패킷 추적 파일을 통한 네트워크 이벤트 분석

작성자: 유주현

1. challenge.pcapng 분석 결과

A. 송신지 주소: 192.168.1.108

B. 수신지 주소: 50.19.229.205

2. 질의 요구사항 답변

A. 이 추적파일에는 얼마나 많은 패킷이 있는가?

: 총 20개의 패킷이 존재함.

B. IP 호스트는 무엇으로 프레임 1, 2, 3 안에서 TCP 연결을 만드는가?

: 프레임 1에서 SYN, 프레임 2에서 SYN, ACK, 프레임 3에서 ACK를 통해 3 Way Handshake 연결 수립함.

C. 프레임 4로 보낸 HTTP 명령어는 무엇인가?

: HTTP GET 요청함.

- 요청 URL: GET /Tracking/V3/Instream/Impression/?start|2873|72147| HTTP/1.1
- 호스트: trk.vindicosuite.com

D. 이 추적 파일 안에서 가장 긴 프레임의 길이는 얼마인가?

: 프레임 9의 1428bytes으로 확인할 수 있음.

E. 어떤 프로토콜이 Protocol 열에 보이는가?

: TCP, HTTP 프로토콜이 확인됨.

F. HTTP 서버가 보낸 응답은 무엇인가?

: 프레임 6에서 최초로 302 Found 상태 코드를 전달하였음. 이는 클라이언트를 다른 위치로 리다이렉트 하라는 의미로 보여짐.

G. 이 추적 파일 안에 IPv6 트래픽이 있는가?

IP Header 부분을 참고하였으나 IPv6 트래픽은 존재하지 않는 것을 확인함.

3. 분석 흐름 요약

A. 192.168.1.108 → 50.19.229.205: TCP SYN

B. 50.19.229.205 → 192.168.1.108: SYN-ACK

C. 192.168.1.108 → 50.19.229.205: ACK → 연결 성립

D. 클라이언트 → HTTP GET 요청

E. 서버 → HTTP 302 응답으로 리다이렉션 요청

F. 이후 연결 종료 (Window size = 0)