활동보고서

※본인의 취향에 맞게 자유롭게 작성 가능. 문서화가 될 수 있다는 점에 유의. 제출 후 수정 불가.※

스터디 팀명, 주제	3팀 / 와이어샤크	작성자(기수, 학적, 이름)	2기, 사이버18, 장보민
스터디 날짜	2020.03.14	튜터링 학기	2020-1

[3장] 트래픽 캡처

1) 네트워크를 살펴보는 위치

1-1) 라우터에 연결된 네트워크 분석

- 라우터는 IP 주소 같이 네트워크 주소에 기반을 둔 트래픽을 분리함. 라우터의 한 족에 와이어샤크를 배치하면 네트워크로부터 송수신되는 트래픽을 볼 수 있음.
- 네트워크 10.1.0.0과 네트워크 10.2.0.0 가 있다 치면, 10.1.0.0 상의 클라이언트와 서버 간의 트래픽은 네트워크 10.2.0.0에 있는 와이어샤크 #2에는 보이지 않을 것이다.
- 와이어샤크 #1는 라우터 A에 연결된 포트를 수신하려고 포트 스패닝으로 구성되어 있다. 이에 따라 와이어샤크 #1이 클라이언트 A,B,C에서 송수신되는 트래픽에서 수신할 수 있다.

1-2) 무선 네트워크 분석

- WLAN 환경을 분석할 때는 프로토콜 스택을 밑에서 시작해 위로 이동한다. WLAN 환경에서 '밑에서부터'라는 말은 라디오 주파수(RF) 신호의 강도를 분석하고 간섭을 찾는 것을 의미.
- 와이어샤크는 모듈화되지 않은 RF 에너지나 간섭을 식별할 수 없기 때문에 스펙트럼 분석기를 사용. Metageek는 우수한 WLAN 스펙트럼 분석기 어댑터와 소프트웨어를 제공함. 무선 네트워크에서 와이어샤크의 위치는 유선 네트워크에서의 위치와 유사.

2) 원격으로 트래픽 캡처

- 로컬에서 프래픽을 분석하지 않고 원격지에서 트래픽 캡처를 원하는 경우. 일부 스위치는 rspan이라는 원격 스패팅 기능을 제공함.
- 원격지 캡처에 대한 간단한 옵션 중 하나는 대상에서 와이어샤크를 실행시켜 소프트웨어를 원격으로 제어하는 것. 또한 WinPcap이 포함돼 있는 원격 캡처 기능을 사용할 수 있음. WinPcap은 rpcapd와 로컬 와이어샤크 호스로 패킷을 캡처해 전송하는 원격 호스트에서 실행 가능한 원격 캡처 데몬을 포함함. rscapd 파일은 WinPcap이 설치되는 동안 winpcap 디렉터리에 복사됨.

2-1) rspcapd에 대한 파라미터 환경 설정

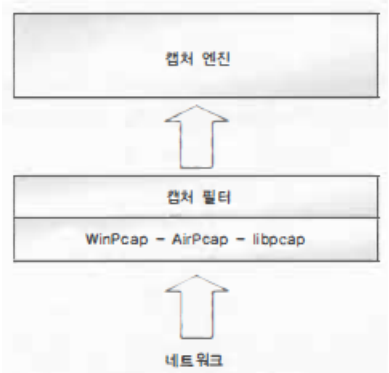
- 다음은 패킷 캡처에 대한 원격 호스트 설정에 사용되는 rpcapd의 파라미터 목록임.

파라미터	설명
-b <address>	바인딩할 주소다(숫자나 문자). 기본 값: 모든 로컬 IPv4 주소를 바인딩한다.
-p <port>	바인딩할 포트다. 기본 값: 2002번 포트를 바인딩한다.
-4	오직 IPv4만 사용(IPv4와 IPv6 대기 소켓 모두 사용한다).
-l <host_list>	이 서버로 연결이 허용되는 호스트의 목록이 있는 파일(서버가 하나 이상이라면 라인마다 하나의 서버를 나열하라). 다른 주소군과의 문제를 피하기 위해 문자 이름(숫자 이름 대신) 사용을 권장한다.
-n	NULL 인증을 허가(일반적으로 -l과 같이 사용)

