

```
1
2
3 *****
4 Peter Knight
5
6
7 This text file contains the answers to the exercises. Some answers are "missing"
8 as these are in picture form and will be in the github.
9 *****
10
11
12
13
14
15 *****
16 https://github.com/shadman48/CS_380_Exercise_5
17 *****
18
19
20 Step 3.2.1 - PACKET SNIFFER
21 *****
22 VM - SEED UBUNTU (MAIN)
23 -----
24 [10/29/2017 18:19] seed@ubuntu:~/Downloads$ sudo ./sniffex eth14
25 sniffex - Sniffer example using libpcap
26 Copyright (c) 2005 The Tcpdump Group
27 THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.
28
29 Device: eth14
30 Number of packets: 10
31 Filter expression: ip
32
33 Packet number 1:
34     From: 10.0.2.4
35     To: 10.0.2.5
36     Protocol: ICMP
37
38 Packet number 2:
39     From: 10.0.2.5
40     To: 10.0.2.4
41     Protocol: ICMP
42
43 Packet number 3:
44     From: 10.0.2.5
45     To: 10.0.2.3
46     Protocol: UDP
47
48 Packet number 4:
49     From: 10.0.2.3
50     To: 255.255.255.255
51     Protocol: UDP
52
53 Packet number 5:
54     From: 10.0.2.4
55     To: 10.0.2.5
56     Protocol: ICMP
57
58 Packet number 6:
59     From: 10.0.2.5
60     To: 10.0.2.4
61     Protocol: ICMP
62
63 Packet number 7:
```

