Matthew Quander
12/17/2021
COSC647

Homework 02

Question 01

A) The vulnerability is that insert_in_table takes a signed integer for the position variable in the array. If a user enters a negative number, it will pass the check that makes sure it does not go beyond the array bounds (800) because it is converted to an unsigned integer when compared to sizeof(). However, the variable will still hold the negative number and cause a segmentation fault since it is trying to place a value in a negative index in the array. A possible fix is to only allow the function to accept positive integer values and validate them. This is done in the attached `int_OF.c file`.

B) The vulnerability is that `copy_something()` takes a signed integer as input to check the bounds of the buffer, but the call to `memcpy()` will convert the signed integer to an unsigned integer which will be very large and overflow the buffer. A possible fix is to change `copy_something()` to only accept positive integers values and valid that input. This is done in the `copy.c` file.

C.) The vulnerability in this code is that there is no check on the value of variable `len`. If the user enters a large number it could allocate too much memory to the array. Also, when the for-loop executes from 0 to `len`, it can overflow the memory if it is too large. A solution to this would be to check the size of `len` from the user's input to make sure it is below a certain amount, and therefore restrict the amount of memory the array can use. This is done in the `myfunction.c` file.

D.) This program is vulnerable to an integer overflow. Variables `size1` and `size2` are declared as unsigned integers which can hold large positive values, but the variable `size` is declared as a signed integer. When `size1` and `size2` are added together and the result stored in `size`, the value could be too large for `size` variable to hold, causing it to wrap around to a negative number. This could result is bypassing the check whether `size` is greater than `len` and result in too much data being written to the out buffer in the `memcpy()` functions. This could be fixed by changing `size` to an unsigned integer and adding another if-statement condition to anticipate for an integer overflow, as done in `get_two_vars.c` file.

E.) This program is potentially vulnerable to an integer overflow through arithmetic. When `arg.get_group_members.maxnum` is compared with 0 to check is it's less than or equal to, it doesn't check if an extremely large number was input by the user. If a large enough number is entered for `arg.get_group_members.maxnum`, then when it is multiplied by the `sizeof` operation within the `vmalloc()` function it can overflow causing the `ttl_array` and `user_array` to be smaller than planned. The r`sbac_acl_get_group_members()` function could end up copying more data than the `ttl_array` and `user_array` buffers can hold. However, since `vmalloc` is used an error will be displayed to prevent overflowing the buffers. This could also be fixed by adding a check on the upper bounds value of `arg.get_group_members.maxnum`.

Question 02

(format-string question)

Matthew Quander
12/17/2021
COSC647

Homework 02

Question 03:

Creating a new MySQL table called ‘client’ in the SEED VM and insert data:

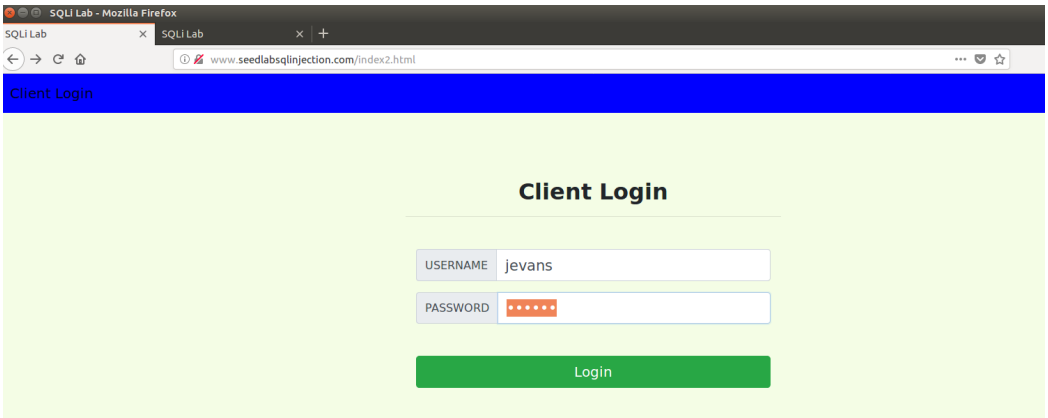
```
ERROR 1146 (42S02): Table 'Users.client' doesn't exist
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> CREATE table client(ID char(3), NAME varchar(20), AGE varchar(2), USERNAM
E varchar(10), PASSWORD varchar(10));
Query OK, 0 rows affected (0.02 sec)
```

```
mysql> INSERT into client VALUES(101, 'Andy', '29', 'asmith','asmith'), (102, 'J
oan', '31', 'jevans', 'jevans'), (103, 'Sean', '25', 'sandrews', 'sandrews');
Query OK, 3 rows affected (0.00 sec)
Records: 3  Duplicates: 0  Warnings: 0

mysql> select * from client;
+------+------+------+----------+----------+
| ID   | NAME | AGE  | USERNAME | PASSWORD |
+------+------+------+----------+----------+
| 101  | Andy | 29   | asmith   | asmith   |
| 102  | Joan | 31   | jevans   | jevans   |
| 103  | Sean | 25   | sandrews | sandrews |
+------+------+------+----------+----------+
3 rows in set (0.00 sec)
```

