2022년 지방기능경기대회 과제

직 종 명	사이버 보안	과제명	인프라 환경 설정 및 보안 강화	과제번호	제 3과제
경기시간	5시간	비번호		감독위원 확인	(인)

1. 요구사항

가. 과제 개요

본 과제를 수행하는 당신은 한 글로벌 기업의 신입 보안 담당자입니다. 당신은 이번 신규 정보도입 사업의 보안을 맡은 책임자로써, 도입된 서버들의 가용성과 보안성을 최대한 고려하여, 시스템, 네트워크, 어플리케이션 각 부문에서 보안 취약점을 탐지하고, 추후 발생할 수 있는 다양한 보안 위협에 대응할 수 있어야 합니다.

현재 사내에는 global.com 도메인을 위한 DNS 서비스와 이메일 서비스 및 데이터베이스 서비스를 운영 중에 있으며, 신규 도입으로 인해 아직 보안설정이 미흡한 상태입니다. 이제 당신은 과제에 주어진 배포자료들을 활용하여 제시된 문제들을 해결해야 합니다.

나. 배포 자료

※ 운영체제 및 소프트웨어(지급될 SW)

- Ubuntu 18.04.5 LTS Desktop VMware image
- Windows Server 2019 64bit iso
- Windows 10 64bit iso
- Ubuntu 18.04.5 LTS Server iso
- VMware Workstation 15.5
- Putty utility

2. 선수 유의사항

가. 작업 시 대소문자를 구별하여 과제를 수행해야합니다.
나. 채점 시 서비스 및 운영체제 재시작은 총 3회로 제한합니다.
다. 특별히 지정된 암호 이외의 모든 암호는 "Global43@!"로 설정합니다.
라. 시스템 재부팅 후에도 과제 채점에 영향이 없도록 설정합니다.
마. 과제에 별도로 지정되지 않은 부분은 기본 값 또는 적절한 값을 입력하여 구성합니다.
바. 대회장에서 제공되지 않은 소프트웨어 설치는 부정행위로 간주됩니다.
사. 선수는 usb 및 저장매체를 가지고 대회장에 입장할 수 없습니다.
아. 휴대폰 등 스마트기기는 경기시작 전 심사위원(또는 관리위원)에게 제출합니다.
자. 대상이 언급되지 않은 리눅스 서버의 경우 **모두 GL-SRV로 한정합니다.**

3. 과제 내용

가. 운영체제 설치 및 네트워크 구성

1) 운영체제 설치

가) 모든 가상머신 파일들은 **"D:₩Cyber-[비번호]₩호스트네임"** 폴더에 각각 저장하도록 하며 모든 호스트 및 GUEST OS는 과제에 제시된 호스트 이름으로 정확하게 변경되어야 합니다.

나) 과제 수행에 필요한 패키지는 모두 제공되므로, 별도로 패키지를 추가하여 사용하지 않도록 주의합니다.

다) 가상머신 파일은 GL-SRV만 제공하며 나머지는 직접 iso 파일을 통해 설치를 진행합니다.

라) GL-SRV 서버는 채점을 위해 미리 **test01 계정**을 생성하도록 합니다.

마) GW-SRV 서버는 global.com을 위한 Active Directory 서비스를 반드시 설치하고 도메인 컨트롤러로 위임하도록 합니다. (**미설치 시 다른 채점에 불이익을 받을 수 있습니다.**)

바) Adm-PC는 방화벽 채점을 위해 Windows 기능에서 telnet client 서비스를 미리 활성화하도록 합니다.

2) 네트워크 구성

가) 부록을 참고하여 토폴로지를 구성하고 네트워크 관련 설정을 진행합니다.

나) 제공된 라우터 가상 머신과 모든 Guest OS들은 **반드시 host-only 방식으로 연결되도록 하며** 모든 연결 후에는 **상호간의 ICMP 통신이 가능해야합니다.**

다) GR-SRV 서버는 라우팅 기능을 활성화하도록 합니다.

