

DVWA 모의해킹 실습 서버 구축

Rocky Linux + Apache + MariaDB + PHP | Bridged IP | 발표자용 큐시트

실습 VM 스펙	하드 20GB / RAM 1GB / NIC: Bridged / Rocky Linux 최소 설치 권장
발표 목표	DVWA를 웹 서버에 올리고, DB를 초기화한 뒤 Kali 또는 호스트 브라우저에서 접속 가능한 샌드박스를 완성한다.
핵심 메시지	APM 설치 → DB 계정 분리 → 웹 루트 배치 → 권한/SELinux/firewalld 정리 → setup.php에서 DB 생성 → Low 보안 레벨 설정

발표 첫 멘트

"오늘은 공격 실습 자체보다, 의도적으로 취약한 웹 애플리케이션 DVWA를 안전한 내부 실습망에 구축하는 과정을 보여드리겠습니다. 이 환경은 공개 서버가 아니라 학습용 샌드박스입니다."

절대 주의

Bridged는 VM이 실제 네트워크에 노출될 수 있다는 뜻입니다. 공유기/학교/회사망에서 공인 IP, 포트포워딩, 인터넷 공개는 금지하고, 발표 후에는 스냅샷 복구 또는 서비스 중지를 권장합니다.

1. 전체 흐름 - 발표 중 이 페이지를 기준으로 진행

각 단계는 앞 단계의 결과를 다음 단계가 사용합니다. 발표할 때는 '왜 지금 이 명령을 치는가'를 한 문장씩 붙이면 자연스럽습니다.

0 VM/네트워크
20GB, 1GB, Bridged + 수동 IP

1 APM 설치
httpd + mariadb + php + git

2 서비스 시작
systemctl enable --now

3 DB 보안 초기화
root 비번, 불필요 계정/DB 제거

4 DVWA DB 생성
dvwa DB + dvwa_user

5 소스 배치
/var/www/html/dvwa

6 설정 연결
config.inc.php에 DB 계정 입력

7 권한/SELinux/방화벽
apache 소유권, firewalld http

8 웹에서 마무리
setup.php → 로그인 → Low

네트워크 구조도

호스트 PC/Kali 브라우저 → 같은 LAN/Bridged → Rocky Linux VM:80 → Apache DocumentRoot → /var/www/html/dvwa → MariaDB(dvwa DB)

한 줄 핵심

웹은 80번 포트로 들어오고, Apache는 PHP 코드를 실행하며, PHP는 MariaDB의 dvwa 데이터베이스를 사용합니다. 우리는 이 연결 고리를 하나씩 만든 뒤 setup.php에서 DB 테이블을 생성합니다.

2. 네트워크 준비 - Bridged + 수동 IP

말할 포인트

- Bridged는 VM이 공유기/스위치에 직접 연결된 별도 PC처럼 동작한다는 뜻입니다.
- Kali나 호스트 PC가 같은 대역에 있으면 http://Rocky_IP/dvwa 로 직접 접근할 수 있습니다.
- 수동 IP는 발표 중 주소가 바뀌지 않게 만드는 장치입니다.
- IP 충돌을 피하려면 공유기 DHCP 범위 밖의 빈 주소를 사용합니다.

비유

공유기라는 건물 안에 호스트 PC, Kali, Rocky VM이 각각 방을 하나씩 얻는 구조입니다. Bridged를 쓰면 Rocky VM도 자기 방 번호(IP)를 갖습니다.

확인/설정 명령

```
# 현재 인터페이스와 IP 확인
ip -br addr
ip route

# GUI 없이 편하게 수동 IP 설정: nmtui 사용
sudo nmtui
# Edit a connection → IPv4 CONFIGURATION: Manual
# Address/Gateway/DNS 입력 → Activate a connection

# nmcli로 설정하는 경우: 값은 본인 네트워크에 맞게 변경
nmcli con show
sudo nmcli con mod "<CONNECTION_NAME>" \
  ipv4.addresses 192.168.0.50/24 \
  ipv4.gateway 192.168.0.1 \
  ipv4.dns "8.8.8.8 1.1.1.1" \
  ipv4.method manual
sudo nmcli con up "<CONNECTION_NAME>"

# 연결 확인
ping -c 3 192.168.0.1
ping -c 3 google.com
```

