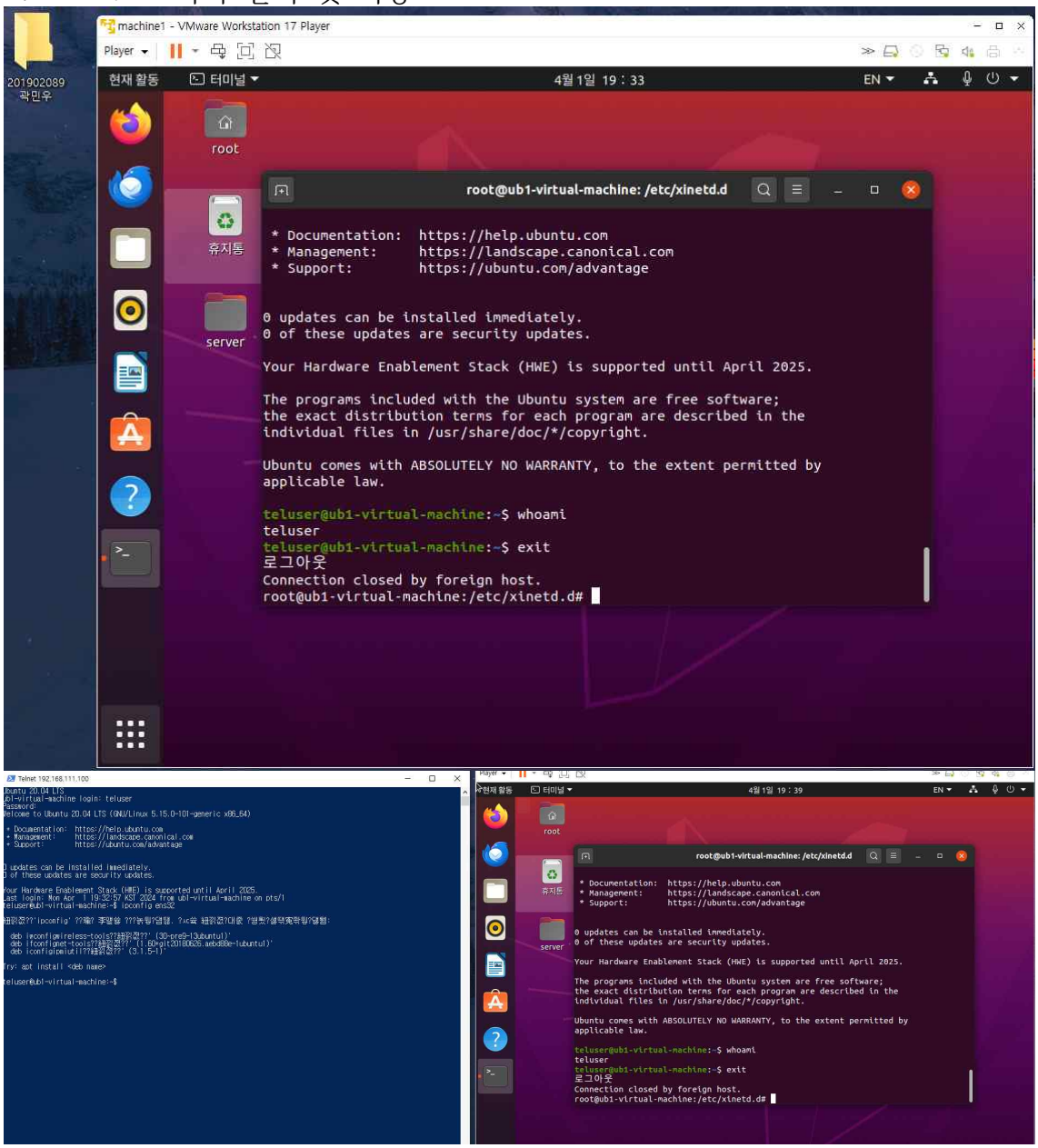
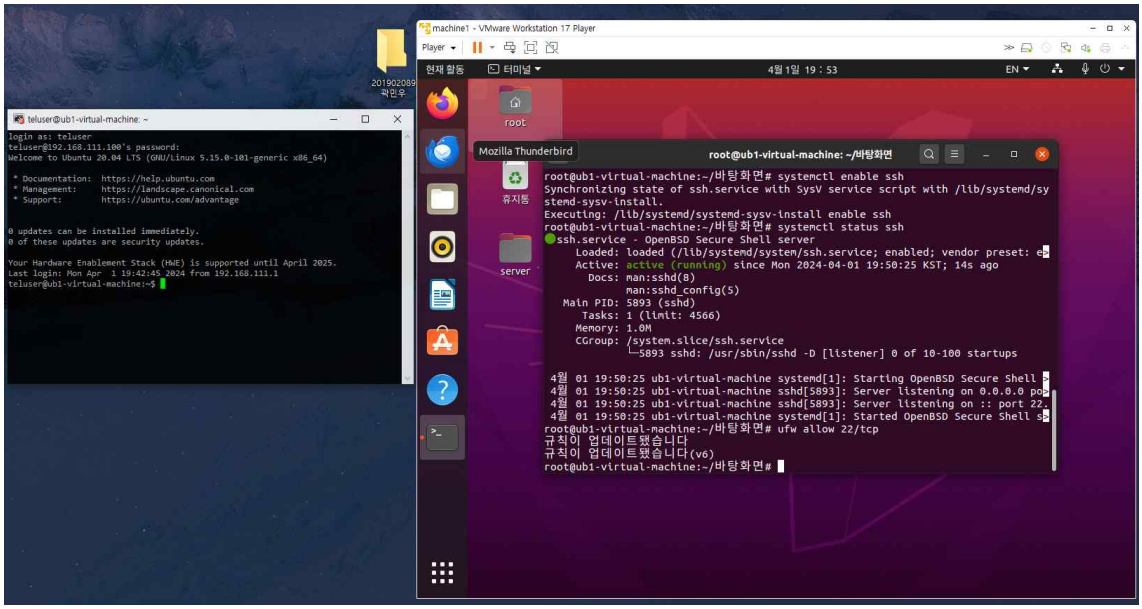
TELNET & OpenSSH 서버 구축 및 실험