라) 모든 Guest OS의 NIC 설정에서 IPv6 프로토콜을 제거하도록 합니다.

마) 외부 네트워크를 제외한 사내 모든 네트워크에서 DNS 서비스를 이용할 수 있어야 합니다.

나. 윈도우 시스템 보안

윈도우 서버 내 administrator 계정의 이름을 gwinadmin으로 변경하고, 로그인 시 마지막 로그아웃된 계정의 이름이 출력되지 않도록 설정합니다.

1) 계정 암호 정책

GW-SRV 서버에 신규 계정 생성 또는 암호 변경 시 다음의 조건을 만족하도록 설정합니다.

- 암호는 복잡성을 만족해야하며, 최소 8자리 이상 설정되어야 한다.
- 최근 암호를 4자리까지 기억하여 암호의 재사용을 방지하도록 한다.
- 암호는 최소 1일 이상 사용되어야하며, 60일마다 변경되도록 한다.

2) 시스템 감사 정책

GW-SRV 서버에서 다음 이벤트들을 감사할 수 있도록 정책을 변경하도록 합니다.

- 시스템 시간 변경, 시스템 시작, 종료 등 시스템 관련 모든 이벤트 - 사용자 로그인 실패 이벤트 - 사용자 신규 생성 및 삭제, 패스워드 변경 성공 이벤트

다. 리눅스 시스템 보안

1) 계정 암호 정책

GL-SRV 서버에 신규 계정 생성 또는 암호 변경 시 다음의 조건을 만족하도록 설정합니다.

- 암호는 반드시 영어 대/소문자, 숫자, 특수문자를 포함하여야 한다. - 암호의 길이는 최소 8자리 이상을 만족하도록 한다. - 자신의 계정 이름이 포함된 패스워드를 사용할 수 없도록 한다. - 암호는 최소 1일 이상 사용되어야하며, 60일마다 변경되도록 한다.

2) 싱글 모드 접근 보안

제3자가 서버에 물리적으로 접근이 가능한 상태에서 싱글 모드를 통해 root 패스워드를 복구하고 불법으로 시스템에 침입하는 것을 방지하기 위해, 부팅 과정에서 부트 편집 메뉴 접근 시 아래의 계정을 통해 인증을 받을 수 있도록 설정합니다.

USERNAME: grubadmin **PASSWORD**: Global43!@

3) 외부 저장매체 접근 보안

GL-SRV 서버에 USB port를 통한 모든 외부 저장 매체의 접근을 원천 차단하도록 설정합니다.

4) sudo 보안 설정

현재 관리자는 시스템에 존재하는 gluser 계정을 통해 패스워드 입력 없이 sudo 명령을 통해 root 권한을 이용하고 있습니다.

해당 취약점을 보완하기 위해 오직 test01 계정만 패스워드 입력 후 sudo 명령을 사용할 수 있도록 수정하되, **시스템의 치명적인 영향을 줄 수 있는 몇 개의 명령어는 사용할 수 없도록 제한합니다.**

□ **A list of Commands**

alt, shutdown, reboot, poweroff, systemctl

5) 취약점 점검 스크립트 작성

리눅스 시스템의 보안 상태를 지속적으로 점검할 수 있도록 bash shell script를 작성합니다.

관리자가 root 계정으로 /root/check.sh 스크립트를 실행할 경우, 아래와 같은 3가지 항목을 검사하여 양호/취약 여부를 출력할 수 있도록 작성합니다.

선수는 반드시 과제에 주어진 출력 결과 예시를 참고하여 스크립트를 작성해야하며, **밑줄 친 부분을 제외한 나머지 문구는 선수 재량으로 수정하여도 무방합니다.**

□ **점검 항목**

1. 패스워드 파일 권한이 적절하게 부여되어 있는지?

=> other 권한에 쓰기 또는 실행 권한이 부여되어 있는 경우 취약한 것으로 판단

2. 해당 시스템에 라우팅 기능이 활성화되어 있는지?