체크 항목	정상 상태	문제 시 확인
IP	192.168.x.x 같은 LAN 주소가 보임	VM 네트워크 어댑터가 Bridged인지, 중복 IP가 아닌지 확인
Gateway	ip route에 default via가 있음	수동 IP 설정에서 gateway 누락 여부 확인
DNS	도메인 ping 가능	DNS 주소 입력, 또는 /etc/resolv.conf 확인

3. APM 설치와 서비스 시작

발표 설명

- APM은 Apache + PHP + MariaDB의 묶음입니다. Apache가 HTTP 요청을 받고, PHP가 DVWA 코드를 실행하고, MariaDB가 데이터를 저장합니다.
- Rocky Linux 계열은 apt가 아니라 dnf를 사용합니다.
- 1GB RAM 환경에서는 GUI보다 최소 설치가 안정적이고, update 시간이 다소 걸릴 수 있습니다.
- enable --now는 '부팅 시 자동 실행 등록'과 '지금 즉시 실행'을 한 번에 처리합니다.

패킷 흐름

브라우저 → TCP/80 → httpd(Apache) → PHP 모듈/프로세스 → DVWA 코드 → MariaDB

명령어

```
# 1. 시스템 패키지 최신화 및 APM 설치
sudo dnf update -y
sudo dnf install -y httpd mariadb-server php php-mysqlnd \
  php-gd php-json php-mbstring git nano

# 2. 서비스 부팅 시 자동 실행 및 즉시 가동
sudo systemctl enable --now httpd
sudo systemctl enable --now mariadb

# 상태 확인
systemctl status httpd mariadb --no-pager
php -v
ss -lntp | grep ':80'
```

발표 중 실수 방지

명령어에 vim이 등장하지만 설치 목록에는 nano가 있습니다. 발표 때는 `sudo nano config.inc.php`를 쓰거나, vim을 쓰려면 `sudo dnf install -y vim`을 먼저 추가하세요.

4. MariaDB 초기화와 DVWA 전용 DB 계정 생성

개념 설명

- DB root는 데이터베이스의 최고 관리자입니다. 웹 앱이 root로 접속하면 위험하므로 별도 계정 (dvwa_user)을 만듭니다.
- dvwa_user는 dvwa 데이터베이스에만 권한을 갖게 합니다. 이것이 최소 권한 원칙입니다.
- mysql_secure_installation은 익명 사용자, 테스트 DB, 원격 root 로그인 같은 불필요한 기본 설정을 정리하는 절차입니다.
- 질문 문구는 MariaDB 버전에 따라 조금 다를 수 있으므로 목표를 기억하세요: root 비번 설정, 불필요 항목 제거, 권한 테이블 재로딩.

mysql_secure_installation 응답 큐

초기 비밀번호는 없으므로 Enter → unix_socket 인증은 실습 편의상 끄기/비활성화 방향 → root 비밀번호 설정 → anonymous user 제거 → remote root login 금지 → test DB 제거 → privilege reload

명령어

```
# 3. DB 초기 설정
sudo mysql_secure_installation
# 초기 비번 없으니 Enter
# 유닉스 소켓 인증은 실습 편의상 끄기/비활성화 방향
# root 비번 설정 → 이후 보안 질문은 전부 y 방향

# 4. 테이블/계정 생성
sudo mysql -u root -p

CREATE DATABASE dvwa;
CREATE USER 'dvwa_user'@'localhost' IDENTIFIED BY 'password123';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa_user'@'localhost';
FLUSH PRIVILEGES;
EXIT;

# 접속 테스트
mysql -u dvwa_user -p dvwa
# password123 입력 후 접속되면 OK
```

발표 질문	답변 키워드
왜 DB 계정을 따로 만드나요?	웹 앱이 침해되어도 DB 전체/root 권한으로 번지는 것을 줄이기 위해서입니다.
왜 localhost인가요?	DVWA와 DB가 같은 VM 안에 있으므로 외부 DB 접속을 열 필요가 없습니다.
password123은 안전한가요?	실습용 예시입니다. 운영 환경에서는 절대 사용하면 안 됩니다.