24.04.06

1. TELNET 서버 설치 및 가동



2. OpenSSH 서버 설치 및 가동



3. Wireshark 실습

(1) TELNET 접속 실습

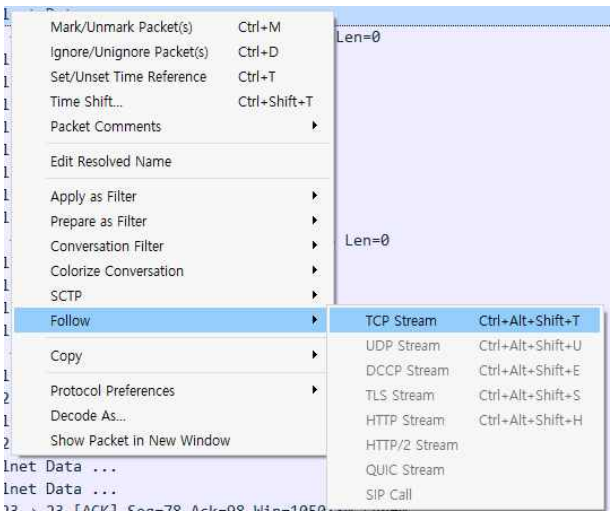
1. 3-way-handshaking 방식 접속

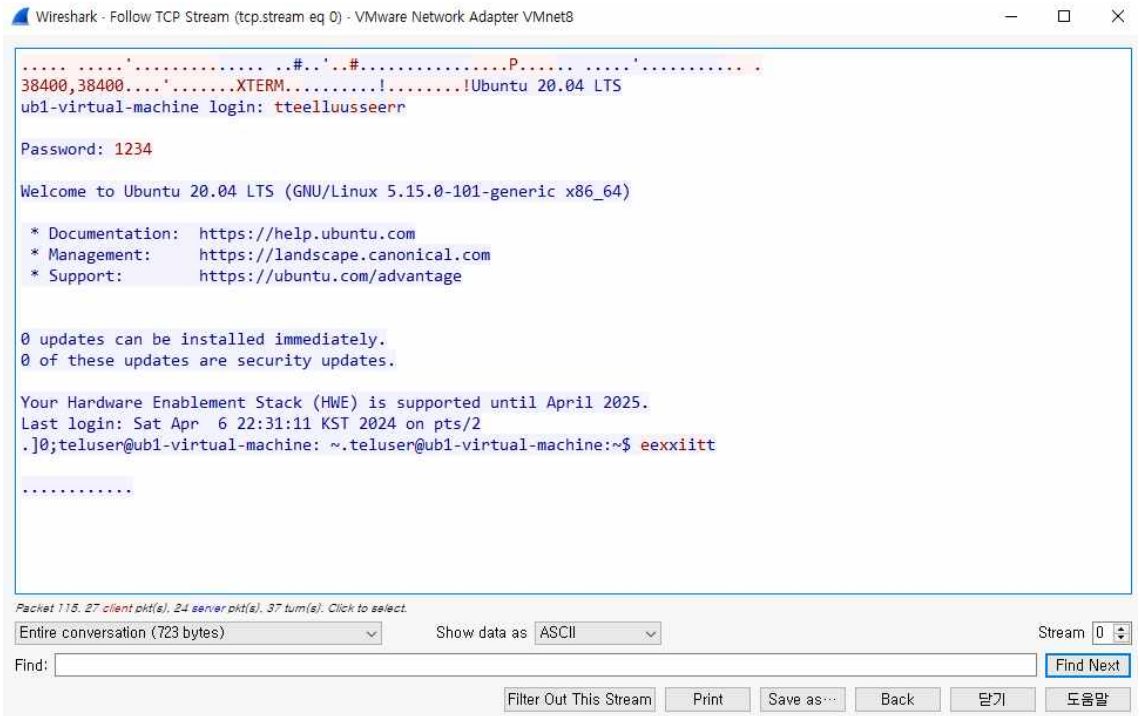
1	0.000000	192.168.111.1	192.168.111.100	TCP	66 9223 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000147	192.168.111.100	192.168.111.1	TCP	66 23 → 9223 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000184	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=1 Ack=1 Win=1051136 Len=0

