보건 제공 제단

단골집

팀장 : 이태호

부팀장 : 김태현

팀원 : 김용문, 황승우, 이서진

목차

프로젝트 개요

프로젝트 개요

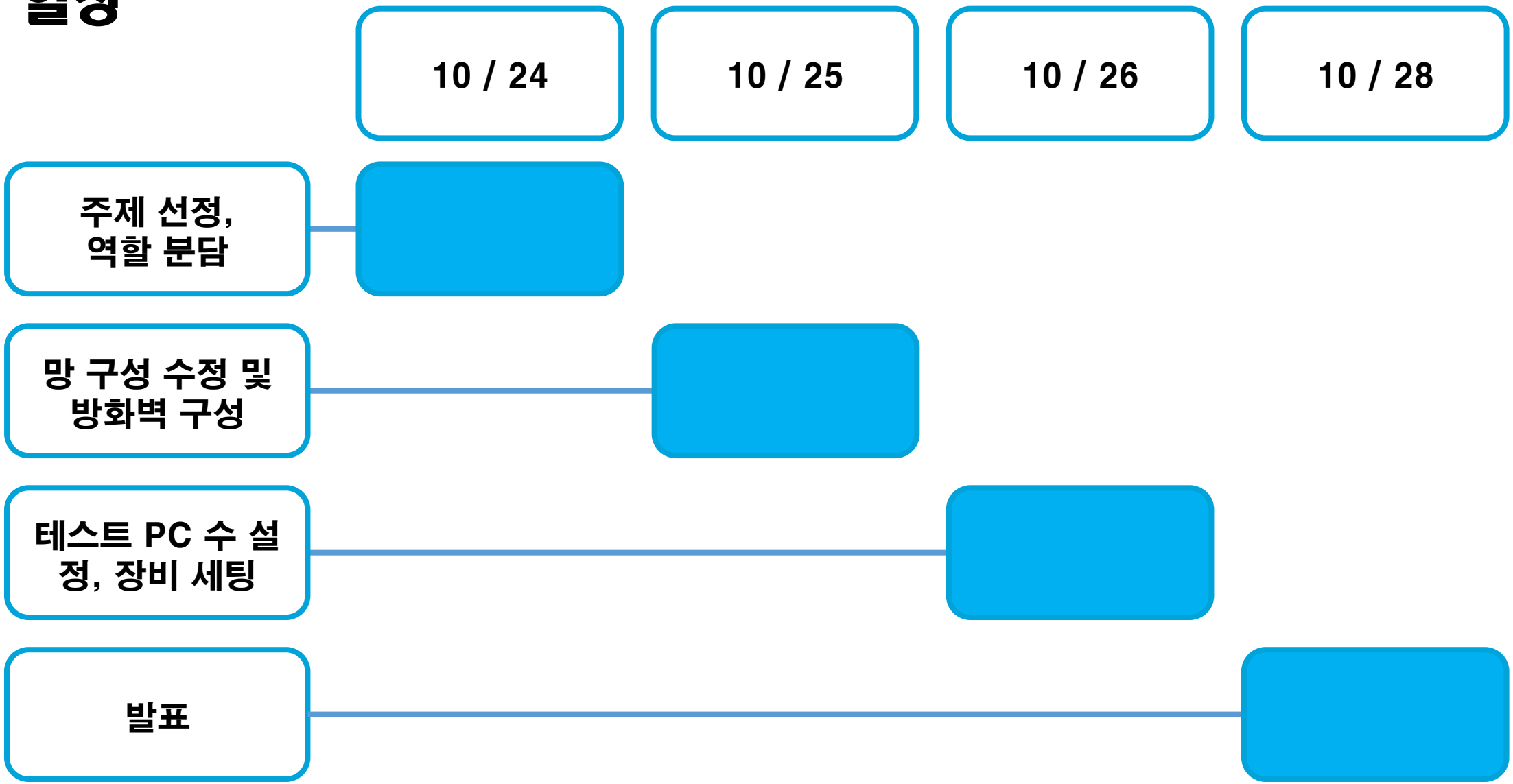
프로젝트 목적 : 병원 내 네트워크 및 인프라 구축

프로젝트 진행을 통해

- 안정적이고 보안성 높은 네트워크 인프라 구축
- 부서 간 효율적 통신
- 트래픽 관리 효율화와 시스템 확장성 확보
- 실무 역량 강화

프로젝트 개요

일정



기대 효과

1. 안정적인 진료 서비스 제공
2. 보안성 강화 및 환자 정보 보호
3. 부서 간 효율적 자원 관리
4. 확장성과 유지 보수 성 확보
5. 실무 역량 파악

