```
*************************************************************************************
Peter Knight


This text file contains the answers to the exercises. Some answers are "missing"
as these are in picture form and will be in the github.
*************************************************************************************





*********************************************************************************************
https://github.com/shadman48/CS_380_Exercise_5
*********************************************************************************************


Step 3.2.1 - PACKET SNIFFER
****************************
VM - SEED UBUNTU (MAIN)
----------------------------
[10/29/2017 18:19] seed@ubuntu:~/Downloads$ sudo ./sniffex eth14
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth14
Number of packets: 10
Filter expression: ip

Packet number 1:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 2:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 3:
       From: 10.0.2.5
         To: 10.0.2.3
   Protocol: UDP

Packet number 4:
       From: 10.0.2.3
         To: 255.255.255.255
   Protocol: UDP

Packet number 5:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 6:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 7:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 8:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 9:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 10:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Capture complete.


----------------------------
VM - SEED UBUNTU (CLONE)
----------------------------
[10/29/2017 18:14] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.470 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.450 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.391 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.351 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.414 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.351/0.415/0.470/0.044 ms








Step 3.2.2 - TCP ONLY PACKETS
****************************
VM - SEED UBUNTU (MAIN)
----------------------------
[10/29/2017 20:10] seed@ubuntu:~/Downloads$ sudo ./sniffex eth14
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth14
Number of packets: 10
Filter expression: tcp

&&&&&&&&&&&&&&&&&&&&&&&&&&&&
After changing what packets to sniff to TCP there were no results as there were no tcp
packets being sent out.
&&&&&&&&&&&&&&&&&&&&&&&&&&&&

----------------------------
```

```
VM - SEED UBUNTU (CLONE)
----------------------------
[10/29/2017 20:09] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.331 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.366 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.412 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.279 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.429 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.279/0.363/0.429/0.057 ms
```

Step 3.3 - PASSWORD SNIFFING.
****************************
SEE PICTURE FOR FIRST PART.

```
----------------------------
VM - SEED UBUNTU (MAIN)
----------------------------
[10/30/2017 19:50] seed@ubuntu:~/Downloads$ sudo ./sniffex eth14
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth14
Number of packets: 45
Filter expression: tcp

Packet number 1:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 2:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 3:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 4:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (27 bytes):
00000   ff fd 03 ff fb 18 ff fb  1f ff fb 20 ff fb 21 ff    ........... ..!.
00016   fb 22 ff fb 27 ff fd 05  ff fb 23                   ."..'.....#
```

```

Packet number 5:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 6:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (12 bytes):
00000   ff fd 18 ff fd 20 ff fd  23 ff fd 27                ..... ..#..'

Packet number 7:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 8:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (39 bytes):
00000   ff fb 03 ff fd 1f ff fd  21 ff fe 22 ff fb 05 ff    ........!.."....
00016   fa 20 01 ff f0 ff fa 23  01 ff f0 ff fa 27 01 ff    . .....#.....'..
00032   f0 ff fa 18 01 ff f0                                .......

Packet number 9:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 10:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (74 bytes):
00000   ff fa 1f 00 3c 00 1c ff  f0 ff fa 20 00 33 38 34    ....<...... .384
00016   30 30 2c 33 38 34 30 30  ff f0 ff fa 23 00 75 62    00,38400....#.ub
00032   75 6e 74 75 3a 30 ff f0  ff fa 27 00 00 44 49 53    untu:0....'..DIS
00048   50 4c 41 59 01 75 62 75  6e 74 75 3a 30 ff f0 ff    PLAY.ubuntu:0...
00064   fa 18 00 78 74 65 72 6d  ff f0                      ...xterm..

Packet number 11:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 12:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (3 bytes):
00000   ff fd 01                                            ...

Packet number 13:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (3 bytes):
00000   ff fc 01                                            ...

Packet number 14:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (3 bytes):
00000   ff fb 01                                            ...

Packet number 15:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (3 bytes):
00000   ff fd 01                                            ...

Packet number 16:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (20 bytes):
00000   55 62 75 6e 74 75 20 31  32 2e 30 34 2e 32 20 4c    Ubuntu 12.04.2 L
00016   54 53 0d 0a                                         TS..

Packet number 17:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 18:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (14 bytes):
00000   75 62 75 6e 74 75 20 6c  6f 67 69 6e 3a 20          ubuntu login:

Packet number 19:
       From: 10.0.2.4
```

```
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 20:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   73                                                  s

Packet number 21:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (1 bytes):
00000   73                                                  s

Packet number 22:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 23:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 24:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (1 bytes):
00000   65                                                  e

Packet number 25:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 26:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e
```

```

Packet number 27:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (1 bytes):
00000   65                                                  e

Packet number 28:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 29:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   64                                                  d

Packet number 30:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (1 bytes):
00000   64                                                  d

Packet number 31:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 32:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (2 bytes):
00000   0d 00                                               ..

Packet number 33:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (12 bytes):
00000   0d 0a 50 61 73 73 77 6f  72 64 3a 20                ..Password:

Packet number 34:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23

Packet number 35:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   64                                                  d

Packet number 36:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 37:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 38:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 39:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 40:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 41:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (1 bytes):
00000   73                                                  s

Packet number 42:
       From: 10.0.2.5
```

```
          To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 43:
        From: 10.0.2.4
          To: 10.0.2.5
   Protocol: TCP
   Src port: 37513
   Dst port: 23
   Payload (2 bytes):
00000   0d 00                                                 ..

Packet number 44:
        From: 10.0.2.5
          To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513

Packet number 45:
        From: 10.0.2.5
          To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 37513
   Payload (2 bytes):
00000   0d 0a                                                 ..

Capture complete.

----------------------------
VM - SEED UBUNTU (CLONE)
----------------------------
[10/30/2017 19:51] seed@ubuntu:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Mon Oct 30 19:38:45 PDT 2017 from ubuntu.local on pts/3
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[10/30/2017 19:51] seed@ubuntu:~$ exit
logout
Connection closed by foreign host.




Step 3.3 - PASSWORD SNIFFING.
****************************
----------------------------
VM - SEED UBUNTU (MAIN)
----------------------------
........... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'.............<...... .3
```

```
ubuntu login: sseeeedd .
Password: dees .
Last login: Mon Oct 30 19:51:24 PDT 2017 from ubuntu.local on pts/3
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[10/30/2017 19:56] seed@ubuntu:~$ eexxiitt .
logout
----------------------------
VM - SEED UBUNTU (CLONE)
----------------------------
[10/30/2017 19:55] seed@ubuntu:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Mon Oct 30 19:51:24 PDT 2017 from ubuntu.local on pts/3
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[10/30/2017 19:56] seed@ubuntu:~$ exit
logout
Connection closed by foreign host
```

