



Swiss Cyber Storm II Unix Hacking

Daniel Stirnimann <daniel.stirnimann@csnc.ch>

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Unix Wargame Challenges



7002 - Got Root

- ✦ To get root privileges and to learn the content of `/root/secret.txt`.

7004 - Restricted Shell Breakout 1

- ✦ Find the file `geheimnis.txt` and know the content.

7004 - Restricted Shell Breakout 2

- ✦ Find the file `geheimnis1.txt` and know the content.

Requirements

- ✦ KubuntuVM from ftp.hack.er

Restricted Shell (rbash)

Shell:

Command language interpreter that executes commands. User interface between user and operating system.

Restricted Shell:

Controlled environment. Disallows certain shell features (must be configured).

What is a restricted shell about?



Restricted Environments are jailing the users

- ✦ Terminal Server
- ✦ SSH Jail
- ✦ Operator Menu's
- ✦ Custom Shells / Perl Scripts

Benefits of Jailing Technique

- ✦ Limit the user functionality to it's minimum
- ✦ Protect the others from the user
- ✦ Protect the user from others



Demo

Restricted Shell Breakout 1

Recommendations



1. **Do not use restricted shells or now the limitations.**
2. **If restricted shells, then:**
 - ✦ Unset PATH
(E.g. unset PATH in .bash_profile of the user)
 - ✦ Remove any write permission in HOME and PATH
 - ✦ Overall set restrictive filesystem permissions -> breaks standard permissions
 - ✦ Trust your Users!
3. **Use jail/chroot instead**
 - ✦ A chroot jail is a subdirectory within a file system that contains a bare-bones version of a standard system install
 - ✦ Jail is a BSD-term for jailing processes

Questions?

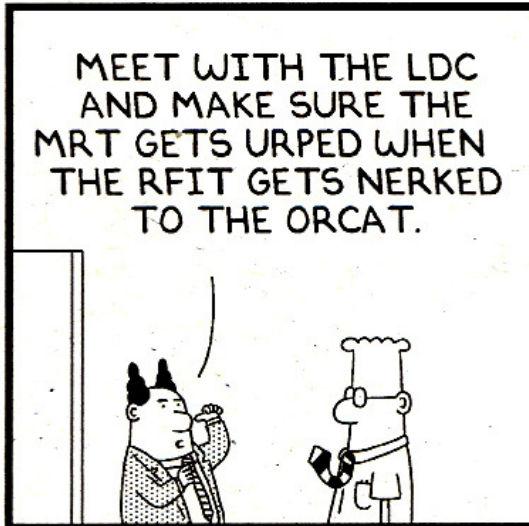


dilbert©

by Scott Adams



www.dilbert.com scottadams@aol.com



8-22-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc.

