Nikkolas Irwin

University of Nevada Reno

CS 450 – Fundamentals of Integrated Computer Security

Ansari Business Building 106

Lab 1

1. When applied to the file crack-these-please, how many of its 50 passwords were cracked at each phase:

a. dictionary attack solved **11** of the passwords

b. hybrid attack solved **12** of the passwords

c. combination attack solved **38** of the passwords

d. **12** of the passwords were never solved within the time spent

2. The password-holding file is /etc/shadow for linux. Where are passwords stored for Windows Systems?

The hashes are stored within the Windows Operating system in the Windows SAM file. The SAM file is located at C:\Windows\System32\config and also in the registry at HKEY_LOCAL_MACHINE\SAM. Both of these locations are not accessible while the system is booted unless you utilize 3rd party software or enter the system through a back-door by logging into another OS on the same disk.

3. Use the Mandylion "Brute Force Attack Estimator" Excel spreadsheet (slightly modified version). Suppose you want a password that requires the rest of your life for a PC to crack. You have 50 years to live. How many days (live each to the fullest) is that? In the spreadsheet, consider passwords consisting of numerals ("Numbers") only.

50 years * 365.25 days / year = 18,262.5 days

a) the length of the numbers-only password that requires at least 50 years to crack, according to the spreadsheet, is **17** characters?

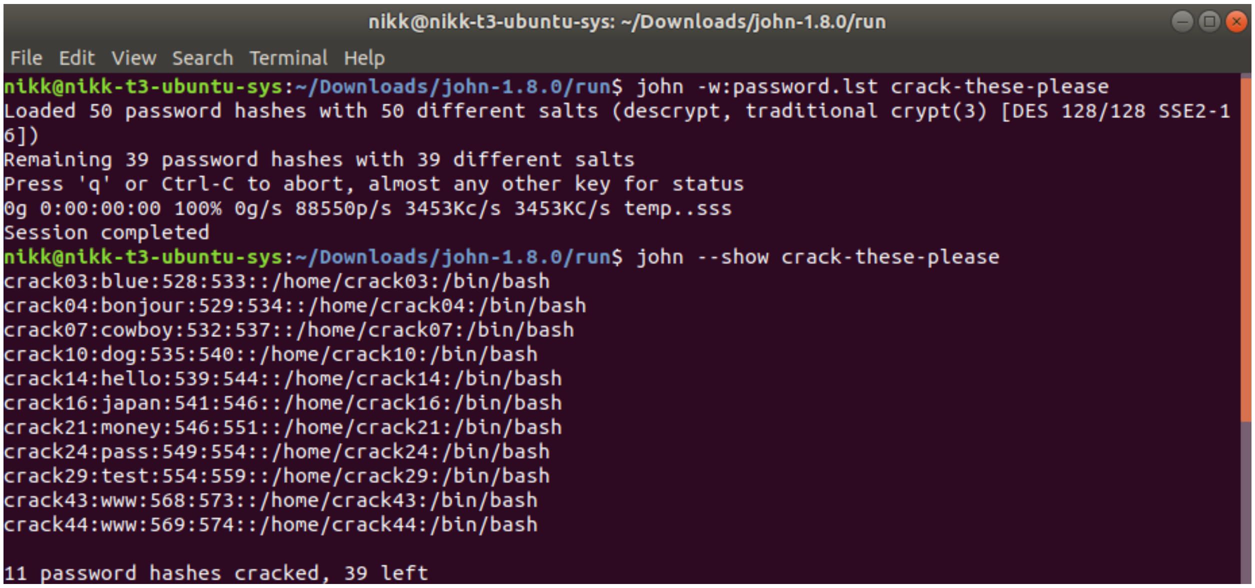
b) account for Moore's law. It says computing power doubles every 2 years. The spreadsheet is created on 2002. It reflects the computing power of 8 years ago . For today, you need to multiply its computing power assumptions with 2^4. Do so by entering 16 as the "Special factor" in cell G1 (which is applied in the "computing power" cell, E24, as a multiplier). Thus, with *today's* computing power, the length of the password that requires at least the rest of your life to crack is **18** characters.

c) account for Moore's law's continued operation. If Moore's law doesn't stop, today's isn't the right computing power for the upcoming 50 years' calculations. Assumuing on average (less near term, more far term) that computing power is 2.5 million times today's (approximately). With that as your future computing power, the length of the password that requires at least 50 years to crack is now **23** characters. (Multipy the current special factor by yet a further 2.5x10^6)

d) if you now allow mixed random characters (spreadsheet's "PURELY Random Combo of Alpha/Numeric/Special") instead of confining your password to numerals only you should be able to use a shorter password with equal effect. The shortest "mixed character" password that'll last 50 years is **12** characters.

