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

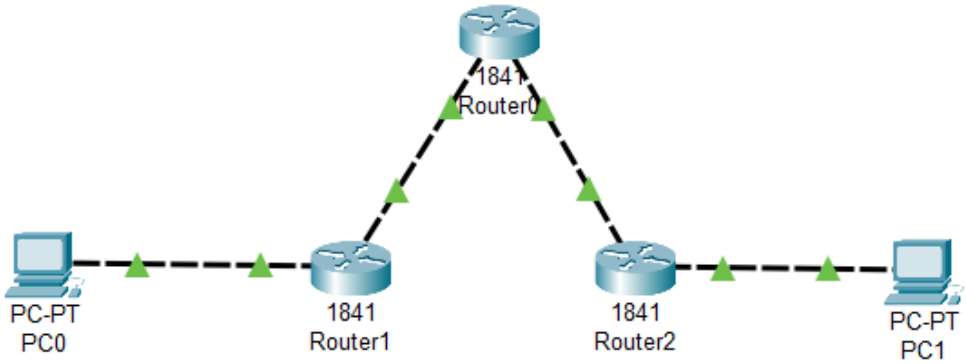
학습 절차:

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




```
R1#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/2/8 ms

R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#
```

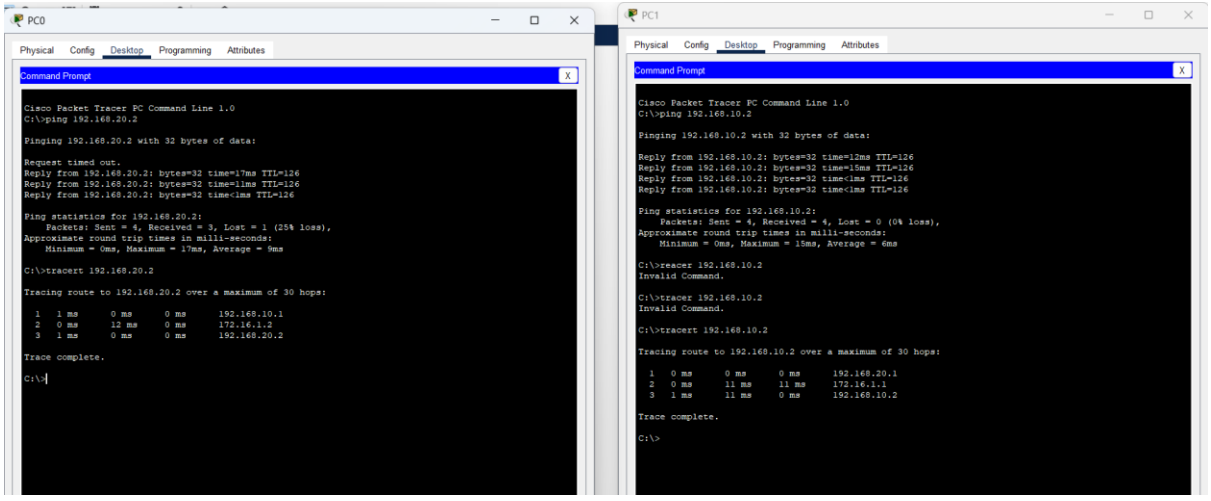
Copy Pas

```
R2(config)#int tunnel 100
R2(config-if)#ip address 172.16.1.2 255.255.0.0
R2(config-if)#tunnel source fa0/0
R2(config-if)#tunnel destination 11.0.0.1
R2(config-if)#no shut
R2(config-if)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#ping 11.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R2#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

R2#
```

네트워크를 라우터로 연결하여 서로 통신 가능하게 한 구조임

네트워크 설정과 라우팅 정보를 입력하고 난 후 라우터 간 연결이 잘 되었는지 Ping으로 테스트 한 결과임

처음에는 초반 연결이 안되었다가 다시 하니 연결이 된걸 의미함



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=17ms TTL=126
Reply from 192.168.20.2: bytes=32 time=11ms TTL=126
Reply from 192.168.20.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 9ms

C:\>tracert 192.168.20.2

Tracing route to 192.168.20.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      192.168.10.1
  2    0 ms      12 ms     0 ms      172.16.1.2
  3    1 ms      0 ms      0 ms      192.168.20.2

Trace complete.

