웹해킹이란 무엇인가?

Web Hacking Tutorial

패킷 분석을 통해 GET 방식과 POST 방식을 구분하기

[BOSS] 손 우 규

https://github.com/swk3169/web-hacking

목차

1. 스니핑

1.1 정의

패킷 가로채기 또는 스니핑(snipping)은 네트워크 통신 내용을 도청하는 행위이다. 이때 사용되는 도구를 패킷 분석기(packet analyzer/network analyzer) 또는 패킷 스니퍼(packet sniffer/network sniffer)라고 하며, 네트워크의 일부나 디지털 네트워크를 통하는 트래픽의 내용을 저장하거나 가로채는 기능을 하는 소프트웨어 또는 하드웨어이다. 프로토콜 분석기라고도 불리며, 특정한 종류의 네트워크에서는 이더넷 스니퍼(ethernet sniffer) 또는 무선 스니퍼(wireless sniffer)라고 불린다. 데이터 스트림은 네트워크를 통해 흐르며, 스니퍼는 각 패킷을 잡아 내서 디코딩하여, 적절한 RFC나 다른 규격에 따라 내용을 분석한다.

1.2 위험성

- 스니핑은 해커 입문자도 스니퍼를 활용해 손쉽게 시도할 수 있다.
- 스니퍼는 해커 사이트에서 쉽게 다운로드할 수 있다. 해커 사이트를 몰라도 검색 사이트에서 '스니퍼'를 입력하면 리눅스, 유닉스, 윈도NT 등 각종 시스템용 스니퍼를 찾을 수 있다. 이더넷스파이, 파일워처 등이 대표적인 스니퍼. 해커들은 스니퍼를 이용하는 것을 치사한 3류 해킹이라고 치부하지만 그것만큼 쉬운 것도 없다고 표현한다.
- 스니핑은 감행하기는 쉬운 반면 대응하기는 아주 까다롭다. 흔적이 남지 않아 정보 유출 후에 사건이 발생하지 않는 이상 피해 사실조차 확인하기 어렵다. 스니핑을 탐지하는 도구들이 개발돼 있지만 이 도구로는 네트워크 상에 스니퍼가 설치돼 접속이 이뤄졌다는 것만 알아낼 수 있을 뿐 사용자 정보가 유출됐는지 여부를 확인할 수 없다.

1.3 공격법

- Switch Jamming

스위치의 MAC Address Table을 모두 채워서 스위치가 더미허브처럼 모든 프레임을 스위치의 모든 포트로 전송(브로드캐스트)하도록 만들어 스니핑이 가능한 환경을 만든다. 공격자는 MAC Address Table을 모두 채우기 위해 변조한 MAC 정보를 담고 있는 ARP Reply 패킷을 계속해서 스위치에게 전송한다.

- ARP Spoofing

공격자가 스니핑하고자 하는 희생자 호스트에게 호스트가 통신하는 상대방의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply 패킷을 희생자에게 지속적으로 보내면 희생자의 ARP Cache Table에 희생자가 통신하고자 하는 호스트의 MAC 주소가 공격자의 맥 주소로 변경되어 스니핑이 가능하다.

- ARP Redirect

공격자가 자신이 게이트웨이(라우터)인 것처럼 MAC주소를 위조한 ARP Reply 패킷을 브로드캐스트하여 네트워크에 연결된 모든 호스트의 MAC 어드레스 테이블의 게이트웨이 MAC 주소를 공격자의 MAC 주소로 변조하여 모든 통신을 스니핑을 하는 공격 기법이다.

- ICMP Redirect

앞의 공격은 모드 ARP 캐시테이블을 변조하는 공격이지만 ICMP 리다이렉트는 L3(네트워크 레이어)의 라우팅 테이블의 게이트웨이 주소를 변조하는 공격이다. 공격자는 라우터에서 호스트 또는 라우터간의 라우팅 경로를 재설정하는 ICMP 리다이렉트 메시지를 희생자에게 전송하여 희생자 호스트의 라우팅 테이블을 변조하여 스니핑을 가능하게 하는 공격기법이다.