3. SetUID, SetGID, Sticky bit가 설정된 파일들의 목록

□ **출력 결과**

```
**********************************************************************
                    시스템 취약점 점검을 실시합니다.
**********************************************************************
시작 시간 : Tue Apr 27 10:23:54 KST 2021

01. /etc/passwd 파일 권한 점검
    ===> [취약] 현재 권한 : -rw-r--rwx

안전한 경우
    ===> [양호] 현재 권한 : -rw-r--r--

02. 라우팅 기능 활성화 여부 점검
    ===> [취약] 라우팅 기능이 활성화 되어 있습니다.

안전한 경우
    ===> [양호] 라우팅 기능이 비활성화 되어 있습니다.

03. SetUID, SetGID, Sticky bit 권한이 설정된 파일을 검색하여 /root/file_list.txt에 저장합니다.
```

6) 로그 백업

/root/backup.sh 스크립트 실행 시 /var/log밑에 저장된 로그들이 **년-월-일-시:분:초-log.tar.gz** 형식으로 /backup 디렉터리에 저장되도록 합니다. 이 때, 처음 백업 명령을 실행했다면 기존 로그들이 **풀 백업(full backup)** 되어야 하며, 이후 두번째 실행부터는 기존 backup 파일과 비교하여 변경이 이루어진 부분만 백업될 수 있도록 **증분 백업(incremental backup)**을 구현합니다.

라. 네트워크 보안

1) 방화벽 구현

GR-SRV 서버에 사내 네트워크를 위한 방화벽을 구축하도록 합니다.
단, 방화벽을 구현하기 위한 소프트웨어는 반드시 ufw를 사용하도록 하며,
아래의 조건에 해당하는 방화벽 규칙들을 적용함으로써 사내 네트워크를 보호하도록 합니다.

□ **Firewall Rules**

- 모든 ICMP 통신은 허용
- Private → ServerFarm 네트워크 접근은 과제에서 제시된 모든 서비스 포트들만 허용 3. Adm-PC에서 GW-SRV로 LDAP port 허용
- Internet에서 접근하는 모든 트래픽 차단 **(단, ICMP는 허용)**
- SeverFarm -> Private 네트워크의 well-known port 접근은 모두 차단

2) 패킷 덤프 분석

현재 GL-SRV 서버에는 tcpdump 유틸리티를 통해 특정 패킷들을 덤프한 pktdump.log 파일이 저장되어 있습니다.
선수는 해당 파일에 기록된 패킷들을 분석하고, 보고서를 작성하여 /root/analysis-[비번호] 파일로 저장해놓도록 합니다. **이때, 반드시 아래의 형식을 준수하여 보고서를 작성해야합니다.**

[출발지 IP:PORT]	[목적지 IP:PORT]	[TCP/UDP 여부]	[프로토콜 이름]
ex) 192.12.35.1:49233	20.10.200.10:23	TCP	TELNET

패킷의 출발지 혹은 목적지 주소가 현재 시스템 내 존재하는 호스트인 경우에만 보고서에 포함하도록 하며, 중복된 패킷에 대해서는 하나만 작성하도록 합니다.
패킷 덤프 파일은 대회 당일날 제공되며, 분석할 패킷의 범주는 아래와 같습니다.

***Packet Category** : FTP, TELNET, SSH, TFTP, DHCP, HTTP, HTTPS, SMTP, IMAP

마. 어플리케이션 보안

1) SSH 서비스 보안

GL-SRV 서버에 SSH 서비스를 활성화하여 관리자가 원격으로 서버를 관리할 수 있도록합니다. **단, root 계정은 로그인이 불가능해야하며,** 관리자는 test01 계정을 통해 서버를 이용하되, 인증 수단은 패스워드가 아닌, **미리 생성해둔 키**를 통해 **패스워드 입력 없이 접속이 가능해야합니다.**

이를 위해 puttygen 프로그램을 실행하여 RSA key 한 쌍을 생성하고, 개인키는 Adm-PC 바탕화면에 **private-[비번호].ppk** 이름으로 미리 저장해놓도록 합니다.