C:\>
```

PC1

Physical Config Desktop Programming Attributes

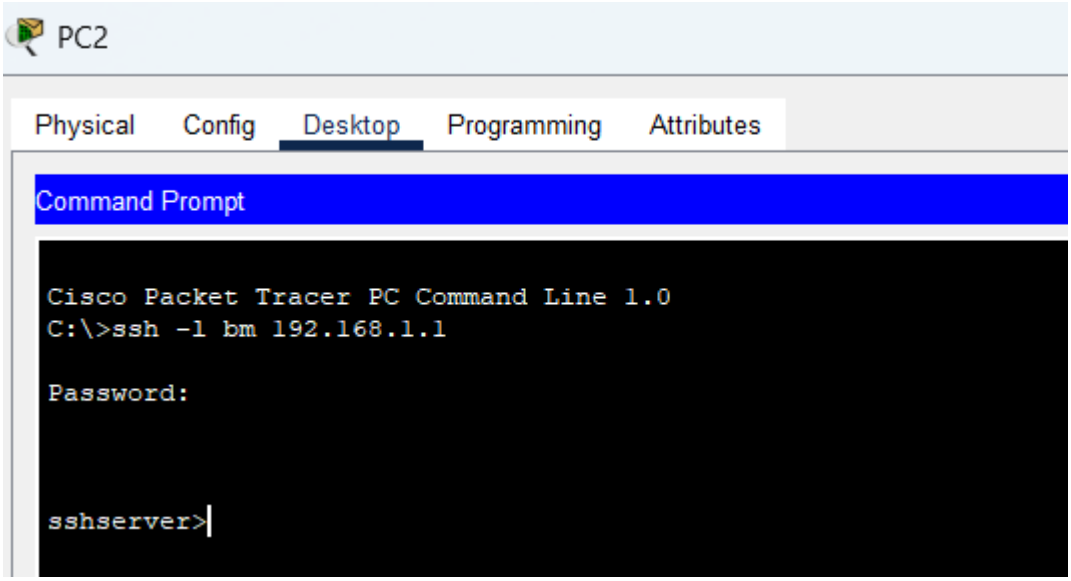
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=12ms TTL=126
Reply from 192.168.10.2: bytes=32 time=15ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>reacer 192.168.10.2
Invalid Command.

C:\>tracer 192.168.10.2
Invalid Command.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.20.1
  2    0 ms      11 ms     11 ms     172.16.1.1
  3    1 ms      11 ms     0 ms      192.168.10.2

Trace complete.

C:\>
```

