PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

Department of Information Technology

Academic Year: 2025-26 **Semester: V**
Class / Branch: TE IT Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

Experiment No. 11

1. **Aim: To study password cracking using John the ripper.**

2. **Theory:**

John The Ripper (JTR) is one of the most popular password cracking tools available in most Penetration testing Linux distributions like Kali Linux, Parrot OS, etc. The tool has been used in most Cyber demos, and one of the most popular was when it was used by the Varonis Incident Response Team. John The Ripper password cracking utility brags of a user-friendly command-line interface and the ability to detect most password hash types. This tutorial will dive into John the Ripper, show you how it works, and explain why you need it for security testing.

John the Ripper (JtR) is a popular password-cracking tool. John supports many encryption technologies for Windows and Unix systems (Mac included). One remarkable feature of John is that it can autodetect the encryption for common formats. This will save you a lot of time in researching the hash formats and finding the correct tool to crack them.

John can work in the following modes:

Single crack

In this mode, john will try to crack the password using the login/GECOS information as passwords.

Wordlist

John will simply use a file with a list of words that will be checked against the

passwords. See RULES for the format of wordlist files.

Incremental

This is the most powerful mode. John will try any character combination to resolve the password. Details about these modes can be found in the MODES file in john's documentation, including how to define your own cracking methods.

To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental".

The files associated with this tool are as below:

/etc/john/john.conf

is where you configure how john will behave.

/etc/john/john-mail.msg

has the message sent to users when their passwords are successfully cracked.

/etc/john/john-mail.conf

is used to configure how john will send messages to users that had their passwords cracked.

What are Password Hashes?

Currently, password login is one of the most authentication methods used for security purposes. When you create a log-in password on most secure systems, it is stored in a hashed format. Some of the common hashing algorithms include MD5, SHA-1, SHA-2, NTLM, and LANMAN. When you want to log in, the system will hash the password with

Password Cracking With John the Ripper (JtR)

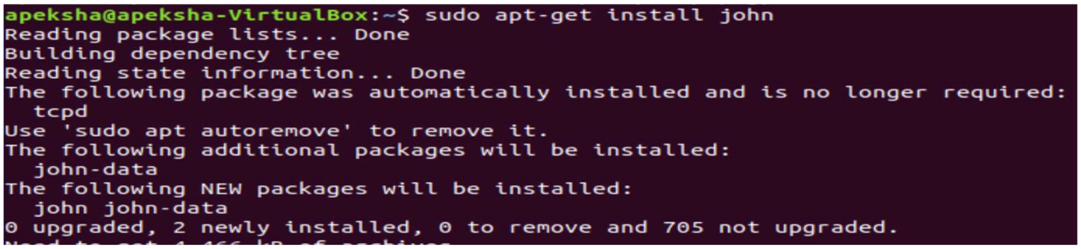
Password cracking with JtR is an iterative process. A word is selected from the wordlist, hashed with the same hash algorithm used to hash the password, and the resulting hash is compared with the password hash. If they match, then the word picked from the wordlist is the original password. If they don't match, JtR will pick another word to repeat the same process until a match is found. And as you guessed it! This process can take some time if the password used was complex. John the Ripper supports most encryption technologies found in UNIX and Windows systems.

Single Mode Password Cracking

By default, the hashed user login passwords are stored in the /etc/shadow directory on any Linux system. To view the contents of the shadow file, execute the command below in your terminal.

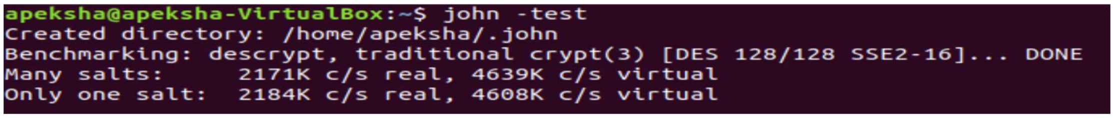
Installation:

sudo apt-get install john



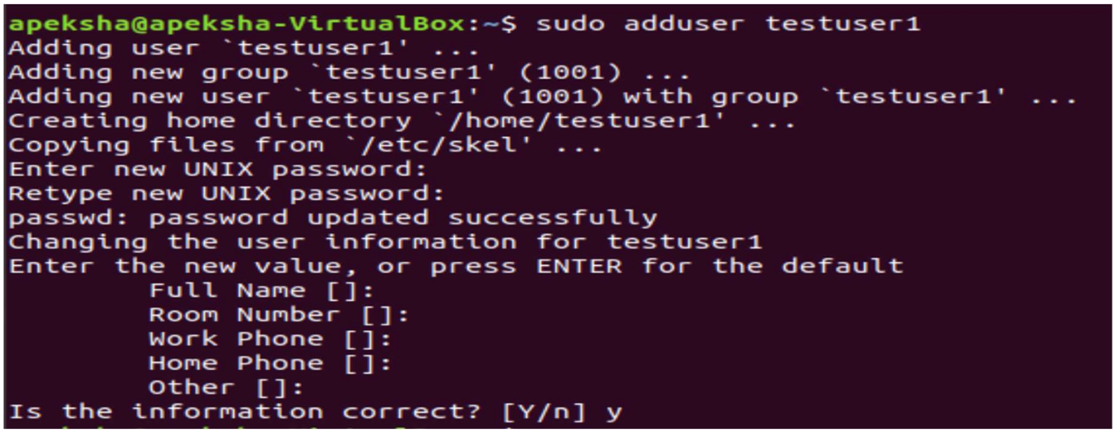
```
apeksha@apeksha-VirtualBox:~$ sudo apt-get install john
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  tcpd
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  john-data
The following NEW packages will be installed:
  john john-data
0 upgraded, 2 newly installed, 0 to remove and 705 not upgraded.
```