파라미터	설명
-a <host,port>	포트에 호스트로 연결될 때 활성화 모드에서 실행한다. 포트가 지정되지 않으면 기본 포트(2003)를 사용한다.
-v	오직 활성화 모드에서만 실행한다(기본 값: -a가 지정되면 수동 연결도 쉽게 허용된다).
-d	데몬 모드(UNIX에서만)에서 혹은 서비스(Win32 에서만)로 실행된다. 경고(Win32): 제어판에서 서비스가 시작할 때 이 스위치가 자동으로 제공된다.
-s <file>	그림 70과 같이 현재 환경 설정을 파일에 저장한다.
-r <file>	파일에서 현재 환경 설정을 불러온다. 커맨드라인에서 지정된 모든 스위치는 무시된다.
-h	hpcapd의 도움말 화면 보기

-l 파라미너틀 '허용된'와이어샤크 호스트의 목록을 볼 수 있게 함. 호스트 파일이 원격 캡처에 대한 연결을 시도하는 호스트로부터의 정보를 포함하지 않는 경우 오류 응답을 받게 될 것.

[4장] 캡처 필터 생성과 적용
- 캡처 필터는 추적 파일을 저앟라 때 패킷을 캡처하는 동안 \ temp나 다른 디렉터리에 저장되지 않게 제한함. 기존 추적 파일에는 적용할 수 없음. 이것은 실시간으로 캡처하는 작업에서만 적용됨. 캡처 필터는 동작 중인 네트워크나 특정 유형의 트래픽에 초점을 맞춰 캡처하는 패킷을 제한하는 데 매우 유용함. 캡처 필터 조건을 통과한 패킷은 아래 그림과 같이 와이어샤크 캡처 엔진에 전달됨.



캡처 필터는 tcpdump와 동일한 필터 구문을 사용.
저장된 캡처 필터를 보려면 Capture>Capture Filters 를 선택하거나, Capture Filters 아이콘을 클릭

와이어샤크의 기본 캡처 필터는 다음과 같음.

캡처 필터 이름	캡처 필터 구문
Ethernet address 00:08:15:00:08:15	ether host 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IP only	ip
IP address 192.168.0.1	host 192.168.0.1
IPX only	ipx
TCP only	tcp
UDP only	udp
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

와이어샤크는 와이어샤크 프로그램 파일 디렉터리에 보관돼 있는 기본 캡처 필터의 집합을 가짐. 캡처 필터 파일 이름은 cfilters. 시스템에는 여러 cfilters 파일이 있을 수 있음. 프로파일을 사용하면서 새로운 캡처 필터를 만들 때 cfilters 파일이 프로파일 디렉터리에 생성됨.

1) 하나의 애플리케이션 트래픽만 캡처
- 애플리케이션 필터링은 애플리케이션이 사용하는 포트 번호에 대해 기본식을 사용해 수행됨. 일단 애플리케이션이 사용하는 포트 번호를 알면 UDP나 TCP를 통한 애플리케이션 트래픽을 검색하기 위한 캡처 필터를 만들 수 있으므로, 하나의 전송 유형에 중점을 둘 수 있거나 단방향으로 흐르는 트래픽을 캡처할 수 잇음.
ex) DNS 쿼리,응답은 일반적으로 포트 53에 UDP를 통해 전송된다. 그러나 DNS zone 전송은 포트 53에 TCP를 통해 이뤄짐.

- 캡처 필터는 캡처되는 패킷의 수를 줄여 관심 대상이 되는 트래픽에 좀 더 세밀하게 집중하기 위해 사용함. 캡처 필터는 tcpdump 구문을 사용하며, 디스플레이 필터와 상호 대체가 되지 않음. 기존 추적 파일에 캡처 필터를 적용할 수 없으며, 이미 적용된 캡처 필터와 일치하지 않는 패킷을 복구할 수 없음.
캡처 필터는 cfiles 파일에 저장되는데, 기본 cfilters 파일은 글로벌 환경 설정 디렉터리에 위치해 있다. 기본 캡처 파일을 추가하거나 변경시킨다면 다른 cfilters 파일은 개이 환경 설정 폴더에 위치할 것임.
캡처 필터는 프로토콜, 주소, 특정한 포트 번호 등을 기반으로 생성될 수 있음.

참고자료