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

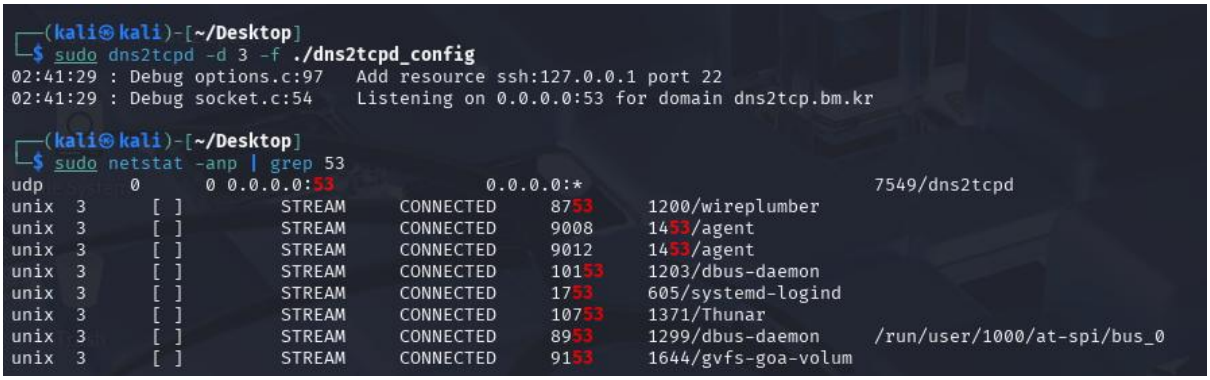
라우터를 2개 경유해서 도착한걸 알 수 있음

2. ssh 터널링

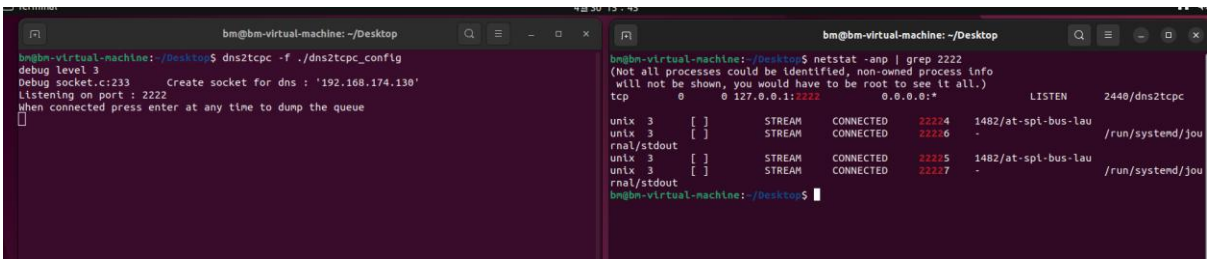


