# NetScan
# Introduction

SWAP팀 팀장 최승환

- 2013.11.05 -

# 목 차





# : 프롤로그

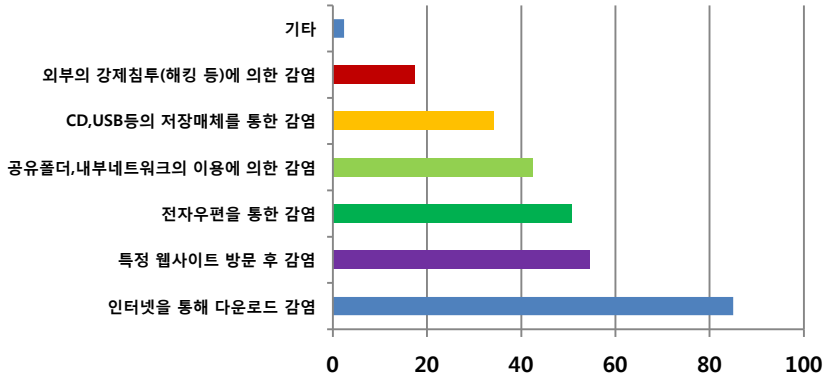
## 1. 보안관련 사고 사례

2. Hot보안 이슈 지능형 APT

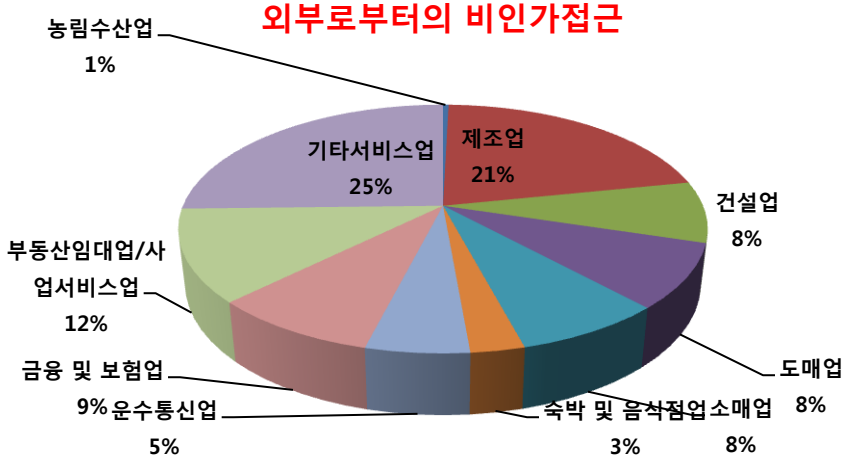
# 1.보안관련 사고사례

## ■ 통계청 자료 분석 보안관련 피해 경로

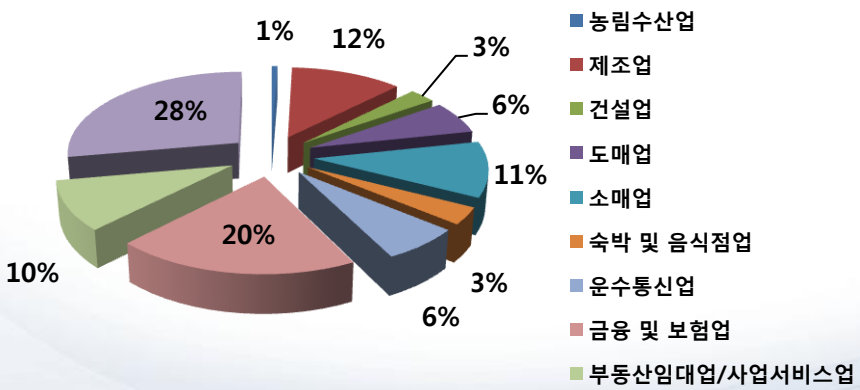
### 바이러스, 웜, 트로이잔 감염 피해 경로




### 사내 데이터나 전산 시스템에 대한 외부로부터의 비인가접근




### 개인정보 유/노출 사고 경험 여부




- 한국인터넷 진흥원 -

**- 보안관련 피해 정리**

- 웹을 이용한 감염 피해 대표적
- 제조/서비스/부동산/금융 대표적
- 개인정보 유출 도매/금융업 절반 이상

- IT업종이 아닌 보안의식이 미약한 업종에 피해 사례가 많다
- 개인 부주의에 대한 피해 증가

# 1.Hot 보안이슈 지능형 APT



- **Advanced Persistent Threat.**


## 지능형 지속 위협 APT란?

- 활동중이며,표적형 그리고 장기적인 작전임
- 특정 기간동안 탐지 되지않고, 지속적인 노력
- 성공률을 높이기 위한 다중 Kill chain을 포함
- 탐지를 우회하기 위한 기법을 사용함
- 고도화된 조직 기술 보유

## APT 공격 대응 방안

- 정보 중심의 보안 전략 구성 : 보호해야할 중요 정보가 어디에 저장돼 있고 해당 정보의 사용을 통제하는 정보보호 프로세스를 마련
- 기초 정보 수집 대응 : 지속적인 각종 보안 위협 징후에 대한 내/외부 모니터링 및 로그를 분석
- 악성코드 침투에 대한 대응 : 지속적인 탐지 및 모니터링을 통해 악성 활동을 차단
- 직원들의 보안 교육 강화 : 교육을 통해 정기적인 비밀 번호 변경 및 모바일 기기 보안의 중요성을 알림
- 엔드포인트 보안 : 최근에는 스마트워크 플랫폼이 확산됨에 따라 엔드포인트에 대한 보안은 취약
- 접근 권한 관리 : 퇴직자 또는 휴가자 등의 권한을 영구 또는 일시 소멸하여, 남용 되지 않도록 권한 관리를 철저
- 중요 정보 암호화 : 모든 중요한 정보를 암호화 하여 저장

