

ARP 모니터 과제

제출 기한: 12월 19일 밤 11시 59분

프로그래밍 언어: C, C++

제출 파일: 주석(영문)이 잘 달린 소스 코드, 윈도우에서 실행 가능한 바이너리

제출 방법: xeraph@nchovy.com 메일 전송

(바이너리 포함 시 자동 필터링 되므로 압축 후 확장자에 .rename을 붙여서 보내기 바랍니다.)

과제 내용:

WinPcap을 이용하여 ARP 패킷을 수집하면서 그 내용을 화면에 출력하고, IP와 연관된 MAC 주소가 바뀌는 경우 SNMP Trap v1 포맷의 로그를 전송합니다. <http://www.winpcap.org>에서 WinPcap 튜토리얼 문서를 참고하시기 바랍니다.

1. 프로그램이 시작되면 Trap을 전송할 IP 주소와 포트를 각각 입력 받습니다.
2. 전체 네트워크 인터페이스 목록을 번호와 이름으로 출력하고, 번호를 입력 받아 해당 네트워크 인터페이스로부터 패킷 수집을 시작합니다.
3. ARP 패킷을 분석해서 (pcap_compile 호출 시 필터링 옵션을 걸어서 ARP만 받아도 상관 없음) 아래와 같이 데이터를 출력합니다.

```
Destination: ff:ff:ff:ff:ff:ff
Source: 00:15:17:9f:bc:76
Opcode: Request (혹은 Reply)
Is gratuitous: False (혹은 True)
Sender MAC address: 00:15:17:9f:bc:76
Sender IP address: 10.0.0.3
Target MAC address: 00:00:00:00:00:00
Target IP address: 10.0.0.20
```

4. Gratuitous ARP나 Reply의 경우 Sender MAC와 IP 항목을 캐시하고, 이후 들어오는 ARP와 대조하여 MAC이 변경된 경우 프로그램 시작할 때 받았던 주소로 아래 OID와 값을 담은 Trap 패킷을 전송합니다.

Enterprise: 1.3.6.1.4.1.33957

Generic-Trap: 6

Specific-Trap: 10

Variable Bindings:

1.3.6.1.4.1.33957.10.1 = IP 주소 (NetworkAddress 타입)

1.3.6.1.4.1.33957.10.2 = 변경 전 MAC 주소 (OctetString 타입, 00:11:22:33:44:55 포맷)

1.3.6.1.4.1.33957.10.3 = 변경 후 MAC 주소 (OctetString 타입, 00:11:22:33:44:55 포맷)

팁: 명령프롬프트에서 arp -d로 캐시를 삭제하고 접속을 시도하면 빨리 ARP 패킷을 다시 받을 수 있습니다. Wireshark를 사용해서 ARP 디코딩 결과 및 Trap 패킷을 교차 검증하시기 바랍니다.