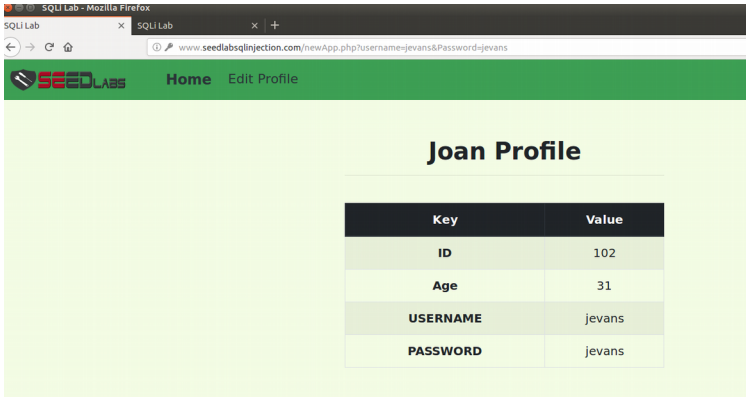
Create web application (html similar to SEED website for demo purposes) using HTML and PHP and demonstrate. See attached index.html and newApp.php files in the folder for Question 03:



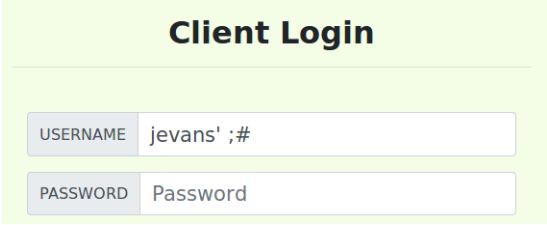
Matthew Quander
12/17/2021
COSC647

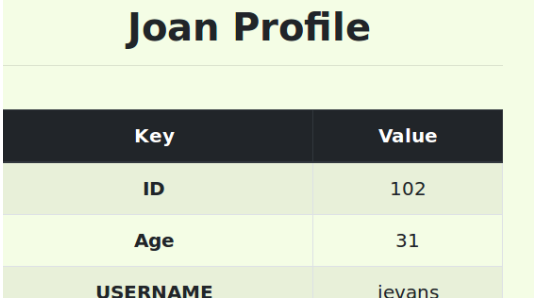
Homework 02

Login works correctly:



Web application suffers from SQL injection vulnerable, able to log in without password by closing the quote and commenting out the rest of the WHERE clause condition:



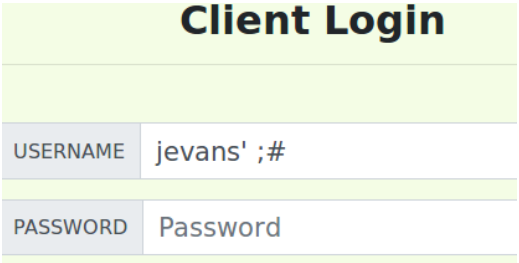


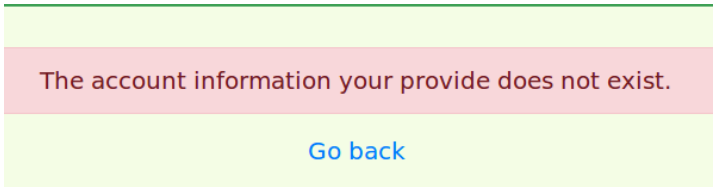
Made changes to `newApp.php`, see `newAppFixed.php`. In `newAppFixed.php`, I used the `prepare()` function a part of the `$conn` object and passed the query as a string to it. In the query, I placed question marks in for the values of the WHERE clause variables. Then I called the `bind_param()` function passing in "ss" for 2 strings and the variables for the `username` and `password`, followed by a call to `exeute()`. Then I called the `bind_result()` function to bind the results to the parameters. The `fetch()` function is called to obtain the results, then the connection is closed with the `close()` function call. SQL Injection no longer works:

```
// create a connection
$conn = getDB();
// Sql query to authenticate the user
$sql = $conn->prepare("SELECT ID, NAME, AGE, USERNAME, PASSWORI
FROM client
WHERE USERNAME= ? and PASSWORD= ?");
  $sql->bind_param("ss", $input_uname, $input_pwd);
  $sql->execute();
  $sql->bind_result($id, $name, $age, $username, $password);
  $sql->fetch();
  $sql->close();
```

Matthew Quander
12/17/2021
COSC647

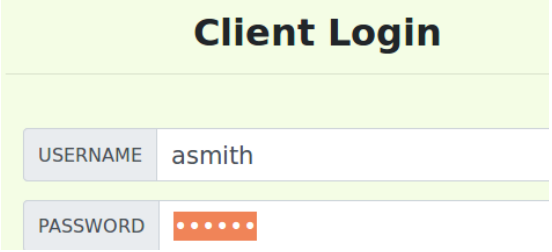
Homework 02

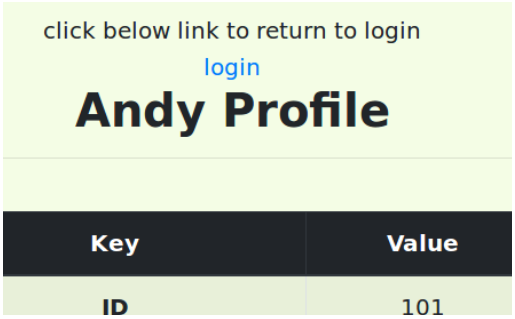




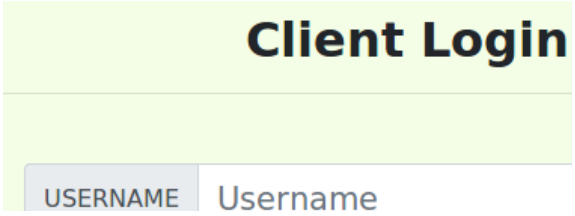
Question 04:

Using the same website, I created a link that is vulnerable to cross-site script exploitation through a link.





When the link is clicked, it returns to the login page but also opens a new tab that displays the current user's session cookie (PHPSESSID):



Matthew Quander
12/17/2021
COSC647

Homework 02

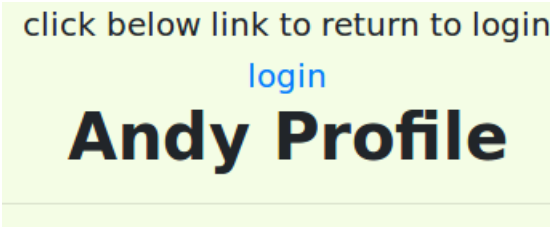
This vulnerability is caused by the script below in lines 131 and 132 of `newAppFixed.php`. The `href` link returns to the home login page, however, the `onclick` action opens a new tab that includes the user's session cookie information. By removing the malicious script to open the browser tab of session cookie info, it will retain the same functionality without the exploit.