# I. NETSCAN 개요

## 1. NetScan 이란?

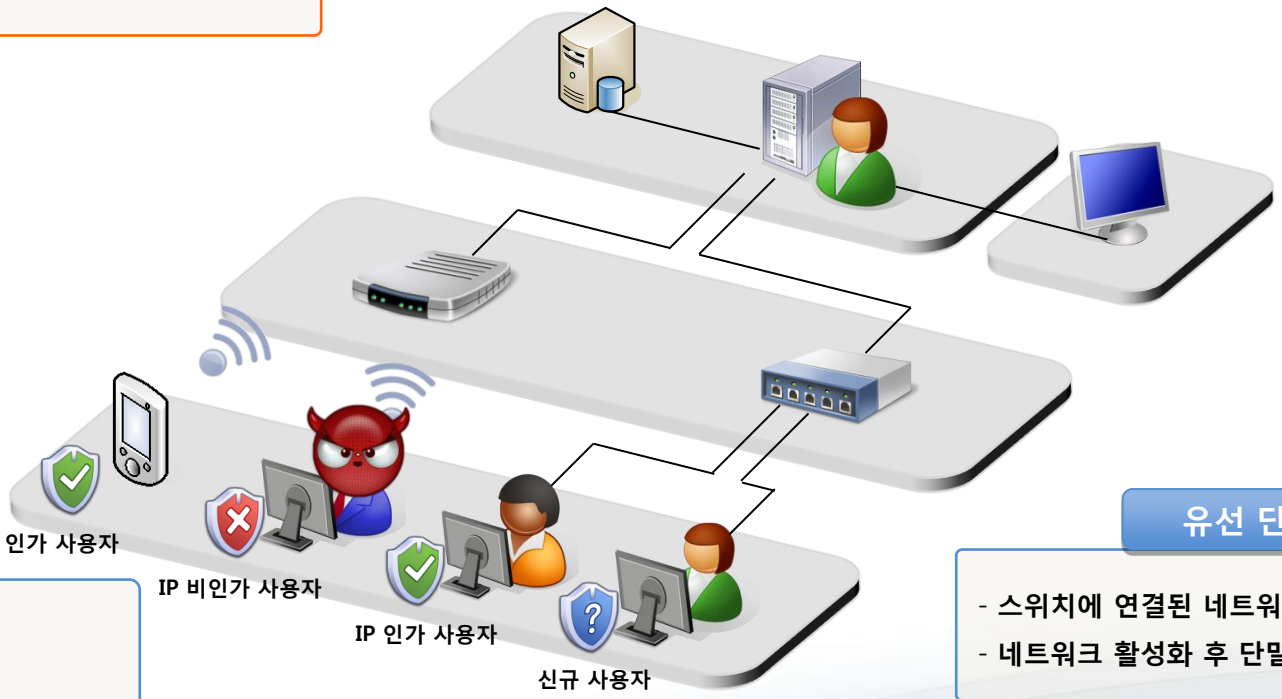
2. Selling Point
3. IP/MAC 관리파악 및 추적
4. OS 탐지
5. 실시간 IP/MAC/OS 변동관리

# 1.NetScan 이란?

## ■ 인가/비인가된 네트워크 탐색 및 분석

### 무선 단말 탐색

- 무선 공유기에 연결된 네트워크 탐색
- 해당 AP 접속 후 단말기 탐색




### IP/MAC/OS 수집

- IP Address IPV4 수집
- MAC 수집 및 제조사 판별
- Linux , Windows … OS 판별
- 활성화된 IP를 수집
- 빠른 수집 및 실시간 이벤트 로그

### 유선 단말 탐색

- 스위치에 연결된 네트워크 탐색
- 네트워크 활성화 후 단말기 탐색

# 2.Selling Point

- 누가 어떻게 사용할지 모르는 IP 실시간으로 스캔

1

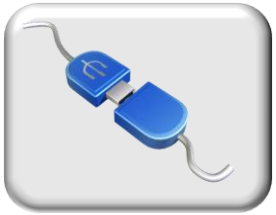
사용자 단말에 대한 IP 현황과 MAC 이제 **실시간 기록** 한다!

- 네트워크 현황을 실시간 이벤트 로그 및 리스트관리

2

IP 수집 및 사용시작 등 네트워크 **이벤트 로그** 한다!

- 단말기 활성화에 따른 IP사용시작 및 IP 수집 상태를 실시간 체크



3

OS Fingerprinting으로 각 IP에 대한 OS를 **판별** 한다!

