|  |
| --- |
| https://www.unr.edu/Images/president/im/basic-logos/downloads/nevada-blockn-black.png  Lab 1 |

### Ansari Business Building 106

### Nikkolas Irwin

University of Nevada Reno

## CS 450 – Fundamentals of Integrated Computer Security

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.**

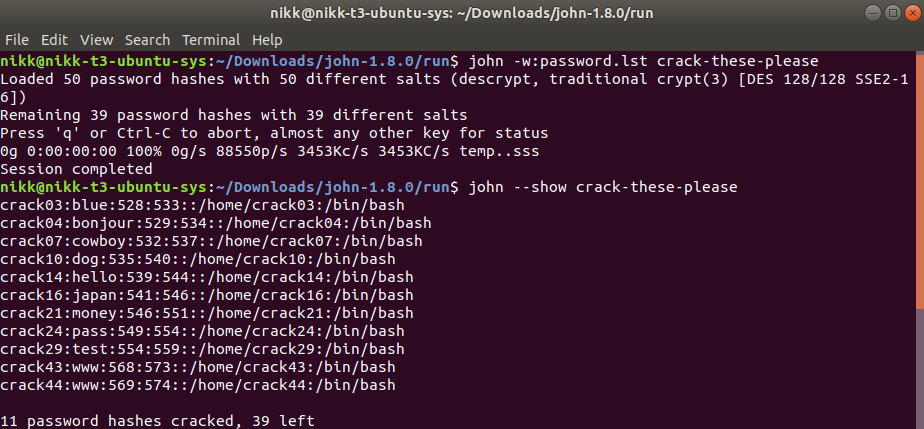
3. Use the Mandylion "Brute Force Attack Estimator" Excel spreadsheet ([slightly modified version](http://www-scf.usc.edu/~csci530l/downloads/BFTCalc-modified.xls)). Suppose you want a password that requires the rest of your life for a PC to crack. You have 50 years to live. How many days (live each 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) 

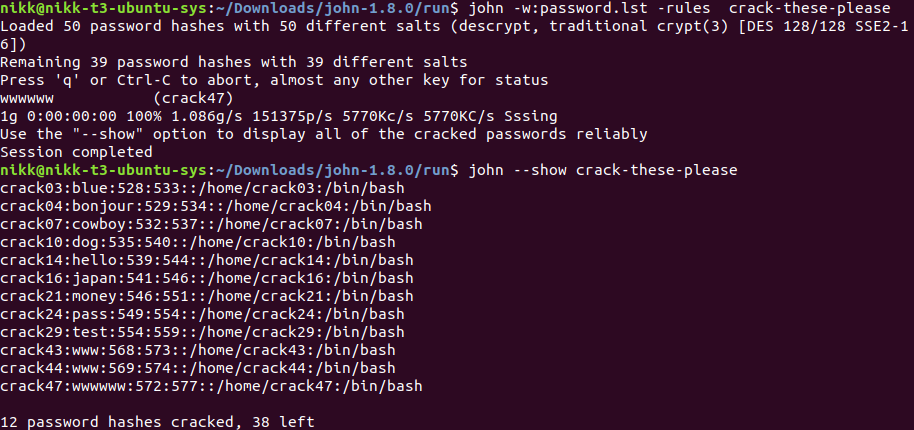
d) if you now allow mixed random characters (spreadsheet's "PURELY Random Combo of Alpha/Numeric/Special") instead of confining your password to numerals only you should be able to use a shorter password with equal effect. The shortest "mixed character" password that'll last 50 years is **12** characters.

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**



**Image 2 – Hybrid Attack**



**Images 3 and 4 – Combination Attack**

