Antonio Shields

CYSE 270: Linux System for Cybersecurity

February 10, 2023

Assignment: Lab 5 – Password cracking

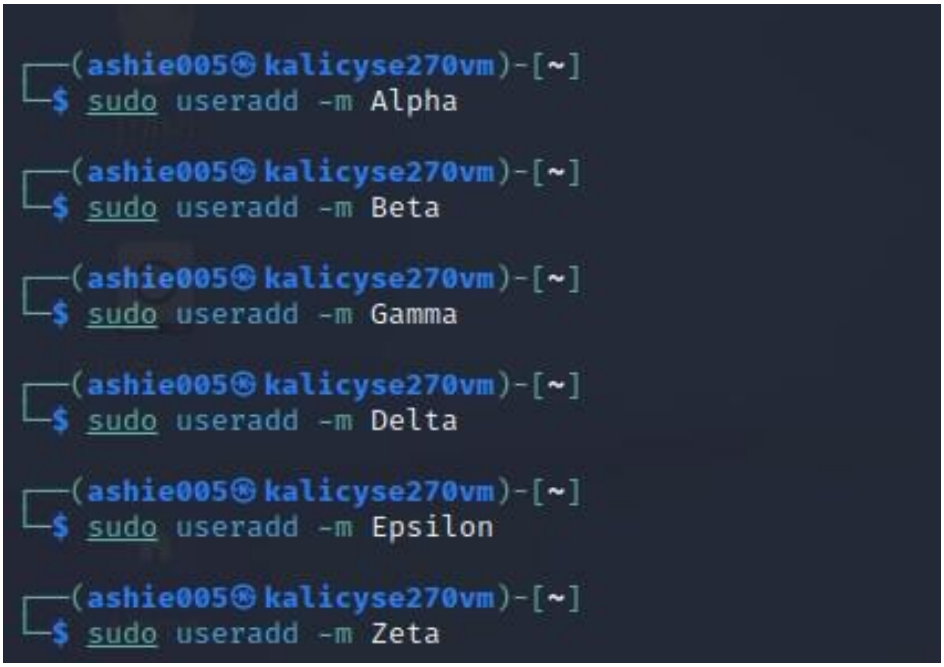
CYSE 270: Linux System for Cybersecurity

The goal of this lab is to test the strength of different passwords.

Task A – Password Cracking

1. Create 6 users in your Linux system, then assign each user a password that meets the following complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30 points]

1. **A simple dictionary word (all lowercase):** Alpha – happy
2. **4-character digits :** Beta – 5678
3. **A simple dictionary word (all lowercase) + digits: Gamma –** sad1234
4. **A simple dictionary word (all lowercase) + digits +symbols:** Delta – mad7890!
5. **A simple dictionary word (all lowercase) + digits:** Epsilon -glad2468
6. **A simple dictionary word (w. a mix of lower and upper case) + digits +symbols:** Zeta – WoRd365!#



The usernames were added first.

```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd Alpha
New password:
Retype new password:
passwd: password updated successfully

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd Beta
New password:
Retype new password:
passwd: password updated successfully

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd Gamma
New password:
Retype new password:
passwd: password updated successfully
```

```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd Delta
New password:
Retype new password:
passwd: password updated successfully

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd Epsilon
New password:
Retype new password:
passwd: password updated successfully

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd Zeta
New password:
Retype new password:
passwd: password updated successfully
```

Then the passwords listed were assigned to the respective user successfully.

Remember, do not use the passwords for your real-world accounts.