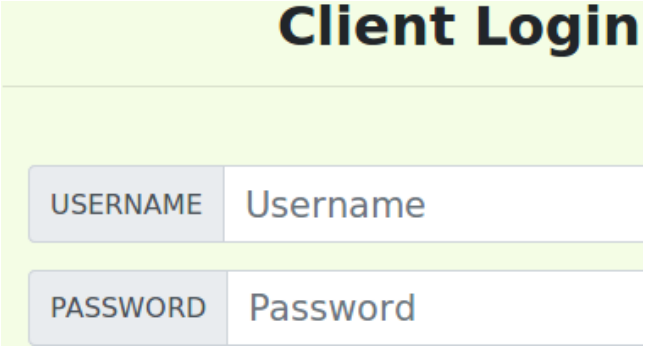
```
129            echo "<br> click below link to return to login<br>";
130
131 echo "<a  href='http://www.seedlabsqlinjection.com/index2.html' onclick='window.open
    (document.cookie)'; >
132          <img src='' style='height: 100px; width: 200px;' alt='login'></a>";
133
134            echo "<br><h1><b> $name Profile </b></h1>";
```

Malicious script removed below:

```
129            echo "<br> click below link to return to login<br>";
130
131 echo "<a  href='http://www.seedlabsqlinjection.com/index2.html'>
132          <img src='' style='height: 100px; width: 200px;' alt='login'></a>";
133
134            echo "<br><h1><b> $name Profile </b></h1>";
```

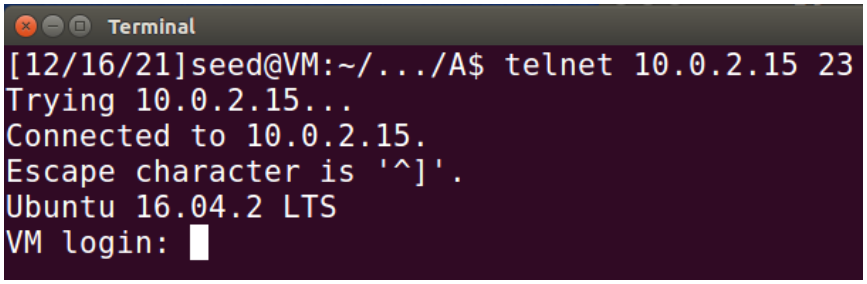
Clicking the link only returns the user to the login page, it doesn't open a new tab displaying the session cookie info.





Question 05:

a.) Blocking all telnet traffic (through port 23). First testing telnet command:



Matthew Quander
12/17/2021
COSC647

Homework 02

Run commands to compile `dropTelPackets.c` into a kernel module and install the kernel module (similar to how done in lab 7):

```
[12/16/21]seed@VM:~/.../A$ make args="dropTelPackets"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/Matthew_Quande
r_HW_02/Question_05/A modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/A/dropTelPackets.
o
/home/seed/Desktop/Matthew_Quander_HW_02/Question_05/A/dropTelPackets.c: In func
tion ‘init_module’:
/home/seed/Desktop/Matthew_Quander_HW_02/Question_05/A/dropTelPackets.c:62:3: wa
rning: ISO C90 forbids mixed declarations and code [-Wdeclaration-after-statemen
t]
   int result = nf_register_hook(&nfho);
   ^
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/A/dropTelPackets.
mod.o
  LD [M]  /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/A/dropTelPackets.
ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/16/21]seed@VM:~/.../A$ sudo insmod dropTelPackets.ko
[12/16/21]seed@VM:~/.../A$
```

Attempt telnet on machine’s port 23 again, no response:

```
[12/16/21]seed@VM:~/.../A$ telnet 10.0.2.15 23
Trying 10.0.2.15...
^C
[12/16/21]seed@VM:~/.../A$
```

Remove the `dropTelPackets` kernel module and attempt telnet command again, response received:

```
[12/16/21]seed@VM:~/.../A$ sudo rmmod dropTelPackets.ko
[12/16/21]seed@VM:~/.../A$ telnet 10.0.2.15 23
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```

b.) Block UDP packets on ports > 2500:
ping espn.com to show udp packets are being transmitted