&&&&&&&&&&&&&&&&&&&&&&&&&&&&

After changing to Wireshark instead of using my own sniffer, I can still locate the users username as well as their password. You can view this in the images.

Telnet as from what I have seen so far and with my limited knowlage, does not seem to present itself as a security wise choice. It was very easy to sniff the packets and gain username and password in matter of seconds.

&&&&&&&&&&&&&&&&&&&&&&&&&&&&

Step 3.3 - SSH.

****************************

```
----------------------------
VM - SEED UBUNTU (MAIN)
----------------------------
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
.........>..t...-........ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie
-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1...:ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-
nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01
@openssh.com,ssh-dss-cert-v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-dss-cert-v00
@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss.
...aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc
,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....aes128-ctr,
aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,
aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....hmac-md5,hmac-sha1,umac-64
@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,
hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....hmac-md5,hmac-sha1,umac-64
@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,
hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....none,zlib@openssh.com,zlib....none,
zlib@openssh.com,zlib......................L.....A.....Y.8...F.Q..4.T.w..F..i..~..Pe6..
W..(\*..B.G.:..0..B.....&...........
............~..;.>..\......x.E........#\h>......+.Y.?$.%.-d.M1..:nWa,.$@.....J.....|..Ub
...."..I.....`.....'s..=..F4.&.8lx...a..b(..:.f6.;.....k.0+w+..eY..1~z...[uu........B<..N
.+h.9.....`z..k..ubZ...2....*.p.#..FI..Piw-..d......F<&y..U.1.Q....:.........J?..#.... .>..
.K.:..w%..h..^.EL....'..N.C~.-..M.C.^...%.....NI7..+.p..>B..M....;c...v...bBq.]..W..C.V..m
...(....f.>.U&..)3..._~..i%...Z.....<T.D.....E;je.d... ...$.B..8..A..C?.X....GSo..5n......
......g.a..$.4..D. a,......9.....2FQ.[...jL...;Z....(O.Q5B..-@..I7@'D.Ym..NF...q.1...2O..J
......A.e.....V0Kjf...3....kF.....v.{w.s#.o.r3...=k.......c/.6...X.49.....G.8.O...@....\..
\..B....K..8r.j.r......F...?...X..u..Z...i.h.]F.5......X.......~..~.(. ......#.p~.I<i..?H3
=Dq....<`.....|Wg."xX._u....?.....}1!.....,...K.'-F.-..5..+.. o..Q....,8....<....t8x).;.%.
..69i
Z..r....!."../..U.....^z..L.....7.....t.<(.............l.M..F.v>.T.n..{.O.F..E)V$.|.^...x
.W.$X@f...'.....Tx../.i.q.......tc...%._W8....*.s..l70....e..mwU?.2S~..hX..F. ...$R aY..4
._.>./........P;..+g.T .'.L.-_gR/.n,.O..= .$"...4.s:.8F............e K.7+..}a....VwK.....
.*#....{.q.....%........(.Vhn:....P..?xy..Q>|.Hs....}...X..s....?......\..SU.c.G...&.7=Y.
..N.a....






----------------------------
VM - SEED UBUNTU (CLONE)
----------------------------
[10/30/2017 20:26] seed@ubuntu:~$ ssh seed@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ECDSA key fingerprint is 81:82:a9:af:bd:93:78:f9:1a:a7:ca:7f:e8:d6:6c:04.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.5' (ECDSA) to the list of known hosts.
seed@10.0.2.5's password: 
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Oct 30 19:56:21 2017 from ubuntu.local
[10/30/2017 20:27] seed@ubuntu:~$ exit
logout
Connection to 10.0.2.5 closed.
```

&&&&&&&&&&&&&&&&&&&&&&&&&&&&

When changing from telnet to SSH and then repeating the above, there is no wayy to openly view the username and password as the SSH has encrypted the data.

&&&&&&&&&&&&&&&&&&&&&&&&&&&&