**Network Security**

**Module 03 Authentication – Passwords**

1. Use the Windows calculator in scientific mode (or another calculator that is capable of the following calculation) to calculate the **password/key space** (number of total permutations) in **decimal** value. Show **steps** of your calculation. Hint: base number is the number of different choices for each digit/character in the password, and the exponent is the length of the password. (10 points, 5 points each)
   1. A randomly generated 128-bit binary key

**The base number is 2, which is binary. Therefore, a randomly generated 128-bit will have a total number of permutations represented as: 2^128 = 3.402 x 10^38**

* 1. A randomly generated 11-character user password using lower case letters, upper case letters, 0~9 numbers, and a set of 10 different special symbols

**Lowercase letters = 26**

**Uppercase letters = 26**

**Numbers (0-9) = 10**

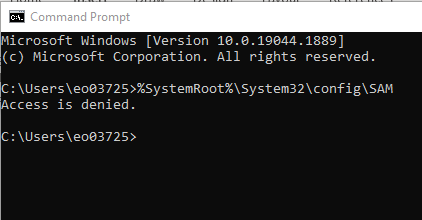
**Set of special symbols = 10**

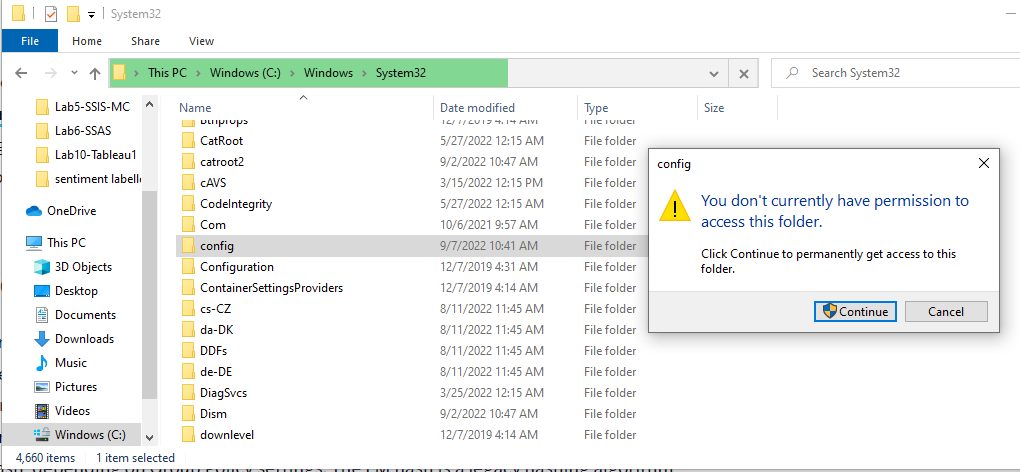
**Total combinations of options = 26+26+10+10=72**

**Therefore, the number of permutations for an 11-character user password = 72^11 =**

1. Locate the SAM file in Windows. Then try to open/edit/delete/move it. What have you discovered? Also locate SAM record in Windows Registry. What happened when you tried to open it? (10 points)

I tried to access the SAM file on my Windows desktop using the Command prompt, the command used was **%SystemRoot%\System32\config\SAM** but the access was denied. I also tried to delete the file, but it proved unsuccessful because I don’t have the authorization to make any changes to it. I also tried accessing the file through the GUI, it was still unsuccessful.