2. 로그인 과정

52	0.007557	192.168.111.1	192.168.111.100	TELNET	75 Telnet Data ...
53	0.007634	192.168.111.100	192.168.111.1	TCP	60 23 → 9223 [ACK] Seq=1 Ack=22 Win=64256 Len=0
57	10.012049	192.168.111.100	192.168.111.1	TELNET	66 Telnet Data ...
58	10.012221	192.168.111.1	192.168.111.100	TELNET	57 Telnet Data ...
59	10.012347	192.168.111.100	192.168.111.1	TELNET	66 Telnet Data ...
60	10.012432	192.168.111.1	192.168.111.100	TELNET	63 Telnet Data ...
61	10.012623	192.168.111.100	192.168.111.1	TELNET	72 Telnet Data ...
62	10.012735	192.168.111.1	192.168.111.100	TELNET	71 Telnet Data ...
63	10.012758	192.168.111.1	192.168.111.100	TELNET	60 Telnet Data ...
64	10.012768	192.168.111.1	192.168.111.100	TELNET	65 Telnet Data ...
65	10.012920	192.168.111.100	192.168.111.1	TCP	60 23 → 9223 [ACK] Seq=43 Ack=68 Win=64256 Len=0
66	10.013078	192.168.111.100	192.168.111.1	TELNET	63 Telnet Data ...
67	10.013186	192.168.111.1	192.168.111.100	TELNET	57 Telnet Data ...
68	10.013201	192.168.111.1	192.168.111.100	TELNET	57 Telnet Data ...
69	10.013210	192.168.111.1	192.168.111.100	TELNET	57 Telnet Data ...
70	10.013328	192.168.111.100	192.168.111.1	TCP	60 23 → 9223 [ACK] Seq=52 Ack=77 Win=64256 Len=0
71	10.013393	192.168.111.100	192.168.111.1	TELNET	72 Telnet Data ...
73	10.067517	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=77 Ack=70 Win=1050880 Len=0
74	10.068364	192.168.111.100	192.168.111.1	TELNET	81 Telnet Data ...
75	10.113283	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=77 Ack=97 Win=1050880 Len=0
76	11.270593	192.168.111.1	192.168.111.100	TELNET	55 Telnet Data ...
77	11.271502	192.168.111.100	192.168.111.1	TELNET	60 Telnet Data ...
78	11.326703	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=78 Ack=98 Win=1050880 Len=0
79	11.485405	192.168.111.1	192.168.111.100	TELNET	55 Telnet Data ...
80	11.485680	192.168.111.100	192.168.111.1	TELNET	60 Telnet Data ...
81	11.526905	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=79 Ack=99 Win=1050880 Len=0
82	11.728034	192.168.111.1	192.168.111.100	TELNET	55 Telnet Data ...
83	11.728315	192.168.111.100	192.168.111.1	TELNET	60 Telnet Data ...
84	11.772103	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=80 Ack=100 Win=1050880 Len=0

계속해서 TELNET data가 교환되는데, TCP Follow 기능을 이용하여 추적하였습니다.





