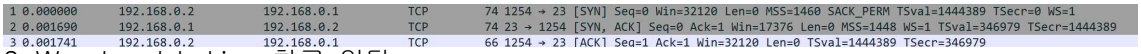


3-Way handshaking 하고 있다.

echo 현상 - 1개 문자열이 2개로 보이는 것

```
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
```

특정 호스트(www.yahoo.com)에 대한 ICMP(Internet Control Message Protocol) 에코 요청의 응답을 보여준다.

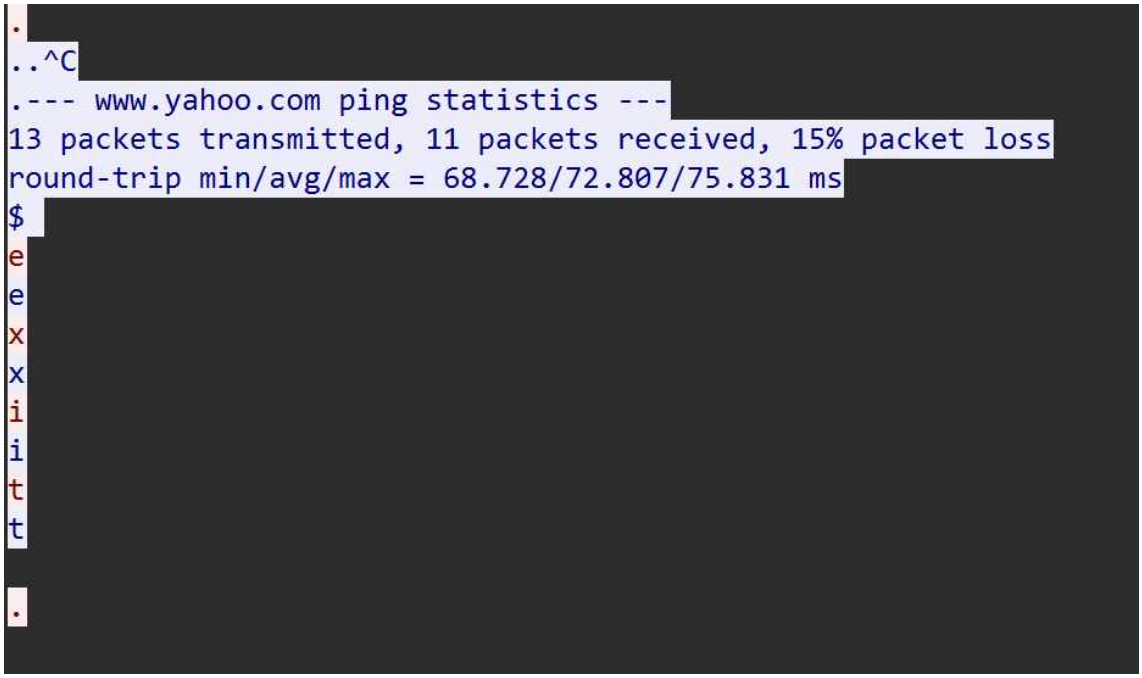
64 bytes from 204.71.200.74 : 서버로부터 수신한 데이터의 크기, 64바이트가 수신되었다

PING 명령은 네트워크 연결을 테스트하기 위해 사용되는데, www.yahoo.com의 IP 주소인 204.71.200.74에 56바이트의 데이터 패킷을 전송하고 있다.

icmp_seq=0~11 : 패킷이 전송된 순서

ttl=239 : 패킷이 네트워크 통해 전송될 수 있는 최대 홉 수. TTL 값이 239 인 경우, 패킷이 239개의 라우터 통과할 수 있다.

time=X ms : 응답 시간, 요청 보낸 후 응답받을 때까지 걸린 시간



ping 통계

- --- www.yahoo.com ping statistics ---: PING 명령에 대한 통계 정보를 시작하는 헤더. www.yahoo.com에 대한 정보를 나타냄

패킷 전송 및 수신

- 총 13개의 패킷 전송
- 그 중 11개 패킷이 성공적으로 수신
- 전체 전송된 패킷 중 15% 손실

왕복 시간 통계

- min : 최소 왕복 시간 68.728 ms
- avg : 평균 왕복 시간 72.807 ms
- max : 최대 왕복 시간 75.831 ms

세션 종료

telnet 23번 포트 사용

Telnet 취약점
- 데이터 평문 통신으로 보안에 취약. 스니핑 공격에 노출되기 쉬움
- 접근 제어 기능 부족하여 특정 사용자에 대한 접근 권한 관리하기 어려움
- 23번 포트 사용하기 때문에 포트 스캔 공격의 쉬운 대상이 될 수 있다.