사용 장비

가상 머신

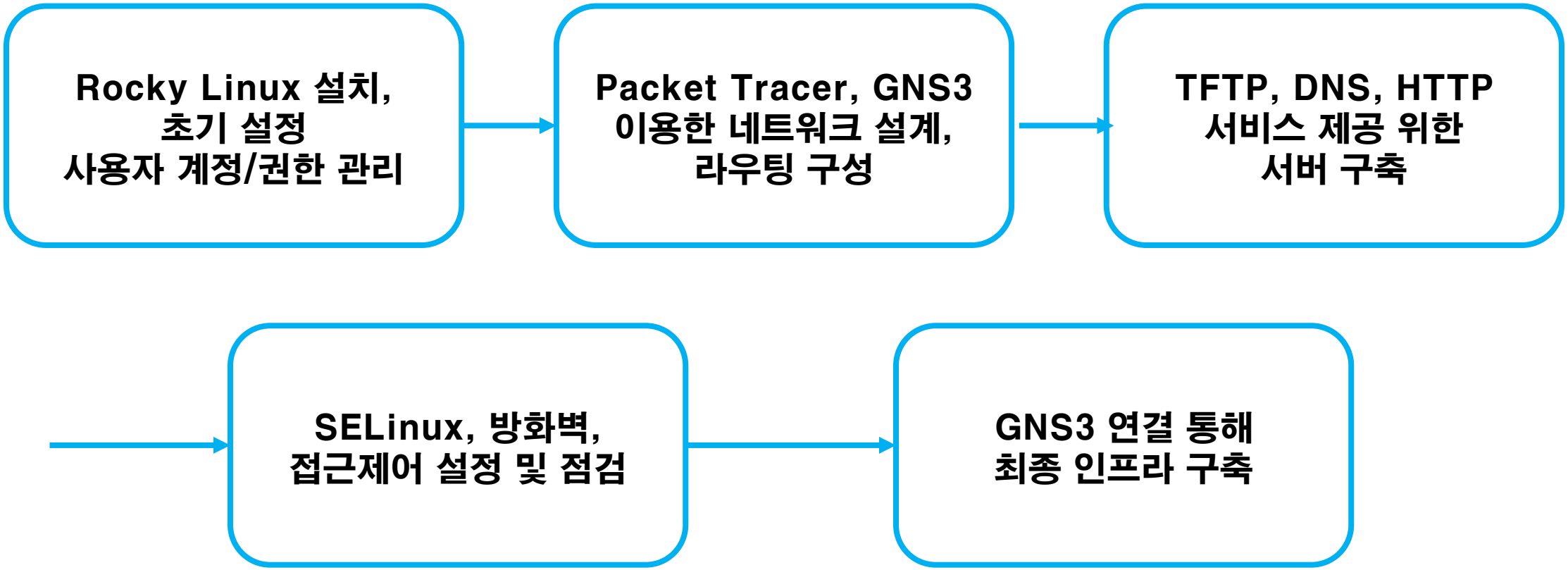
네트워크 에뮬레이터 도구

Cisco Packet Tracer

테스트 장비

wireshark

프로젝트 진행 흐름


Rocky Linux 설치,
초기 설정
사용자 계정/권한 관리
Packet Tracer, GNS3
이용한 네트워크 설계,
라우팅 구성
TFTP, DNS, HTTP
서비스 제공 위한
서버 구축
SELinux, 방화벽,
접근제어 설정 및 점검
GNS3 연결 통해
최종 인프라 구축

네트워크 구축 방향

재무인사, 진료과,
병동, 관리/전산으로
내부망 구축

외부망에
HTTP, DNS 서버 구축

DMZ존 이용하여
내부망과 외부망
통신 관리

팀 소개

팀 소개

이태호
(총괄 책임자)

전체 네트워크
인프라 구축

김태현
(서비스 운영자)

FTP/HTTP/DNS/
TFTP 서버 구축 및
권한 설정

황승우
(시스템 관리자)

Rocky Linux
설치 및 초기 설정
사용자 계정/권한 관리

김용문
(네트워크 엔지니어)

GNS3, Packet Tracer
네트워크 설계 및
라우팅 구성

이서진
(보안 담당자)