- Switch의 SPAN/MONITOR 포트를 이용하는 방법

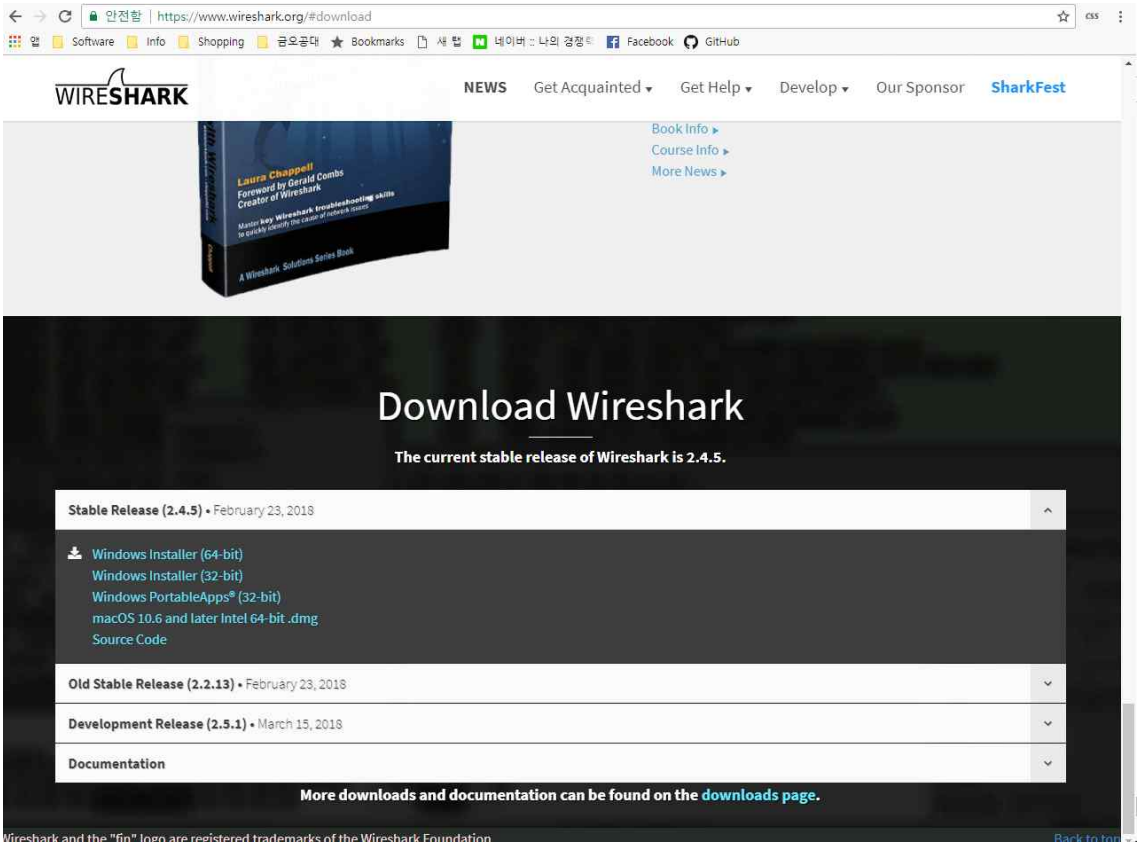
특별한 공격을 수행하지 않고 스위치의 포트미러링이 가능한 Monitor 포트에 노트북이나 컴퓨터를 접속하여 물리적으로 스니핑을 가능하게 하는 방법이다.