Ssh를 통해 라우터에 정상적으로 원격 접속을 성공하였음

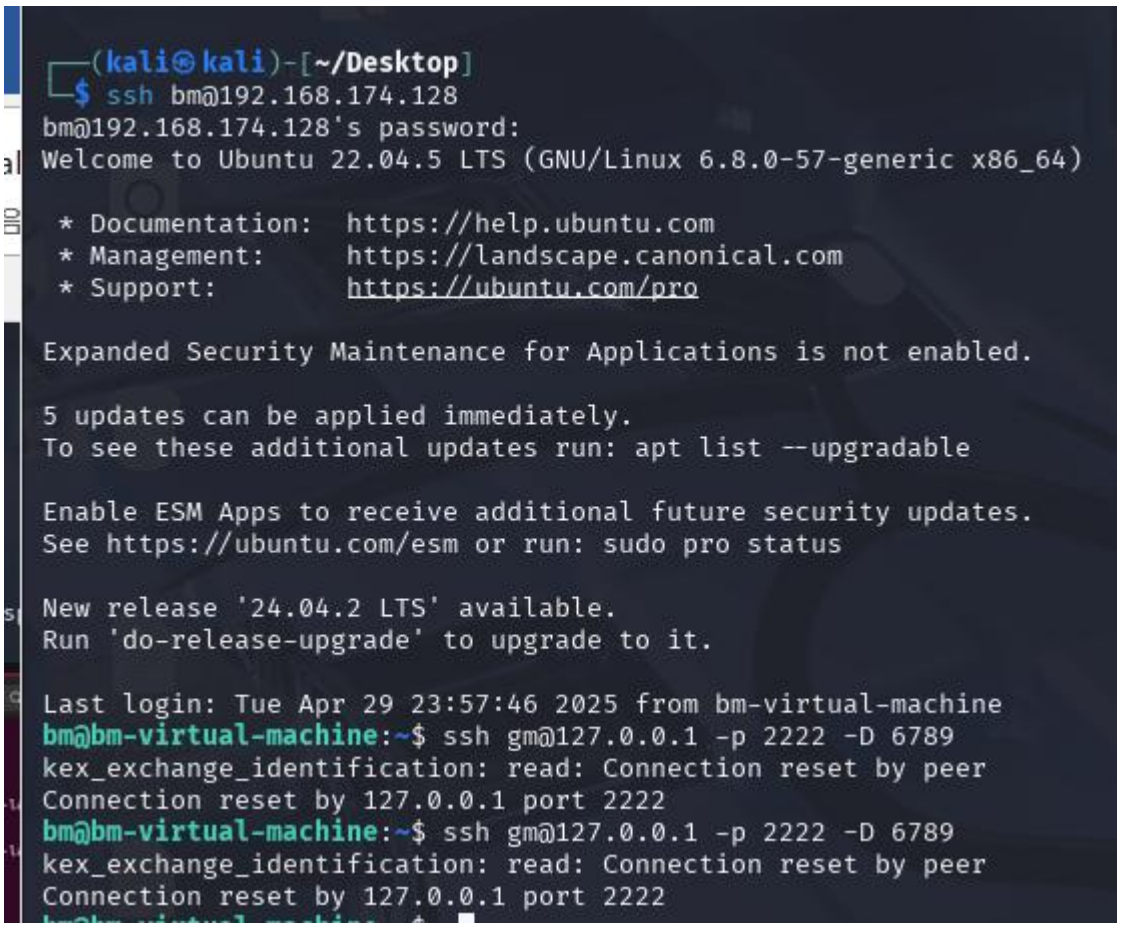
3. 셸 백도어

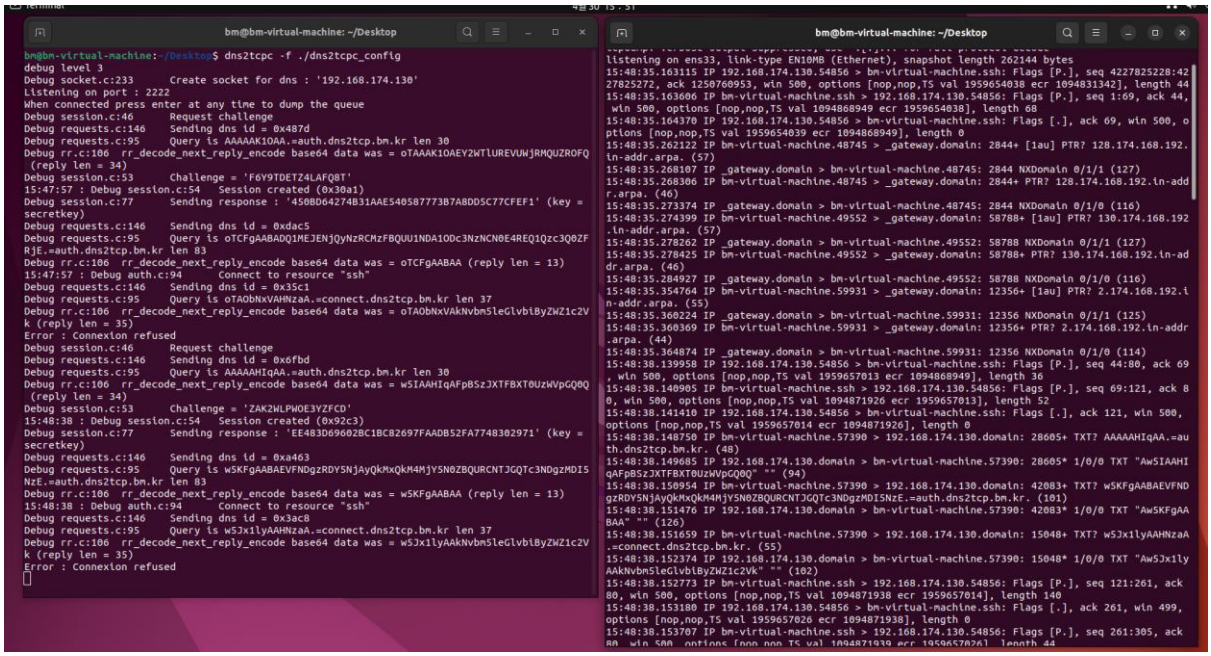


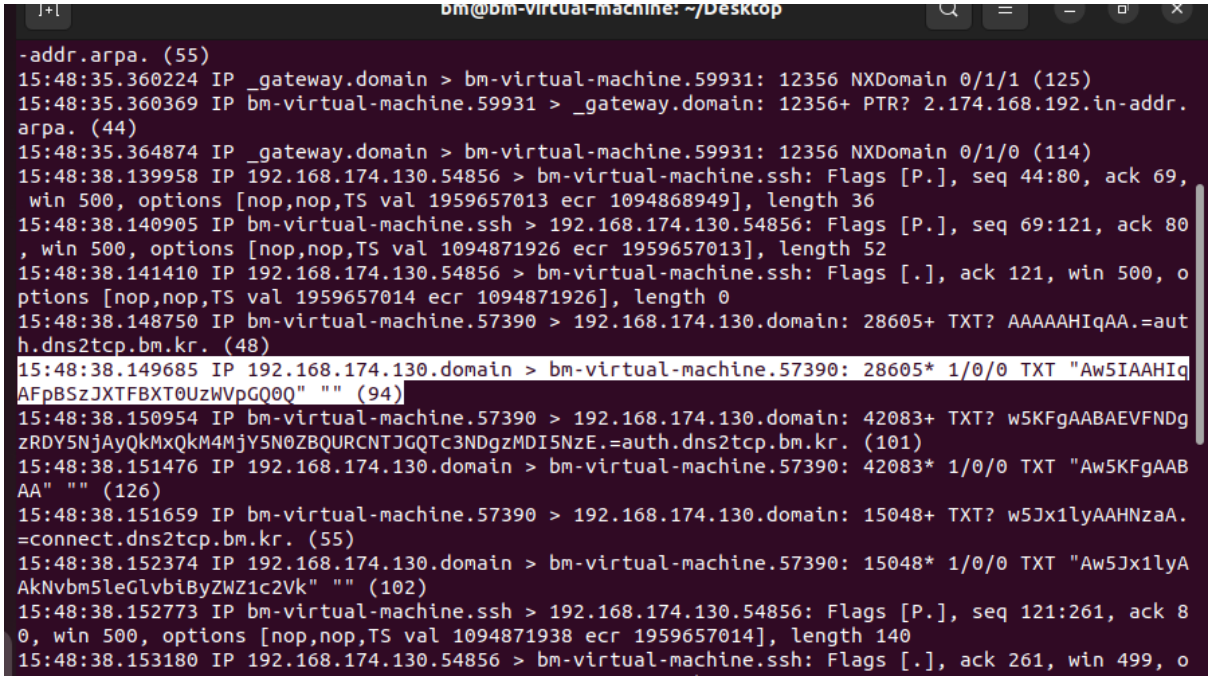