방화벽
접근제어
설정 및 점검

시스템 구축 과정

보안 설정

이서진

시스템 구축 과정

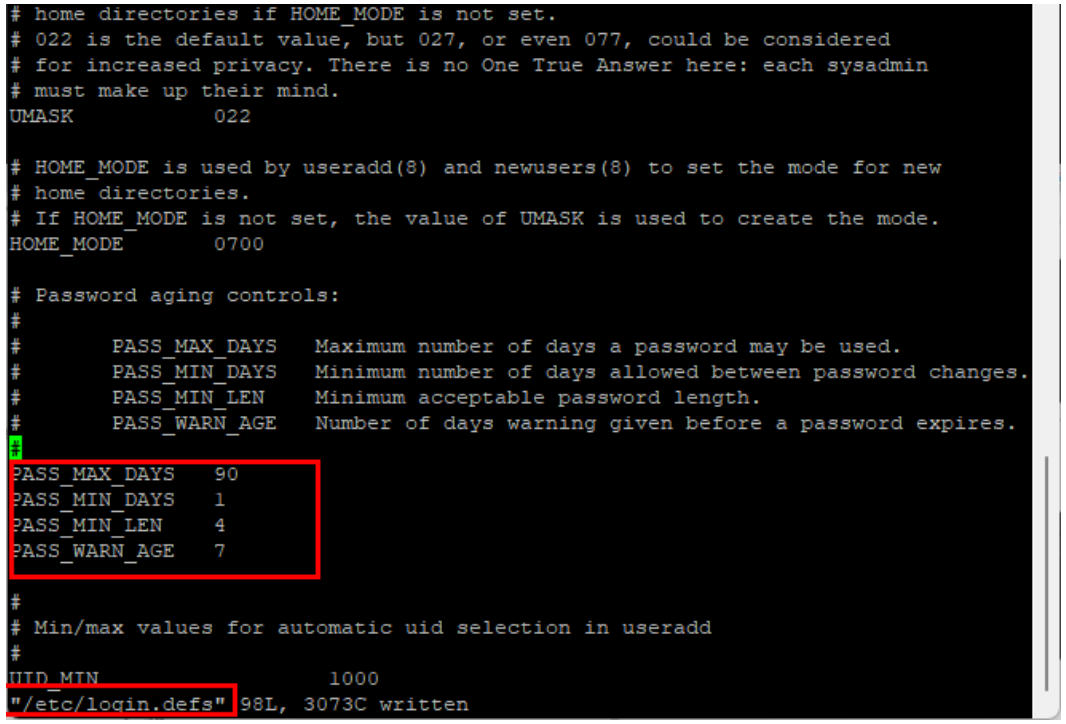

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: cockpit dhcpv6-client dns ftp http https ssh
  ports: 80/tcp 53/udp 22/tcp 69/udp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