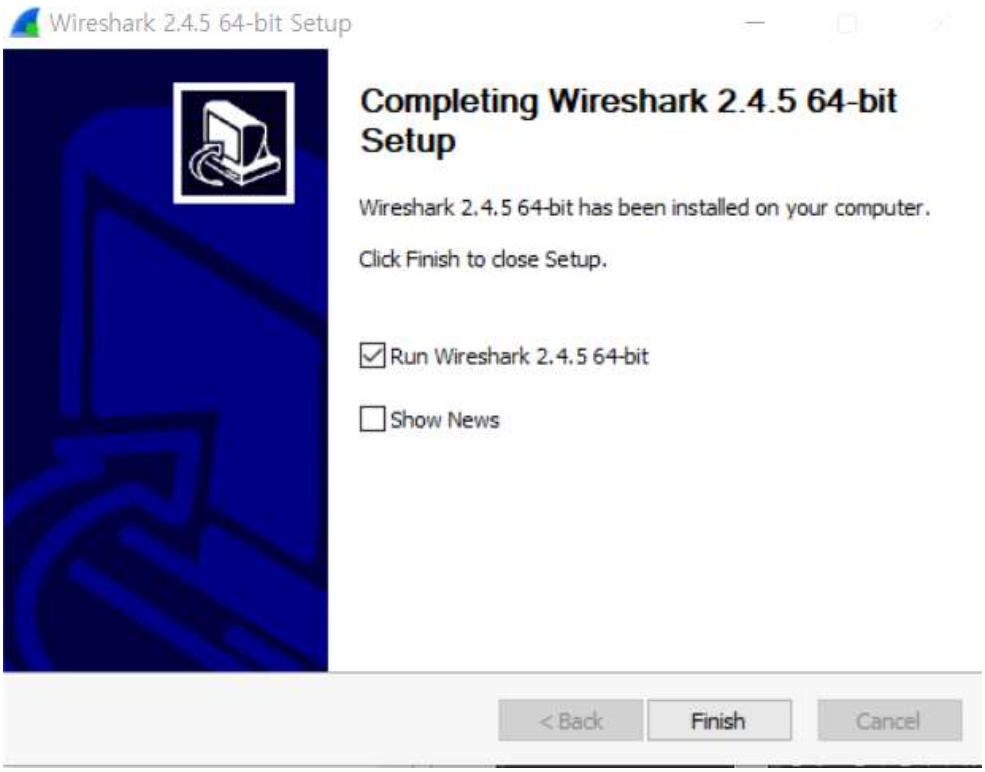
1.4 방어법

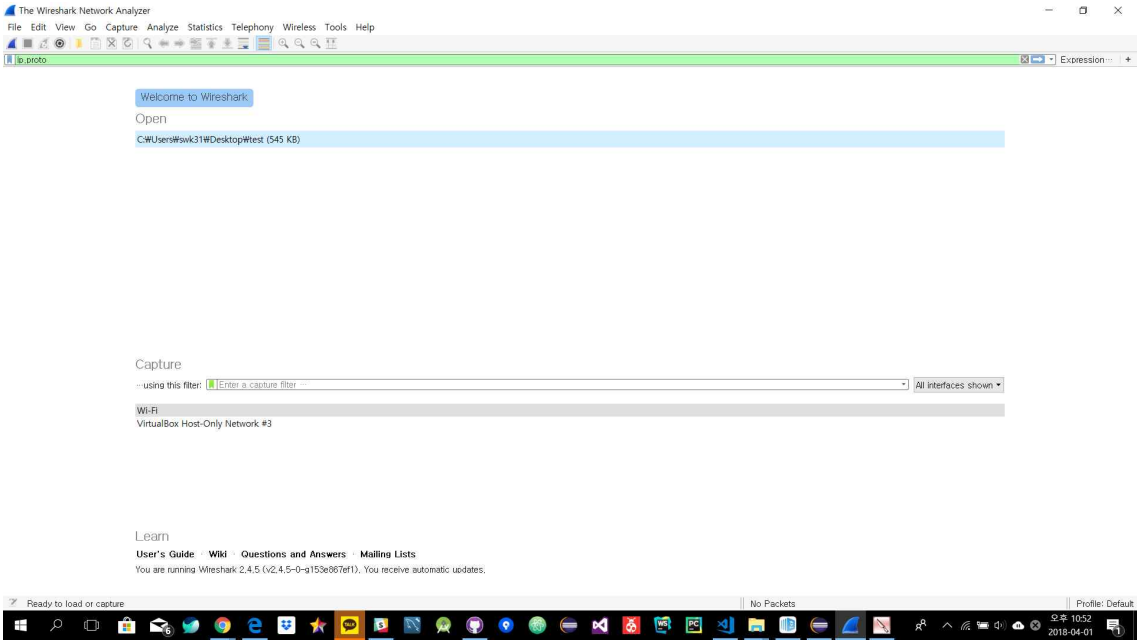
- 사전에 해킹을 막기위해 해킹방어 툴 등을 자신의 컴퓨터에 깔아야 한다
- 가급적 개인정보 유출을 요하는 무료사이트 등에 등록하지 않는 것이 정보 유출을 막는 길
- 근본적으로 차단하기 위해서는 웹 서버와 이용자간에 전송되는 모든 패킷을 암호화해야 한다.
- 패킷이 암호화된 상태에서는 패킷을 중간에서 가로채더라도 암호해독이 불가능하며 개인정보를 보호할 수 있다.