- TCP Packet의 특성을 이용하여 OS를 분석

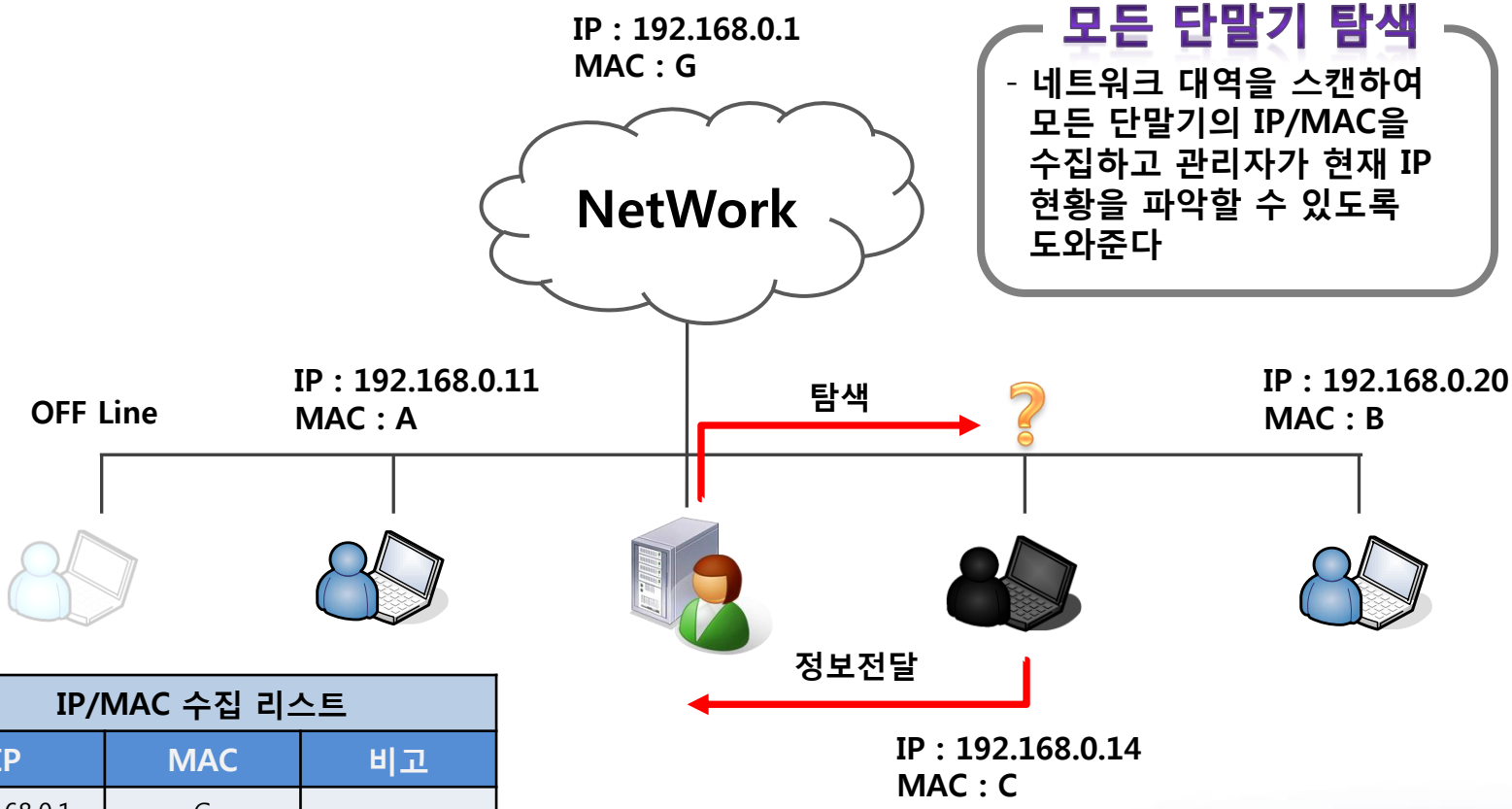
4

공유기 및 무선 네트워크에서도 IPV4라면 **네트워크 탐색** 한다!

- 유/무선 상관없이 IPV4에 연결된 곳에 실행시 네트워크를 바로 탐색 가능

# 3.IP/MAC 관리 파악 및 추적

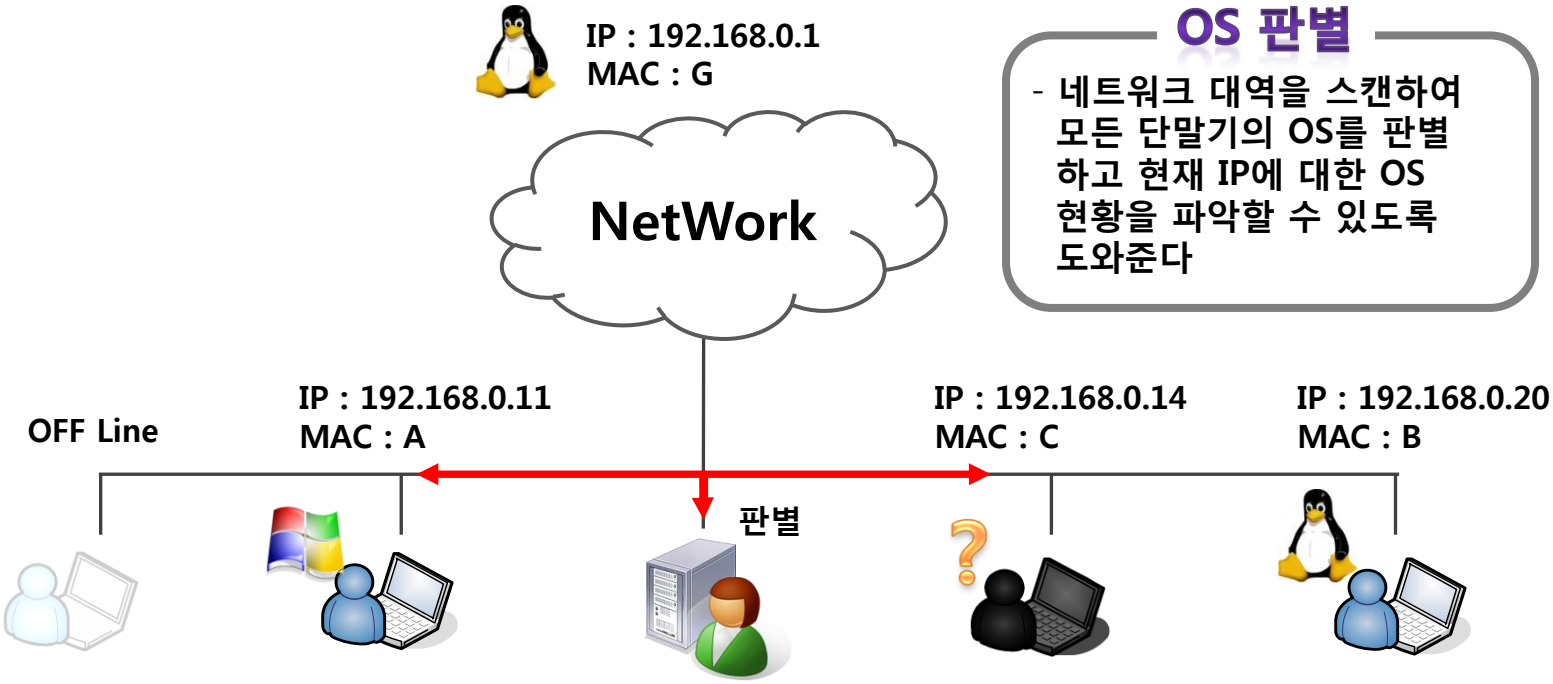
- 네트워크에 온라인된 단말기의 IP/MAC을 수집




| IP/MAC 수집 리스트 | | |
|---|---|---|
| IP | MAC | 비고 |
| 192.168.0.1 | G | |
| 192.168.0.11 | A | |
| 192.168.0.14 | C | |
| 192.168.0.20 | B | |

# 4.OS 탐지

- 네트워크에 온라인된 단말기의 OS를 판별




| OS 수집 리스트 | | |
|---|---|---|
| IP | MAC | OS |
| 192.168.0.1 | G | Linux |
| 192.168.0.11 | A | Windows 7 |
| 192.168.0.14 | C | Unknown |
| 192.168.0.20 | B | Linux |