5. DVWA 설치와 DB 설정 연결

개념 설명

- /var/www/html은 Rocky/RHEL 계열 Apache의 기본 웹 루트입니다. 여기에 dvwa 폴더를 두면 /dvwa 경로로 접근할 수 있습니다.
- config.inc.php는 DVWA가 MariaDB에 접속할 때 사용할 DB 이름, 사용자, 비밀번호를 저장합니다.
- GitHub에서 받은 config.inc.php.dist는 예시 파일이므로 실제 config.inc.php로 복사한 뒤 수정합니다.
- config 파일 수정 후 오류가 나면 DB 사용자/비밀번호/DB 이름의 오타를 가장 먼저 의심합니다.

웹 경로 대응

파일 경로: /var/www/html/dvwa/setup.php
브라우저 URL: http://Rocky_IP/dvwa/setup.php

명령어

```
# 5. DVWA 설치
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git
sudo mv DVWA dvwa
cd /var/www/html/dvwa/config
sudo cp config.inc.php.dist config.inc.php

# 6. DVWA 설정
sudo nano config.inc.php
# 또는 sudo vim config.inc.php

# 아래 두 줄을 수정
$_DVWA[ 'db_user' ] = 'dvwa_user';
$_DVWA[ 'db_password' ] = 'password123';

# 참고: 저장 후 빠져나오기
# nano: Ctrl+O → Enter → Ctrl+X
# vim : Esc → :wq → Enter
```

발표 멘트

"여기까지는 웹 애플리케이션 파일을 웹 서버의 문서 루트에 올리고, 그 애플리케이션이 사용할 데이터베이스 접속 정보를 입력하는 단계입니다."

6. 로그 파일, 권한, SELinux, firewalld 정리

왜 필요한가

명령어

항목	역할
소유권 chown	Apache 프로세스 사용자인 apache가 DVWA 파일을 읽고 필요한 일부 파일을 쓸 수 있게 함
chmod	디렉터리는 진입/목록 권한, 파일은 읽기 권한 중심으로 정리
SELinux	파일 라벨과 웹 프로세스 권한을 강제하는 리눅스 보안 계층
firewalld	외부에서 80번 HTTP 포트로 들어오는 것을 허용

777 주의

phpids_log.txt에 777을 주는 것은 실습 편의용입니다. 운영 환경에서는 필요한 계정/그룹에 만 쓰기 권한을 주는 방식으로 줄여야 합니다.

```
# 7. 로그파일 생성
sudo mkdir -p /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/
sudo touch /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt
sudo chmod 777 /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt

# 8. 권한, SELinux, 방화벽 설정
sudo chown -R apache:apache /var/www/html/dvwa
sudo find /var/www/html/dvwa -type d -exec chmod 755 {} \;
sudo find /var/www/html/dvwa -type f -exec chmod 644 {} \;
sudo setsebool -P httpd_can_network_connect 1
sudo setsebool -P httpd_unified 1
sudo restorecon -v -R /var/www/html/dvwa
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --reload
sudo systemctl restart httpd
```

확인 명령	정상 예시
sudo firewall-cmd --list-services	http가 포함되어 있음
ls -ld /var/www/html/dvwa	소유자/그룹이 apache apache
getenforce	Enforcing이어도 설정 후 정상 접근 가능해야 함

7. 브라우저에서 DB 생성, 로그인, Low 레벨 변경

접속 흐름

발표용 단계별 대본

URL	화면	말할 내용
http://[Rocky_Linux_IP_주소]/dvwa/setup.php	setup.php	이 페이지는 DVWA가 사용할 테이블과 기본 데이터를 DB에 생성합니다.
	Create / Reset Database	앞에서 만든 dvwa DB와 dvwa_user 접속 정보가 맞아야 성공합니다.
	login.php	기본 관리자 계정으로 들어갑니다. 이 계정은 실습용 기본값입니다.
	DVWA Security	Impossible은 방어가 적용된 상태, Low는 원리를 보기 쉬운 취약 상태입니다.
	완료 화면	이제 Kali에서 Burp, Nmap, 브라우저로 합법적인 로컬 실습이 가능합니다.