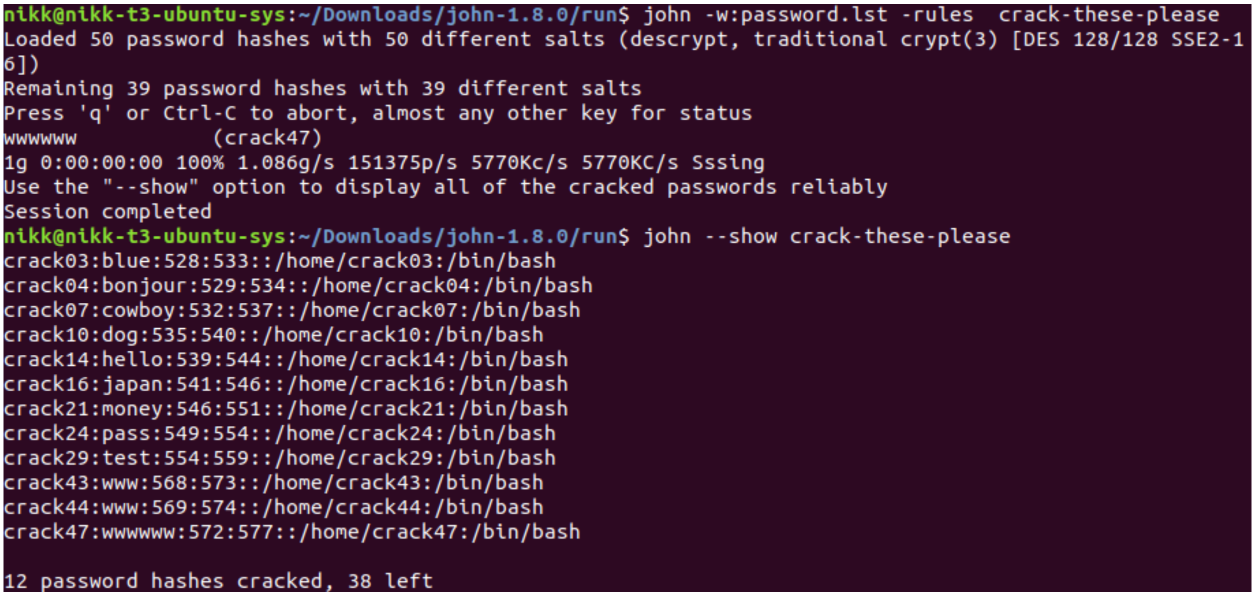
Below are some photos just to demonstrate that I completed the lab and ran the “John the Ripper” tool to crack the password.lst file.

Image 1 – Dictionary Attack


nikk@nikk-t3-ubuntu-sys: ~/Downloads/john-1.8.0/run
File Edit View Search Terminal Help

