
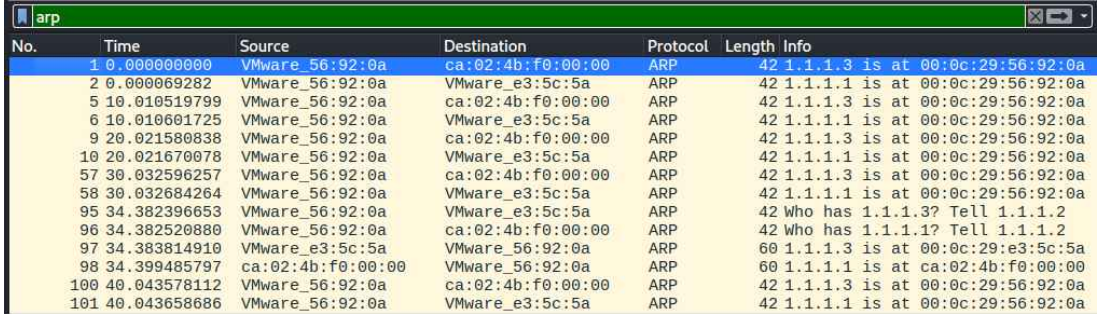
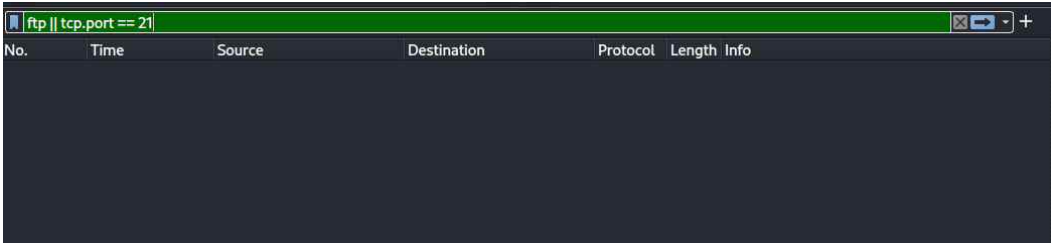
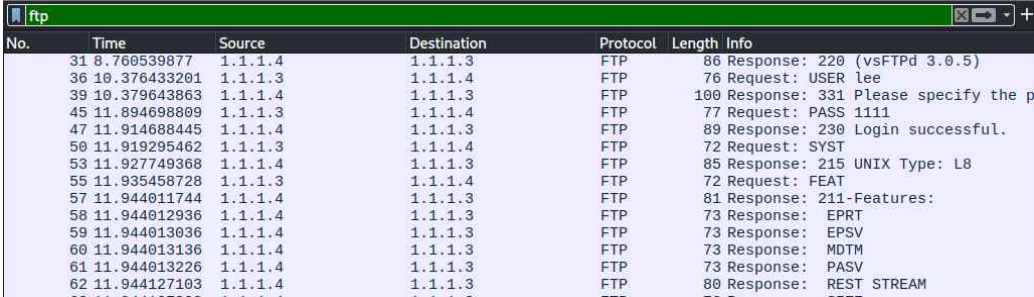


[시나리오 1] 패킷 식별 계획 - 내부망 침투 및 시스템 파괴

| 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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|-------------|----------|--------|---|
| 1 | 0.000000 | 192.168.1.100 | 192.168.1.1 | TCP | 60 | 65535 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |

비정상 패킷

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|---------------|---------|-------------|----------|--------|---|
| 2747 | 142.594667170 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 50494 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2751 | 142.599148586 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 50496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2754 | 142.599655786 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52194 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2766 | 142.651802090 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52210 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2799 | 142.756193568 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 50502 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2808 | 142.759719370 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 47974 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2812 | 142.811603843 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52212 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2824 | 142.864925430 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52226 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2839 | 142.916252852 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 50508 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2860 | 143.021798689 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52236 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2864 | 143.022939488 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 47978 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2870 | 143.073845764 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 50522 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2876 | 143.076919637 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52240 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2906 | 143.234703155 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 50526 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2913 | 143.284676078 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52244 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2935 | 143.394626452 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 47986 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2944 | 143.497884109 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52254 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2961 | 143.652529319 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 47994 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2968 | 143.705375844 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 52264 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |
| 2987 | 143.913732729 | 1.1.1.2 | 1.1.1.3 | TCP | 74 | 48008 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897 Tsecr=0 |