- Kali 또는 호스트 PC 브라우저에서 접속합니다.
- setup.php 맨 아래 [Create / Reset Database]를 클릭합니다.
- 성공하면 login.php로 이동합니다.
- 초기 계정: admin / password
- 좌측 [DVWA Security]에서 Impossible → Low로 바꾸고 Submit합니다.

Low로 바꾸는 이유

DVWA는 보안 레벨별로 같은 취약점의 방어 강도를 바꿉니다. Low는 입문자가 원리를 관찰하기 쉬운 상태입니다. 실습이 끝나면 VM을 끄거나 네트워크를 격리하세요.

화면이 안 열릴 때 첫 3개

1) Rocky IP가 맞는지 `ip -br a` 확인 → 2) httpd가 켜졌는지 `systemctl status httpd` 확인 → 3) 방화벽에 http가 열렸는지 `firewall-cmd --list-services` 확인

8. 발표 당일 데모 순서 - 5분/10분 버전

5분 압축 버전

- 1 VM 스펙과 Bridged IP를 보여줍니다: ``ip -br a``.
- 2 APM 서비스가 살아있는지 확인합니다: ``systemctl status httpd mariadb --no-pager``.
- 3 Apache가 80번 포트를 듣는지 확인합니다: ``ss -lntp | grep ':80'``.
- 4 브라우저에서 setup.php 접속 후 Create / Reset Database 클릭.
- 5 admin/password 로그인 후 DVWA Security를 Low로 변경.
- 6 마지막으로 '교육용 취약 앱이므로 격리 환경에서만 사용'을 강조합니다.

5분 핵심 멘트

"서버 구성 자체는 평범한 APM 웹 서버입니다. 차이는 DVWA가 의도적으로 취약한 앱이라는 점이고, 그래서 네트워크 격리와 Low 설정의 의미를 이해하는 것이 중요합니다."

10분 상세 버전

- 1 Bridged와 수동 IP의 의미를 설명합니다: VM이 같은 LAN에 보이는 독립 호스트.
- 2 dnf 설치 명령에서 httpd/mariadb/php/git/nano의 역할을 짚습니다.
- 3 mysql_secure_installation의 목적을 말합니다: 기본 위험 설정 제거.
- 4 DB root 대신 dwwa_user를 만드는 이유를 설명합니다: 최소 권한.
- 5 DocumentRoot와 /dwa URL 매핑을 보여줍니다.
- 6 SELinux/firewalld가 왜 웹 접속을 막을 수도 있는지 설명합니다.
- 7 setup.php → login.php → Low 순서로 화면을 보여줍니다.
- 8 트러블슈팅 표를 마지막 백업 페이지로 둡니다.

발표 중 시간 부족 시

DB 생성과 config 수정은 미리 끝내두고, 발표에서는 `ip` 확인 → 서비스 상태 → 브라우저 setup/login → Low 변경만 보여줘도 흐름은 전달됩니다.

9. 트러블슈팅 치트시트

증상	흔한 원인	바로 확인할 명령/조치
브라우저 접속 불가	IP 오타, Bridged 미적용, httpd 중지, firewalld 차단	ip -br a systemctl status httpd sudo firewall-cmd --list-services curl -I http://localhost
403 Forbidden	파일 권한/SELinux 라벨 문제	ls -ld /var/www/html/dvwa sudo restorecon -v -R /var/www/html/dvwa sudo systemctl restart httpd
PHP 코드가 그대로 보임	PHP 패키지/연동 문제 또는 httpd 재시작 누락	php -v rpm -qa grep php sudo systemctl restart httpd
DB 연결 실패	config.inc.php의 사용자/비번/DB명 오타	sudo nano /var/www/html/dvwa/config/config.inc.php mysql -u dvwa_user -p dvwa
Create DB 실패	DB 권한 부족, MariaDB 중지, config 불일치	systemctl status mariadb SHOW GRANTS FOR 'dvwa_user'@'localhost';
git clone 실패	DNS/인터넷 연결 문제	ping -c 3 google.com ping -c 3 github.com ip route
Low 변경 안 됨	세션/쿠키 문제 또는 DB 초기화 미완료	로그아웃 후 재로그인 setup.php에서 Reset 재시도
SELinux 의심	웹 접근은 되지만 일부 쓰기/연결 실패	getenforce sudo ausearch -m avc -ts recent tail

발표 중 문제 발생 시 대처 멘트

"실습 서버 구축은 네트워크, 웹 서버, DB, 리눅스 보안 정책이 모두 연결되기 때문에 한 군데만 어긋나도 접속이 실패합니다. 그래서 증상별로 IP → 서비스 → 방화벽 → 권한 → DB 순서로 좁혀갑니다."