# 5.실시간 IP/MAC/OS 변동 감지



- 연결된 네트워크에 대한 실시간 IP/MAC/OS 정보를 감지

### IP/MAC 실시간 탐지

- 현재 사용하는 IP/MAC 수집
- 새로운 단말기 IP/MAC 수집
- 변경된 IP에 대한 MAC 수집

➔ 네트워크에 대한 대역을 실시간으로 스캔한다

### OS 판별

- 사용하는 IP에 대한 OS 판별
- 패킷에 대한 OS 유형 분석
- Windows , Linux등 판별

➔ TCP 패킷을 이용한 OS를 대략적 판별

### 리스트 및 이벤트 로그

- IP/MAC/OS 리스트 출력
- 실시간 이벤트 로그 출력
- IP/MAC/OS 대한 검색/정렬

➔ 관리자가 한눈에 파악할 수 있는 UI 제공

**No Ping Yes NetScan!**

*단말기 정보 활용*
*IP/MAC/OS 종류 분석*

*Network TooL*
*연결만 되면 스캔 OK*

*리스트 활용한 검색*
*실시간 이벤트로그*

# II. NETSCAN 소개

## 1. NetScan 차별화

2. 네트워크 정보 수집
3. IP/MAC 정보 수집
4. OS 정보 수집
5. 실시간 이벤트 현황

# 1.NetScan의 차별화

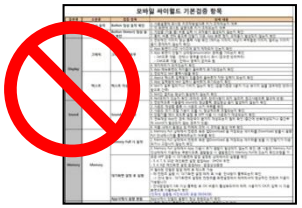
- 누구나 쉽게 사용할 수 있는 심플한 Tool

NetScan
원클릭으로 동작하는 네트워크 Tool

## 1 센서 장비가 필요 없음

➔ SW로 구현되어 별도의 장비 불 필요

## 2 별도의 설정 필요 없음

➔ 자동으로 네트워크 정보 및 대역 로드

## 3 원클릭 심플한 UI 및 조작


➔기능의 심플함 강조 , 쉬운 UI

## 4 One NetWork One Tool

*IP/MAC/MAC제조사/OS 분석*

- Packet을 이용한 분석
  - ARP , TCP등 패킷을 이용하여 정보를 습득
    수집 대상 호스트에서는 별도의 프로그램을 설치하지 않아도 위의 정보를 수집할 수 있다.

➔ 하나의 PC에서 모든 동작이 활성화

# 2.네트워크 정보 수집

## ■ 네트워크 카드 정보를 자동으로 수집

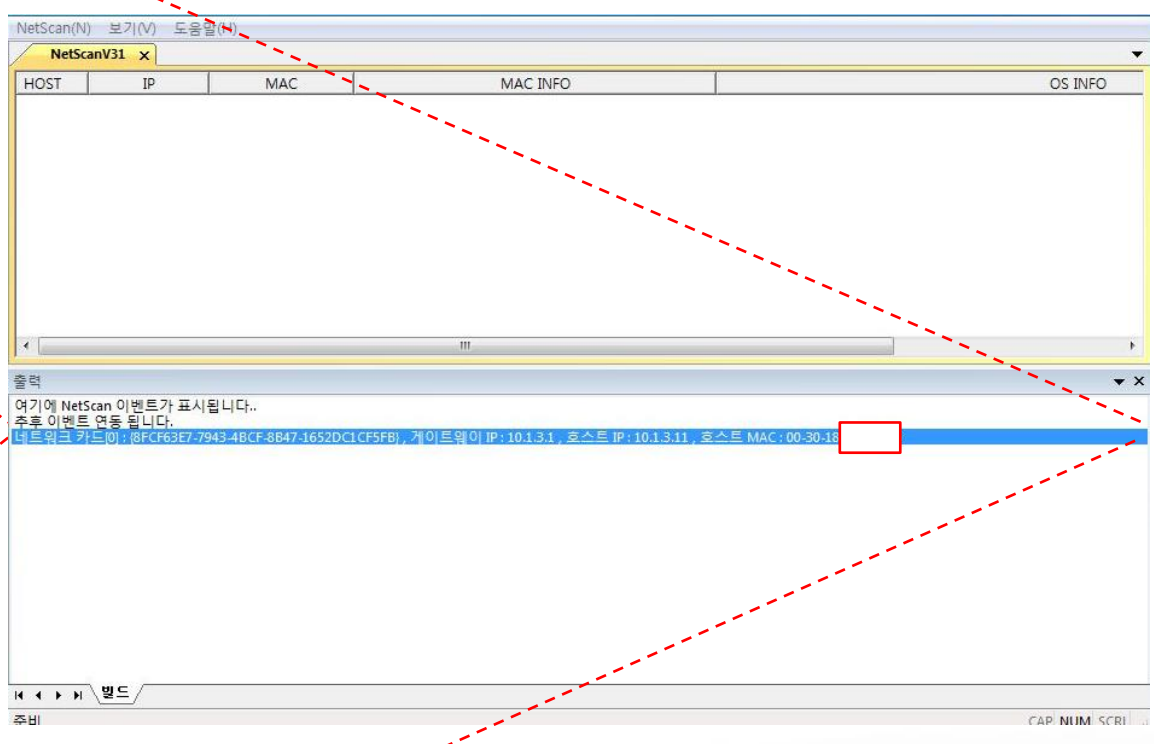
### NetWork Card Info

**• 활성화된 네트워크 카드별 정보를 가져온다**

- ✓ 네트워크 카드의 GUID정보를 수집하여 실제 패킷 분석할 디바이스를 활성화 시킨다
- ✓ DHCP가 아닌 고정 IP인 경우 초기 네트워크가 원활하게 활성화 된 상태여야 한다