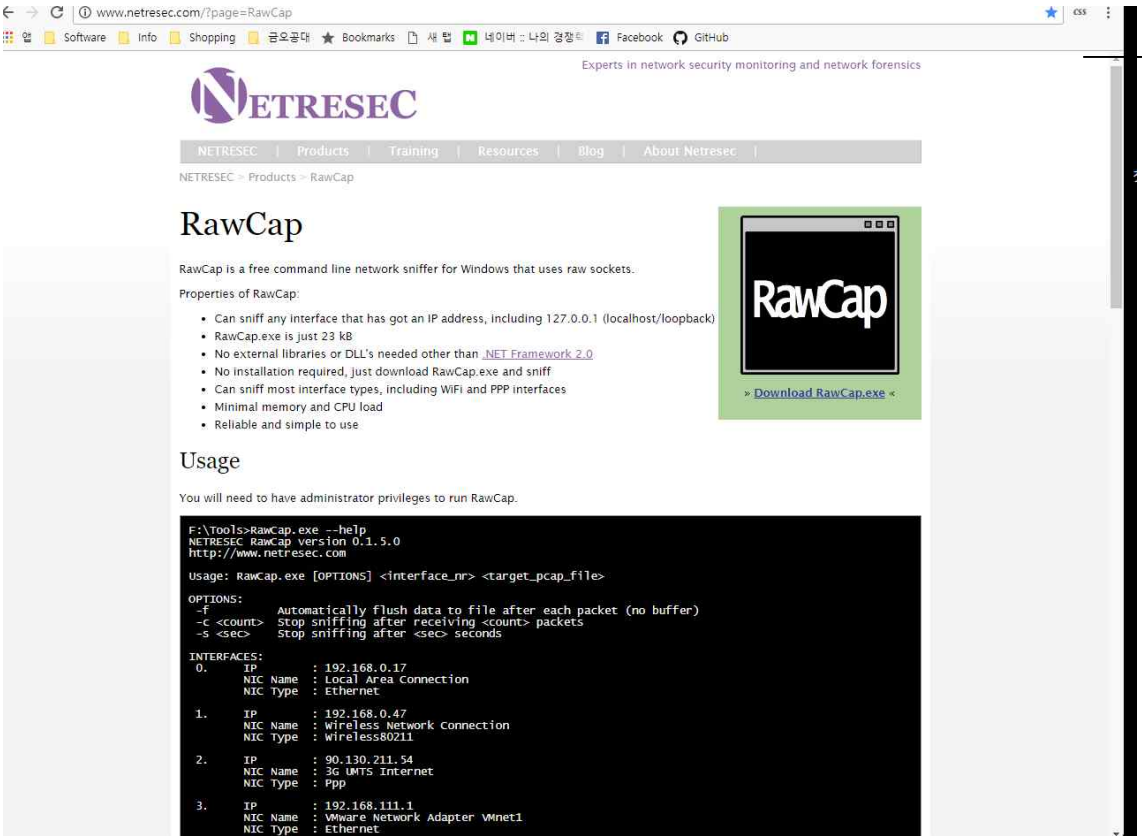
2. 실습

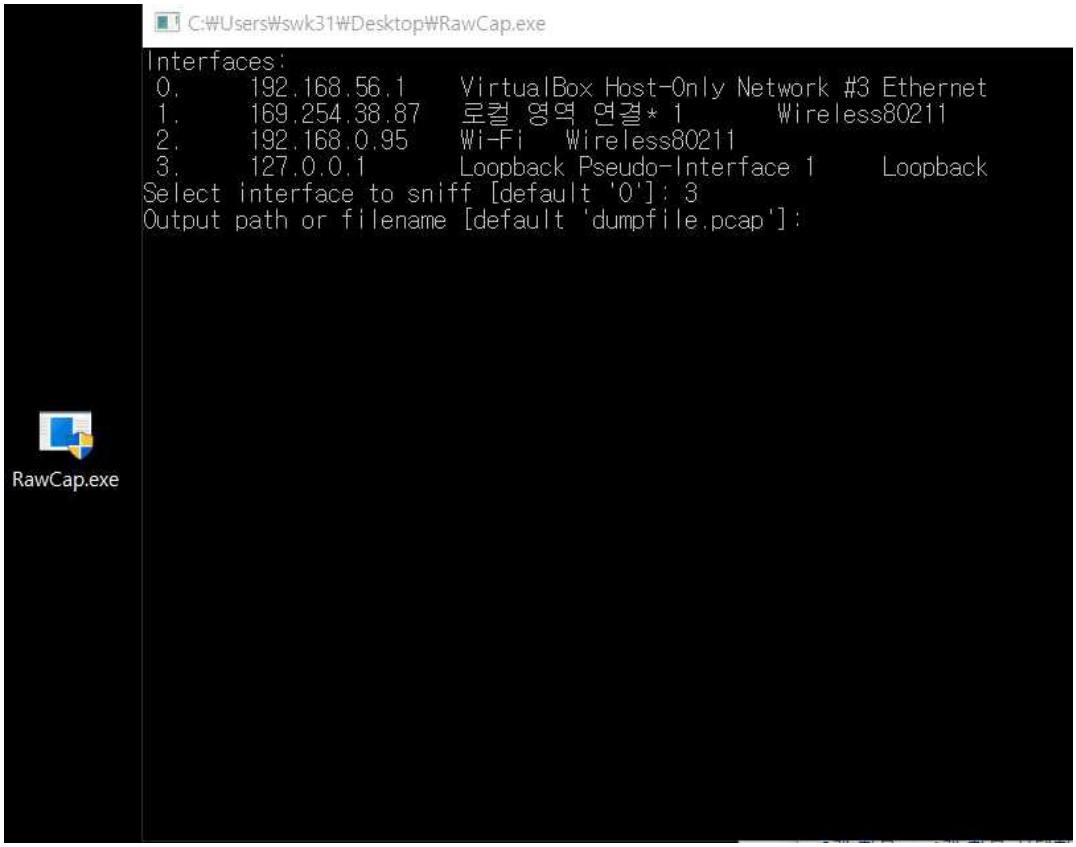
2.1 패킷 분석을 통해 GET 방식과 POST 방식을 구분하기

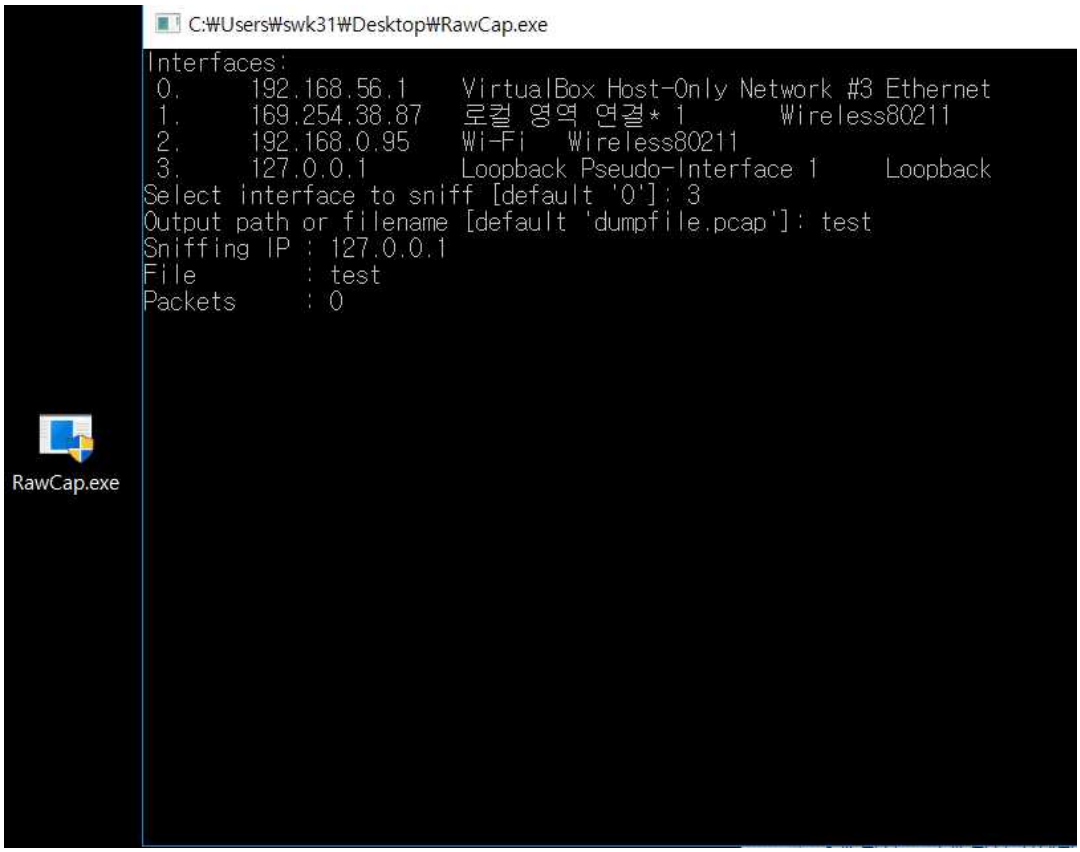


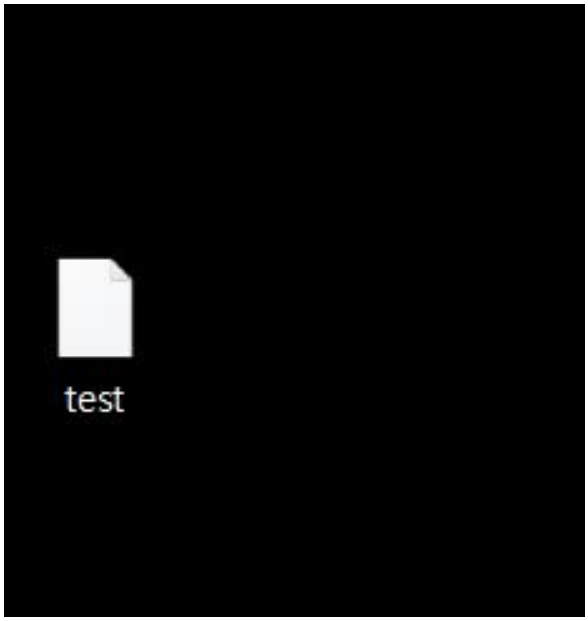



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.proto
Expression
Welcome to Wireshark
Open
C:₩Users₩swk31₩Desktop₩test (545 KB)
Capture
using this filter:
Enter a capture filter
All interfaces shown
Wi-Fi
VirtualBox Host-Only Network #3
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.5 (v2.4.5-0-g153e867ef1). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
오후 10:52
2018-04-01