방화벽 설정

허용 서비스 :
FTP, HTTP,
SSH, DNS

허용 포트 :
80/TCP, 53/UDP,
22/TCP, 69/UDP

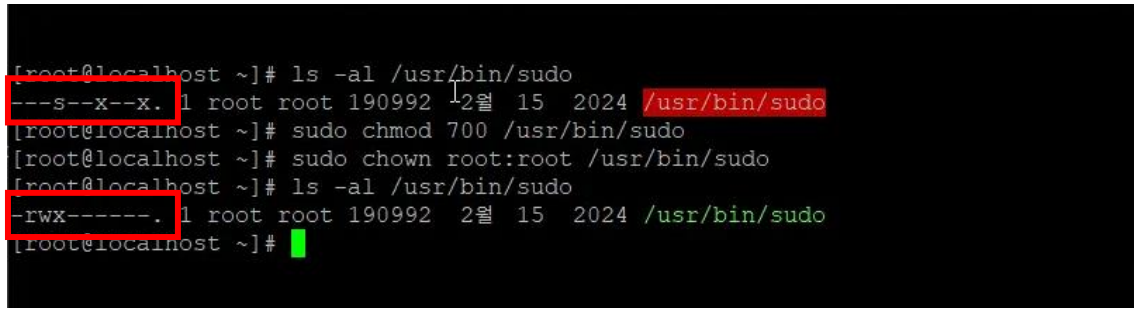
시스템 구축 과정



비밀번호 유효일 설정

최대사용일 90일
최소사용일 1일
경고일수 7일
최소길이 4

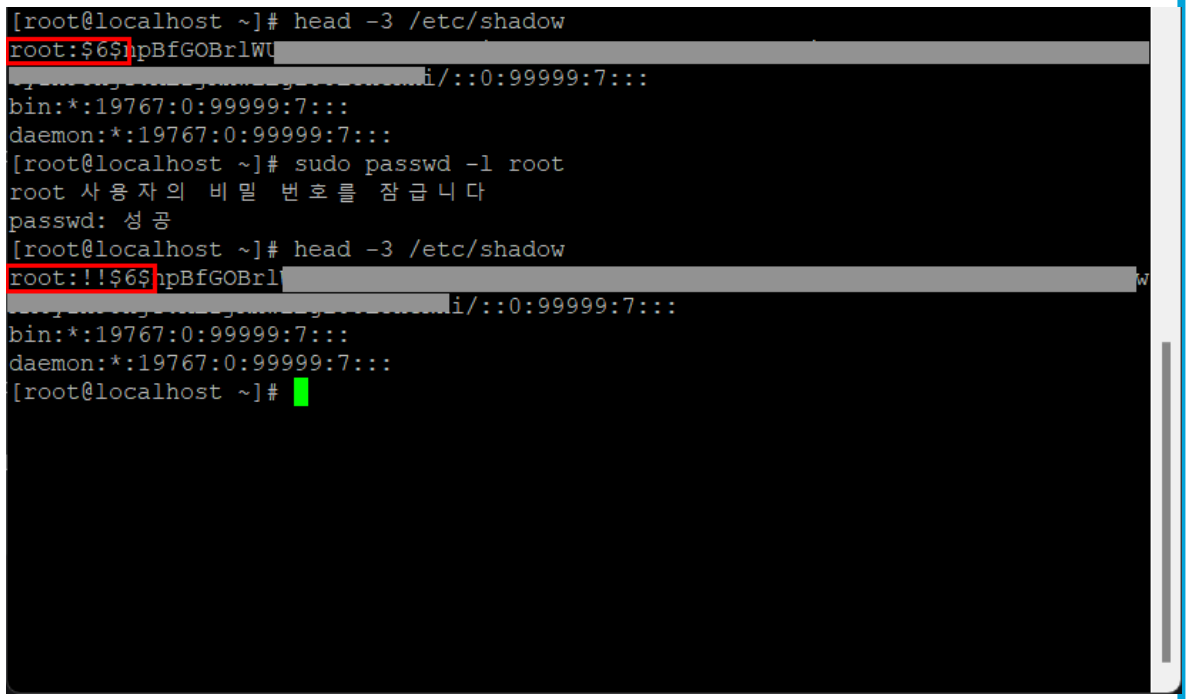
시스템 구축 과정



sudo 명령어 제한

/usr/bin/sudo
파일 자체에
접근권한 변경하여
sudo 명령어를
다른 계정이 사용 못하게
차단

시스템 구축 과정



root 계정 잠금

sudo passwd –l root
root 비밀번호를 잠금
root 계정으로
전환 불가

시스템 구축 과정


```
ALL: 192.168.10.1
[root@localhost portsentry-1.0]# vi /etc/hosts.deny
[root@localhost portsentry-1.0]# cat /etc/hosts.deny
ALL: ALL
[root@localhost portsentry-1.0]#
```

Source	Destination	Protocol	Lengt	Info
192.168.10.1	192.168.10.131	TCP	74	48296 → 783 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3228538253
192.168.10.1	192.168.10.131	TCP	74	41238 → 3914 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322853829
192.168.10.1	192.168.10.131	TCP	74	45506 → 5666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322853829
192.168.10.1	192.168.10.131	TCP	74	58236 → 222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3228539079
192.168.10.1	192.168.10.131	TCP	74	46416 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322853907
192.168.10.131	192.168.10.1	ICMP	102	Destination unreachable (Communication administratively filtered)
192.168.10.1	192.168.10.131	TCP	74	48054 → 34571 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=32285390
192.168.10.1	192.168.10.131	TCP	74	60428 → 911 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3228539079
192.168.10.1	192.168.10.131	TCP	74	60162 → 1071 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322853916
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 59610 → 3007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 55014 → 5801 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 43202 → 4998 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 60806 → 2288 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 53988 → 2042 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 58566 → 3551 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 45792 → 109 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 48296 → 783 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 35030 → 2035 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 44442 → 1106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 34276 → 259 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 33246 → 3077 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 46810 → 4343 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 37380 → 32785 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 43430 → 464 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
192.168.10.1	192.168.10.131	TCP	74	[TCP Retransmission] 36288 → 2000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK

libwrap 설정

TCP rappers로
외부 호스트의
TCP 서비스 접근을 거부

시스템 구축 과정


```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
#SELINUX=disabled
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


~
~
~
```