2. Export above users' hash into a file named xxx.hash (replace xxx with your MIDAS ID) and use John the Ripper to crack their passwords in wordlist mode (use rockyou.txt). [40 points]

```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo tail -6 /etc/shadow
Alpha:$y$j9T$WD5XzZLMAZrPpU9FvpVYP/$jH5YJqF3pUeIE32q0gwyvDswLkMmy61uzhDBP0BTKb0:19398:0:99999:7:::
Beta:$y$j9T$Hy.D8WJEodWUMT3ZCRfAb.$FlRnrVRdtyYGboimgFsSM9IzQS.kCBFugiTBC1u/dk/:19398:0:99999:7:::
Gamma:$y$j9T$vmaj6yu4Wu.tXMXgwWbnj0$5EdGUTfykVnzJ88.HekpqDUWWguq121j8byzDPtqOG9:19398:0:99999:7:::
Delta:$y$j9T$ALtP9GYzNKvQoTMu3cl.Z1$XQL.tKM.pSBPujuzXC/FUYOopAtkIQHXLpyX600.PsB:19398:0:99999:7:::
Epsilon:$y$j9T$nuIFe37Jll6fNKQpzSljW.$Lc/5pAW8TxrEh2m/algT0iVE5Zjc35MKOOC9FIm4hZ0:19398:0:99999:7:::
Zeta:$y$j9T$134LpRNlNC9/pxD4SOpz1/$mh5s8GnxI2bFirBCjZbDRIygYE/LCLcqF65pnQDQ/c2:19398:0:99999:7:::

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo tail -6 /etc/shadow >> ashie005.hash

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ cat ashie005.hash
Alpha:$y$j9T$WD5XzZLMAZrPpU9FvpVYP/$jH5YJqF3pUeIE32q0gwyvDswLkMmy61uzhDBP0BTKb0:19398:0:99999:7:::
Beta:$y$j9T$Hy.D8WJEodWUMT3ZCRfAb.$FlRnrVRdtyYGboimgFsSM9IzQS.kCBFugiTBC1u/dk/:19398:0:99999:7:::
Gamma:$y$j9T$vmaj6yu4Wu.tXMXgwWbnj0$5EdGUTfykVnzJ88.HekpqDUWWguq121j8byzDPtqOG9:19398:0:99999:7:::
Delta:$y$j9T$ALtP9GYzNKvQoTMu3cl.Z1$XQL.tKM.pSBPujuzXC/FUYOopAtkIQHXLpyX600.PsB:19398:0:99999:7:::
Epsilon:$y$j9T$nuIFe37Jll6fNKQpzSljW.$Lc/5pAW8TxrEh2m/algT0iVE5Zjc35MKOOC9FIm4hZ0:19398:0:99999:7:::
Zeta:$y$j9T$134LpRNlNC9/pxD4SOpz1/$mh5s8GnxI2bFirBCjZbDRIygYE/LCLcqF65pnQDQ/c2:19398:0:99999:7:::
```

The 6 users' hash from the /etc/shadow fi were placed into the ashie005.hash file using the ">>" operator. Then verified that all users' hash were in the file.

3. Keep your john the ripper cracking for at least 10 minutes. How many passwords have been successfully cracked? [30 points]

```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo john --format=crypt ashie005.hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
happy            (Alpha)
1g 0:00:09:49 0.09% (ETA: 2023-02-18 10:43) 0.001697g/s 25.58p/s 129.0c/s 129.0C/s reinaldo..aleluya
1g 0:00:26:41 0.24% (ETA: 2023-02-18 06:21) 0.000624g/s 26.37p/s 132.1c/s 132.1C/s bronco1..PAULA
1g 0:00:26:42 0.24% (ETA: 2023-02-18 06:28) 0.000624g/s 26.36p/s 132.1c/s 132.1C/s bronco1..PAULA
1g 0:00:34:10 0.31% (ETA: 2023-02-18 06:19) 0.000487g/s 26.35p/s 132.0c/s 132.0C/s booboo14..alexis22
1g 0:00:34:17 0.31% (ETA: 2023-02-18 06:37) 0.000486g/s 26.31p/s 132.0c/s 132.0C/s alexandrina..881005
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Jon the ripper ran for 34 minutes and during that time, only one password was successfully cracked. User "Alpha" with the password "happy".

Extra credit (10 points):

1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show your steps and results.

- 5f4dcc3b5aa765d61d8327deb882cf99
- 63a9f0ea7bb98050796b649e85481845

```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ vi extracreditLab5.txt

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ cat extracreditLab5.txt
5f4dcc3b5aa765d61d8327deb882cf99
63a9f0ea7bb98050796b649e85481845

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo john --format=raw-md5 extracreditLab5.txt
[sudo] password for ashie005:
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
Proceeding with incremental:ASCII
root             (?)
2g 0:00:00:01 DONE 3/3 (2023-02-10 17:10) 1.562g/s 4397Kp/s 4397Kc/s 4397KC/s rome..rycd
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo john --show --format=raw-md5 extracreditLab5.txt
?:password
?:root

2 password hashes cracked, 0 left
```

- Used the vi editor to create the file “extracreditLab5.txt” and verified that the MD5 hash were in the file using the “cat” command.
- Used “sudo john –format=raw-md5 extracreditLab5.txt” to crack the two MD5 hash.
- Results showed the first hash password was “password” and the second hash password was “root”
- Ran “sudo john –show –format=raw-md5 extracreditLab5.txt to just show the password cracking results.