또한 원활한 채점을 위해 Adm-PC 바탕화면에 putty.exe를 저장해두고, putty에서 미리 SSH세션 정보를 저장해놓도록 합니다.

2) 데이터베이스 보안

현재 GL-SRV 서버에는 **postgreSQL 10 기반**의 데이터베이스가 설치되어 운용되고 있습니다. 사용 중인 데이터베이스는 mydb이며, 테이블은 student이고, 소유자는 pgadmin 계정입니다.

관리자는 데이터베이스의 기본 포트를 11106으로 변경하고, 로컬이나 원격에서 데이터베이스에 접근 시 반드시 관리자 IP와 pgadmin 계정을 통해서만 접근이 가능하도록 보안 설정합니다.

또한, DB 내에서 수행되는 모든 쿼리는 모두 **var/lib/postgresql/10/main/my_log 밑에 postgresql-%Y-%m-%d_%H%M%S 형태**로 저장되도록하며, pgadmin외 다른 유저가 mydb에 접근하여 테이블을 생성할 수 없도록 public schema 권한을 조절하도록 합니다.

3) 이메일 서비스 보안

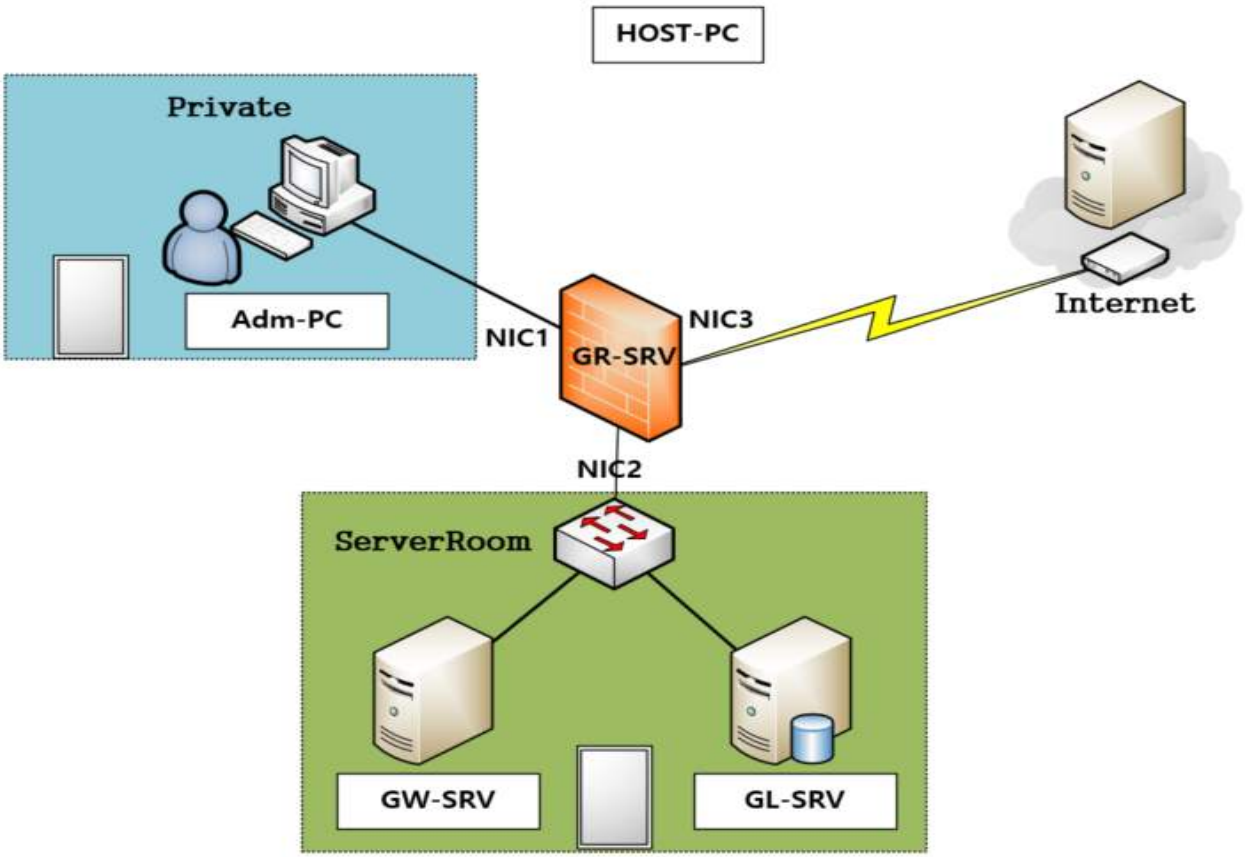
현재 GL-SRV 서버에는 **postfix + dovecot-imapd + squirrelmail 기반의 웹메일 서버**가 구축되어있습니다.