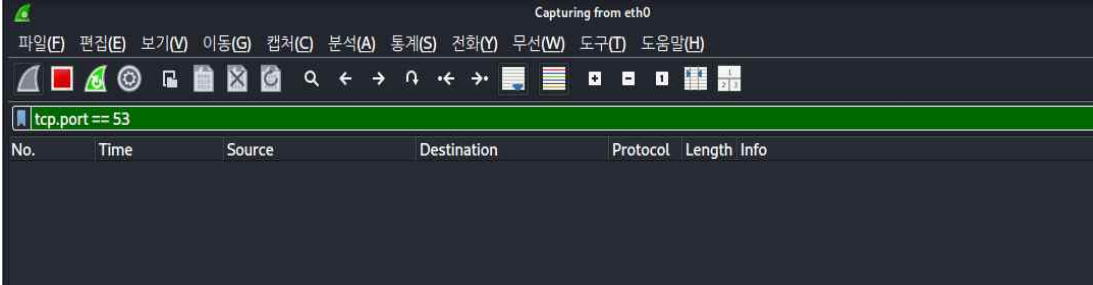
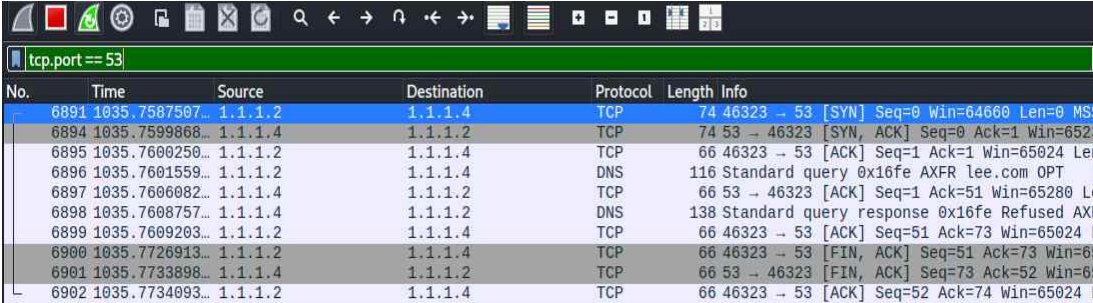

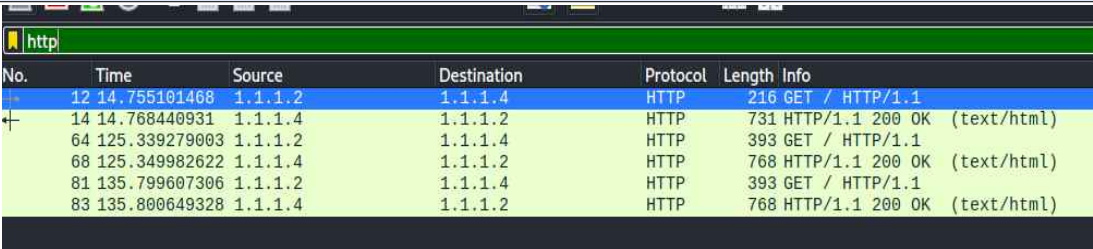
| 공격 시나리오 | 공격 기법 | 필터 | 정상/비정상 식별 기준 |
|-----------------|-----------------|----------------|--------------------|
| SSH 크래킹 (hydra) | SSH Force Brute | tcp.port == 22 | 동일 IP의 인증 시도 횟수 폭증 |