```
Terminal
[12/16/21]seed@VM:~/.../B$ ping www.espn.com
PING www.espn.com (52.85.91.6) 56(84) bytes of data.
64 bytes from server-52-85-91-6.ord53.r.cloudfront.net (52.85.91.6): icmp_seq=1
ttl=227 time=36.5 ms
64 bytes from server-52-85-91-6.ord53.r.cloudfront.net (52.85.91.6): icmp_seq=2
ttl=227 time=39.1 ms
64 bytes from server-52-85-91-6.ord53.r.cloudfront.net (52.85.91.6): icmp_seq=3
ttl=227 time=41.2 ms
^C
--- www.espn.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 36.572/38.982/41.239/1.915 ms
[12/16/21]seed@VM:~/.../B$
```

Matthew Quander
12/17/2021
COSC647

Homework 02

Run commands to compile `dropUdpPackets.c` into a kernel module and install the kernel module (similar to previous steps):

```
Terminal
[12/16/21]seed@VM:~/.../B$ make args="dropUdpPackets"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/Matthew_Quande
r_HW_02/Question_05/B modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/B/dropUdpPackets.
o
/home/seed/Desktop/Matthew_Quander_HW_02/Question_05/B/dropUdpPackets.c: In func
tion ‘init_module’:
/home/seed/Desktop/Matthew_Quander_HW_02/Question_05/B/dropUdpPackets.c:47:3: wa
rning: ISO C90 forbids mixed declarations and code [-Wdeclaration-after-statemen
t]
   int result = nf_register_hook(&nfho);
   ^
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/B/dropUdpPackets.
mod.o
  LD [M]  /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/B/dropUdpPackets.
ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/16/21]seed@VM:~/.../B$
```

```
Terminal
12/16/21]seed@VM:~/.../B$ sudo insmod dropUdpPackets.ko
12/16/21]seed@VM:~/.../B$
```

packets not received, espn.com not recognized:

```
12/16/21]seed@VM:~/.../B$ ping www.espn.com
ping: unknown host www.espn.com
12/16/21]seed@VM:~/.../B$
```

check syslog, it displays string from the `dropUdpPackets.c` file, that Udp packets on ports > 2500 were dropped:

```
Terminal
[12/16/21]seed@VM:~/.../B$ tail /var/log/syslog
Dec 16 13:23:42 VM kernel: [ 4172.338499] Firewall : drop udp traffic on ports >
 2500
Dec 16 13:24:04 VM kernel: [ 4194.315284] Firewall : drop udp traffic on ports >
 2500
Dec 16 13:24:09 VM kernel: [ 4199.335987] Firewall : drop udp traffic on ports >
 2500
Dec 16 13:24:14 VM kernel: [ 4204.340748] Firewall : drop udp traffic on ports >
 2500
Dec 16 13:24:19 VM kernel: [ 4209.340896] Firewall : drop udp traffic on ports >
 2500
```

Matthew Quander
12/17/2021
COSC647

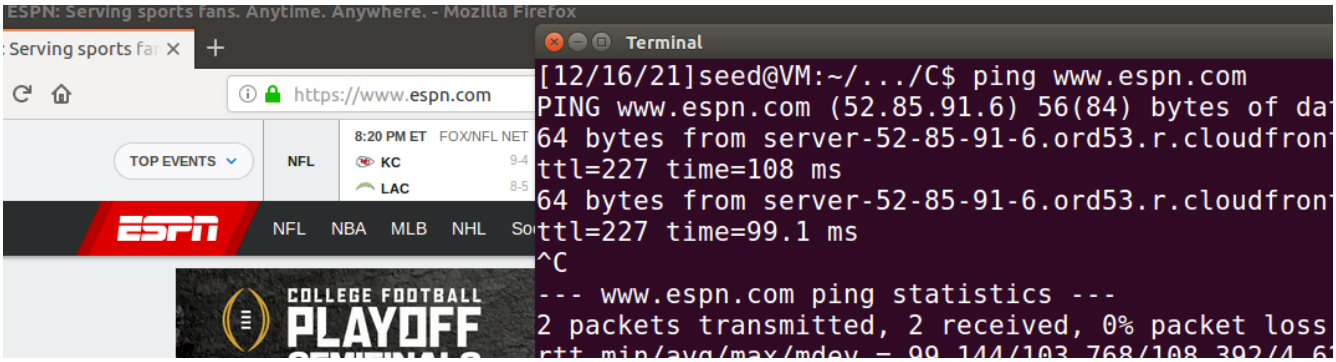
Homework 02

Removing the dropUdpPackets kernel object and pinging espn.com, packets are received again:

