

# How I got hacked ...

The beginning of the cyber security journey from 1999 to 200X  
Or what worked back then ...

Ganbold Ts, MNSEC 2022

# About me

- Major/Specialty - Computer Science, Systems engineer
- Work experience
  - Senior programmer - The Secretariat, Parliament of Mongolia
  - Systems engineer - UNDP project, Government of Mongolia
  - Senior programmer, Systems engineer, Tech manager - Micom Co Ltd., ISP
  - Director of IT division - MobiCom Corporation
  - Advisor - MNCERT/CC
- FreeBSD src and doc committer

# Overview

- RedHat and mountd
- After mountd ...
- sfbayautos.com mistakes
- BSOD, buffer overflow learning on FreeBSD, war games
- Got hacked again ...

# RedHat ...

- Sometime in 1999 ...
  - Leased line – Micom
  - First RedHat installation
    - HP Vectra Desktop
    - RedHat v5.0
- Tried Russian localization
  - Font edit
  - keyboard input, output
- I liked it 

```
root@beastie:/usr/freebsd-src/tools # ls -l
total 99
drwxr-xr-x  2 tsgan  tsgan    9 19 авг.  13:19 boot
drwxr-xr-x  2 tsgan  tsgan   12 30 сент.  05:18 bsdbox
drwxr-xr-x  9 tsgan  tsgan   23 19 авг.  13:19 build
drwxr-xr-x  5 tsgan  tsgan   11 24 дек.   2020 bus_space
drwxr-xr-x  2 tsgan  tsgan    3 24 дек.   2020 coccinelle
drwxr-xr-x  2 tsgan  tsgan    7 24 дек.   2020 debugscripts
drwxr-xr-x  5 tsgan  tsgan    6 24 дек.   2020 diag
drwxr-xr-x  2 tsgan  tsgan    3 24 дек.   2020 ifnet
-rw-r--r--  1 tsgan  tsgan 2355 24 дек.   2020 install.sh
drwxr-xr-x  3 tsgan  tsgan    5 24 дек.   2020 kerneldoc
drwxr-xr-x  2 tsgan  tsgan    3 24 дек.   2020 LibraryReport
drwxr-xr-x  2 tsgan  tsgan    3 24 дек.   2020 lua
-rw-r--r--  1 tsgan  tsgan 3683 24 дек.   2020 make_libdeps.sh
drwxr-xr-x  2 tsgan  tsgan    4  9 июля  05:38 pkgbase
-rw-r--r--  1 tsgan  tsgan  347 24 дек.   2020 README
drwxr-xr-x 49 tsgan  tsgan   51 24 дек.   2020 regression
drwxr-xr-x  2 tsgan  tsgan    5 17 марта  2022 sched
drwxr-xr-x 22 tsgan  tsgan   23 17 марта  2022 test
-rwxr-xr-x  1 tsgan  tsgan 2206 24 дек.   2020 tinder.sh
drwxr-xr-x 84 tsgan  tsgan   85 17 марта  2022 tools
drwxr-xr-x  3 tsgan  tsgan    3 24 дек.   2020 uma
root@beastie:/usr/freebsd-src/tools #
```



RedHat ...

One day something got changed ... 

# LANG env var

- One day ...
  - LANG env var was changed
  - I changed back to Russian
- Few days later ...
  - LANG was changed again



