PRESENTATION

4주차 주제 네트워크

~스머프 공격~

by mun

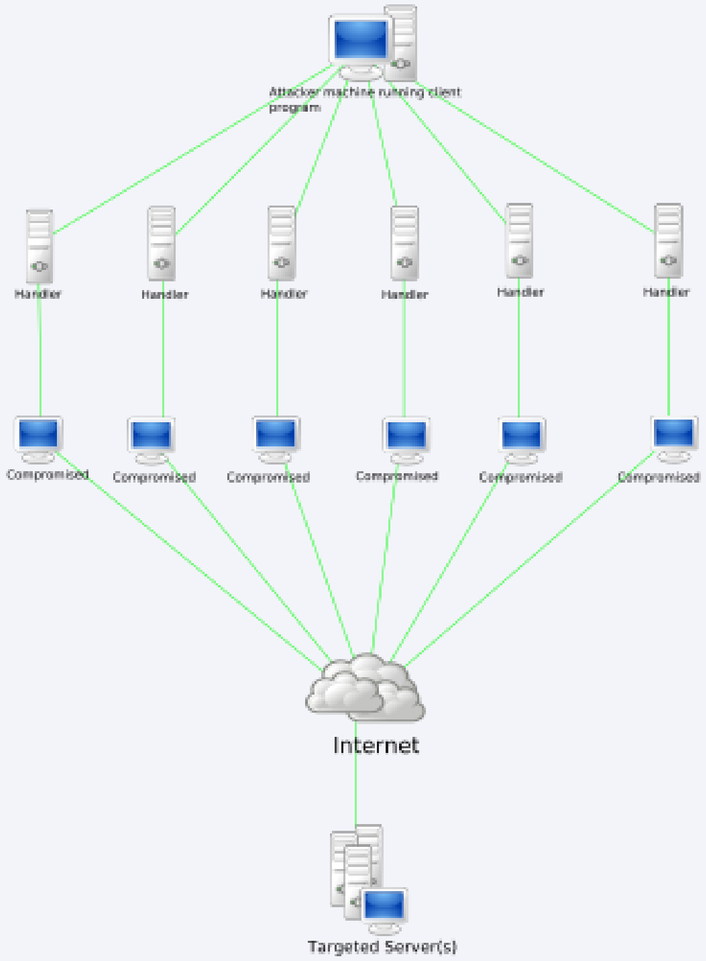
네트워크

https://www.whatap.io/ko/blog/149/

Net + Work

연결하는 선이나 장치 같은 물리적인 측면부터
데이터를 주고받는 데에 필요한 메시지나 규약과 같은
물리적이지 않은 측면까지 모두 포함한
통신 과정 전체를 아우르는 개념

DoS/DDoS 공격



서비스 거부 공격

DoS

시스템을 악의적으로 공격해
해당 시스템의 리소스를 부족하게 하여
원래 의도된 용도로 사용하지 못하게 하는 공격
시스템->시스템

DDoS

여러 대의 공격자를 분산적으로 배치해
동시에 서비스 거부 공격을 하는 방법
여러 시스템->시스템

SMURF 공격

희생자의 스푸핑된 원본 IP를 가진 수많은 ICMP 패킷들이
IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는
분산 서비스 거부 공격

