4. Password Crack

패스워드 크래킹은 공격자들이 공격 대상 시스템의 **중요 계정의 패스워드를 알아내어 공격에 사용**하기 위해 주로 사용한다.

John the Ripper는 가장 유명한 패스워드 크래킹 툴 중 하나이다. Unix, Windows, OpenVMS 등에서 사용 가능하다. Brute Force Attack, Dictionary Attack, Rainbow Attack에서 사용할 수 있으며 **패스워드의 해쉬 타입을 자동으로 탐지**한다.

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

4. Password Crack

1. 실습 개요

본 실습에서는 John the Ripper 도구를 이용한다. 흔히 쓰이는 패스워드를 모두 저장하여 대입해 보는 방식인 사전 공격/사전 대입 공격(Dictionary Attack) 기법으로 패스워드 크래킹을 진행한다.

2. 시스템 정보

* CentOS7_CLI 관리자 계정 : root/root123

3. 문제풀이

1) root계정으로 로그인(root/root123)

```
www login: root
Password:
Last login: Thu Aug  5 09:02:34 on tty1
[root@www ~]#
```

2) shadow 파일에 cjudoor, cju, subin, yoonsu 패스워드가 해쉬값으로 저장되어 있는지 확인
> cat /etc/shadow

```
[root@www ~]# cat /etc/shadow
cjudoor:$6$wcHSKxRG8SgBNIZU$..b6Hb9O/zhaGHVsQIALYrb6nvHkPhXi1B/EYigVq8g/EuvNV2SufyI/U1NJzZhwMElceJqe
ea5bUtuUglFrP/::0:99999:7:::
cju:$6$3fRP1tTU$/RbQJE1txtVCwLprjOWnxNZZP1oO/C9imc.EOkm4w/f7isJfeBKdJxbfJmIHXkBf6/yTDMQ.odjdEsRCYz2e
61:18844:0:99999:7:::
subin:$6$xTejj2Jx$FVScJKxMIl6gDYRq1jjI3oWiJOYS5KDcH4xU0/BYIpKx5Jkfy2B5wEB7.sTrM4kKRQxMO506hcqkeBxmId
DQW.:18844:0:99999:7:::
yoonsu:$6$NfHDTOOj$iQBORha0Tlv/9HzvbkiZ0SYB.mb/BXdabpMgTthDSIH6rO.9vxlVUDwEeWT2ST0eXl7biquZt0I/0NiOj
JZSM.:18844:0:99999:7:::
[root@www ~]# _
```

※ /etc/shadow 파일
- shadow 파일은 /etc/passwd 파일에 있는 패스워드 부분을 /etc/shadow에 두고 root만이 읽을 수 있는 400 권한으로 설정해두어 보안을 강화하기 위한 목적이다.
- shadow파일은 9개 항목으로 구성되며, 존더리퍼를 사용하면서 알아야할 부분은 암호가 해쉬되어 저장된 encryped 항목이다.
*** 구조 : [$Hashid $Salt $Hash Value]**
=> Hash Value는 Hashid에 따른 해쉬방법과 Salt 값을 이용하여 Hash Function을 수행한 결과이다.

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

4. Password Crack

[공격]

3) john-1.8.0/run로 이동
> cd /root/john-1.9.0/run

```
[root@www ~]# cd /root/john-1.9.0/run/
[root@www run]#
```

4) unshadow 명령어를 사용하여 /etc/shadow 와 /etc/passwd 파일에 있는 패스워드를 해당 디렉터리에 mypasswd 파일로 저장
> ./unshadow /etc/passwd /etc/shadow > mypasswd

```
[root@www run]# ./unshadow /etc/passwd /etc/shadow > mypasswd
[root@www run]#
```

5) 크래킹 시작하고 패스워드가 나오는 것을 확인, 크랙 패스워드 보려면 --show 옵션 사용
> ./john mypasswd
> ./john --show mypasswd

```
[root@www run]# ./john mypasswd
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
yoonsu           (yoonsu)
subin            (subin)
root123          (root)
1234             (cju)
1111             (cjudoor)
5g 0:00:00:15 100% 2/3 0.3146g/s 212.3p/s 224.3c/s 224.3C/s sniper..bigben
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[root@www run]# _
```

PW

ID

```
[root@www run]# ./john --show mypasswd
root:root123:0:0:root:/root:/bin/bash
cjudoor:1111:1000:1000:cjudoor:/home/cjudoor:/bin/bash
cju:1234:1001:1001::/home/cju:/bin/bash
subin:subin:1002:1002::/home/subin:/bin/bash
yoonsu:yoonsu:1003:1003::/home/yoonsu:/bin/bash

5 password hashes cracked, 0 left
[root@www run]#
```

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

4. Password Crack

[공격]

6) Logout 하고 탈취한 계정(cju)으로 로그인 시도
> logout
> ID : cju
> PW : 1234

```
[root@www ~]# logout
```

```
www login: cju
Password:
Last login: Sat Aug  7 11:09:02 on tty1
[cju@www ~]$ _
```

7) 중요한 개인정보가 있는 파일 열람 > 금융정보 탈취 -> 2차 피해 위험
> cd secret
> ls
> cat personal_data.txt

```
[cju@www ~]$ cd secret
[cju@www secret]$ ls
personal_data.txt
[cju@www secret]$ cat personal_data.txt
registration number : 951204-0000000

account number : 423-0101-0101-00
Password : 1234
[cju@www secret]$ _
```