**• 네트워크 세부 정보**

- ✓ 게이트 웨이 IP정보 수집
- ✓ 호스트 IP 정보 수집
- ✓ 호스트 MAC 정보 수집



# 3.IP/MAC 정보 수집

## ■ 네트워크에 활성화된 IP/MAC 정보를 수집

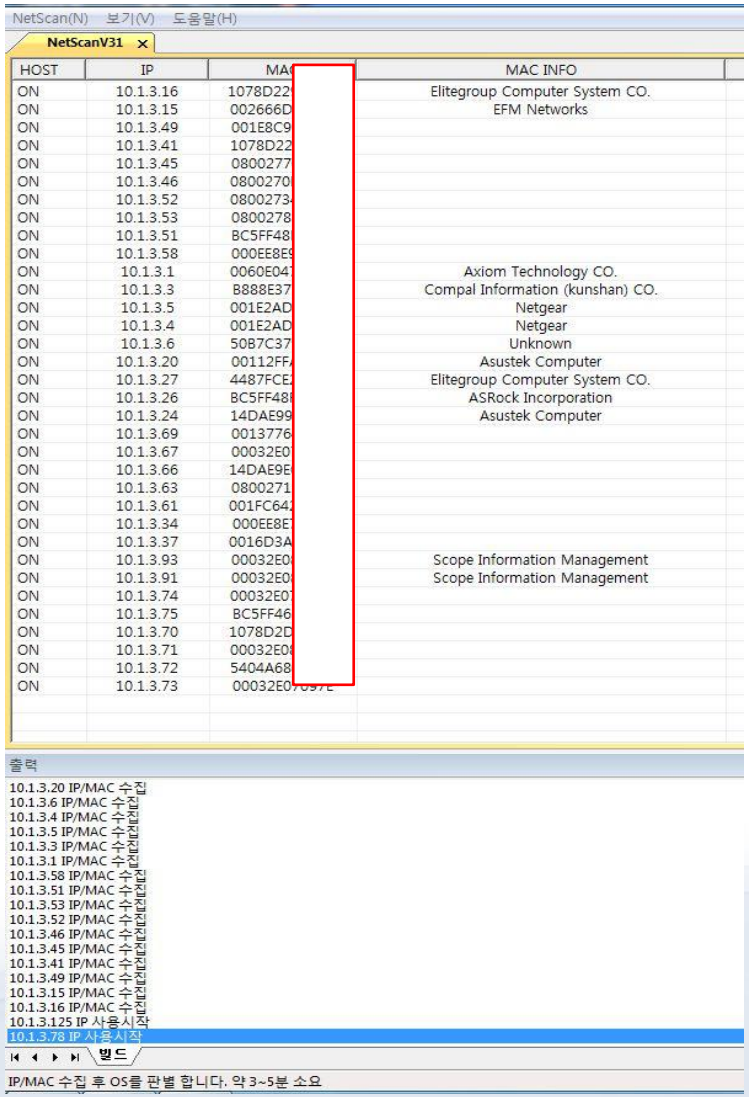
**NetWork IP/MAC Info**

**•활성화된 네트워크 대역 정보**

- ✓ 네트워크 카드에 설정된 IP대역을 범위로 활성화된 단말기를 찾는다
- ✓ 유선 및 무선에 상관없이 네트워크가 셋팅된 상태에서는 해당 IP대역을 스캔하여 원하는 정보를 가져온다

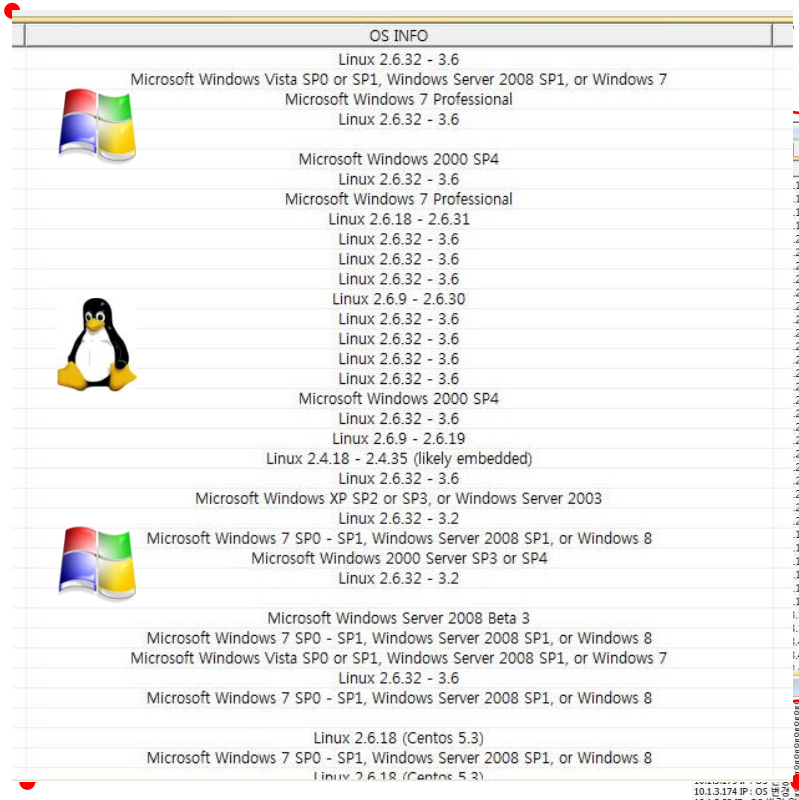
**•활성화된 네트워크 세부 정보**

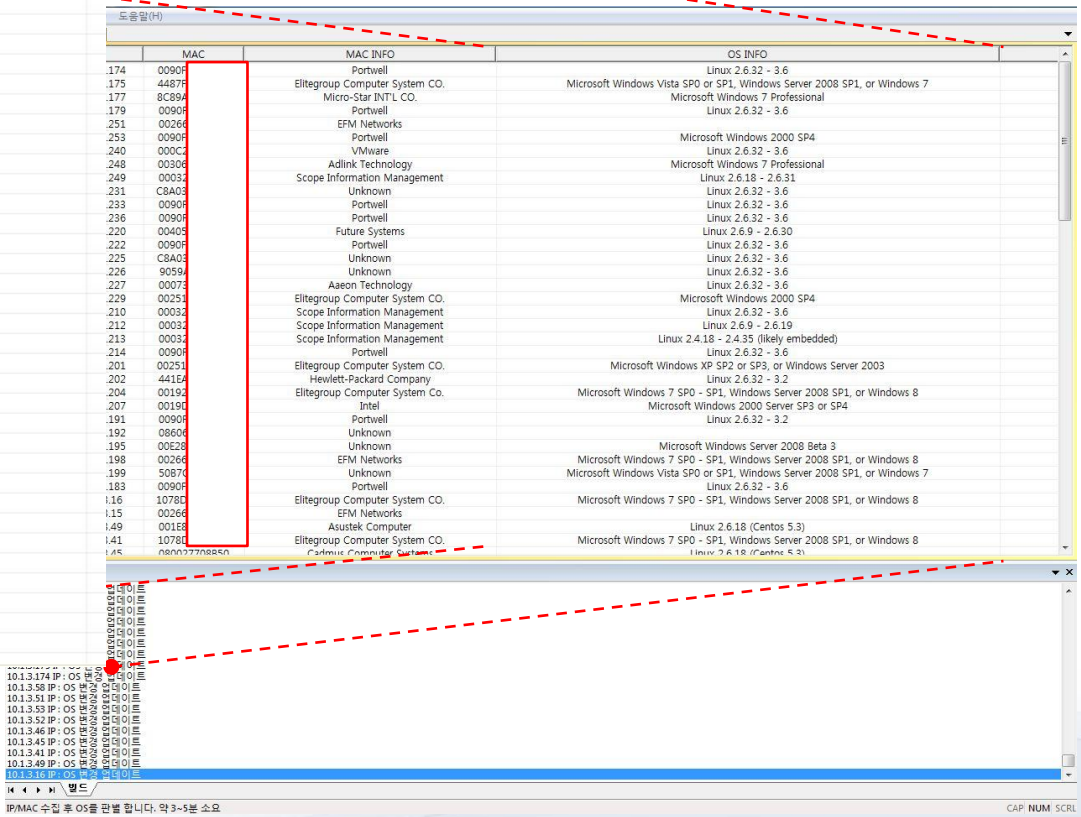
- ✓ 네트워크 대역 IP정보 수집
- ✓ 네트워크 대역 MAC 정보 수집
- ✓ 네트워크 대역 제조사 정보 수집