Dns2tcp서버를 실행한 후 udp53번 포트가 열려있음을 확인함



클라이언트를 실행한 후 2222번 포트가 열려있는지 확인을 하였음







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

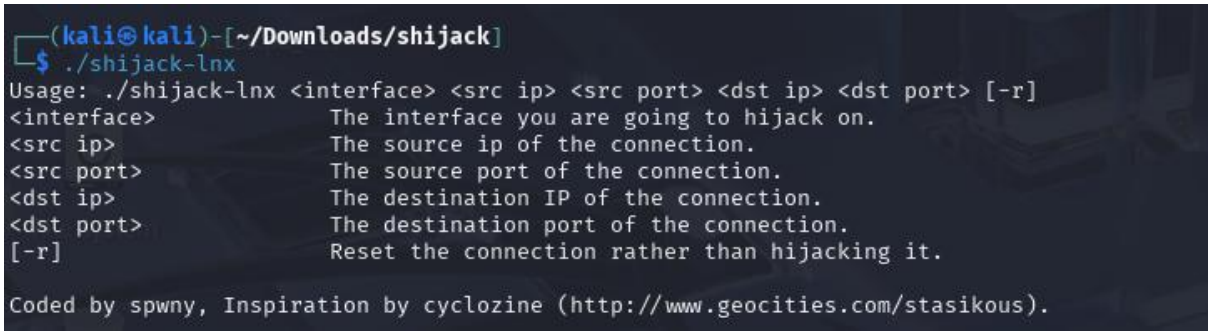