정상 패킷

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------|-------------|----------|--------|---|
| 90 | 29.854961749 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 110 | Server: Encrypted packet (len=44) |
| 91 | 29.855289773 | 1.1.1.2 | 1.1.1.3 | SSHv2 | 126 | Client: Encrypted packet (len=60) |
| 92 | 29.856969457 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 330 | Server: Encrypted packet (len=264) |
| 93 | 29.905949169 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 45344 → 22 [ACK] Seq=3022 Ack=3098 Win=76288 Len=0 TSval=409344726 TSecr=0 |
| 94 | 32.222691240 | 1.1.1.2 | 1.1.1.3 | SSHv2 | 150 | Client: Encrypted packet (len=84) |
| 95 | 32.234909410 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 94 | Server: Encrypted packet (len=28) |
| 96 | 32.234909500 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 45344 → 22 [ACK] Seq=3106 Ack=3126 Win=76288 Len=0 TSval=409347054 TSecr=0 |
| 97 | 32.243694285 | 1.1.1.2 | 1.1.1.3 | SSHv2 | 178 | Client: Encrypted packet (len=112) |
| 98 | 32.285591174 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 45344 [ACK] Seq=3126 Ack=3218 Win=71840 Len=0 TSval=3059564854 TSecr=0 |
| 99 | 33.109219812 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 694 | Server: Encrypted packet (len=620) |
| 100 | 33.157111390 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 45344 → 22 [ACK] Seq=3218 Ack=3754 Win=79360 Len=0 TSval=409347977 TSecr=0 |
| 101 | 33.158006736 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 110 | Server: Encrypted packet (len=44) |
| 102 | 33.158058916 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 45344 → 22 [ACK] Seq=3218 Ack=3798 Win=79360 Len=0 TSval=409347978 TSecr=0 |
| 103 | 33.158255801 | 1.1.1.2 | 1.1.1.3 | SSHv2 | 594 | Client: Encrypted packet (len=528) |
| 104 | 33.158766211 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 45344 [ACK] Seq=3798 Ack=3746 Win=73856 Len=0 TSval=3059565727 TSecr=0 |
| 105 | 33.162456398 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 174 | Server: Encrypted packet (len=108) |
| 106 | 33.163798712 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 1126 | Server: Encrypted packet (len=1060) |
| 107 | 33.163872391 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 45344 → 22 [ACK] Seq=3746 Ack=4966 Win=69120 Len=0 TSval=409666322 TSecr=0 |
| 109 | 33.245624277 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 198 | Server: Encrypted packet (len=132) |
| 110 | 33.289180155 | 1.1.1.3 | 1.1.1.3 | TCP | 66 | 45344 → 22 [ACK] Seq=3746 Ack=5098 Win=84992 Len=0 TSval=409348109 TSecr=0 |