10. 명령어 통합판 - 발표 전 체크용

아래는 전체 흐름을 한 번에 훑기 위한 페이지입니다. 발표 중에는 세부 설명 페이지를 보고, 리허설 전에는 이 페이지로 누락을 확인하세요.

```
# 0. 네트워크 확인
ip -br addr
ip route

# 1. 시스템 패키지 최신화 및 APM 설치
sudo dnf update -y
sudo dnf install -y httpd mariadb-server php php-mysqlnd \
  php-gd php-json php-mbstring git nano

# 2. 서비스 부팅 시 자동 실행 및 즉시 가동
sudo systemctl enable --now httpd
sudo systemctl enable --now mariadb
systemctl status httpd mariadb --no-pager

# 3. DB 초기설정
sudo mysql_secure_installation

# 4. DB/계정 생성
sudo mysql -u root -p
CREATE DATABASE dvwa;
CREATE USER 'dvwa_user'@'localhost' IDENTIFIED BY 'password123';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa_user'@'localhost';
FLUSH PRIVILEGES;
EXIT;

# 5. DVWA 설치
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git
sudo mv DVWA dvwa
cd /var/www/html/dvwa/config
sudo cp config.inc.php.dist config.inc.php
sudo nano config.inc.php
# db_user = dvwa_user, db_password = password123

# 7~8. 로그/권한/SELinux/방화벽
sudo mkdir -p /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/
sudo touch /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt
sudo chmod 777 /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt
sudo chown -R apache:apache /var/www/html/dvwa
sudo find /var/www/html/dvwa -type d -exec chmod 755 {} \;
sudo find /var/www/html/dvwa -type f -exec chmod 644 {} \;
sudo setsebool -P httpd_can_network_connect 1
sudo setsebool -P httpd_unified 1
sudo restorecon -v -R /var/www/html/dvwa
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --reload
sudo systemctl restart httpd
```

웹 마무리

브라우저: [http://\[Rocky_Linux_IP_주소\]/dvwa/setup.php](http://[Rocky_Linux_IP_주소]/dvwa/setup.php) → Create / Reset Database → admin / password 로그인 → DVWA Security → Low → Submit

11. 실습 후 정리와 보안 주의

왜 정리가 필요한가

- DVWA Low는 취약점이 의도적으로 노출된 상태입니다.
- Bridged 네트워크에서는 같은 LAN의 다른 장비도 접근할 수 있습니다.
- 발표 후에는 VM 스냅샷으로 되돌리거나, httpd/mariadb를 중지하고 방화벽에서 http를 제거하세요.
- 학교/회사망에서는 담당자 허가 없이 취약 서버를 열어두지 않습니다.

좋은 마무리 멘트

"오늘 만든 환경은 공격 대상이 아니라 학습 대상입니다. 보안을 배우는 목적은 취약점을 이해해서 안전하게 고치기 위한 것입니다."

정리 명령

```
# 발표 후 서비스 중지
sudo systemctl stop httpd mariadb

# 부팅 자동 실행 해제
sudo systemctl disable httpd mariadb

# 방화벽에서 HTTP 제거
sudo firewall-cmd --permanent --remove-service=http
sudo firewall-cmd --reload
sudo firewall-cmd --list-services

# 필요 시 VM 스냅샷 복구 또는 네트워크 어댑터를 NAT/Host-only로 변경
```

항목	권장
수업/발표 전	스냅샷 생성
발표 중	사설망/허가된 망에서만 접속
발표 후	서비스 중지 또는 스냅샷 복구
운영망	DVWA 배치 금지

끝. 발표 중 막히면 9쪽 트러블슈팅에서 IP → 서비스 → 방화벽 → 권한/SELinux → DB 순서로 좁혀가세요.