4.1 과제 주제

DDOS 공격과 관련된 사건 및 사례를 찾아보세요.

레빌(REvil) 이라는 랜섬웨어 조직이 영국의 이동통신사 VoIP Unlimited 와 Voipfone 에 디도스 공격을 펼친 후 막대한 몸값을 요구하여, 며칠간 서비스가 중단 되었다. Voipfone 은 9 월 3 일 공격을 당해 SMS 서비스 및 수신발신 통화가 마비가 되었고, VoIP Unlimited 는 8 월 31 일 오후 2 시 공격을 당해 인터넷 서비스가 손실 되었던 사례가 있다.

4.2 과제 주제

방화벽과 IDS 와의 차이에 대해서 간단하게 설명하세요.

방화벽(Firewall)
- 네트워크에서 보안을 높이기 위한 1 차적인 방법
- 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나가는 패킷들을 미리 정한 규칙에 따라 차단 또는 통과시켜 주는 기능

침입탐지시스템(IDS)
- 시스템에 대한 원치 않은 조작을 탐지
- 설치 위치 및 목적에 따라 호스트 기반과 네트워크 기반의 침입시스템으로 나뉨

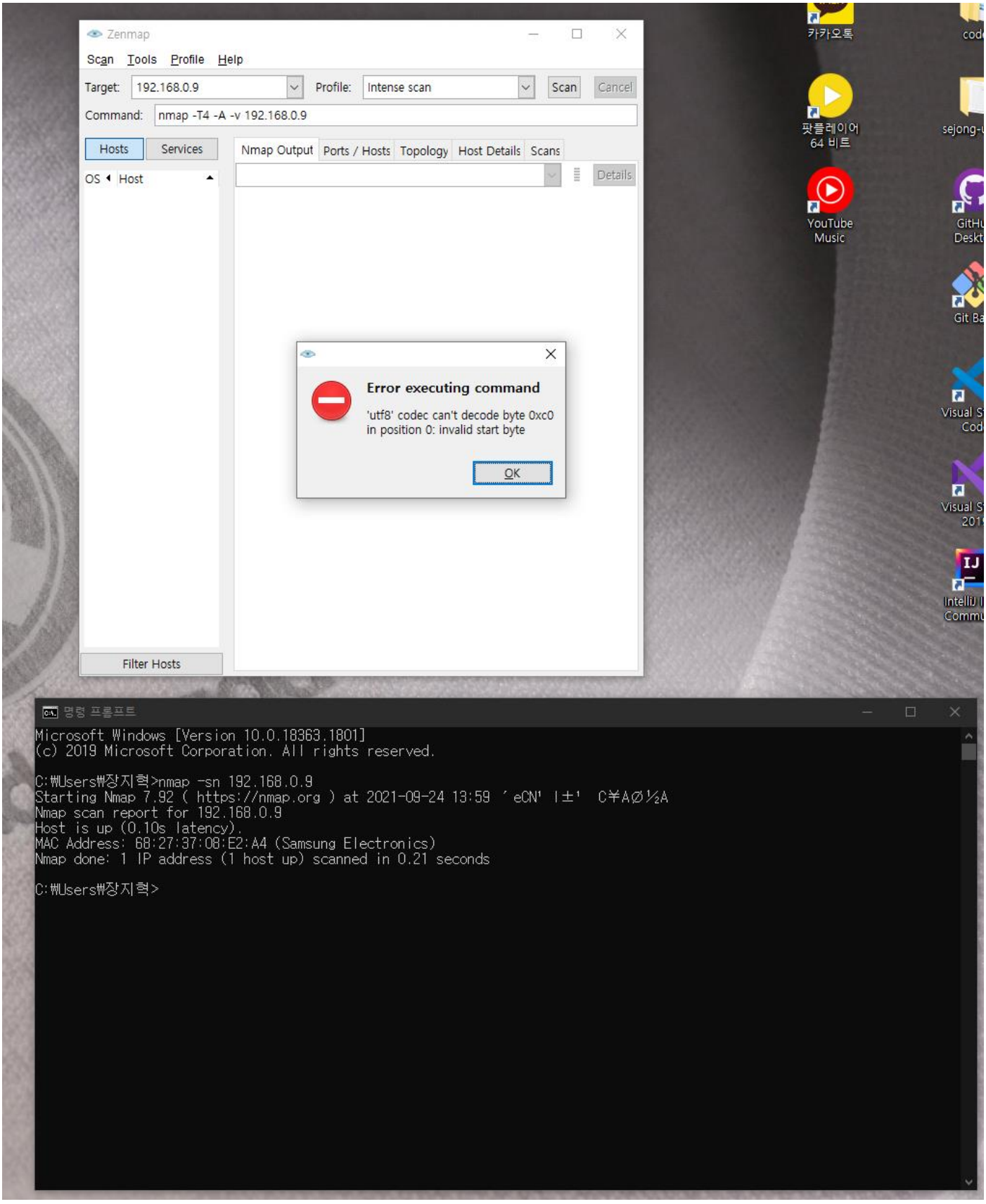
방화벽은 '차단' 기능으로써 패킷을 차단하는 기능을 수행한다. 엄격한 접근통제로 인가된 트래픽만 허용한다.

침임탐지시스템은 '탐지' 기능으로써 패킷 내용분석 과 오용 및 이상을 탐지하는 기능을 수행한다. 실시간 탐지 후 사후 분석 대응에 장점이 있다.

4.3 과제 주제

fping 또는 nmap 을 사용해서 특정 IP 주소를 스캔후 결과 화면을 캡쳐해서 제출하세요.

Nmap 프로그램에서 인코딩 오류가 나서 cmd 창에서 nmap 을 실행하였다.


Zenmap
Scan Tools Profile Help
Target: 192.168.0.9
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.9
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts
Error executing command
'utf8' codec can't decode byte 0xc0 in position 0: invalid start byte
OK
명령 프롬프트
Microsoft Windows [Version 10.0.18363.1801]
(c) 2019 Microsoft Corporation. All rights reserved.
C:₩Users₩장지혁>nmap -sn 192.168.0.9
Starting Nmap 7.92 (https://nmap.org) at 2021-09-24 13:59 ´eCN' I±' C¥AØ½A
Nmap scan report for 192.168.0.9
Host is up (0.10s latency).
MAC Address: 68:27:37:08:E2:A4 (Samsung Electronics)
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
C:₩Users₩장지혁>