보완 방법
1. SSH로 대체
2. VPN 사용
3. 접근 제어 설정 강화
   방화벽 사용하여 포트에 대한 접근 제한, 특정 IP 주소나 네트워크에서만 접속할 수 있도록 설정

Keep-Alive : TCP 세션에서 데이터가 전송되지 않은 상태에서 나오는 패킷

4번
Do Suppress Go Ahead: Suppress Go Ahead 옵션 사용 - 특정 제어 신호(Go Ahead 신호)를 억제, 상대방의 응답을 기다리지 않고 계속 데이터를 보낼 수 있도록 제어하는 역할.
Will Terminal Type: 터미널 유형 협상의 의미.
Will Negotiate About Window Size: 윈도우 크기에 대해 협상할 의향이 있음. 터미널 창의 크기를 설정하는 데 사용.
Will Terminal Speed: 터미널 속도에 협상.
Will Remote Flow Control: 원격 흐름 제어에 대해 협상. 데이터 흐름을 조정 가능.
[Malformed Packet]: 패킷이 제대로 형식화되지 않았거나 구조에 오류가 있다는 경고. 분석 도구가 데이터를 완벽하게 해석하지 못할 때 나타나는 메시지.

5번, 7번
Do Authentication : 서버 또는 네트워크 장치가 클라이언트에게 인증을 요구하는 의미
Won't Authentication option : 인증 옵션을 사용하지 않겠다는 의미

9번
Will Suppress Go Ahead : 양방향 통신에서 Go Ahead 신호를 제거하는 역할을 함.
Do Terminal Type : 클라이언트가 사용하는 터미널 유형을 서버에 알려주는 기능
Do Negotiate About Window Size : 클라이언트가 사용하고 있는 터미널 창의 크기를 서버에 전달하는 옵션.
Do Terminal Speed : 널의 전송 속도(bps)를 설정하는 옵션
Do Remote Flow Control : 네트워크 흐름 제어에 관한 옵션. 서버가 클라이언트와의 데이터 전송 속도를 관리하여 패킷 손실을 최소화하고 네트워크가 과부하 되지 않도록 제어.

10번
Suboption Negotiate About Window Size : 윈도우크기 협상의 의미
Suboption Linemode : 텔넷 클라이언트가 각 입력을 서버로 바로 보내는 것이 아니라 사용자가 한 줄을 완료한 후에 데이터를 전송
Do Suppress Go Ahead : Go Ahead 신호 비활성화
Suboption Linemode : 다시 등장하는 것은 협상하는 도중 반복해서 협상이 이루어졌거나 추가 설정이 진행되었기 때문

12번
Do New Environment Option: "New Environment Option" 기능을 사용하도록 요청. 이는 일반적으로 환경 변수와 같은 정보를 설정할 때 사용.
Will Status: 상태 정보(Status)에 대해 협상할 의사를 표시함.
Do X Display Location: X Display Location 옵션을 사용하도록 요청하는 것.
Will Encryption Option: 암호화 옵션을 사용할 의사를 표시함. 데이터 통신의 보안성을 높이기 위한 옵션 협상.

13번
Don't Encryption Option: 암호화 기능을 사용하지 않겠다는 의사
Won't Encryption Option: 암호화 옵션을 지원하지 않거나 사용할 의사가 없음.
Won't Environment Option: 환경 변수 전송 기능 비활성화. 서버 측에서 이 옵션을 거부하면 클라이언트는 환경 변수에 접근하거나 이를 설정 할 수 없음.