목적지 포트 : 57390 클라이언트

28605* : dns트래잭션 id , txt : 응답 타입 txt레코드

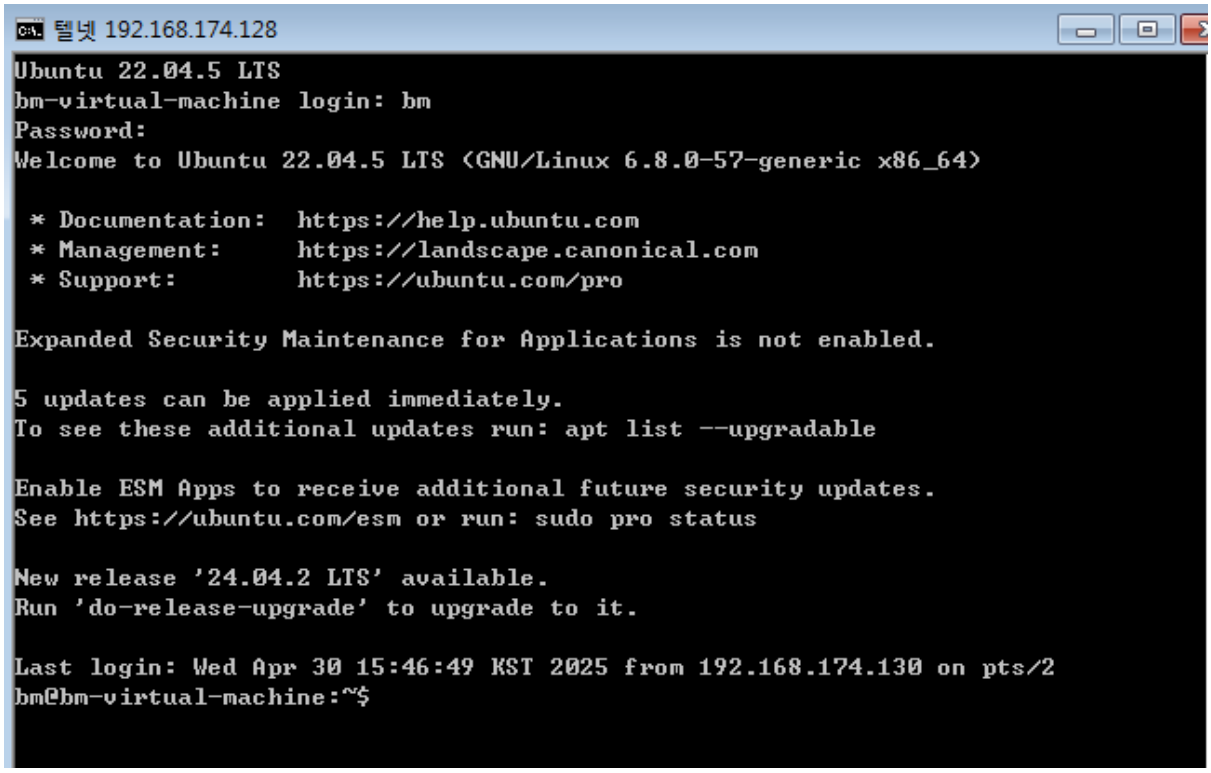
"Aw5IAAHIqAFpBSzJXTFBXT0UzWVpGQ0Q" : 인코딩된 데이터