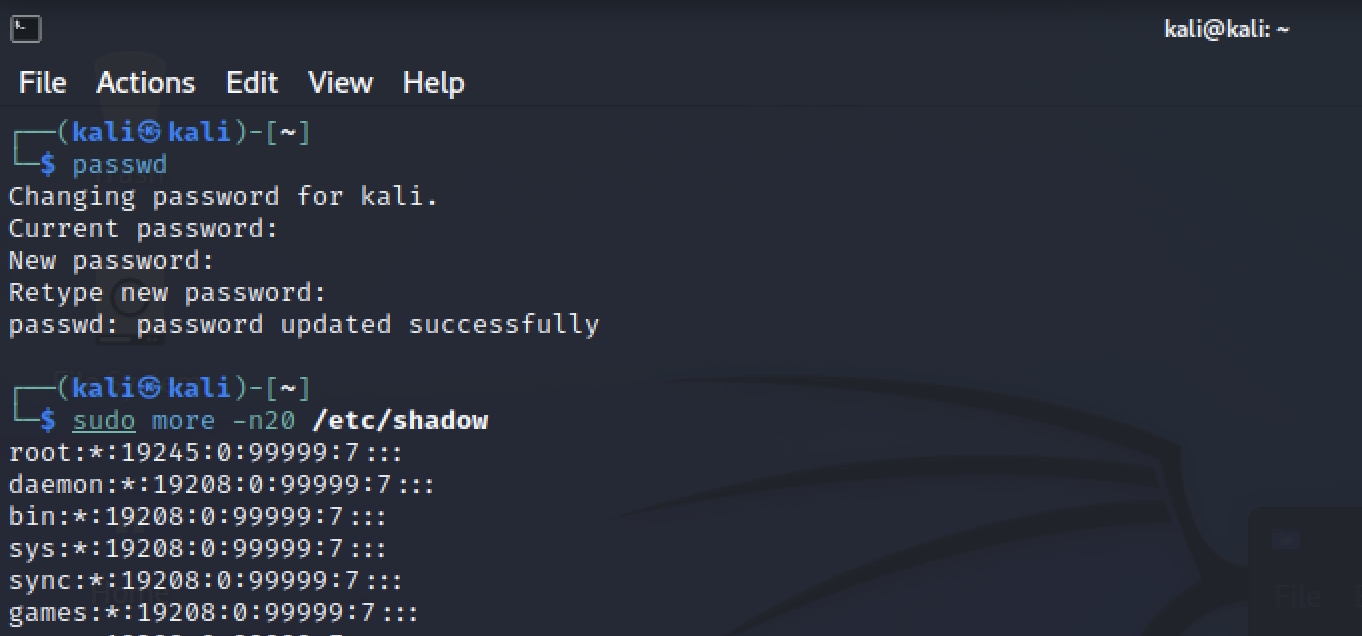




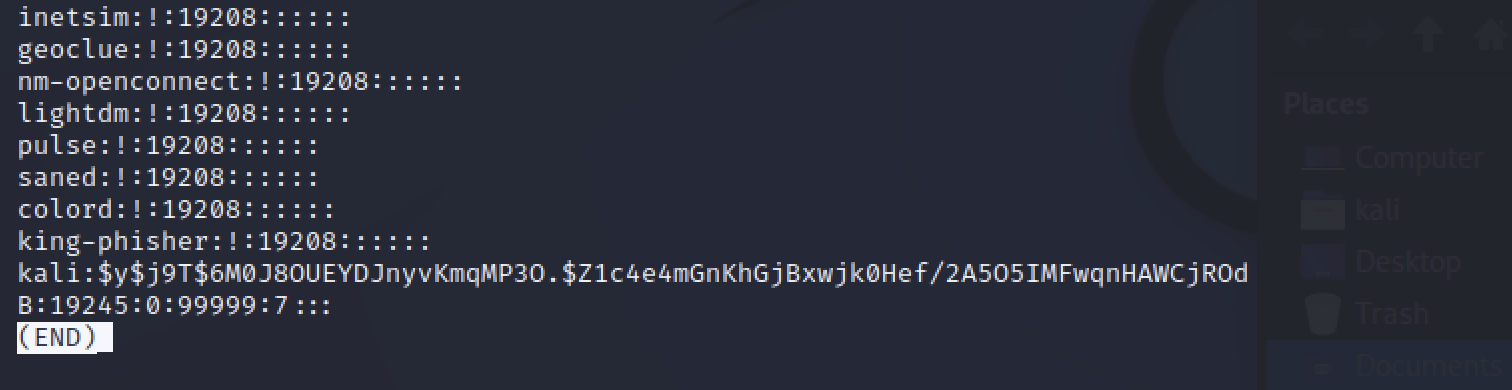
1. **Windows password evaluation**. Because the university campus network and many ISP networks prohibit the downloads and use of password crackers such as Cain & Abel, this task is to conduct research online using reliable resources to compare **three** popular **Windows** password evaluators/crackers/auditing software. Use a table to compare their **capabilities**, **performance in speed**, and any **advantages**/**disadvantages**. (25 points)

|  |  |  |  |
| --- | --- | --- | --- |
| **Windows Password Evaluators** | **Capabilities and Performance** | **Advantages** | **Disadvantages** |
| THC Hydra | * This is an online password evaluation tool that is utilized to extract a user’s credentials from the system. * This application utilizes brute-force strategy for credentials recovery. | * It supports many network protocols such as Cisco AAA, Cisco auth, Cisco enable, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY. * It is compatible with different operating systems such as Windows, MacOS, Linux, Solaris. | * It is time consuming due to the strategy utilized in this application. |
| Rainbow Crack | * This application was designed to work using rainbow tables. * The rainbow tables contain pre-computed password hashes, it also can generate custom rainbow tables. | * It can evaluate passwords that uses the following hashes, LM, NTLM, MD5 and SHA1. * Custom generated rainbow tables can easily evaluate hashes faster. | * It is very ineffective against salting in newer windows and Linux systems. |
| Medusa | * This application is an online password-cracking tool like THC Hydra. It has a speedy parallel evaluation process. * It utilizes a modular and login brute-forcing strategy | * It is very fast during evaluation. On a local system, it can test 2000 passwords per minute, but this depends on the ISP being utilized. | * This tool is solely a command line tool, so only users with prior knowledge in command line can easily operate this application. |

