level02

태그	Packet Pcap
상태	완료

풀이과정

겪었던 어려움

인트라 영상에서 제공되는 정보 중 하나인 `cloudshark.org`에 접속을 하면 다른 도메인으로 리다이렉트 되는 이슈가 있었다.

그리고 level01과 같이 라이브러리 및 패키지 설치가 안되기 때문에 `tshark`, `wireshark` 를 어떻게 사용해야하는지 어려움을 겪었다.

그래서 최대한 tcpdump를 이용하는 방법을 사용했다.

풀이과정

pcap

packet capture의 줄인말로 네트워크 트래픽을 분석하는데 사용되는 파일 형식이다.

packet payload

각 패킷은 페이로드를 가지고 있는데, 거기서 데이터 정보는 가장 마지막 문자가 가지고 있다. 해당 문제는 포트번호 39247 과 12121이 통신을 한 내용이 level02.pcap에 담겨있는데 `tcpdump -X -r level02.pcap` 명령어로 확인해봤을 때 `password:` 라는 문자열을 기준으로 아래의 정보를 하나씩 확인해보면 된다.

ascii

분석 했을 때 문자열은 `‘ft_wandrNDRelL0L’` 하지만 이게 정답이 아니라 패킷 데이터의 `7f`, 이걸 10진수로 표현하면 `127` 인데 이건 아스키 숫자 상 DEL을 나타내는 거라 127이 나올 때 마다 지워줘야 한다. 위 문자열에서 DEL까지 포함하면 `‘ft_wandr'127''127''127'NDRel'127'L0L’` 이다 127이 나올 때 마다 누적된 문자열을 지운다면 결과적으로 최종 문자열은 `‘ft_waNDReL0L’`이다.

정답

```
Don't forget to launch getflag !
flag02@SnowCrash:~$ getflag
Check flag.Here is your token : kooda2puivaav1idi4f57q8iq
flag02@SnowCrash:~$
```

`'kooda2puivaav1idi4f57q8iq'`

출처

https://ko.wikipedia.org/wiki/Pcap

Pcap 파싱하기

1. Pcap 파일이란 무엇인가? -Packet capture의 약자로 네트워크 트래픽을 캡쳐하기 위한 API로 구성되어 있습니다. 윈도우 시스템에서는 Winpcap이며, 리눅스 시스템에서는 libpcap입니다. 네트워크 트래픽을 분석하기에 아주 용이한 라이브러리의 모음이라고 볼 수 있습니다. -Pcap file

https://dragon82.tistory.com/10

tcpdump - packet capture / 분석

tcpdump - dump traffic on a network http://www.tcpdump.org/ tcpdump 는 네트워크 인터페이스상의 패킷 헤더를 출력한다. 그리고 파일로 출력하여 분석해 볼수도 있다. 파일로 출력할 경우에는 -w 옵션을 사용하며 저장된 파일내용을 볼때는 -r 옵션을 사용한다. tcpdump 는 패킷을

https://logwatch.tistory.com/entry/tcpdump-packet-capture-분석