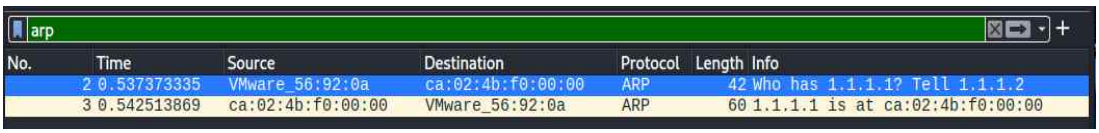
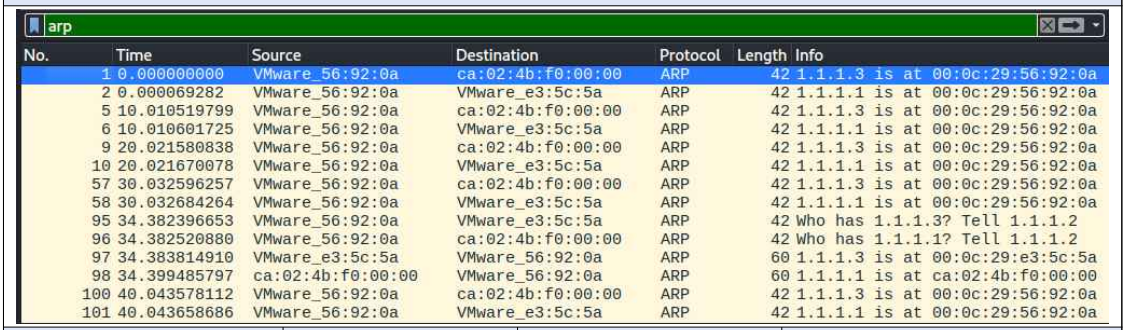
[시나리오 1] 패킷 식별 계획 - 내부망 침투 및 시스템 파괴

타겟 식별 및 초기 침투			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
네트워크 스캔 및 OS 분석	arp spoofing	arp	동일 IP에 MAC 주소 지속 변조

정상 패킷



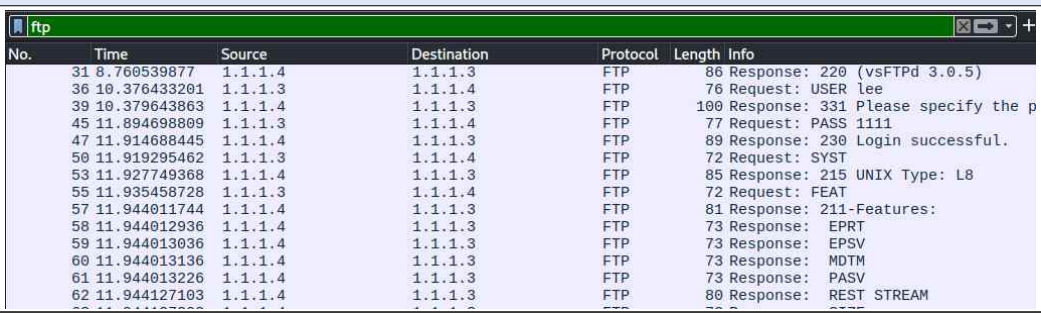
비정상 패킷



공격 시나리오	공격 기법	필터	정상/비정상 식별 기준
네트워크 스캔 및 OS 분석	FTP 패킷 스니핑	ftp || tcp.port == 21	Payload 내 계정 정보 노출 여부