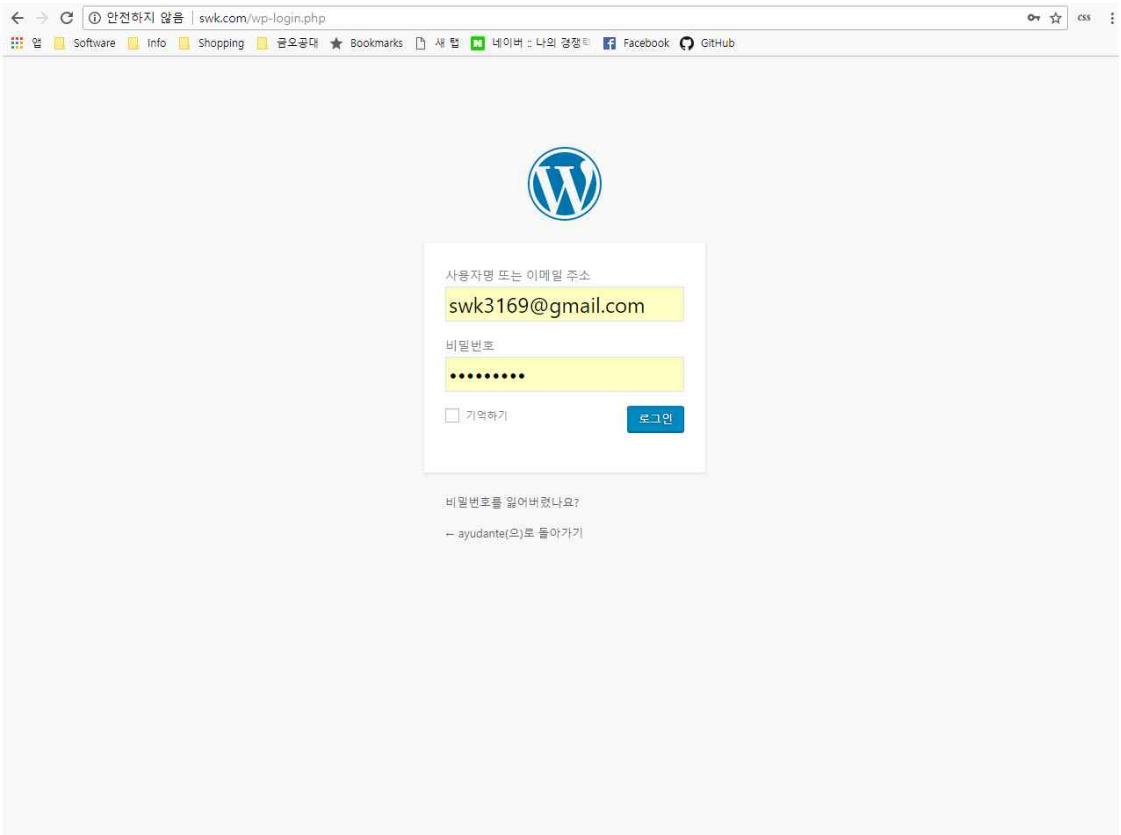

www.netresec.com/?page=RawCap
Software
Info
Shopping
Bookmarks
Facebook
GitHub
Experts in network security monitoring and network forensics
NETRESEC
NETRESEC | Products | Training | Resources | Blog | About Netresec
NETRESEC > Products > RawCap
RawCap
RawCap is a free command line network sniffer for Windows that uses raw sockets.
Properties of RawCap:
Can sniff any interface that has got an IP address, including 127.0.0.1 (localhost/loopback)
RawCap.exe is just 23 kB
No external libraries or DLL's needed other than .NET Framework 2.0
No installation required, just download RawCap.exe and sniff
Can sniff most interface types, including WiFi and PPP interfaces
Minimal memory and CPU load
Reliable and simple to use
» Download RawCap.exe «
Usage
You will need to have administrator privileges to run RawCap.
F:\Tools>RawCap.exe --help
NETRESEC RawCap version 0.1.5.0
http://www.netresec.com
Usage: RawCap.exe [OPTIONS] <interface_nr> <target_pcap_file>
OPTIONS:
-f Automatically flush data to file after each packet (no buffer)
-c <count> Stop sniffing after receiving <count> packets
-s <sec> Stop sniffing after <sec> seconds
INTERFACES:
0. IP : 192.168.0.17
NIC Name : Local Area Connection
NIC Type : Ethernet
1. IP : 192.168.0.47
NIC Name : Wireless Network Connection
NIC Type : Wireless80211
2. IP : 90.130.211.54
NIC Name : 3G UMTS Internet
NIC Type : Ppp
3. IP : 192.168.111.1
NIC Name : VMware Network Adapter VMnet1
NIC Type : Ethernet