15번, 16번
Suboption Terminal Speed: 터미널과 서버 간의 데이터 전송 속도를 협상, 네트워크 상황과 터미널 기능에 맞춰 최적화되어 데이터 전송 지연을 줄이는 역할
Suboption X Display Location: X11 프로토콜을 사용하여 GUI 프로그램을 원격으로 표시, 클라이언트가 지정된 호스트에서 원격 X 서버를 실행 중임을 서버에 알려주는 것
Suboption New Environment Option: 텔넷 세션에서 추가 환경 변수를 설정할 수 있는 옵션, 클라이언트와 서버 간의 설정이 통일되며, 사용자 맞춤형 환경을 원격 서버에서 그대로 사용
Suboption Terminal Type: 클라이언트의 터미널 종류를 서버에 알려주는 역할, 화면 출력 호환성과 기능을 보장하여, 서버가 클라이언트의 터미널 특성에 맞게 텍스트와 색상을 출력

18번
Do Echo : 에코(Echo) 기능을 활성화하라는 요청

19번
Won't Echo : 에코 기능을 사용하지 않겠다는 의미

21번
Will Echo : 에코 기능을 활성화하겠다는 의사
Suboption Remote Flow Control : 데이터 흐름 제어를 의미. 주로 대량의 데이터 전송이 있을 때 서버와 클라이언트 간 데이터 전송 속도를 조정하기 위해 사용.
Won't Echo : 에코 기능을 비활성화하겠다는 의사. 에코 기능을 비활성화하면 입력한 내용이 보이지 않아 보안성이 강화됨.

22번
Do Echo : 클라이언트 입력을 화면에 표시
Don't Echo : 클라이언트 입력을 화면에 표시하지 않음

24번ip.dst == 192.168.0.1
Suboption Linemode : 텔넷 클라이언트가 각 입력을 서버로 바로 보내는 것이 아니라 사용자가 한 줄을 완료한 후에 데이터를 전송
30번
Won't Linemode와 Do Echo가 함께 설정된 경우:
사용자의 입력은 Character mode로 문자 단위로 즉시 서버로 전송.
서버는 입력한 내용을 클라이언트 화면에 반향시킴.

실시간 피드백이 필요한 상황에서 유용함.

32번
Will Echo: 에코 기능을 활성화하겠다는 의사

34번
Don`t Linemode:
Linemode를 사용하지 않도록 설정하겠다는 의사, Character mode로 작동

246번
Malformed Packet:
패킷이 제대로 형식화되지 않았거나 구조에 오류가 있다는 경고. 분석 도구가 데이터를 완벽하게 해석하지 못할 때 나타나는 메시지.

주요 텔넷 협상 커맨드
텔넷 커맨드는 네 개의 기본 커맨드와 여러 옵션 코드로 구성
WILL (251)
의미: 송신자가 특정 옵션을 사용하겠다고 선언.
용도: 특정 기능을 활성화하겠다는 의사.
예시: WILL ECHO는 송신자가 에코 기능을 사용하겠다고 알리는 의미.
WONT (252)
의미: 송신자가 특정 옵션을 사용하지 않겠다고 선언.
용도: 특정 기능을 비활성화하겠다는 의사.
예시: WONT ECHO는 송신자가 에코 기능을 사용하지 않겠다는 의미.
DO (253)
의미: 상대방이 특정 옵션을 사용해 달라고 요청.
용도: 상대방이 특정 기능을 활성화하도록 요구.
예시: DO ECHO는 수신자에게 에코 기능을 사용해 달라고 요청.
DONT (254)
의미: 상대방이 특정 옵션을 사용하지 않기를 요청.
용도: 상대방이 특정 기능을 비활성화하도록 요구.
예시: DONT ECHO는 수신자에게 에코 기능을 사용하지 말라고 요청.
텔넷 협상 커맨드 구조 예시
텔넷 협상 커맨드는 옵션 코드와 함께 전송.
DO ECHO (253 1): 수신자에게 에코 기능을 사용하도록 요청.
WILL SUPPRESS-GO-AHEAD (251 3): 송신자가 SUPPRESS-GO-AHEAD 옵션을 사용할 것임을 알림.
기타 관련 코드
텔넷 프로토콜에서 사용되는 일반적인 코드들.
IAC (255): Interpret As Command의 약자로, 텔넷 커맨드가 시작됨을 알림.
ECHO (1): 텍스트 에코 기능으로, 입력한 텍스트를 화면에 그대로 표시.

SUPPRESS-GO-AHEAD (3): "Go Ahead" 신호를 억제하여 네트워크의 지연을 줄임.