...

```
root@beastie:/usr/freebsd-src/tools# ls -l
total 99
drwxr-xr-x  2 tsgan  tsgan   3 Dec 24  2020 LibraryReport
-rw-r--r--  1 tsgan  tsgan 347 Dec 24  2020 README
drwxr-xr-x  2 tsgan  tsgan   9 Aug 19 13:19 boot
drwxr-xr-x  2 tsgan  tsgan  12 Sep 30 05:18 bsdbox
drwxr-xr-x  9 tsgan  tsgan  23 Aug 19 13:19 build
drwxr-xr-x  5 tsgan  tsgan  11 Dec 24  2020 bus_space
drwxr-xr-x  2 tsgan  tsgan   3 Dec 24  2020 coccinelle
drwxr-xr-x  2 tsgan  tsgan   7 Dec 24  2020 debugscripts
drwxr-xr-x  5 tsgan  tsgan   6 Dec 24  2020 diag
drwxr-xr-x  2 tsgan  tsgan   3 Dec 24  2020 ifnet
-rw-r--r--  1 tsgan  tsgan 2355 Dec 24  2020 install.sh
drwxr-xr-x  3 tsgan  tsgan   5 Dec 24  2020 kerneldoc
drwxr-xr-x  2 tsgan  tsgan   3 Dec 24  2020 lua
-rw-r--r--  1 tsgan  tsgan 3683 Dec 24  2020 make_libdeps.sh
drwxr-xr-x  2 tsgan  tsgan   4 Jul  9 05:38 pkgbase
drwxr-xr-x 49 tsgan  tsgan  51 Dec 24  2020 regression
drwxr-xr-x  2 tsgan  tsgan   5 Mar 17  2022 sched
drwxr-xr-x 22 tsgan  tsgan  23 Mar 17  2022 test
-rwxr-xr-x  1 tsgan  tsgan 2206 Dec 24  2020 tinder.sh
drwxr-xr-x 84 tsgan  tsgan  85 Mar 17  2022 tools
drwxr-xr-x  3 tsgan  tsgan   3 Dec 24  2020 uma
```

# mountd exploit

- Found z user in /etc/passwd
- Who is z user? 🤔
- mountd exploit
  - NFS enabled by default
  - Logging code - buffer overflow
  - Remotely exploitable
  - Created z user with UID/GID 0:0
  - Rootkit was installed
    - xferlog
    - Somewhere from South Africa
    - changed LANG
  - Installed ircii – irc client

- I got hacked ... 😡

EXPLOIT DATABASE

## RedHat Linux 5.1 / Caldera OpenLinux Standard 1.2 - Mountd

<b>EDB-ID:</b> 19096	<b>CVE:</b> 1999-0002	<b>Author:</b> LUCYSOFT	<b>Type:</b> REMOTE
-------------------------	--------------------------	----------------------------	------------------------

**EDB Verified:** ✓

<b>Platform:</b> LINUX	<b>Date:</b> <u>1998-08-28</u>
---------------------------	-----------------------------------

really ugly code. It does :

```
int fd = open("/etc/passwd", O_RDWR);
lseek(fd, 0, SEEK_END);
write(fd, "z::0:0:::/bin/sh\n", 18);
close(fd);

int fd = open("/etc/hosts.allow", O_RDWR);
lseek(fd, 0, SEEK_END);
write(fd, "ALL:ALL\n", 8);
close(fd);
```



# After mountd ...

- Sometime in 1999 – 2000 ...
- Port scans
- Found some RedHat
- mountd exploit 🤪
  - Packet captures on telnet, pop3 etc.
    - telnet, pop3 – clear text protocols
    - Got some credentials ...

- **Got anonymous email**



# sfbayautos.com

- Sometime in 2000 - 2001
- Car buy/sell site
  - Php/mysql
- Friend asked
- Worked well for sometime ...
- Some email came ...
  - No SSL
  - Credit card info in plaintext