SELinux 활성화

SELinux 보안정책 적용

문제점 및 문제 해결

TCP 접근 거부 실패

문제점 및 문제 해결


```
ALL: 192.168.10.1
[root@localhost portsentry-1.0]# vi /etc/hosts.deny
[root@localhost portsentry-1.0]# cat /etc/hosts.deny
ALL: ALL
[root@localhost portsentry-1.0]#
```

root@kali: ~

File Actions Edit View Help

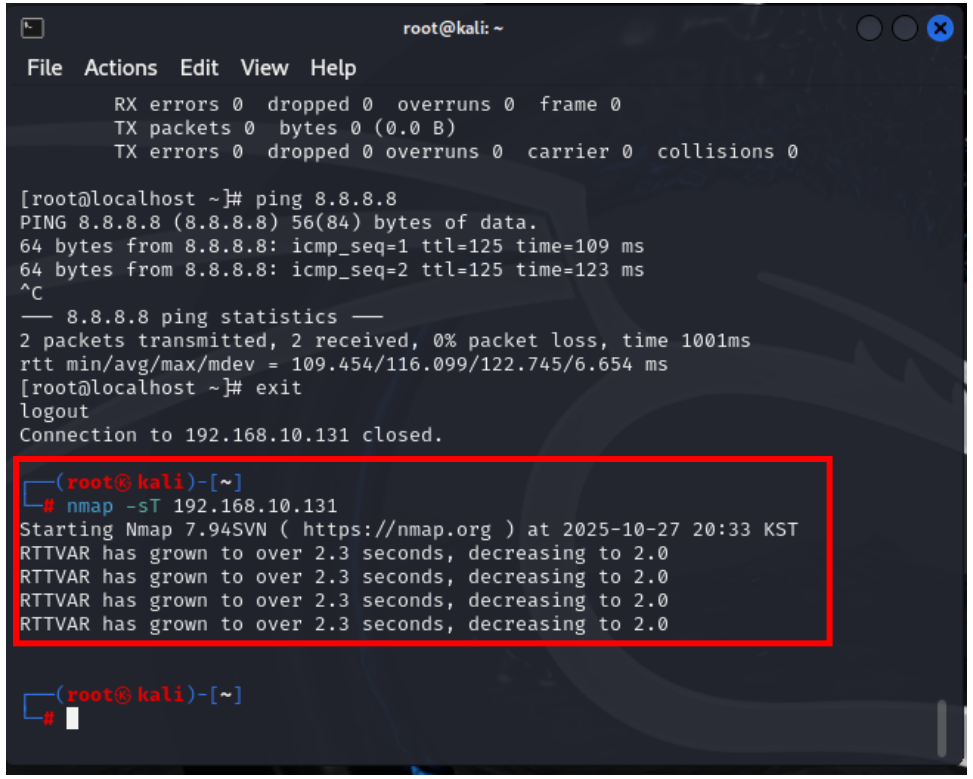
```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.10.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 20:43 KST
Nmap scan report for 192.168.10.131
Host is up (0.28s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE
1/tcp     open  tcpmux
21/tcp    open  ftp
22/tcp    open  ssh
79/tcp    open  finger
80/tcp    open  http
111/tcp   open  rpcbind
119/tcp   open  nntp
143/tcp   open  imap
1080/tcp  open  socks
1524/tcp  open  ingreslock
2000/tcp  open  cisco-sccp
6667/tcp  open  irc
12345/tcp open  netbus
31337/tcp open  Elite
32771/tcp open  sometimes-rpc
32772/tcp open  sometimes-rpc
32773/tcp open  sometimes-rpc
32774/tcp open  sometimes-rpc1

Nmap done: 1 IP address (1 host up) scanned in 21.77 seconds
```

hosts.deny는
어플리케이션 레벨
접근 제어 일 뿐
네트워크 레벨에서의
스캔은 차단불가

록키리눅스에서
테스트를 위해 꺼둔
방화벽을 활성화하여 해결

문제점 및 문제 해결



hosts.deny는
어플리케이션 레벨
접근 제어 일 뿐
네트워크 레벨에서의
스캔은 차단불가

록키리눅스에서
테스트를 위해 꺼둔
방화벽을 활성화하여 해결

감사합니다.