[illegible]

```
127 VM - SEED UBUNTU (CLONE)
128 -----
129 [10/29/2017 20:09] seed@ubuntu:~$ ping -c 5 10.0.2.5
130 PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
131 64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.331 ms
132 64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.366 ms
133 64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.412 ms
134 64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.279 ms
135 64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.429 ms
136
137 --- 10.0.2.5 ping statistics ---
138 5 packets transmitted, 5 received, 0% packet loss, time 3997ms
139 rtt min/avg/max/mdev = 0.279/0.363/0.429/0.057 ms
140
141
142
143
144 Step 3.3 - PASSWORD SNIFFING.
145 *****
146 SEE PICTURE FOR FIRST PART.
147
148 -----
149 VM - SEED UBUNTU (MAIN)
150 -----
151 [10/30/2017 19:50] seed@ubuntu:~/Downloads$ sudo ./sniffex eth14
152 sniffex - Sniffer example using libpcap
153 Copyright (c) 2005 The Tcpdump Group
154 THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.
155
156 Device: eth14
157 Number of packets: 45
158 Filter expression: tcp
159
160 Packet number 1:
161     From: 10.0.2.4
162     To: 10.0.2.5
163     Protocol: TCP
164     Src port: 37513
165     Dst port: 23
166
167 Packet number 2:
168     From: 10.0.2.5
169     To: 10.0.2.4
170     Protocol: TCP
171     Src port: 23
172     Dst port: 37513
173
174 Packet number 3:
175     From: 10.0.2.4
176     To: 10.0.2.5
177     Protocol: TCP
178     Src port: 37513
179     Dst port: 23
180
181 Packet number 4:
182     From: 10.0.2.4
183     To: 10.0.2.5
184     Protocol: TCP
185     Src port: 37513
186     Dst port: 23
187     Payload (27 bytes):
188 00000  ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb 21 ff ..... ..!.
189 00016  fb 22 ff fb 27 ff fd 05 ff fb 23 .....#
```

```
190
191 Packet number 5:
192     From: 10.0.2.5
193     To: 10.0.2.4
194     Protocol: TCP
195     Src port: 23
196     Dst port: 37513
197
198 Packet number 6:
199     From: 10.0.2.5
200     To: 10.0.2.4
201     Protocol: TCP
202     Src port: 23
203     Dst port: 37513
204     Payload (12 bytes):
205 00000 ff fd 18 ff fd 20 ff fd 23 ff fd 27 ..... ..#..'
206
207 Packet number 7:
208     From: 10.0.2.4
209     To: 10.0.2.5
210     Protocol: TCP
211     Src port: 37513
212     Dst port: 23
213
214 Packet number 8:
215     From: 10.0.2.5
216     To: 10.0.2.4
217     Protocol: TCP
218     Src port: 23
219     Dst port: 37513
220     Payload (39 bytes):
221 00000 ff fb 03 ff fd 1f ff fd 21 ff fe 22 ff fb 05 ff .....!..."....
222 00016 fa 20 01 ff f0 ff fa 23 01 ff f0 ff fa 27 01 ff . ....#.....'..
223 00032 f0 ff fa 18 01 ff f0 .....
224
225 Packet number 9:
226     From: 10.0.2.4
227     To: 10.0.2.5
228     Protocol: TCP
229     Src port: 37513
230     Dst port: 23
231
232 Packet number 10:
233     From: 10.0.2.4
234     To: 10.0.2.5
235     Protocol: TCP
236     Src port: 37513
237     Dst port: 23
238     Payload (74 bytes):
239 00000 ff fa 1f 00 3c 00 1c ff f0 ff fa 20 00 33 38 34 ....<..... .384
240 00016 30 30 2c 33 38 34 30 30 ff f0 ff fa 23 00 75 62 00,38400.....#.ub
241 00032 75 6e 74 75 3a 30 ff f0 ff fa 27 00 00 44 49 53 untu:0.....'..DIS
242 00048 50 4c 41 59 01 75 62 75 6e 74 75 3a 30 ff f0 ff PLAY.ubuntu:0...
243 00064 fa 18 00 78 74 65 72 6d ff f0 ...xterm..
244
245 Packet number 11:
246     From: 10.0.2.5
247     To: 10.0.2.4
248     Protocol: TCP
249     Src port: 23
250     Dst port: 37513
251
252 Packet number 12:
```

```
253      From: 10.0.2.5
254      To: 10.0.2.4
255      Protocol: TCP
256      Src port: 23
257      Dst port: 37513
258      Payload (3 bytes):
259 00000  ff fd 01      ...
260
261 Packet number 13:
262      From: 10.0.2.4
263      To: 10.0.2.5
264      Protocol: TCP
265      Src port: 37513
266      Dst port: 23
267      Payload (3 bytes):
268 00000  ff fc 01      ...
269
270 Packet number 14:
271      From: 10.0.2.5
272      To: 10.0.2.4
273      Protocol: TCP
274      Src port: 23
275      Dst port: 37513
276      Payload (3 bytes):
277 00000  ff fb 01      ...
278
279 Packet number 15:
280      From: 10.0.2.4
281      To: 10.0.2.5
282      Protocol: TCP
283      Src port: 37513
284      Dst port: 23
285      Payload (3 bytes):
286 00000  ff fd 01      ...
287
288 Packet number 16:
289      From: 10.0.2.5
290      To: 10.0.2.4
291      Protocol: TCP
292      Src port: 23
293      Dst port: 37513
294      Payload (20 bytes):