# 4.OS 정보 수집

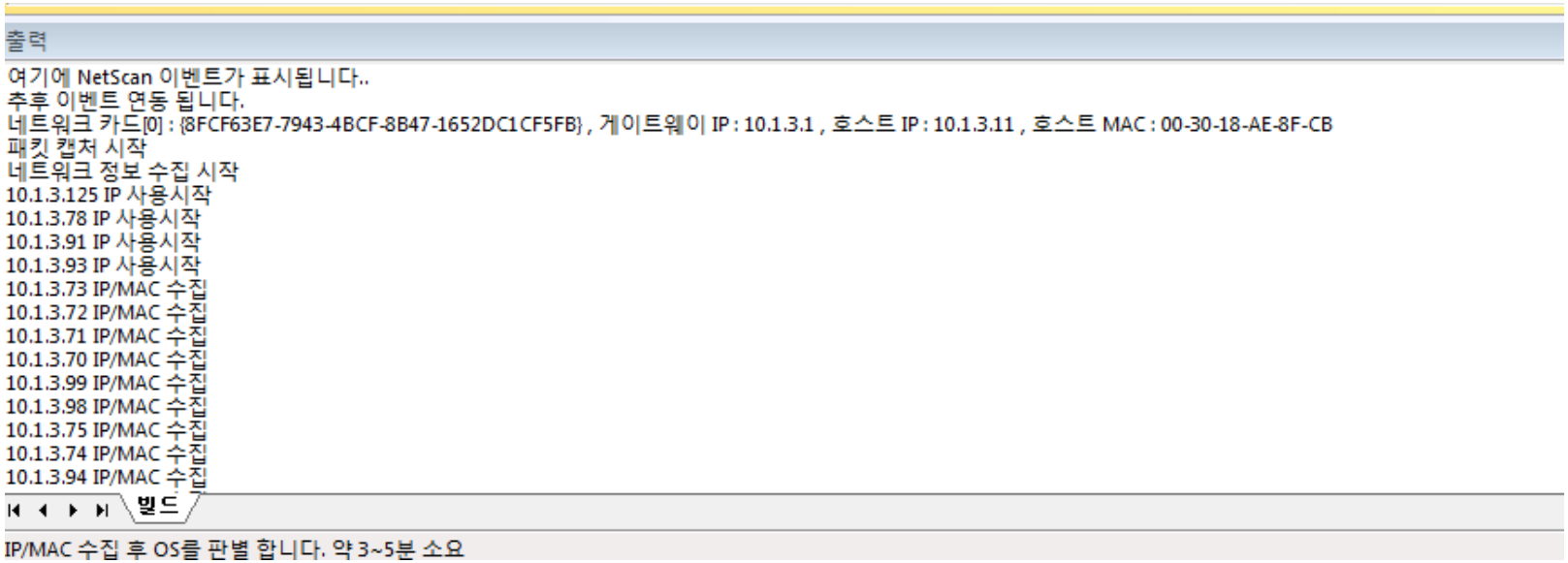
- 네트워크 대역 IP/MAC을 이용한 OS 판별



# 5.실시간 이벤트 현황

## IP/MAC/OS 실시간 변동 이벤트 확인




**네트워크에 활성화된 IP대역을 감지 하여 실시간 이벤트 로그를 출력**

- ✓ NetScan 시스템 상태에 따른 로그 출력
- ✓ IP 수집 / 사용 / 시작에 따른 로그 출력
- ✓ OS에 대한 수집 / 변동에 따른 로그 출력

