최종정리본

↗ 과목(Class)	네트워크 보안
≔ 키워드	

네트워크 보안 (Network Security)

> 학습 개요
>
> - **기간:** 2025.08 ~ 2025.11 (한국폴리텍대학 하이테크과정 2학기)
> - **환경:** Ubuntu Server, Kali Linux, Zabbix, VMware
> - **핵심 역량:** Linux 방화벽(iptables) 정책 수립, 통합 모니터링 시스템(Zabbix) 운영, 시스템 부하 테스트 및 대응

🛡️ 상세 학습 내용 (Technical Skills & Practices)

1. 리눅스 방화벽 정책 및 트래픽 제어 (Firewall & Traffic Control)

- **iptables 정책 수립:** 기본 정책(Default Policy)을 설정하고, 특정 IP(Windows Host)나 포트(SSH, HTTP)에 대한 **Allow/Drop/Reject** 규칙을 체계적으로 적용하여 접근 통제 구현.
- **고급 필터링 기술:**
  - **상태 추적 (Stateful Inspection):** `ESTABLISHED`, `RELATED` 상태의 패킷을 허용하여 정상적인 세션 연결을 유지하고 불필요한 재검사를 방지하는 효율적 정책 적용.
  - **공격 방어:** `hping3`를 이용한 테스트 공격에 대응하여, TCP Flags(SYN이 없는 첫 패킷 차단) 검사 및 ICMP Echo Request(Ping) 차단 정책 구현.
  - **접속 제한 및 로깅:** SSH 무차별 대입 공격 방지를 위해 `connlimit` 모듈로 동시 접속 수를 제한하고, `-log-prefix` 옵션을 사용하여 특정 트래픽(SSH 접속 시도 등)을 시스템 로그(`/var/log/syslog`)에 기록.

2. 시스템 모니터링 및 가용성 관리 (Monitoring & Availability)

- **통합 모니터링 (Zabbix):** 오픈소스 모니터링 솔루션인 **Zabbix**를 구축하여 서버의 CPU, 메모리, 네트워크 상태를 실시간으로 시각화하고, 장애 발생 시 알림을 받는 관제 시스템의 기초 원리 학습.

- **부하 테스트 및 오토스케일링:** `stress` 도구를 사용하여 인위적인 CPU 과부하 상황을 만들고, `top` 명령어로 실시간 리소스 점유율을 분석하며 클라우드 환경에서의 **Auto Scaling(자동 확장)** 필요성 및 임계치 설정 개념 이해.

3. 네트워크 아키텍처 및 패킷 분석 (Architecture & Analysis)

- **OSI 7계층 기반 트래픽 분석:** 데이터가 방화벽(FW), L3/L4 스위치를 거칠 때마다 변하는 **Header 정보(MAC, IP, TTL)**의 변화를 추적하여 네트워크 흐름의 전체 맵(Map)을 그리는 역량 확보.
- **NAT 및 망 구성:** 공인 IP 부족 문제를 해결하기 위한 **SNAT/DNAT** 및 **PAT**의 동작 원리를 이해하고, 내부망(Internal)과 외부망(External), DMZ 구간을 분리하는 보안 네트워크 아키텍처 설계.

💻 주요 활용 도구 및 명령어 (Key Tools & Commands)

- **Firewall (iptables):**
  - 정책 추가/삭제: `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`, `iptables -F` (초기화)
  - 고급 옵션: `m state --state ESTABLISHED`, `m connlimit --connlimit-above 3`, `j LOG --log-prefix "[SSH_Access] "`
  - 차단 방식: `j DROP` (무응답), `j REJECT` (거부 응답 전송)
- **Monitoring & Test:** `top` (프로세스 모니터링), `stress --cpu 2` (부하 생성), `tail -f /var/log/syslog` (실시간 로그 확인)
- **Analysis:** `hping3 -S -p 80 [IP]` (TCP SYN 패킷 생성), `tracert` / `traceroute` (경로 추적)

💡 학습 회고 (Learning Reflection)

> "단순히 네트워크를 '연결'하는 것을 넘어, 들어오고 나가는 모든 패킷을 '통제'하고 '관찰'하는 보안 관리자의 시각을 갖게 되었습니다. 특히 iptables 실습을 통해 정책의 순서(Order) 하나가 전체 보안에 미치는 영향을 체감했고, DROP과 REJECT의 차이를 통해 공격자에게 정보를 주지 않는 '보안의 디테일'을 배웠습니다. 또한 Zabbix와 top을 활용한 모니터링 실습을 통해, 장애가 발생하기 전에 징후를 포착하는 관제 업무의 중요성을 깊이 이해하게 되었습니다."