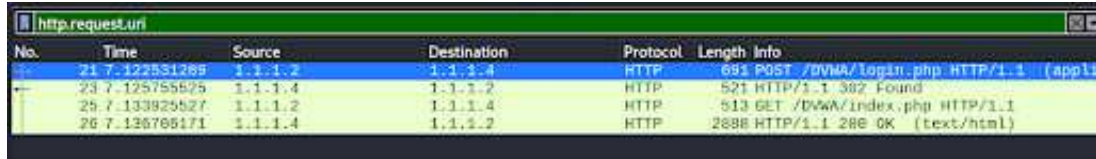
비정상 패킷

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|---------|-------------|----------|--------|--|
| 277 | 202.120563558 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40838 → 22 [FIN, ACK] Seq=1244 Ack=1826 Win=69120 Len=0 TSval=40966579 TSecr=0 |
| 278 | 202.162207951 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 40838 [ACK] Seq=1826 Ack=1245 Win=64256 Len=0 TSval=3050883593 TSecr=0 |
| 279 | 202.647485888 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 40838 [FIN, ACK] Seq=1826 Ack=1245 Win=64256 Len=0 TSval=3050883593 TSecr=0 |
| 280 | 202.647560069 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40838 → 22 [ACK] Seq=1245 Ack=1827 Win=69120 Len=0 TSval=409666322 TSecr=0 |
| 281 | 203.807318973 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 118 | Server: Encrypted packet (len=52) |
| 282 | 203.812145936 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40796 → 22 [FIN, ACK] Seq=1252 Ack=1850 Win=69120 Len=0 TSval=40966748 TSecr=0 |
| 283 | 203.815263770 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 40796 [FIN, ACK] Seq=1850 Ack=1253 Win=64256 Len=0 TSval=30508852 TSecr=0 |
| 284 | 203.815300991 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40796 → 22 [ACK] Seq=1253 Ack=1851 Win=69120 Len=0 TSval=409667490 TSecr=0 |
| 285 | 203.834657019 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 118 | Server: Encrypted packet (len=52) |
| 286 | 203.837529583 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40812 → 22 [FIN, ACK] Seq=1244 Ack=1850 Win=69120 Len=0 TSval=40966751 TSecr=0 |
| 287 | 203.841436372 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 40812 [FIN, ACK] Seq=1850 Ack=1245 Win=64256 Len=0 TSval=30508852 TSecr=0 |
| 288 | 203.841486397 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40812 → 22 [ACK] Seq=1245 Ack=1851 Win=69120 Len=0 TSval=409667516 TSecr=0 |
| 289 | 203.854209695 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 118 | Server: Encrypted packet (len=52) |
| 290 | 203.856389991 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40848 → 22 [FIN, ACK] Seq=1244 Ack=1850 Win=69120 Len=0 TSval=40966753 TSecr=0 |
| 291 | 203.859518367 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 40848 [FIN, ACK] Seq=1850 Ack=1245 Win=64256 Len=0 TSval=30508852 TSecr=0 |
| 292 | 203.859558659 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40848 → 22 [ACK] Seq=1245 Ack=1851 Win=69120 Len=0 TSval=409667534 TSecr=0 |
| 293 | 203.864629727 | 1.1.1.3 | 1.1.1.2 | SSHv2 | 118 | Server: Encrypted packet (len=52) |
| 294 | 203.868341617 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40822 → 22 [FIN, ACK] Seq=1244 Ack=1850 Win=69120 Len=0 TSval=40966754 TSecr=0 |
| 295 | 203.872225537 | 1.1.1.3 | 1.1.1.2 | TCP | 66 | 22 → 40822 [FIN, ACK] Seq=1850 Ack=1245 Win=64256 Len=0 TSval=30508853 TSecr=0 |
| 296 | 203.872759552 | 1.1.1.2 | 1.1.1.3 | TCP | 66 | 40822 → 22 [ACK] Seq=1245 Ack=1851 Win=69120 Len=0 TSval=409667547 TSecr=0 |

| 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



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------|-------------|----------|--------|--------------------------------------|
| 21 | 7.122531269 | 1.1.1.2 | 1.1.1.4 | HTTP | 691 | POST /DVWA/login.php HTTP/1.1 (appli |
| 23 | 7.125755575 | 1.1.1.4 | 1.1.1.2 | HTTP | 521 | HTTP/1.1 302 Found |
| 25 | 7.133825527 | 1.1.1.2 | 1.1.1.4 | HTTP | 513 | GET /DVWA/index.php HTTP/1.1 |
| 26 | 7.136705171 | 1.1.1.4 | 1.1.1.2 | HTTP | 2888 | HTTP/1.1 200 OK (text/html) |

비정상 패킷



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------|-------------|----------|--------|---|
| 25 | 1.735779920 | 1.1.1.2 | 1.1.1.4 | HTTP | 525 | GET /vulnerabilities/sqli/ HTTP/1.1 |
| 27 | 1.737934371 | 1.1.1.4 | 1.1.1.2 | HTTP | 1855 | HTTP/1.1 200 OK (text/html) |
| 41 | 11.420784029 | 1.1.1.2 | 1.1.1.4 | HTTP | 577 | GET /vulnerabilities/sqli/?id=1%27+or+%271%27%3D%271&Submit=Submit HTTP/1.1 |
| 43 | 11.423674180 | 1.1.1.4 | 1.1.1.2 | HTTP | 1935 | HTTP/1.1 200 OK (text/html) |

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 | | | |
| | | | |