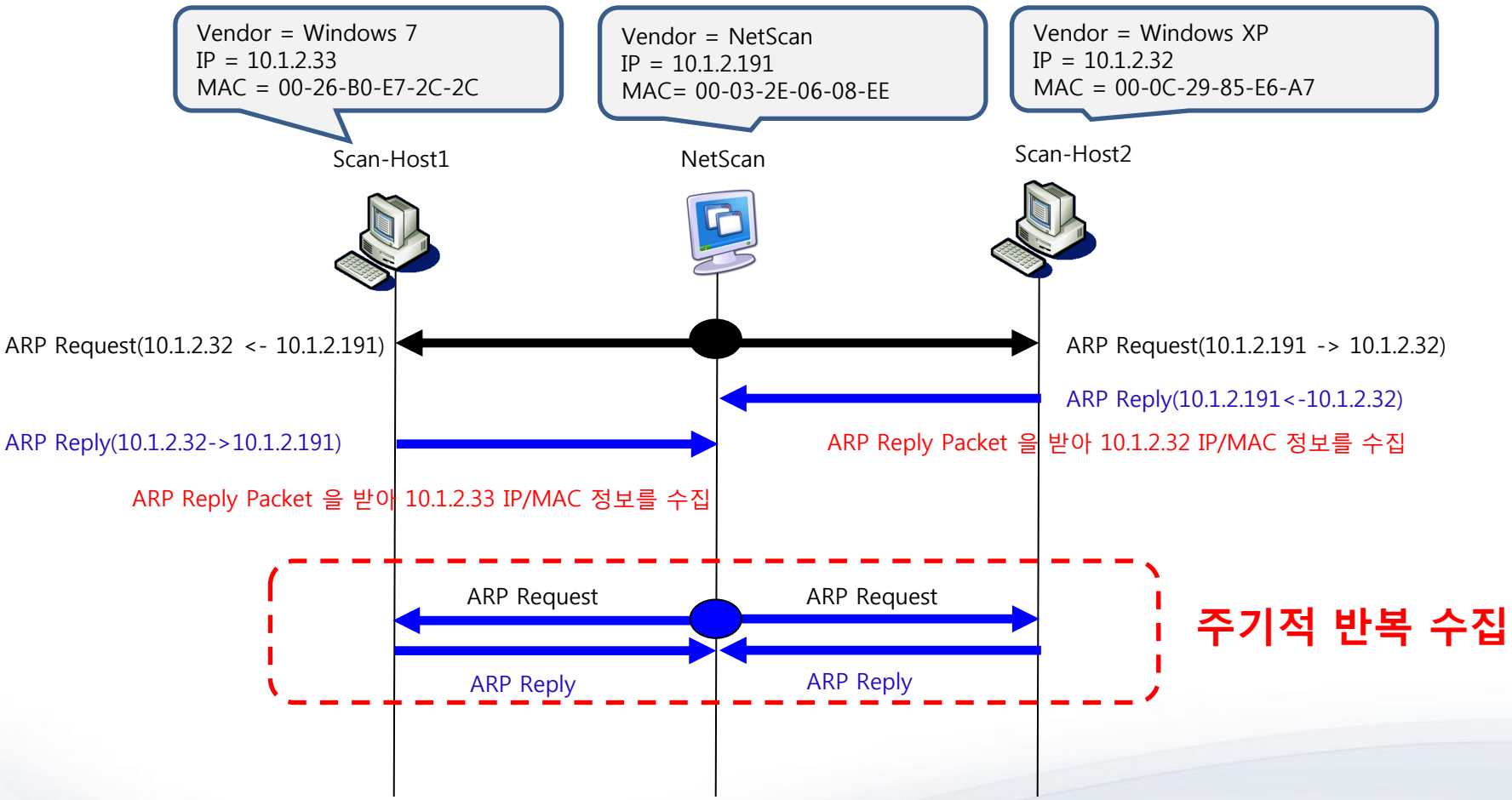
# III. NETSCAN 기술

## 1. ARP Packet 분석

2.TCP SYN/ACK/RST Packet OS분석

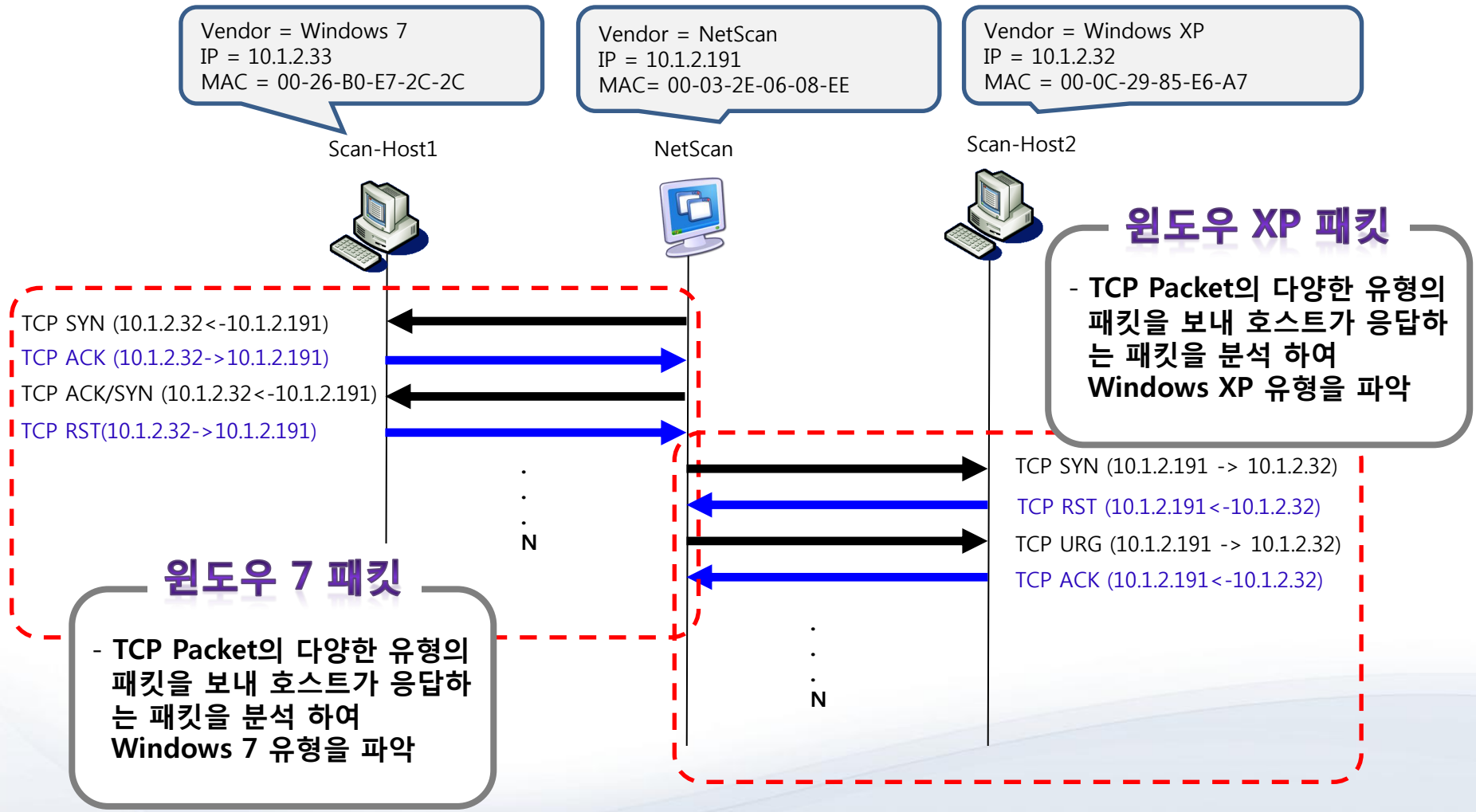
# 1.ARP Packet 분석

- 네트워크 대역의 ARP Packet을 분석 하여 IP/MAC을 수집



# 2.TCP SYN/ACK/RST Packet OS 분석

- 네트워크 대역의 TCP Packet에 대한 recv를 분석하여 OS를 판별



# IV. NETSCAN 발전

## 1. Open Source Library

2.NetWork 보안 tool
3.솔루션으로서의 가능성

# 1.Open Source Library

## ■ 모든 개발자가 쉽게 Open Source 활용을 보여주는 Tool

### 다양하게 활용 가능한 TOOL

- 네트워크 분석 용이
- 타 보안 솔루션과 연동 가능 (NAC , 자산 …)
- 빠른 보안 관련 대처 및 분석 가능

### Winpcap / Nmap Lib 활용

- Open Library 사용으로 모든 것이 공개
- Winpcap의 다른 기능을 활용 할 수 있음
  - packet dump 및 sfooping 감지 등
- Nmap의 다른 기능을 활용 할 수 있음
  - port 분석 등


### IPV4 , IPV6 공개 프로젝트

- IPV4 / IPV6 연구
  - 다양한 Packet 프로토콜 분석 및 네트워크 분석 프로젝트로 OSS의 이념을 충족
- 네트워크 연구 개발
  - 네트워크를 배우면서 실습하고 업그레이드 해볼 수 있는 학습용 Open Source

### 타 Open Source 활용

- IDS Open Source Snort 활용
  - Snort의 패킷 상세 분석을 이용하여 프로젝트 확대
- SNMP 등 새로운 기술 활용
  - 패킷 프로토콜 규약으로 발전된 기술 활용

# 2.NetWork 보안 Tool

## ■ 누구나 손쉽게 사용할 수 있는 Tool

- **타 보안 솔루션 및 Open Tool의 어려운 사용법과 연동이 필요 없이 쉽게 동작하는 NetScan**

### CASE 1 - 보안솔루션 없음 (소규모 회사)

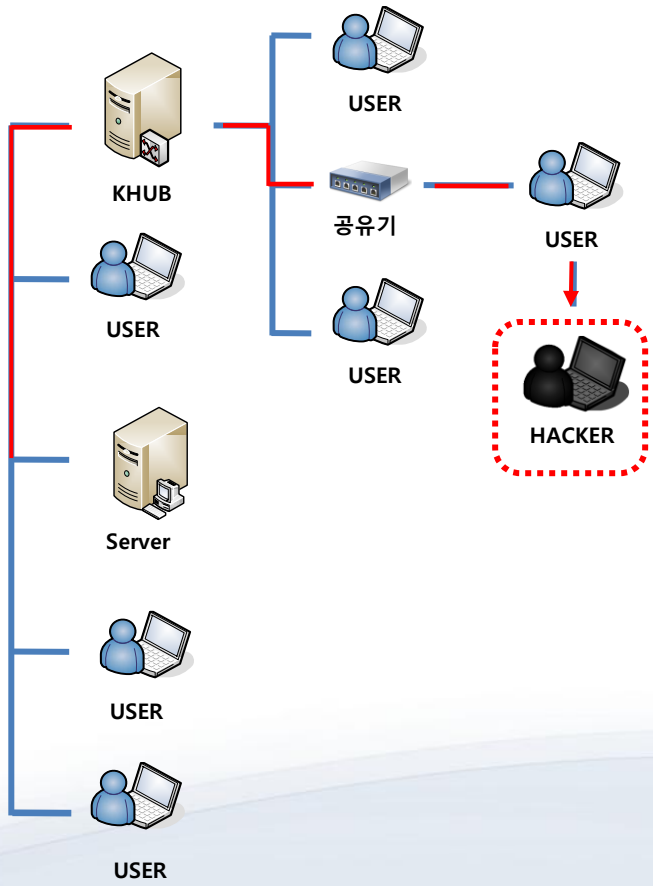