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

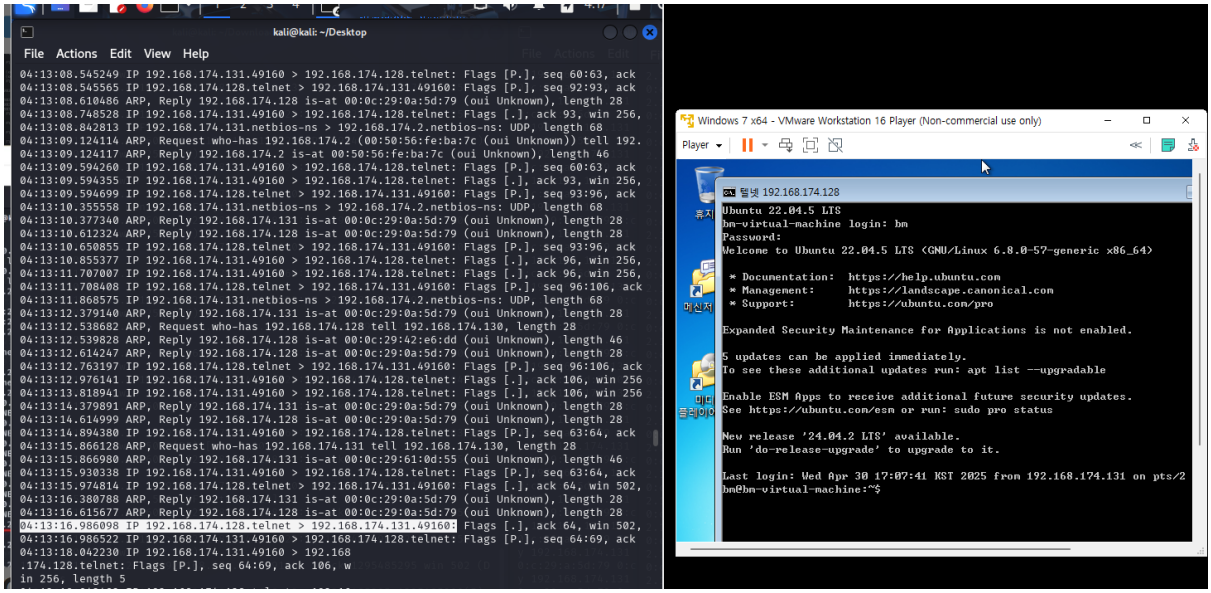
4. 텔넷 세션 하이재킹



Shijack를 다운받고 실행 옵션을 먼저 확인함.

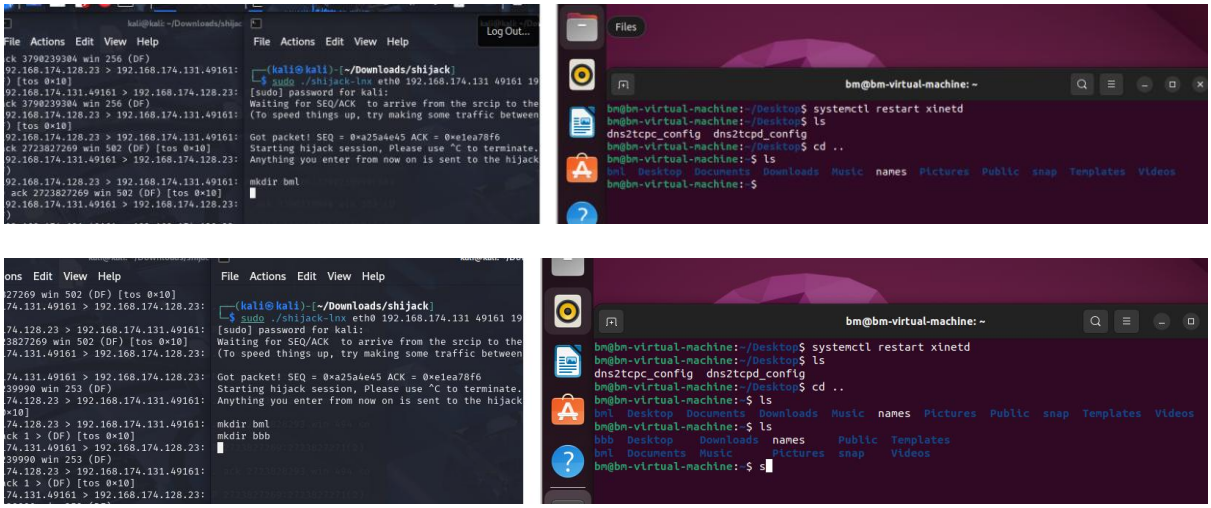


telnet으로 서버에 접속 성공



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