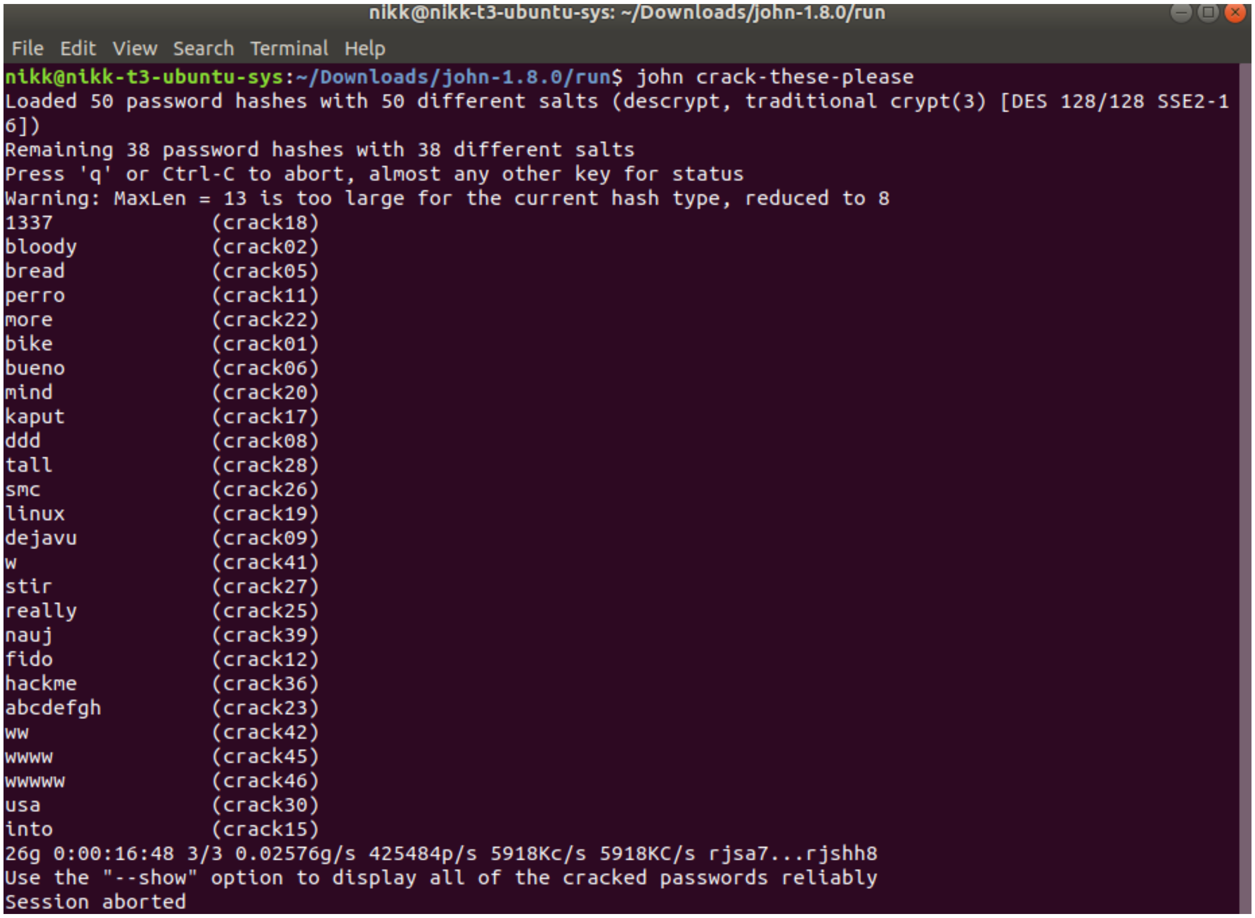
```
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ john -w:password.lst crack-these-please
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-1
6])
Remaining 39 password hashes with 39 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 100% 0g/s 88550p/s 3453Kc/s 3453KC/s temp..sss
Session completed
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ john --show crack-these-please
crack03:blue:528:533::/home/crack03:/bin/bash
crack04:bonjour:529:534::/home/crack04:/bin/bash
crack07:cowboy:532:537::/home/crack07:/bin/bash
crack10:dog:535:540::/home/crack10:/bin/bash
crack14:hello:539:544::/home/crack14:/bin/bash
crack16:japan:541:546::/home/crack16:/bin/bash
crack21:money:546:551::/home/crack21:/bin/bash
crack24:pass:549:554::/home/crack24:/bin/bash
crack29:test:554:559::/home/crack29:/bin/bash
crack43:www:568:573::/home/crack43:/bin/bash
crack44:www:569:574::/home/crack44:/bin/bash

11 password hashes cracked, 39 left
```

