Auditing Passwords with a Password Cracking Utility

(CompTIA Security + SY – 601)

Objectives:

- To analyze potential indicators to determine the type of attack

Resources:

- John the Ripper
- Kali Virtual Machine

Instructions:

<u>Create the necessary accounts and passwords</u>

- Sign-in as root using **Pa$$w0rd** as the password
- Launch the **Terminal** application from the toolbar on the top of the Kali desktop
- Run the following command to create the first user: **adduser –gecos "user01**; when prompted set **06101988** as the password (You will type in twice)

```
root@KALI:~# adduser --gecos "" user01
Adding user `user01' ...
Adding new group `user01' (1000) ...
Adding new user `user01' (1000) with group `user01' ...
Creating home directory `/home/user01' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
```

- Create the following additional accounts by using the **adduser** command and set specified passwords

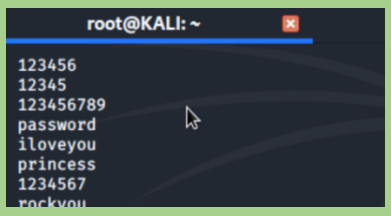
Username:	Password:
user02	Password
user03	Duke
user04	george
user05	$p0T
user06	G00dPa$$w0rd

Add probable passwords to the word list files

- Run the following command to extract the: **/usr/share/wordlists/rockyou.txt.gz** word list file

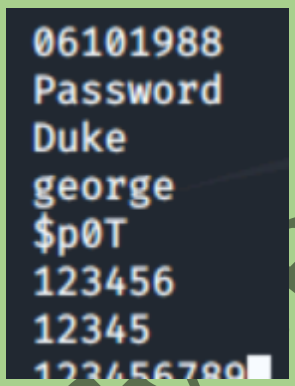
```
root@KALI:~# gunzip /usr/share/wordlists/rockyou.txt.gz
```

- Enter the following command to open the **rockyou.txt** wordlist file for editing




```
vim /usr/share/wordlists/rockyou.txt
```

- Select the **I** key to enter Vim's Insert mode and then add the passwords provided each on a separate line at the top of the file



- In Vim press **Esc** and then type **wq** and press Enter to save your changes and exit the file

Run John to crack passwords

- Run the following command to create a text file of usernames and password hashes

```
root@KALI:~# unshadow /etc/passwd/etc/shadow > crack-this-file
```

- Run the following command to crack passwords

```
root@KALI:~# john --wordlist=/usr/share/wordlists/rockyou.txt crack-this-file
```

- Open a second tab in the **Terminal** and then run the following command to view the status of the audit

```
root@KALI:~# john --show crack-this-file
user01:06101988:1000:1000:,,,:/home/user01:/bin/bash
user02:Password:1001:1001:,,,:/home/user02:/bin/bash
user03:Duke:1002:1002:,,,:/home/user03:/bin/bash
user04:george:1003:1003:,,,:/home/user04:/bin/bash
user05:$p0T:1004:1004:,,,:/home/user05:/bin/bash

5 password hashes cracked, 2 left
```

- Type **top** to display the system utilization information. Observe that John is consuming most of the system's processing power

```
top - 05:13:14 up 41 min,  1 user,  load average: 1.53, 2.12, 1.46
Tasks: 129 total,   1 running, 128 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.2 us,  0.1 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   5949.7 total,   4808.7 free,    487.5 used,    653.5 buff/cache
MiB Swap:   4094.0 total,   4094.0 free,      0.0 used.   5217.7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    730 root      20   0  741476  96952  35504 S   0.3   1.6   0:08.68 Xorg
      1 root      20   0  166456  10908   8136 S   0.0   0.2   0:01.54 systemd
```

- Select **q** to exit top
- Switch to the Terminal tab where John the Ripper is running, and then type **q** to interrupt the cracking attempt
- Redirect the results of the **John –show crack-this-file** to a text file

```
root@KALI:~# john --show crack-this-file > results.txt
root@KALI:~# ls
crack-this-file  Documents  LOD     nmap.xsl  Public      set        Videos
Desktop          Downloads  Music   Pictures  results.txt Templates
```

- Display the **results.txt** file contents by using the **cat** command

Observations:

- **Setup**:
  - Created user accounts with specific passwords using adduser.
  - Initial password set to "06101988".
- **Password List**:
  - Extracted and edited rockyou.txt to include probable passwords.
- **Password Cracking**:
  - Used John the Ripper to create username and password hash file.
  - Monitored system utilization with top.

- **System Utilization**:
    - John the Ripper consumed high CPU during cracking.
- **Results**:
    - Cracked several passwords.
    - Displayed results with cat.

Results:

- Successfully cracked several passwords.
- High CPU usage during cracking.

Conclusion:

- Demonstrated the need for strong, unpredictable passwords.
- Highlighted importance of robust password policies.

Future Work:

- Implement stricter password policies.
- Conduct regular password audits.
- Explore advanced cracking techniques.
- Educate users on strong password practices.