Test the tool:



```
apeksha@apeksha-VirtualBox:~$ john -test
Created directory: /home/apeksha/.john
Benchmarking: descrypt, traditional crypt(3) [DES 128/128 SSE2-16]... DONE
Many salts:     2171K c/s real, 4639K c/s virtual
Only one salt:  2184K c/s real, 4608K c/s virtual
```

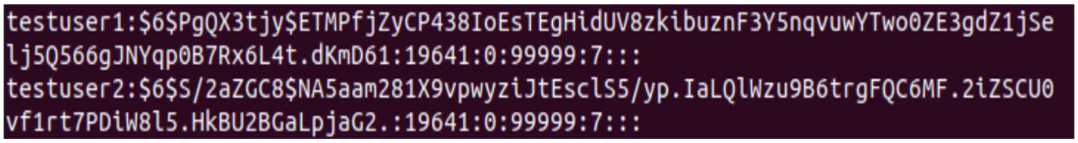
Create a user account:



```
apeksha@apeksha-VirtualBox:~$ sudo adduser testuser1
Adding user `testuser1' ...
Adding new group `testuser1' (1001) ...
Adding new user `testuser1' (1001) with group `testuser1' ...
Creating home directory `/home/testuser1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for testuser1
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

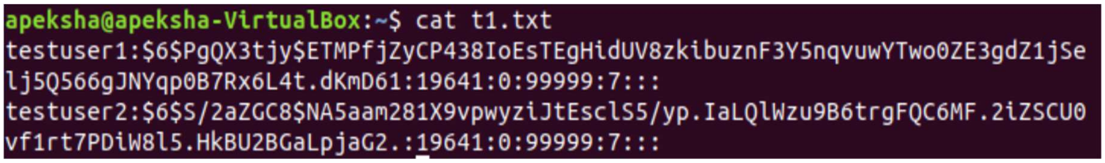
Get the password hashes for password from shadow file:

sudo cat /etc/shadow



```
testuser1:$6$PgQX3tjy$ETMPfjZyCP438IoEsTEgHidUV8zkibuznF3Y5nqvuwYTwo0ZE3gdZ1jSe
lj5Q566gJNYqp0B7Rx6L4t.dKmD61:19641:0:99999:7:::
testuser2:$6$S/2aZGC8$NA5aam281X9vpwyziJtEsclS5/yp.IaLQlWzu9B6trgFQC6MF.2iZSCU0
vf1rt7PDiW8l5.HkBU2BGaLpjaG2.:19641:0:99999:7:::
```

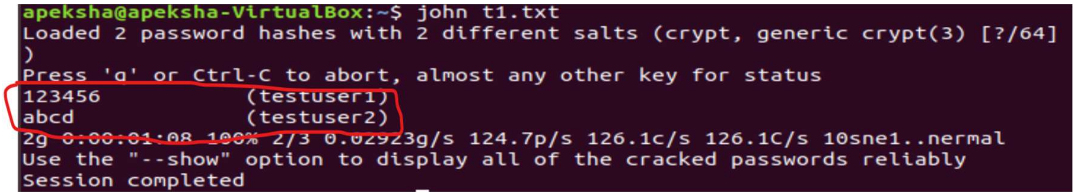
Copy the hashes to a text file:



```
apeksha@apeksha-VirtualBox:~$ cat t1.txt
testuser1:$6$PgQX3tjy$ETMPfjZyCP438IoEsTEgHidUV8zkibuznF3Y5nqvuwYTwo0ZE3gdZ1jSe
lj5Q566gJNYqp0B7Rx6L4t.dKmD61:19641:0:99999:7:::
testuser2:$6$S/2aZGC8$NA5aam281X9vpwyziJtEsclS5/yp.IaLQlWzu9B6trgFQC6MF.2iZSCU0
vf1rt7PDiW8l5.HkBU2BGaLpjaG2.:19641:0:99999:7:::
```

From the image, we will crack the password for users testuser1 and testuser2 . Password cracking can be, at times, a lengthy process for complex passwords. We will copy the whole field and save it in a file with a name t1.txt in home directory. To crack the password hash, we will use the syntax below:

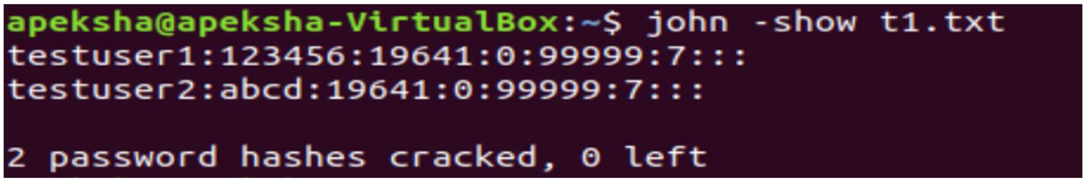
Password cracking using john:



```
apeksha@apeksha-VirtualBox:~$ john t1.txt
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64]
)
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (testuser1)
abcd             (testuser2)
2g 0:00:01:08 100% 2/3 0.02923g/s 124.7p/s 126.1c/s 126.1C/s 10sne1..nermal
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

From the image, you can see JtR cracked the password for users testuser1 and testuser2.The users are the ones enclosed in brackets.

View the cracked passwords:



```
apeksha@apeksha-VirtualBox:~$ john -show t1.txt
testuser1:123456:19641:0:99999:7:::
testuser2:abcd:19641:0:99999:7:::

2 password hashes cracked, 0 left
```

3. Conclusion:

Even though there are many password-cracking utilities available today, John the Ripper is with no doubt one of the best and most reliable. It has been used with other tools in most Cyber Attack Conferences to exploit the vulnerability of a system of elevated privileges on a compromised system.