295 00000  55 62 75 6e 74 75 20 31 32 2e 30 34 2e 32 20 4c  Ubuntu 12.04.2 L
296 00016  54 53 0d 0a      TS..
297
298 Packet number 17:
299      From: 10.0.2.4
300      To: 10.0.2.5
301      Protocol: TCP
302      Src port: 37513
303      Dst port: 23
304
305 Packet number 18:
306      From: 10.0.2.5
307      To: 10.0.2.4
308      Protocol: TCP
309      Src port: 23
310      Dst port: 37513
311      Payload (14 bytes):
312 00000  75 62 75 6e 74 75 20 6c 6f 67 69 6e 3a 20  ubuntu login:
313
314 Packet number 19:
315      From: 10.0.2.4
```

```
316         To: 10.0.2.5
317     Protocol: TCP
318     Src port: 37513
319     Dst port: 23
320
321 Packet number 20:
322     From: 10.0.2.4
323     To: 10.0.2.5
324     Protocol: TCP
325     Src port: 37513
326     Dst port: 23
327     Payload (1 bytes):
328 00000    73                                     s
329
330 Packet number 21:
331     From: 10.0.2.5
332     To: 10.0.2.4
333     Protocol: TCP
334     Src port: 23
335     Dst port: 37513
336     Payload (1 bytes):
337 00000    73                                     s
338
339 Packet number 22:
340     From: 10.0.2.4
341     To: 10.0.2.5
342     Protocol: TCP
343     Src port: 37513
344     Dst port: 23
345
346 Packet number 23:
347     From: 10.0.2.4
348     To: 10.0.2.5
349     Protocol: TCP
350     Src port: 37513
351     Dst port: 23
352     Payload (1 bytes):
353 00000    65                                     e
354
355 Packet number 24:
356     From: 10.0.2.5
357     To: 10.0.2.4
358     Protocol: TCP
359     Src port: 23
360     Dst port: 37513
361     Payload (1 bytes):
362 00000    65                                     e
363
364 Packet number 25:
365     From: 10.0.2.4
366     To: 10.0.2.5
367     Protocol: TCP
368     Src port: 37513
369     Dst port: 23
370
371 Packet number 26:
372     From: 10.0.2.4
373     To: 10.0.2.5
374     Protocol: TCP
375     Src port: 37513
376     Dst port: 23
377     Payload (1 bytes):
378 00000    65                                     e
```

```
379
380 Packet number 27:
381     From: 10.0.2.5
382     To: 10.0.2.4
383     Protocol: TCP
384     Src port: 23
385     Dst port: 37513
386     Payload (1 bytes):
387 000000 65 e
388
389 Packet number 28:
390     From: 10.0.2.4
391     To: 10.0.2.5
392     Protocol: TCP
393     Src port: 37513
394     Dst port: 23
395
396 Packet number 29:
397     From: 10.0.2.4
398     To: 10.0.2.5
399     Protocol: TCP
400     Src port: 37513
401     Dst port: 23
402     Payload (1 bytes):
403 000000 64 d
404
405 Packet number 30:
406     From: 10.0.2.5
407     To: 10.0.2.4
408     Protocol: TCP
409     Src port: 23
410     Dst port: 37513
411     Payload (1 bytes):
412 000000 64 d
413
414 Packet number 31:
415     From: 10.0.2.4
416     To: 10.0.2.5
417     Protocol: TCP
418     Src port: 37513
419     Dst port: 23
420
421 Packet number 32:
422     From: 10.0.2.4
423     To: 10.0.2.5
424     Protocol: TCP
425     Src port: 37513
426     Dst port: 23
427     Payload (2 bytes):
428 000000 0d 00 ..
429
430 Packet number 33:
431     From: 10.0.2.5
432     To: 10.0.2.4
433     Protocol: TCP
434     Src port: 23
435     Dst port: 37513
436     Payload (12 bytes):
437 000000 0d 0a 50 61 73 73 77 6f 72 64 3a 20 ..Password:
438
439 Packet number 34:
440     From: 10.0.2.4
441     To: 10.0.2.5
```

```
442 Protocol: TCP
443 Src port: 37513
444 Dst port: 23
445
446 Packet number 35:
447     From: 10.0.2.4
448     To: 10.0.2.5
449 Protocol: TCP
450 Src port: 37513
451 Dst port: 23
452 Payload (1 bytes):
453 00000 64
454
455 Packet number 36:
456     From: 10.0.2.5
457     To: 10.0.2.4
458 Protocol: TCP
459 Src port: 23
460 Dst port: 37513
461
462 Packet number 37:
463     From: 10.0.2.4
464     To: 10.0.2.5
465 Protocol: TCP
466 Src port: 37513
467 Dst port: 23
468 Payload (1 bytes):
469 00000 65
470
471 Packet number 38:
472     From: 10.0.2.5
473     To: 10.0.2.4
474 Protocol: TCP
475 Src port: 23
476 Dst port: 37513
477
478 Packet number 39:
479     From: 10.0.2.4
480     To: 10.0.2.5
481 Protocol: TCP
482 Src port: 37513
483 Dst port: 23
484 Payload (1 bytes):
485 00000 65
486
487 Packet number 40:
488     From: 10.0.2.5
489     To: 10.0.2.4
490 Protocol: TCP
491 Src port: 23
492 Dst port: 37513
493
494 Packet number 41:
495     From: 10.0.2.4
496     To: 10.0.2.5
497 Protocol: TCP
498 Src port: 37513
499 Dst port: 23
500 Payload (1 bytes):
501 00000 73
502
503 Packet number 42:
504     From: 10.0.2.5
```