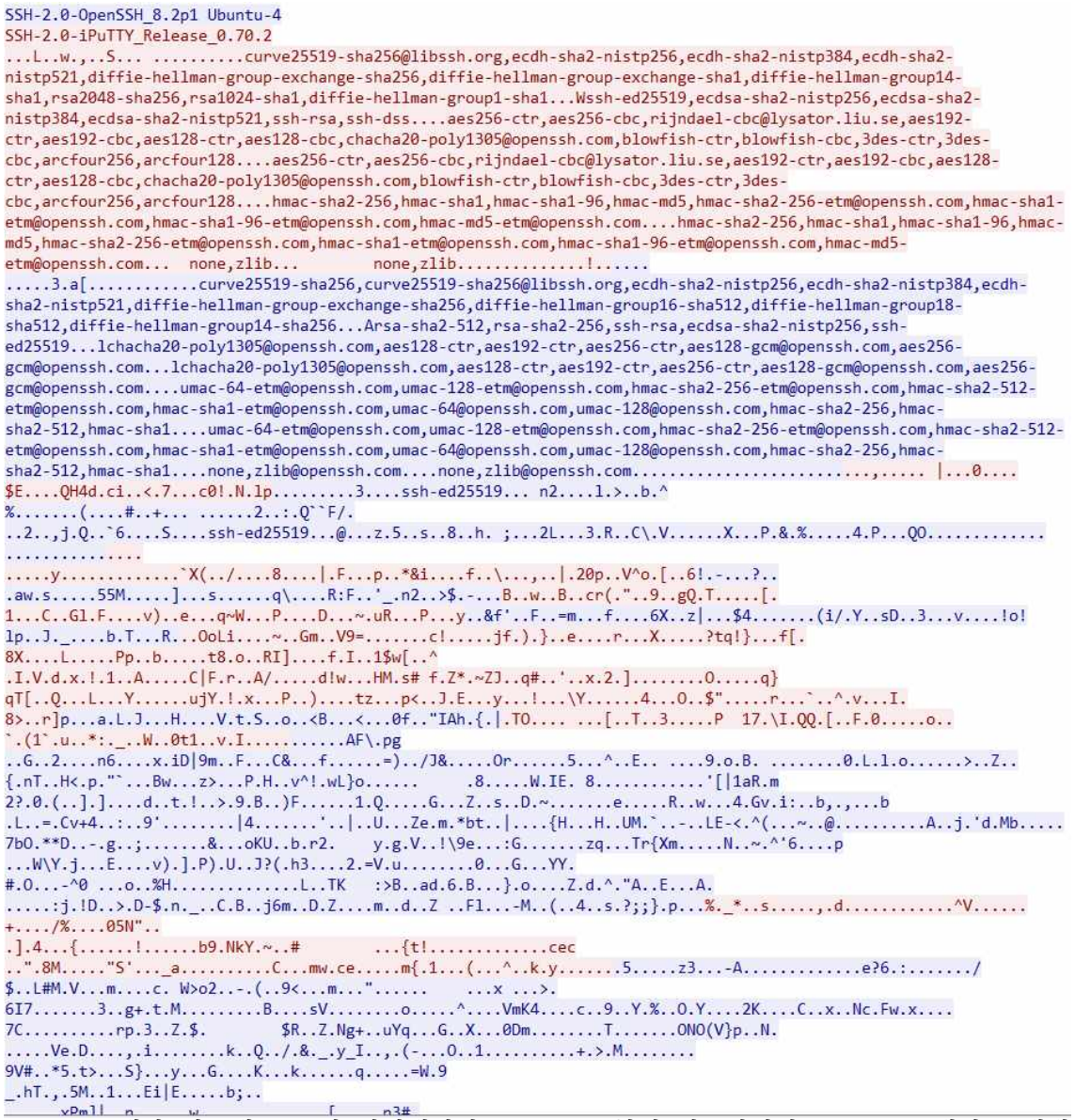
붉은색은 client packet, 푸른색은 server packet입니다. 로그인을 하기 위한 과정이 드러난 채로 packet이 교환되는 것을 볼 수 있습니다. 그리고 마지막에 exit를 입력함으로써 통신이 종료된 것을 볼 수 있습니다. 아래는 종료 과정입니다.

134	20.458017	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [ACK] Seq=98 Ack=628 Win=1050368 Len=0
135	20.458125	192.168.111.1	192.168.111.100	TCP	54 9223 → 23 [FIN, ACK] Seq=98 Ack=628 Win=1050368 Len=0
136	20.458225	192.168.111.100	192.168.111.1	TCP	60 23 → 9223 [ACK] Seq=628 Ack=99 Win=64256 Len=0

(2) SSH 접속 실습

1. 접속 : TELNET 때와 동일

2. 로그인 과정



TELNET 때와 다르게 로그인 과정에서의 packet 교환이 암호화되어 wireshark에서는 제대로 볼 수 없습니다. exit 하는 과정도 보이지 않습니다.