```
Terminal
[12/16/21]seed@VM:~/.../B$ sudo rmmod dropUdpPackets.ko
[12/16/21]seed@VM:~/.../B$ ping www.espn.com
PING www.espn.com (13.226.190.113) 56(84) bytes of data.
64 bytes from server-13-226-190-113.dfw55.r.cloudfront.net (13.226.190.113): icm
p_seq=1 ttl=227 time=45.5 ms
64 bytes from server-13-226-190-113.dfw55.r.cloudfront.net (13.226.190.113): icm
p_seq=2 ttl=227 time=48.4 ms
^C
--- www.espn.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
```

c.) Only allow web traffic

ping espn.com and open in the browser to show web packets allowed:



Run commands to compile `allowWebPackets.c` into a kernel module and install the kernel module (similar to previous steps):

```
Terminal
[12/16/21]seed@VM:~/.../C$ make args="allowWebPackets"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/Ma
r_HW_02/Question_05/C modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/16/21]seed@VM:~/.../C$ sudo insmod allowWebPackets.ko
[12/16/21]seed@VM:~/.../C$
```

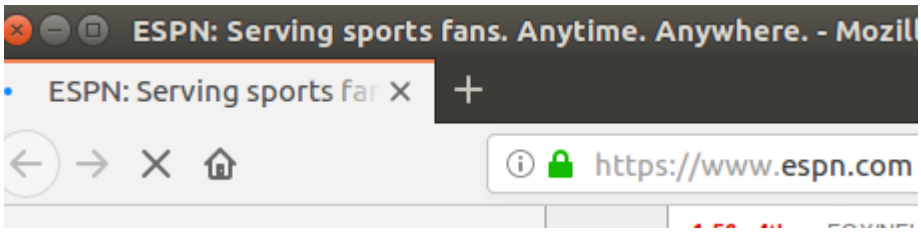
Matthew Quander
12/17/2021
COSC647

Homework 02

Ping espn.com to test, no response; checking the system log, the packets were dropped; in the browser the page partially reloads after the allowWebPackets module is installed:

```
Terminal
[12/16/21]seed@VM:~/.../C$ ping www.espn.com
ping: unknown host www.espn.com
[12/16/21]seed@VM:~/.../C$
```

```
/16/21]seed@VM:~/.../C$ tail /var/log/syslog
 16 15:51:23 VM kernel: [13033.229711] Firewall : Packet dropped
 16 15:51:23 VM kernel: [13033.239998] Firewall : Packet dropped
 16 15:51:23 VM kernel: [13033.240001] Firewall : Packet dropped
 16 15:51:23 VM kernel: [13033.301401] Firewall : Packet dropped
 16 15:51:27 VM kernel: [13038.060072] Firewall : Packet dropped
 16 15:51:27 VM kernel: [13038.060075] Firewall : Packet dropped
 16 15:51:28 VM kernel: [13038.234775] Firewall : Packet dropped
 16 15:51:28 VM kernel: [13038.234778] Firewall : Packet dropped
 16 15:51:28 VM kernel: [13038.245744] Firewall : Packet dropped
 16 15:51:28 VM kernel: [13038.245746] Firewall : Packet dropped
/16/21]seed@VM:~/.../C$
```



d.) Only block web traffic from espn.com, allow all other traffic.

Ping espn.com to check that packets are sent and received:

```
Terminal
[12/16/21]seed@VM:~/.../D$ ping www.espn.com
PING www.espn.com (52.85.91.32) 56(84) bytes of data.
64 bytes from server-52-85-91-32.ord53.r.cloudfront.n
1 ttl=227 time=34.2 ms
64 bytes from server-52-85-91-32.ord53.r.cloudfront.n
2 ttl=227 time=33.0 ms
64 bytes from server-52-85-91-32.ord53.r.cloudfront.n
3 ttl=227 time=33.2 ms
64 bytes from server-52-85-91-32.ord53.r.cloudfront.n
4 ttl=227 time=33.1 ms
64 bytes from server-52-85-91-32.ord53.r.cloudfront.n
5 ttl=227 time=34.1 ms
^C
--- www.espn.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, ti
rtt min/avg/max/mdev = 33.082/33.580/34.289/0.557 ms
```

Matthew Quander
12/17/2021
COSC647

Homework 02

Run commands to compile `dropEspnPackets.c` into a kernel module and install the kernel module (similar to previous steps):