Image 2 – Hybrid Attack



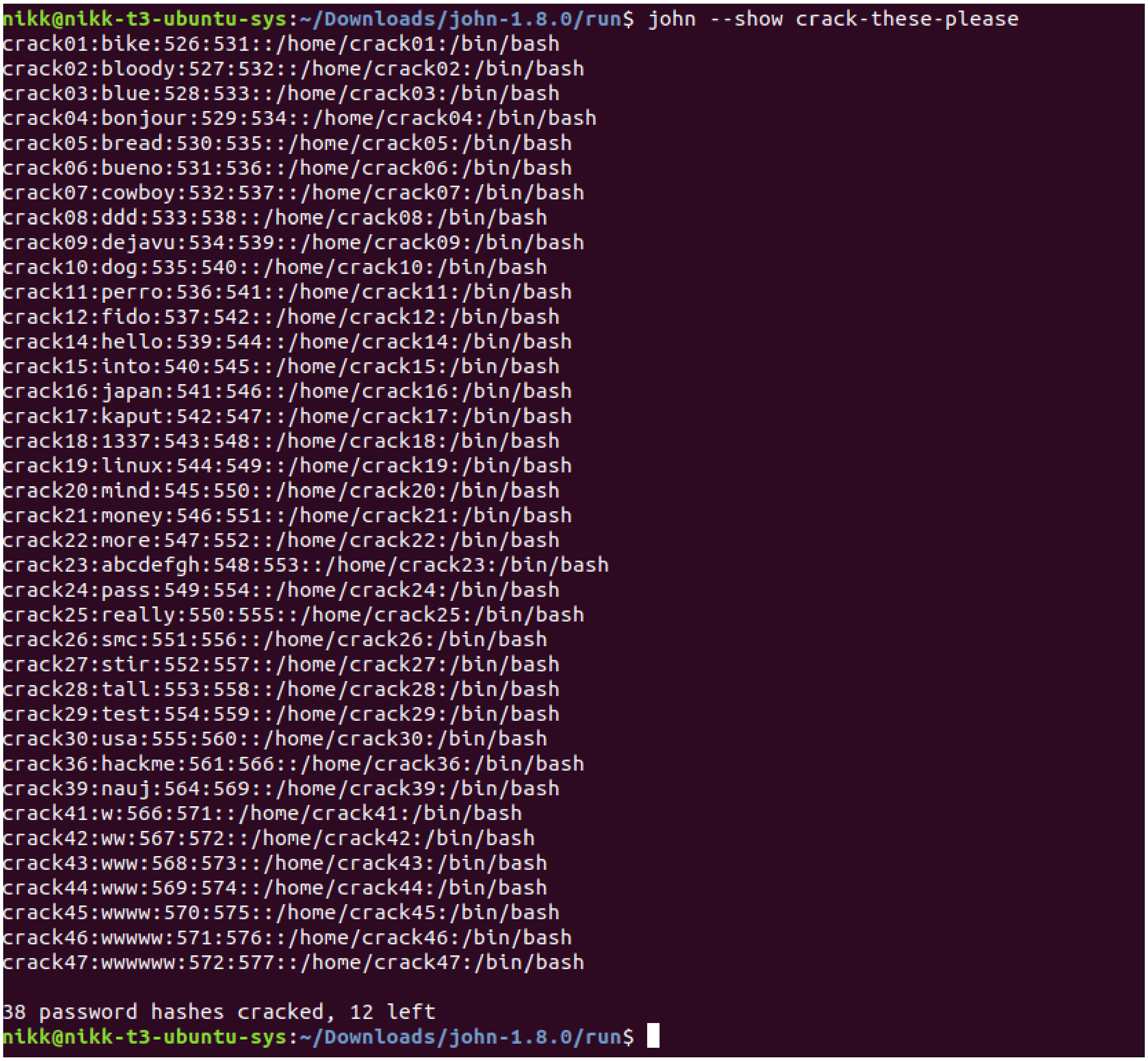
```
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ john -w:password.lst -rules  crack-these-please
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-1
6])
Remaining 39 password hashes with 39 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
wwwwww           (crack47)
1g 0:00:00:00 100% 1.086g/s 151375p/s 5770Kc/s 5770KC/s Sssing
Use the "--show" option to display all of the cracked passwords reliably
Session completed
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ john --show crack-these-please
crack03:blue:528:533::/home/crack03:/bin/bash
crack04:bonjour:529:534::/home/crack04:/bin/bash
crack07:cowboy:532:537::/home/crack07:/bin/bash
crack10:dog:535:540::/home/crack10:/bin/bash
crack14:hello:539:544::/home/crack14:/bin/bash
crack16:japan:541:546::/home/crack16:/bin/bash
crack21:money:546:551::/home/crack21:/bin/bash
crack24:pass:549:554::/home/crack24:/bin/bash
crack29:test:554:559::/home/crack29:/bin/bash
crack43:www:568:573::/home/crack43:/bin/bash
crack44:www:569:574::/home/crack44:/bin/bash
crack47:wwwwww:572:577::/home/crack47:/bin/bash

12 password hashes cracked, 38 left
```