- NetScan Tool로 모니터링
- MAC 제조사 분류 후 이상 단말기 포착
- 해당 호스트 대역 운영체제 분석
- 비인가된 PC 확인

### CASE 2 - 보안솔루션 보유 (대기업 회사)


- 보안 솔루션 유해 트래픽 감지
- 해당 IP 관련 네트웍 분석
- 공유기 IP 확인
- 공유기 대역 네트웍 NetScan Tool 실행
- IP/MAC/제조사/OS 검출 및 추적

### CASE 1 - 보안솔루션 없음 (개인)


- 트래픽 속도 감소
- 허브 및 공유기 의심
- NetScan Tool 모니터링
- 타 단말기 접속 확인
- 인터넷 회사 문의 및 추적



# 3.솔루션으로서의 가능성

■ 다양한 보안 프로세스 접목으로 솔루션으로서의 발전

## 통합 보안 솔루션 NetScan

### ▪ 파일 제어

**모니터링**

**Agent 기반 정책을 통한 이벤트 모니터링 End-Point 매체 제어 가능**

- HW/SW , Process, 서비스 상태 체크
- 사용량 임계설정
- 정책 및 실시간 현황 파악

**파일 관리**

**파일 관련 이벤트를 감지하여 필요한 파일관리 정책을 적용한다.**

- 문서 파일 삭제 금지
- 해당 폴더 이동,쓰기 금지
- 중요 파일 서버 전송

### 네트워크 제어

**네트워크 관리**

**다양한 DDOS 및 악성 패킷 등 분석을 통한 침입 예방 및 네트워크 보안을 강화한다.**

- IDS , IPS 침입탐지 감지
- 유해트래픽 감지
- 네트워크 제어 및 감시

### ▪ 저장장치 제어

**USB , CD-ROM**

**외부 저장장치를 감지하여 원천적인 자료 유출을 막을 수 있다.**

- USB 복사 금지
- CD-ROM 사용 금지
- Plug in Play 감지 및 제어

**메일 발송 감시**

**인터넷을 이용한 메일 및 파일 전송을 감지하여 제어 한다.**

- 업로드 금지
- 인가된 웹 메일 발송허가

***NetWork 분석과 Agent를 이용한 범용적이고 강력하게 보안을 지킬 수 있다***

# THANK YOU

**SWAP 팀**
**팀장 : 최승환**
**팀원 : 김정민 , 이동훈**
**E-mail : friendok82@gmail.com**