1. In a Linux environment (such as an Ubuntu or Kali Linux virtual machine) where you have root/administer access, locate, and show the content of the Shadow file. Choose an appropriate line in the shadow file (each line corresponds to a different account). Identify and briefly explain the **first 6 items (refer to lecture slides)** in that specific line. Attach **screenshot** of the Shadow file showing these items and values. (15 points)



First, I had to change the root password for my kali linux to something more complex. Then, I used the superuser command to access the shadow file, showing everything within the file.



The last line in the screenshot shows the contents of the password.

The first column- Username: **Kali**

**The “y” in between the dollar sign shows the Hashing algorithm used for this kali linux, which is SHA512.**

**The “j9T” in between the dollar sign shows the Salt value for the hashed password.**

**After the dollar sign, the hash value for the password is shown.**

**After the hash value password, there is a colon and some numbers “19245”. This number shows the minimum number of days between password changes.**

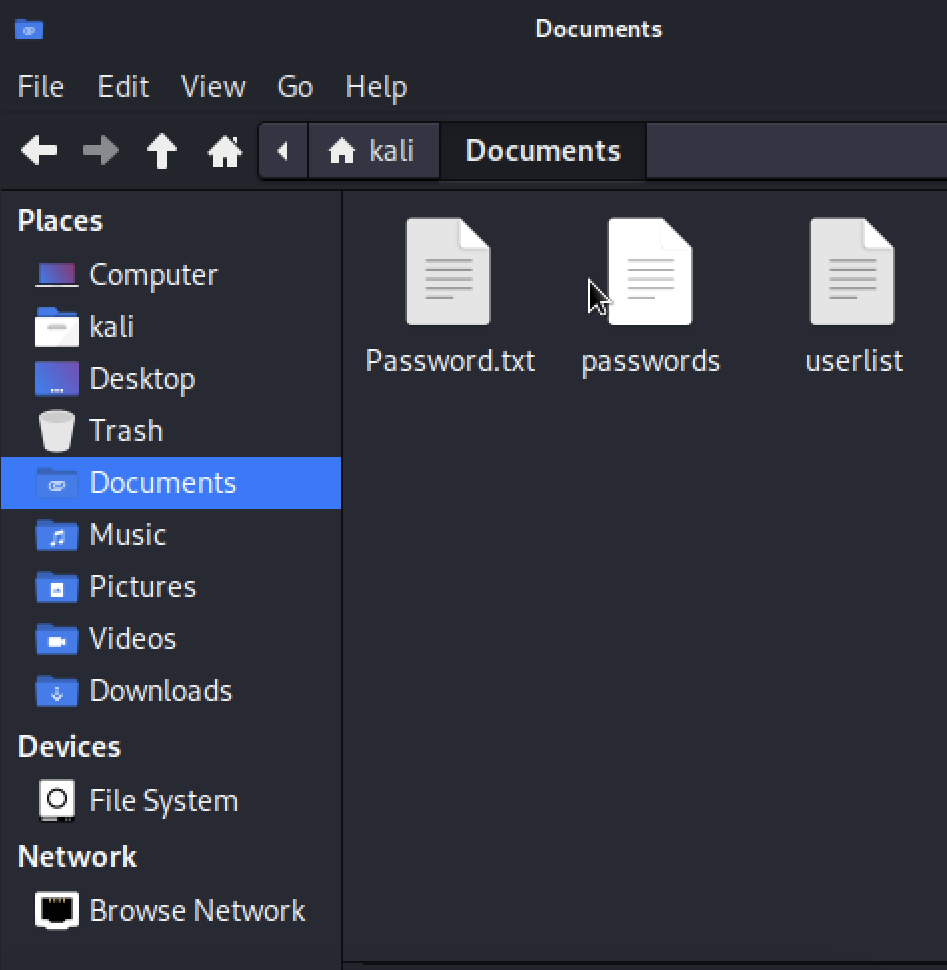
**The number “0” shows the maximum number of days the password is valid.**