d

e

e

s


```
505         To: 10.0.2.4
506     Protocol: TCP
507     Src port: 23
508     Dst port: 37513
509
510 Packet number 43:
511     From: 10.0.2.4
512     To: 10.0.2.5
513     Protocol: TCP
514     Src port: 37513
515     Dst port: 23
516     Payload (2 bytes):
517 00000 0d 00 ..
518
519 Packet number 44:
520     From: 10.0.2.5
521     To: 10.0.2.4
522     Protocol: TCP
523     Src port: 23
524     Dst port: 37513
525
526 Packet number 45:
527     From: 10.0.2.5
528     To: 10.0.2.4
529     Protocol: TCP
530     Src port: 23
531     Dst port: 37513
532     Payload (2 bytes):
533 00000 0d 0a ..
534
535 Capture complete.
536
537 -----
538 VM - SEED UBUNTU (CLONE)
539 -----
540 [10/30/2017 19:51] seed@ubuntu:~$ telnet 10.0.2.5
541 Trying 10.0.2.5...
542 Connected to 10.0.2.5.
543 Escape character is '^]'.
544 Ubuntu 12.04.2 LTS
545 ubuntu login: seed
546 Password:
547 Last login: Mon Oct 30 19:38:45 PDT 2017 from ubuntu.local on pts/3
548 Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)
549
550 * Documentation:  https://help.ubuntu.com/
551
552 New release '14.04.1 LTS' available.
553 Run 'do-release-upgrade' to upgrade to it.
554
555 [10/30/2017 19:51] seed@ubuntu:~$ exit
556 logout
557 Connection closed by foreign host.
558
559
560
561
562 Step 3.3 - PASSWORD SNIFFING.
563 *****
564 -----
565 VM - SEED UBUNTU (MAIN)
566 -----
567 ..... ..!..".'.#..... ..#..'.!..".#.....'.<.....
```

```

568 ubuntu login: sseeedd .
569 Password: dees .
570 Last login: Mon Oct 30 19:51:24 PDT 2017 from ubuntu.local on pts/3
571 Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)
572 
573 * Documentation: https://help.ubuntu.com/
574 
575 New release '14.04.1 LTS' available.
576 Run 'do-release-upgrade' to upgrade to it.
577 
578 [10/30/2017 19:56] seed@ubuntu:~$ eexxiitt .
579 logout
580 -----
581 VM - SEED UBUNTU (CLONE)
582 -----
583 [10/30/2017 19:55] seed@ubuntu:~$ telnet 10.0.2.5
584 Trying 10.0.2.5...
585 Connected to 10.0.2.5.
586 Escape character is '^]'.
587 Ubuntu 12.04.2 LTS
588 ubuntu login: seed
589 Password:
590 Last login: Mon Oct 30 19:51:24 PDT 2017 from ubuntu.local on pts/3
591 Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)
592 
593 * Documentation: https://help.ubuntu.com/
594 
595 New release '14.04.1 LTS' available.
596 Run 'do-release-upgrade' to upgrade to it.
597 
598 [10/30/2017 19:56] seed@ubuntu:~$ exit
599 logout
600 Connection closed by foreign host
601 
602 
603 
604 
605 
606 
607 
608 &&&&&&&&&&&&&&&&&&&&&&&&&&
609 After changing to Wireshark instead of using my own sniffer,
610 I can still locate the users username as well as their password.
611 You can view this in the images.
612 
613 
614 Telnet as from what I have seen so far and with my limited knowlage, does not seem to
615 present itself as a security wise choice. It was very easy to sniff the packets and gain
616 username and password in matter of seconds.
617 &&&&&&&&&&&&&&&&&&&&&&&&&&
618 
619 
620 
621 
622 
623 
624 
625 
626 
627 
628 Step 3.3 - SSH.
629 *****
630 