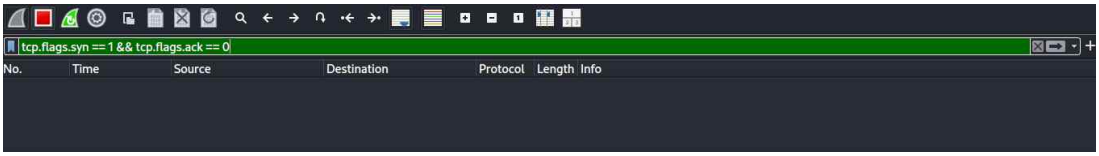
정상 패킷

비정상 패킷

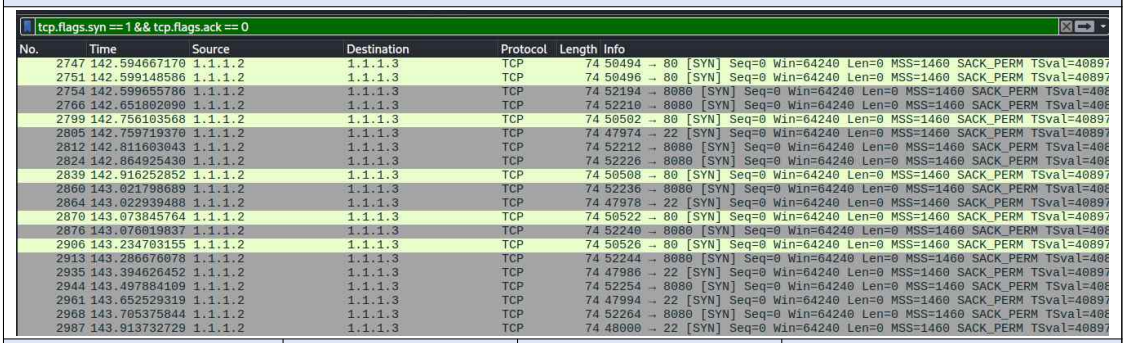


공격 시나리오	공격 기법	필터	정상/비정상 식별 기준
네트워크 스캔 및 OS 분석	nmap 스캔	tcp.flags.syn == 1	단시간 내 다수 포트 접속 시도

정상 패킷

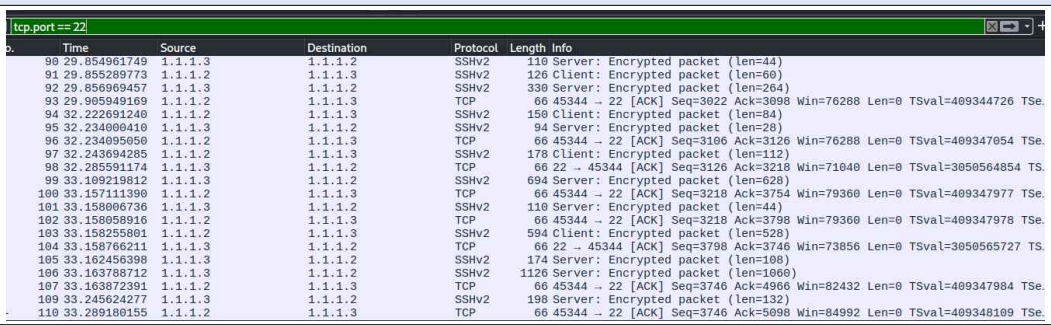


비정상 패킷



공격 시나리오	공격 기법	필터	정상/비정상 식별 기준
SSH 크래킹 (hydra)	SSH Brute Force	tcp.port == 22	동일 IP의 인증 시도 횟수 폭증

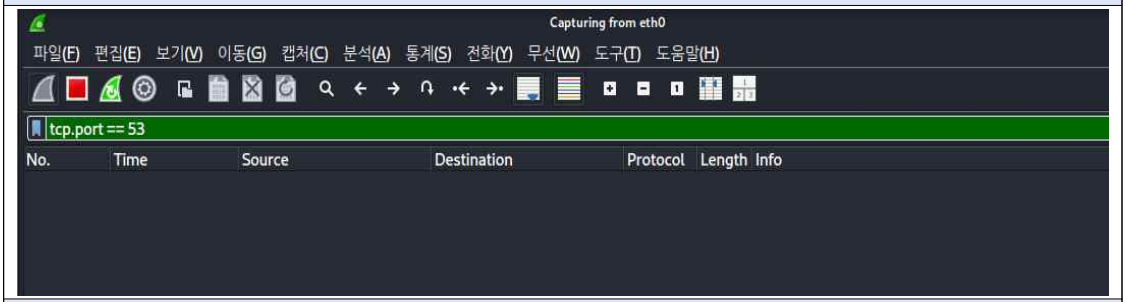
정상 패킷



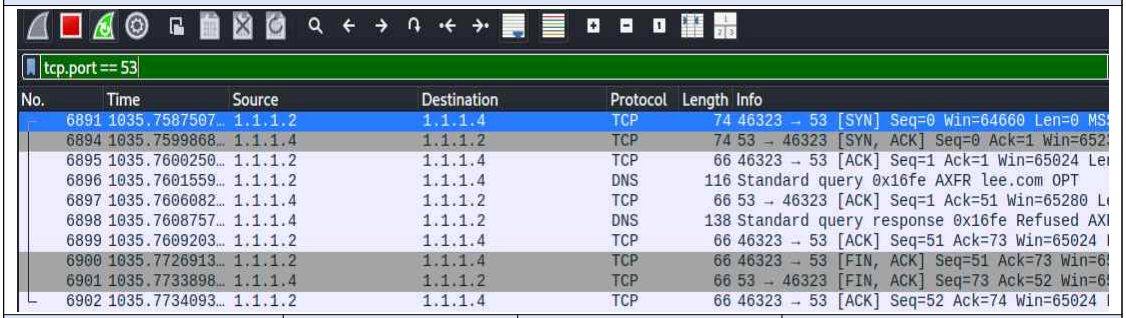
비정상 패킷

내부망 확장 및 관리자 권한 획득			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
DNS 정보 탈취	AXFR	tcp.port == 53	헤더 내 스캐너 명시