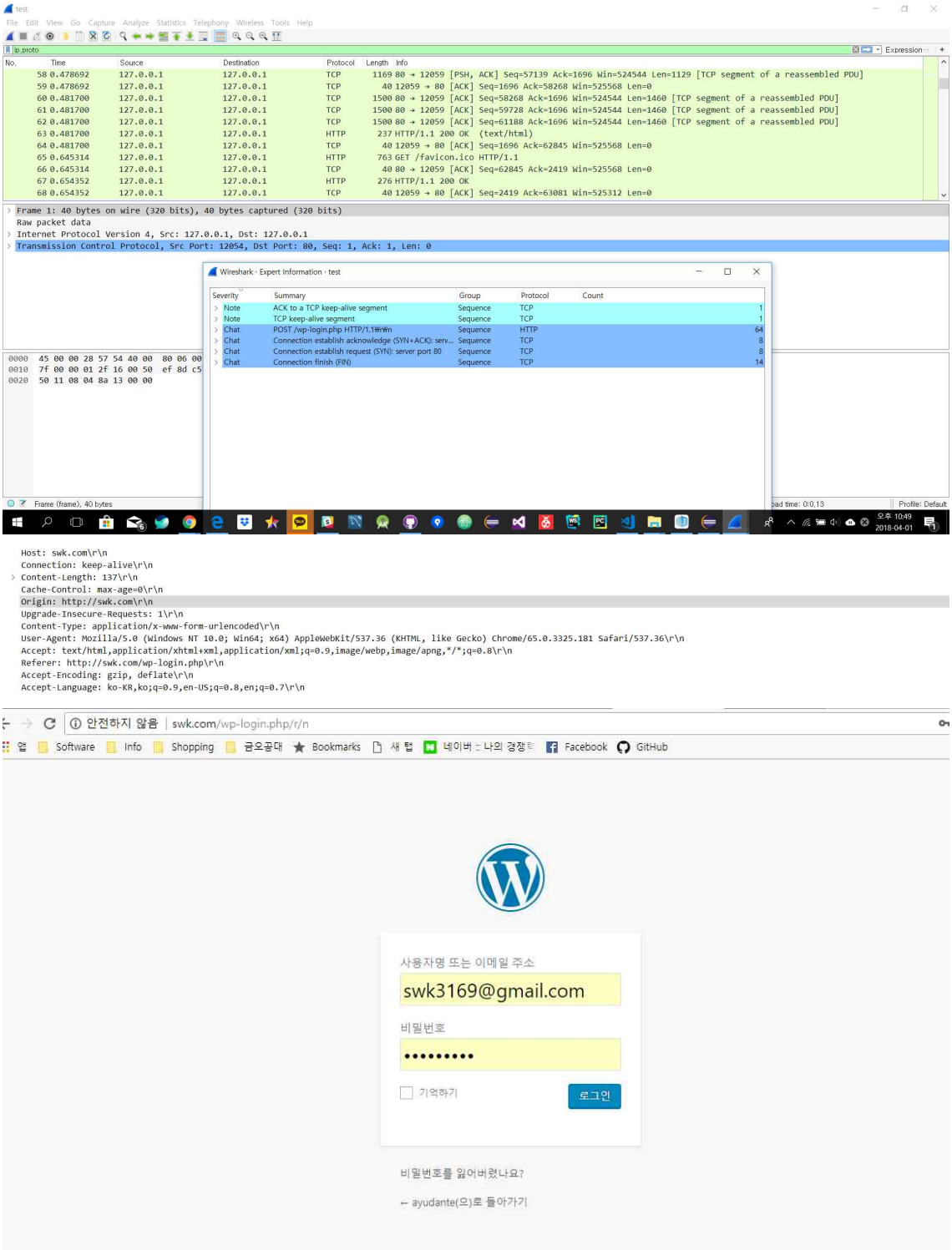

C:₩Users₩swk31₩Desktop₩RawCap.exe
Interfaces:
0. 192.168.56.1 VirtualBox Host-Only Network #3 Ethernet
1. 169.254.38.87 로컬 영역 연결* 1 Wireless80211
2. 192.168.0.95 Wi-Fi Wireless80211
3. 127.0.0.1 Loopback Pseudo-Interface 1 Loopback
Select interface to sniff [default '0']: 3
Output path or filename [default 'dumpfile.pcap']:
RawCap.exe


C:₩Users₩swk31₩Desktop₩RawCap.exe
Interfaces:
0. 192.168.56.1 VirtualBox Host-Only Network #3 Ethernet
1. 169.254.38.87 로컬 영역 연결* 1 Wireless80211
2. 192.168.0.95 Wi-Fi Wireless80211
3. 127.0.0.1 Loopback Pseudo-Interface 1 Loopback
Select interface to sniff [default '0']: 3
Output path or filename [default 'dumpfile.pcap']: test
Sniffing IP : 127.0.0.1
File : test
Packets : 0
RawCap.exe


test


swk.com/wp-admin/
앱
Software
Info
Shopping


안전하지 않음 | swk.com/wp-login.php
앱
Software
Info
Shopping
금오공대
Bookmarks
새 탭
네이버 : 나의 경쟁력
Facebook
GitHub
사용자명 또는 이메일 주소
swk3169@gmail.com
비밀번호
기억하기
로그인
비밀번호를 잃어버렸나요?
← ayudante(으)로 돌아가기



3. 참조

https://www.wireshark.org/

http://www.netresec.com/?page=RawCap