```

```
631 -----
632 VM - SEED UBUNTU (MAIN)
633 -----
634 SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
635 .....>.t...-.....ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie
636 -hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
637 sha1,diffie-hellman-group1-sha1....:ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-
638 nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01
639 @openssh.com,ssh-dss-cert-v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-dss-cert-v00
640 @openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss.
641 ...aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc
642 ,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....aes128-ctr,
643 aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,
644 aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....hmac-md5,hmac-sha1,umac-64
645 @openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,
646 hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....hmac-md5,hmac-sha1,umac-64
647 @openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,
648 hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....none,zlib@openssh.com,zlib....none,
649 zlib@openssh.com,zlib.....L.....A.....Y.8...F.Q..4.T.w..F..i...~..Pe6...
650 W..(\*..B.G...0..B.....&.....
651 .....~...;>..\.....x.E.....#\h>.....+Y.?$.%.-d.Ml...:nWa,.$@.....J.....|..Ub
652 ...."..I.....`.....'s...=.F4.&.8lx...a..b(...:f6.;.....k.0+w+..eY..1~z...[uu.....B<..N
653 .+h.9.....`z..k..ubZ...2....*.p.#..FI..Piw-..d.....F<&y..U.1.Q.....:.....J?..#....>..
654 .K:...w%..h..^EL.....'.N.C~-.M.C.^...%.....NI7..+.p..>B..M....;c...v...bBq.].W..C.V..m
655 ...((...f.>U&..)3..._~..i%...Z.....<T.D.....E;je.d... ..$.B..8..A..C?.X....GSo..5n.....
656 .....g.a..$.4..D. a,.....9.....2FQ.[...jL...;Z....(O.Q5B...-@..I7@'D.Ym..NF...q.1...2O...J
657 .....A.e.....VOKjf...3....kF.....v.{w.s#.o.r3...=k.....c/.6...X.49.....G.8.O....@.....\..
658 \..B....K..8r.j.r.....F...?...X..u..Z...i.h.]F.5.....X.....~...~.(. ....#..p~.I<i..?H3
659 =Dq....<`.....|Wg."xX._u....?.....}l!.....,...K.'-F.-.5..+.. o..Q.....,8....<....t8x).;.%..
660 ..69i
661 Z..r.....!."../..U.....^z..L.....7.....t.<(.....l.M..F.v>.T.n..{.O.F..E)V$.|^...x
662 .W.$X@f....'.....Tx../.i.q.....tc...%._W8.....*.s..l70....e..mwU?.2S~..hX..F. ...$R aY...4
663 ..>../.....P;..+g.T ..'.L._gR/.n,.O..= . $"...4.s:.8F.....e K.7+..}a....VwK.....
664 .*#.....{.q.....%.....(.Vhn:...P..?xy..Q>|.Hs....}...X..s....?.....\..SU.c.G...&.7=Y..
665 ..N.a....
666
667
668
669
670
671 -----
672 VM - SEED UBUNTU (CLONE)
673 -----
674 [10/30/2017 20:26] seed@ubuntu:~$ ssh seed@10.0.2.5
675 The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
676 ECDSA key fingerprint is 81:82:a9:af:bd:93:78:f9:1a:a7:ca:7f:e8:d6:6c:04.
677 Are you sure you want to continue connecting (yes/no)? yes
678 Warning: Permanently added '10.0.2.5' (ECDSA) to the list of known hosts.
679 seed@10.0.2.5's password:
680 Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)
681
682 * Documentation:  https://help.ubuntu.com/
683
684 New release '14.04.1 LTS' available.
685 Run 'do-release-upgrade' to upgrade to it.
686
687 Last login: Mon Oct 30 19:56:21 2017 from ubuntu.local
688 [10/30/2017 20:27] seed@ubuntu:~$ exit
689 logout
690 Connection to 10.0.2.5 closed.
691
692
693
```

694
695
696
697
698
699
700

#####

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

#####