스푸핑

네트워크에서 다른 컴퓨팅 시스템인 것처럼
가장하기 위해 거짓 소스 IP 주소로
인터넷 프로토콜 패킷을 만드는 일

브로드캐스트 주소

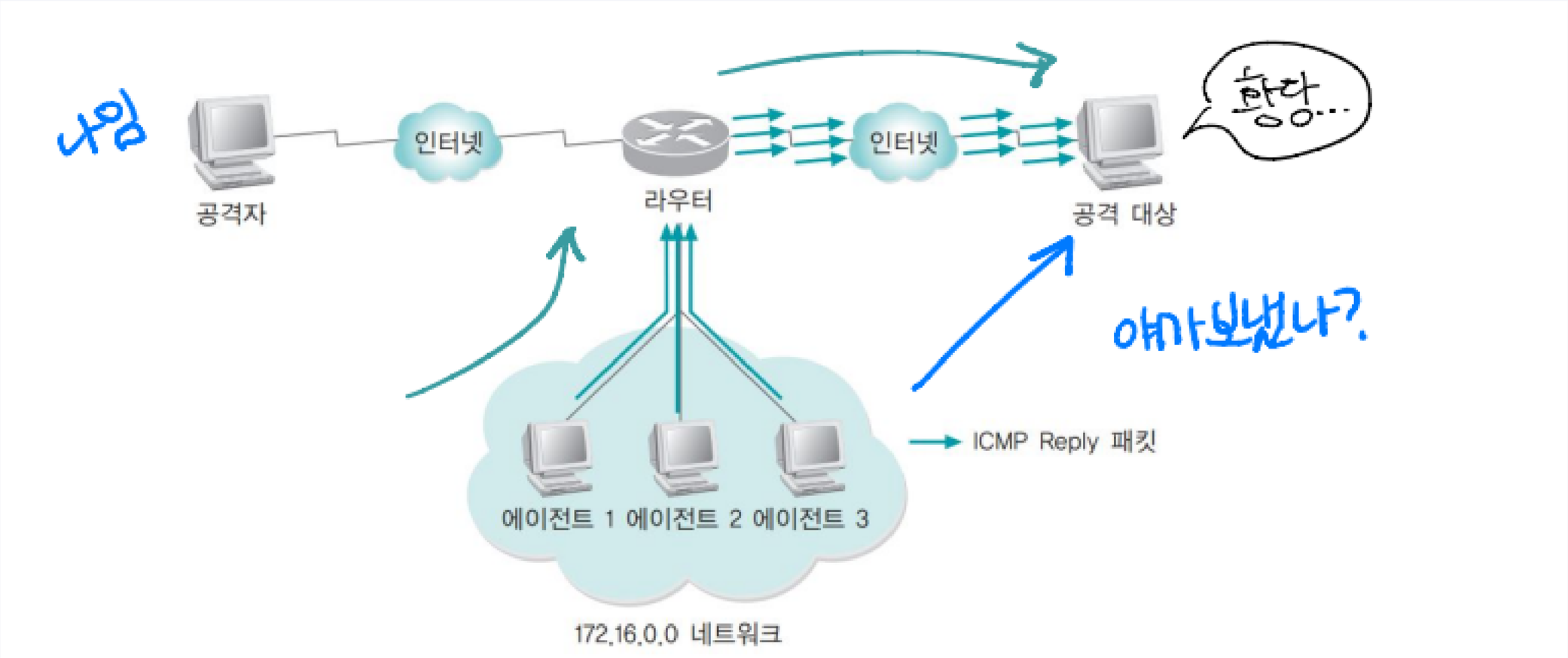
네트워크에 있는 컴퓨터나 장비 모두에
한 번에 데이터를 전송하는데 사용되는 전용 IP주소
192.168.1.0 → 192.168.1.255(호스트주소 255)

ICMP(인터넷제어메시지프로토콜)

인터넷 프로토콜의 주요 구성원 중 하나
네트워크 컴퓨터 위에서 돌아가는 운영체제에서
오류 매시지를 전송받는 데 주로 쓰임

스머프공격

스머프공격


나임
공격자
인터넷
라우터
인터넷
공격 대상
황당...
에이전트 1
에이전트 2
에이전트 3
ICMP Reply 패킷
172.16.0.0 네트워크

개선 방법

지속적인 모니터링

패킷 차단

추가 대역폭 프로비저닝

유해사이트 차단

보안!
보안을 강화합시다!

감사합니다

참고 : 위키백과, https://www.linux.co.kr/bbs/board.php?bo_table=lecture&wr_id=2621
https://greate-future.tistory.com/36, https://www.whatap.io/ko/blog/149/