

[Skip to content](#)

DcLabs

A Binary LifeStyle

- > [About](#)
- > [Log In](#)

Search

Categories:

- > [Hacking](#)
- > [Pentesting](#)

How Strong is your Fu? Novel

book 0x10 – noob-filter

chapter 0x1 – Looking for flaws a.k.a. Whining

We started on noob-filter doing the usual network scans to get services, ports and OS but there was nothing much interesting at the first glance so we skipped to SQL injection. At the first try we got an error from dotDefender that “mysteriously” disappeared some minutes later and all we got was “HAHAHA!” pages, even if we didn’t have the luck to get that dotDefender page we could find it through the page source keywords as it lead us to dotDefender.

chapter 0x2 – Getting the key a.k.a. Trying Harder

Finding a vulnerability was easy as we thought, it was just a filter for the n00bs. We were able to exploit it sending a malicious post to www1.noob-filter.com and getting the key.

book 0x21 – killthen00b

chapter 0x1 – Looking for flaws a.k.a. Deciding the Fu path

At beginning we were divided by the fact that we had a valid ftp user and password to explore inside but we also thought it could just be a trap, so we did some scans first and found many opened ports and nothing too obvious to try so we navigated throughout the website and then we started to play with the ftp.

chapter 0x2 – Getting inside a.k.a. Loading the gun

The first thing we tried was to upload malicious php and asp pages to get in but the interpreters were disabled/inexistents.

Inside ftp we did some tests and ended up on C:\, after that we explored the directories and we saw some directories that could be useful that was inside C:\surgemail, when we were navigating we discovered a path to the CGI directory was .../scripts and there was one like that inside C:\surgemail, after gathering those informations we uploaded an executable reverse shell to .../scripts directory and accessed <http://192.168.6.72/scripts/reverse.exe>.

chapter 0x3 – Getting the key a.k.a. Killing the n00b

Once we were in we checked the privileges and w00t, we had system privileges already so all we had to do is look for the proof, that was at Administrator's Desktop.

book 0x22 – ghost

chapter 0x1 – Looking for flaws a.k.a. Canalizing the Fu

After scanning ports and source code from <http://192.168.6.68> we found nothing so we started scanning the web interface with w3af to enumerate directories and files and we found <http://192.168.6.68/1/index.asp> with a form that send post information to slogin.inc.php. We found a pattern at the inputs that fits with Simple Text-File Login that have a RFI flaw.

chapter 0x2 – Getting inside a.k.a. Breaking into Ryujin's Love

We hosted a malicious php code for reverse shell at local apache and disabled the php so it wouldn't interpret it before sending, after playing a bit with the RFI flaw we were able to make 192.168.6.68 execute our malicious reverseshell.php which gave us access to ghost machine with www-data user access.

chapter 0x3- Escalating privileges a.k.a. Exorcising the ghost

Once we were in we analysed the structure of the machine, looked for services versions and gathered information of suid apps and versions, we found a weird directory at / named /apachelogs that we had permission to hang around. After reading fstab we noticed that /apachelogs was actually another partition running on reiserfs. With that information we started trying to exploit it with CVE-2010-1146 exploit. We noticed too that /dev/sdb1 (/apachelogs) partition was not mounted actually and after mounting it /apachelogs became owned by root, but inside it there was a directory .../data in which we had permission, after all that all we had to do is to modify the exploit, upload it and run it and successfully getting root privileges. With root we found the other proof.txt that was (of course) inside /root.

All I have to say to Offensive-Security is TRY HARDER! 😊

Thank you for the great time and challenge.

Regards,

raph0x88

Posted in [Hacking](#), [Pentesting](#).

By [raph0x88](#)

May 11, 2010

[No comments](#)

0 Responses

Stay in touch with the conversation, subscribe to the [RSS feed for comments on this post](#).

Post a comment

Some HTML is OK

Name (required)

Email (required, but never shared)

Web

or, reply to this post via [trackback](#).

Subscribe

[Site RSS feed](#)

About DcLabs

raph0x88's blog



Archives

> [May 2010](#)

Tags

Proudly powered by [WordPress](#) and [Carrington](#).

[Carrington Theme](#) by [Crowd Favorite](#)