• Oh

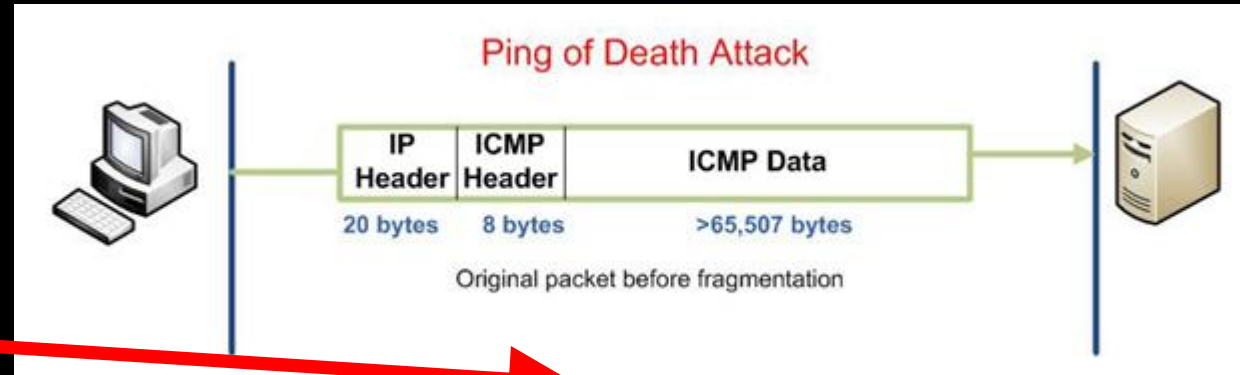


The screenshot shows the website's header with the logo 'SFBayAutos.com' featuring a bridge icon and the phone number '880 101'. A navigation menu includes 'Home', 'Sell a car', 'Buy a car', 'Modify your ad', 'Used car price', and 'Contact us'. A yellow banner contains a welcome message: 'Welcome to SFBayAutos.com, the Bay Area's only active website featuring Classified Auto Listings. We keep our database updated with cars priced to sell quick and easy.' To the right is a photo of several cars parked in front of a city skyline. Below the banner are three sections: 'Sell a car' (describing a \$9.95 fee and 14-day trial), 'Buy a car' (describing a search function and 'must sell' cars), and 'Delete & Modify' (describing ad management options). On the left side, there are two logos: 'CARFAX VEHICLE HISTORY REPORTS' with a 'FREE Instant Lemon Check' badge, and 'edmunds.com'.

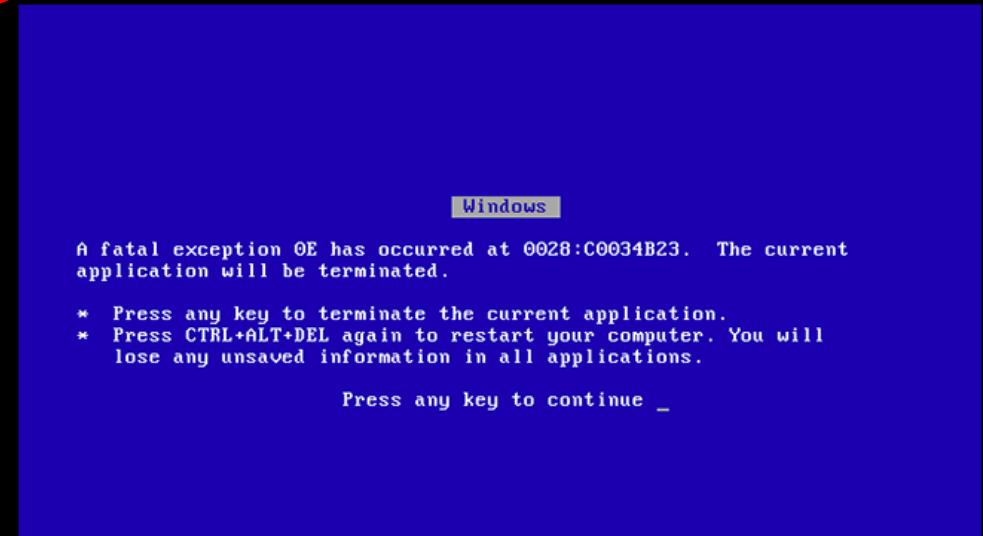
©2001 SFBayAutos.com, All rights reserved.

# BSOD, Buffer overflow, FreeBSD, wargames

- Sometime in 2001 - 2003
- Ping of Death – BSOD
  - Windows 95
  - IRC – Monstudnet -> got IP



- Buffer overflow learning on FreeBSD
  - [http://www.dusal.net/downloads/books/pdf/Security/remote\\_buffer\\_overflow\\_mon.pdf](http://www.dusal.net/downloads/books/pdf/Security/remote_buffer_overflow_mon.pdf)
- Shell based war games
  - <https://overthewire.org/wargames/>



# Got hacked again ...

- Sometime in 200x
- Micom - ISP
  - Mostly FreeBSD
  - IRC chat
  - Shell server
  - Email Server Provider (corporate, individuals) - Web Mail Client
  - Etc ...
- Friend ...
  - Hacked shell server – Fake login prompt – 2nd username/password
  - PHP file upload check - `$_FILES['file']['tmp_name']`



- Lessons learned

Thank you