정상 패킷

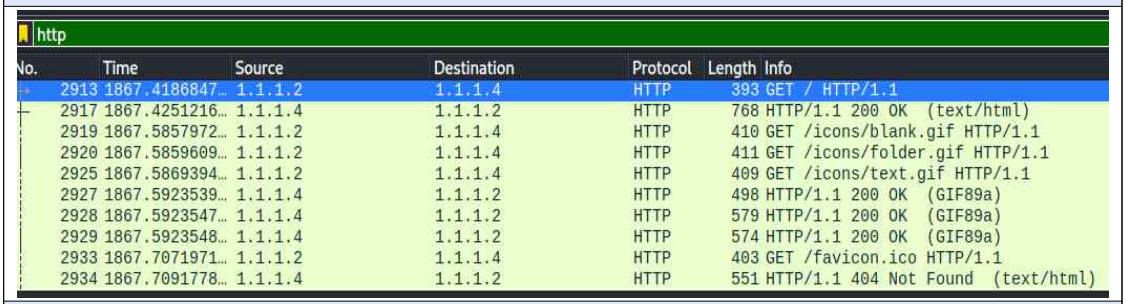


비정상 패킷

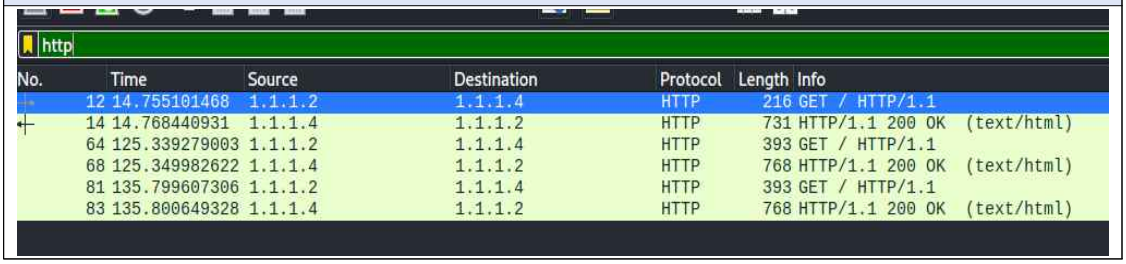


공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
DNS 정보 탈취	WhatWeb	http	DNS 서버 설정 상태

정상 패킷

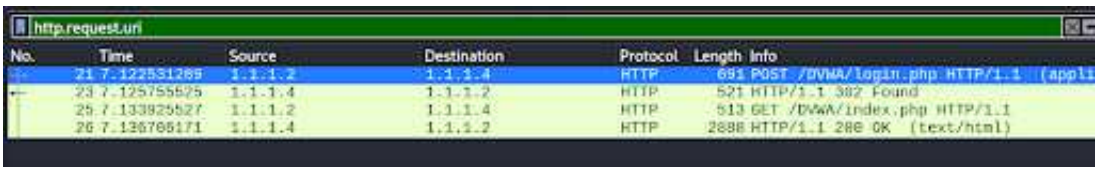


비정상 패킷

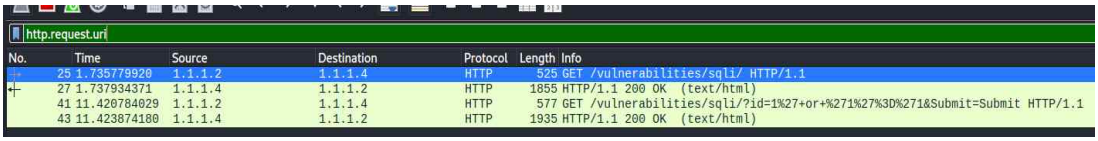


공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
SQL Injection	SQL Injection	http.request.uri	요청 데이터 내 DB 예약어 포함

정상 패킷



비정상 패킷



시나리오1 차단 정책
시나리오 1은 서버 단에서 iptables로 차단할 예정

[시나리오 2]

공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
정상 패킷			
비정상 패킷			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
정상 패킷			
비정상 패킷			