**The number “99999” shows the number of days before the password is about to expire to warn the user.**

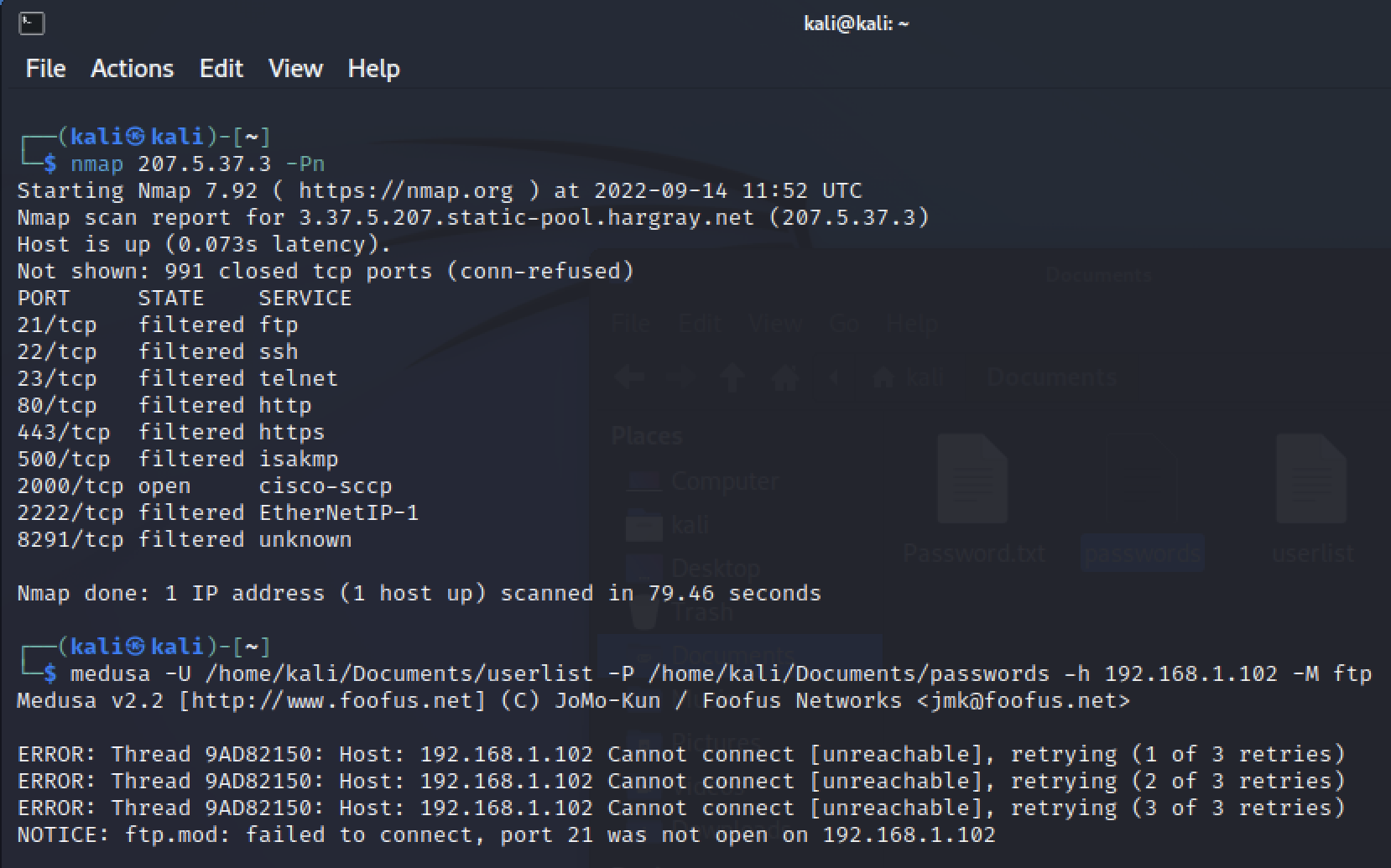
1. **Linux (e.g., Kali or Ubuntu) or Mac OS password evaluation. Show the process of using an appropriate tool to retrieve and crack a Linux account password. Log major steps and attach screenshots. Include your findings. (up to 30 bonus points)**

**For the bonus question I utilized the Medusa password evaluation tool in Kali linux.**

**When using this tool, I created two text document lists. The first contained the user login details(UserList.txt) and the second contained frequently used passwords. This approach is referred to as a dictionary approach. It runs the user login against the possible password created in the second list.**

****

**Then I opened a terminal window where I initialized the medusa tool, then I checked for opened ports to run the commands through. The list of opened and closed ports were shown.**

****

**The target host ip address is required when performing this evaluation, so i used the ip address the VM-ware generated. Then the Userlist location is specified and the passwords location is specified. Finally, the module and port number is also required to run this evaluation.**