calls that remove or change files, violating integrity and possibly availability.

The Phrack article that helped the hacker can help us as well.

In perl, to eliminate the NUL character you can:

```
$insecure_data=~s/\0//g;
```

You can then escape out the remaining shell characters with:

```
$insecure_data=~s/([\&;\'\\"\\|\"*?~<>^\(\)\[\]\{\}\$\n\r])/\\  
$1/g;
```

If you keep up with the latest security updates from your vendor, and make sure that those parameters are scrutinized, this hack can be prevented. Do not, and this must be stressed, do NOT simply assume your firewall will totally protect you.

Conclusion

In 1999 a hacker going by the name Jfs successfully answered PC WEEK'S challenge to break into their Linux box. He managed to do so by exploiting a CGI vulnerability. PC Week secured the system according to recommendations in the Linux How-TO, as well as the configuration changes on the Apache Software Foundation's Site. This is a good start in security, however it is obvious more is needed to make a box secure.

Interestingly, PC Week magazine had set up an NT server with a concurrent contest that was not hacked. This could be because they installed various service packs and security upgrades for NT, and chose not to install them for Linux. They got a lot of flak on www.slashdot.com, "News for Nerds, Stuff that Matters" for this. PC WEEK claims that NT is easier to secure and that they were put off by the 21 open-source security fixes for Red Hat 6.0 at the time. This claim holds little water though, as the security patches are all fairly small, quick to apply, and require few if any reboots, unlike NT Service packs which can take two or three system reboots each.

PC Week sums it up nicely by stating "Companies that don't keep on top of application fixes will be at the mercy of hackers who do."

References:

Jfs, "A practical vulnerability analysys"
<http://his.pahack.ccc.de/en/mi019en.htm>
(02/01/2001)

Chowdhry, Pankaj, "CGI script opens door" (10/04/1999)
<http://www.zdnet.com/eweek/stories/general/0,11011,2346293,00.html>
(02/05/2001)

Chowdhry, Pankaj, "PC Week Labs' site gets hacks and flak" (09/27/1999)
<http://www.zdnet.com/enterprise/stories/linux/news/0,6423,2341342,00.html>
(02/05/2001)

Tascheck, John, "Hack this: PC Week Labs site begs attacks" (09/20/1999)
<http://www.zdnet.com/eweek/stories/general/0,11011,2336675,00.html>
(02/05/2001)

Chowdhry, Pankaj, "Attacked and hacked!" (10/11/1999)
<http://www.zdnet.com/eweek/stories/general/0,11011,2350743,00.html>
(02/07/2001)

rain forest puppy, "Perl CGI problems", Phrack Magazine, Vol. 9 Issue 55 p 7,
(09/09/1999)
<http://phrack.infonexus.com/search.phtml?view&article=p55-7>
(02/05/2001)

© SANS Institute 2000 - 2002, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event