

# 보건 제공 제단

## 단골집



**팀장 : 이태호**

**부팀장 : 김태현**

**팀원 : 김용문, 황승우, 이서진**

# 목차

1. 프로젝트 개요
2. 팀 소개
3. 시스템 구축 과정
4. 문제점 및 문제 해결

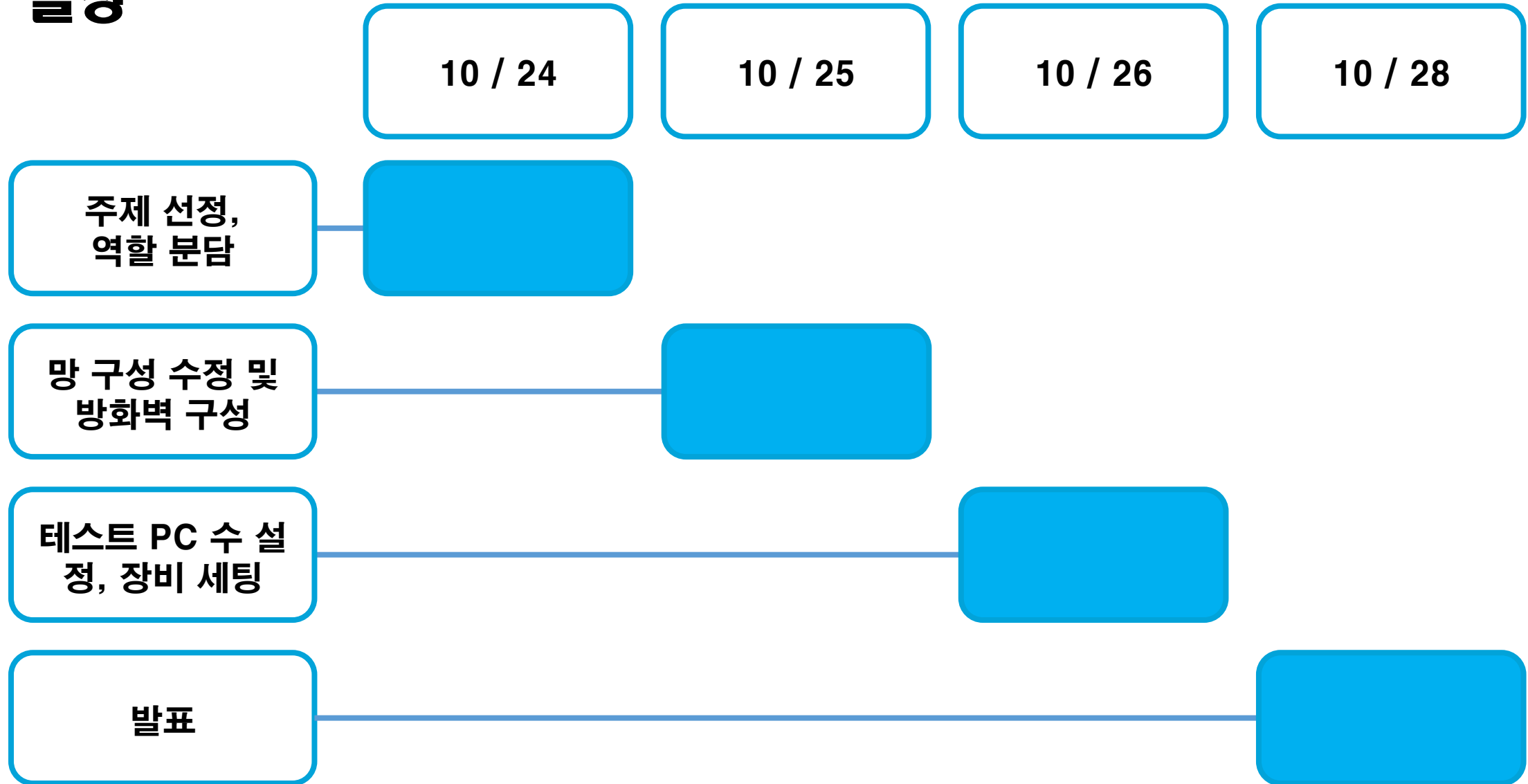
# 프로젝트 개요

## 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

## 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

**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

```
[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

```
# home directories if HOME_MODE is not set.
# 022 is the default value, but 027, or even 077, could be considered
# for increased privacy. There is no One True Answer here: each sysadmin
# must make up their mind.
UMASK          022

# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE      0700

# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_MIN_LEN     Minimum acceptable password length.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
PASS_MAX_DAYS   90
PASS_MIN_DAYS   1
PASS_MIN_LEN     4
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN         1000
"/etc/login.defs" 98L, 3073C written
```

## 비밀번호 유효일 설정

최대사용일 90일  
최소사용일 1일  
경고일수 7일  
최소길이 4

```
[root@localhost ~]# ls -al /usr/bin/sudo
---s--x--x. 1 root root 190992 2월 15 2024 /usr/bin/sudo
[root@localhost ~]# sudo chmod 700 /usr/bin/sudo
[root@localhost ~]# sudo chown root:root /usr/bin/sudo
[root@localhost ~]# ls -al /usr/bin/sudo
-rwx-----. 1 root root 190992 2월 15 2024 /usr/bin/sudo
[root@localhost ~]#
```

sudo 명령어 제한

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



```
[root@localhost ~]# head -3 /etc/shadow
root:$6$hpBfGOBrlWU
bin:!:19767:0:99999:7:::
daemon:!:19767:0:99999:7:::
[root@localhost ~]# sudo passwd -l root
root 사용자의 비밀번호를 잠금니다
passwd: 성공
[root@localhost ~]# head -3 /etc/shadow
root:!!$6$hpBfGOBrlWU
bin:!:19767:0:99999:7:::
daemon:!:19767:0:99999:7:::
[root@localhost ~]#
```

root 계정 잠금

`sudo passwd -l root`  
root 비밀번호를 잠금  
root 계정으로  
전환 불가

```
[root@localhost ~]# vi /etc/hosts.deny
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	Length	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 SACK
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

```
# 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

A blurred background image of an office space. It shows several desks with computer monitors, a printer, and office chairs. The lighting is bright, and the overall scene is out of focus. A solid blue vertical bar is on the left side of the image.

**TCP 접근 거부 실패**



**록키리눅스에서  
테스트를 위해 꺼둔  
방화벽을 활성화하여 해결**

```

root@kali: ~
File Actions Edit View Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=125 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=125 time=123 ms
^C
— 8.8.8.8 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 109.454/116.099/122.745/6.654 ms
[root@localhost ~]# exit
logout
Connection to 192.168.10.131 closed.

(root@kali)-[~]
# nmap -sT 192.168.10.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 20:33 KST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

(root@kali)-[~]
#

```

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

**록키리눅스에서  
테스트를 위해 꺼둔  
방화벽을 활성화하여 해결**

**감사합니다.**