메일 사용자들은 최근 스팸 메일의 증가로 인해 어려움을 겪고 있으며, 따라서 관리자는 game, free, new 단어가 내용에 포함된 메일은 스팸 메일로 인지하여 사전에 차단 될 수 있도록 설정해야 합니다.(**이 문제를 해결하기 위해서, 별도의 패키지를 설치하지 않으며, 반드시 postfix만을 이용하도록 합니다.**)

테스트를 위해 해당 서버에는 미리 global01, global02 계정이 생성되어 있습니다. 웹 브라우저를 실행하고 http://mail.global.com/mail 주소로 접속한 뒤, 로그인을 수행하여 상호 메일 테스트를 진행하도록 합니다.

4. 도면 및 부록

가. 네트워크 구성도



나. 서브넷 할당

구분	네트워크	인터페이스	IP주소
Private	192.168.56.0/24	Gateway	192.168.56.1
		Adm-PC	192.168.56.200
ServerRoom	210.200.150.0/24	Gateway	210.200.150.1
		GW-SRV	210.200.150.50
		GL-SRV	210.200.150.100
Internet	30.30.30.0/24	Gateway	30.30.30.1
		Ext-SRV	30.30.30.100

다. 제공되는 DNS 레코드

Internal Zone	FQDN	IP Address
	gw-srv.global.com	210.200.150.50
	gl-srv.global.com	210.200.150.100
	mail.global.com	210.200.150.100
	remote.global.com	210.200.150.100

라. 운영체제 구성

☐ HOST-PC

OS	Windows 10 Pro 64bit
컴퓨터 이름	HOST-PC
추가 사용자	-
Administrator 암호	Global43@!
가상 머신 설치 경로	D:₩Cyber-비번호

☐ Adm-PC

OS	Windows 10 Pro 64bit
컴퓨터 이름	Adm-PC
추가 사용자	user
Administrator 암호	-
가상 머신 설치 경로	D:₩Cyber-비번호
기타	윈도우 방화벽 비활성화. telnet client 서비스 활성화

☐ GW-SRV

OS	Windows Server 2019 Desktop
파티션	C:₩ - 40G, D:₩ - 20G
호스트 이름	GW-SRV
추가 사용자	gwuser
Administrator 암호	Global43@!
기타	윈도우 방화벽 비활성화. Active Directory 서비스 설치

☐ GR-SRV

OS	GNU/LNX Ubuntu 18.04.5 LTS Server
파티션	/ - 18G xfs, /boot - 2G ext4 swap - 2G
컴퓨터 이름	GR-SRV
추가 사용자	gruser
root 암호	Global43@!

☐ GL-SRV

OS	GNU/LNX Ubuntu 18.04.5 LTS Desktop
파티션	/ - 20G xfs, /boot - 2G ext4, swap - 2G
호스트 이름	GL-SRV
추가 사용자	gluser
root 암호	Global43@!
기타	X-Windows 설치 x

☐ Ext-SRV

OS	GNU/LNX Ubuntu 18.04.5 LTS Server
파티션	/ - 18G xfs, /boot - 2G ext4, swap - 2G
호스트 이름	Ext-SRV
추가 사용자	user
root 암호	Global43@!
기타	X-window 설치 x