```
Terminal
[12/16/21]seed@VM:~/.../D$ make args="dropEspnPackets"
make -C /lib/modules/4.8.0-36-generic/build  M=/home/seed/Desktop/Matthew_Quande
r_HW_02/Question_05/D modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/D/dropEspnPackets
.o
/home/seed/Desktop/Matthew_Quander_HW_02/Question_05/D/dropEspnPackets.c: In fun
ction 'init_module':
/home/seed/Desktop/Matthew_Quander_HW_02/Question_05/D/dropEspnPackets.c:39:3: w
arning: ISO C90 forbids mixed declarations and code [-Wdeclaration-after-stateme
nt]
   int result = nf_register_hook(&nfho);
   ^
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/D/dropEspnPackets
.mod.o
  LD [M]  /home/seed/Desktop/Matthew_Quander_HW_02/Question_05/D/dropEspnPackets
.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[12/16/21]seed@VM:~/.../D$ sudo insmod dropEspnPackets.ko
[12/16/21]seed@VM:~/.../D$
```

First get all associated IP addresses of espn.com through `$nslookup` and `$ping` commands.

```
Terminal
[12/16/21]seed@VM:~/.../C$ nslookup www.espn.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   www.espn.com
Address: 52.85.91.93
Name:   www.espn.com
Address: 52.85.91.129
Name:   www.espn.com
Address: 52.85.91.32
Name:   www.espn.com
Address: 52.85.91.6

[12/16/21]seed@VM:~/.../C$
```

Matthew Quander
12/17/2021
COSC647

Homework 02

Add those IP addresses to the condition to compare to the character array `url` in `dropEspnPackets.c`. Use `$ping` command on espn.com again and observe no packets received, but packets from other url's received:

```
Terminal
[12/16/21]seed@VM:~/.../C$ ping www.espn.com
PING www.espn.com (52.85.91.129) 56(84) bytes of data.
^C
--- www.espn.com ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10242ms

[12/16/21]seed@VM:~/.../C$ ping www.bing.com
PING dual-a-0001.a-msedge.net (13.107.21.200) 56(84) bytes of data.
64 bytes from 13.107.21.200: icmp_seq=1 ttl=115 time=15.6 ms
64 bytes from 13.107.21.200: icmp_seq=2 ttl=115 time=16.5 ms
^C
--- dual-a-0001.a-msedge.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 15.630/16.102/16.574/0.472 ms
[12/16/21]seed@VM:~/.../C$ ping www.yahoo.com
PING new-fp-shed.wg1.b.yahoo.com (74.6.231.21) 56(84) bytes of data.
64 bytes from media-router-fp74.prod.media.vip.ne1.yahoo.com (74.6.231.21
_seq=1 ttl=49 time=46.4 ms
64 bytes from media-router-fp74.prod.media.vip.ne1.yahoo.com (74.6.231.21
_seq=2 ttl=49 time=45.2 ms
^C
--- new-fp-shed.wg1.b.yahoo.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 45.229/45.854/46.480/0.661 ms
```

Remove kernel module and ping espn.com, packets are received again:

```
[12/16/21]seed@VM:~/.../D$ sudo rmmod dropEspnPackets.ko
[12/16/21]seed@VM:~/.../D$ ping www.espn.com
PING www.espn.com (52.85.91.93) 56(84) bytes of data.
64 bytes from server-52-85-91-93.ord53.r.cloudfront.net (52.85.91.93
1 ttl=227 time=32.9 ms
64 bytes from server-52-85-91-93.ord53.r.cloudfront.net (52.85.91.93
2 ttl=227 time=33.5 ms
64 bytes from server-52-85-91-93.ord53.r.cloudfront.net (52.85.91.93
3 ttl=227 time=34.2 ms
^C
--- www.espn.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.962/33.602/34.287/0.562 ms
[12/16/21]seed@VM:~/.../D$
```