Images 3 and 4 – Combination Attack



nikk@nikk-t3-ubuntu-sys: ~/Downloads/john-1.8.0/run
File Edit View Search Terminal Help

```
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ john crack-these-please
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-1
6])
Remaining 38 password hashes with 38 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
1337             (crack18)
bloody           (crack02)
bread            (crack05)
perro            (crack11)
more             (crack22)
bike             (crack01)
bueno            (crack06)
mind             (crack20)
kaput            (crack17)
ddd              (crack08)
tall             (crack28)
smc              (crack26)
linux            (crack19)
dejavu           (crack09)
w                (crack41)
stir             (crack27)
really           (crack25)
nauj             (crack39)
fido             (crack12)
hackme           (crack36)
abcdefgh         (crack23)
ww               (crack42)
wwww             (crack45)
wwwww            (crack46)
usa              (crack30)
into             (crack15)
26g 0:00:16:48 3/3 0.02576g/s 425484p/s 5918Kc/s 5918KC/s rjsa7...rjshh8
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```



```
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ john --show crack-these-please
crack01:bike:526:531::/home/crack01:/bin/bash
crack02:bloody:527:532::/home/crack02:/bin/bash
crack03:blue:528:533::/home/crack03:/bin/bash
crack04:bonjour:529:534::/home/crack04:/bin/bash
crack05:bread:530:535::/home/crack05:/bin/bash
crack06:bueno:531:536::/home/crack06:/bin/bash
crack07:cowboy:532:537::/home/crack07:/bin/bash
crack08:ddd:533:538::/home/crack08:/bin/bash
crack09:dejavu:534:539::/home/crack09:/bin/bash
crack10:dog:535:540::/home/crack10:/bin/bash
crack11:perro:536:541::/home/crack11:/bin/bash
crack12:fido:537:542::/home/crack12:/bin/bash
crack14:hello:539:544::/home/crack14:/bin/bash
crack15:into:540:545::/home/crack15:/bin/bash
crack16:japan:541:546::/home/crack16:/bin/bash
crack17:kaput:542:547::/home/crack17:/bin/bash
crack18:1337:543:548::/home/crack18:/bin/bash
crack19:linux:544:549::/home/crack19:/bin/bash
crack20:mind:545:550::/home/crack20:/bin/bash
crack21:money:546:551::/home/crack21:/bin/bash
crack22:more:547:552::/home/crack22:/bin/bash
crack23:abcdefgh:548:553::/home/crack23:/bin/bash
crack24:pass:549:554::/home/crack24:/bin/bash
crack25:really:550:555::/home/crack25:/bin/bash
crack26:smc:551:556::/home/crack26:/bin/bash
crack27:stir:552:557::/home/crack27:/bin/bash
crack28:tall:553:558::/home/crack28:/bin/bash
crack29:test:554:559::/home/crack29:/bin/bash
crack30:usa:555:560::/home/crack30:/bin/bash
crack36:hackme:561:566::/home/crack36:/bin/bash
crack39:nauj:564:569::/home/crack39:/bin/bash
crack41:w:566:571::/home/crack41:/bin/bash
crack42:ww:567:572::/home/crack42:/bin/bash
crack43:www:568:573::/home/crack43:/bin/bash
crack44:www:569:574::/home/crack44:/bin/bash
crack45:wwww:570:575::/home/crack45:/bin/bash
crack46:wwwww:571:576::/home/crack46:/bin/bash
crack47:wwwwww:572:577::/home/crack47:/bin/bash

38 password hashes cracked, 12 left
nikk@nikk-t3-ubuntu-sys:~/Downloads/john-1.8.0/run$ 
```