Task 5

DVWA Capstone — Essential Commands

Short list of necessary commands for setup, testing, evidence, and containment

A. Prep — Target (DVWA + MariaDB)

Essential: install webserver, PHP, MariaDB, create DVWA DB, install DVWA, restart services.

Commands (run on target VM):

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y apache2 php php-mysqli git unzip curl mariadb-server
sudo systemctl enable --now mariadb apache2
# Create DB & user (non-interactive)
sudo mariadb -e "CREATE DATABASE IF NOT EXISTS dvwa; CREATE USER IF NOT EXISTS
'dvwa'@'localhost' IDENTIFIED BY 'dvwa'; GRANT ALL PRIVILEGES ON dvwa.* TO
'dvwa'@'localhost';
FLUSH PRIVILEGES;"
# Install DVWA
cd /var/www/html && sudo git clone https://github.com/digininja/DVWA.git && sudo chown -R
www-
data:www-data DVWA
# Open http://<target-ip>/DVWA/setup.php and click Create / Reset Database
```

B. Attacker — Key Tools

Install only required tools (attacker VM):

```
sudo apt update
sudo apt install -y nmap gobuster sqlmap tcpdump
# Optional for analysis: wireshark, burpsuite (download separately)
```

C. Recon (attacker)

Quick, essential scans (replace <target-ip>):

```
nmap -sV -p80,443 -T4 <target-ip> -oN quick_nmap.txt
curl -I http://<target-ip>/DVWA/ | sed -n '1,8p'
gobuster dir -u http://<target-ip>/DVWA/ -w /usr/share/wordlists/dirb/common.txt -o
gobuster.txt
```

D. Proof-of-Concept Exploit (DVWA only)

Manual check (browser): on DVWA SQLi page enter: ' OR '1'='1

Automated (sqlmap) — replace PHPSESSID and use only on DVWA:

```
sqlmap -u "http://<target-ip>/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="security=low; PHPSESSID=<PHPSESSID>" --batch --level=2
```

E. Evidence Collection (minimal)

Capture network traffic and save web logs (preserve before changing system):

```
# On attacker (start capture)
sudo tcpdump -i eth0 host <target-ip> and host <attacker-ip> -w /tmp/attack_capture.pcap &
echo
$! > /tmp/tcpdump.pid
```

Task 5

```
# After exploit, stop capture
sudo kill $(cat /tmp/tcpdump.pid) 2>/dev/null || sudo pkill -f "tcpdump"
# On target (collect logs)
mkdir -p ~/evidence && sudo cp /var/log/apache2/access.log /var/log/apache2/error.log
~/evidence/ || true
cd ~/evidence && tar czvf evidence_$(date +%F_%T).tar.gz access.log error.log
/tmp/attack_capture.pcap 2>/dev/null || true
sha256sum *.tar.gz > evidence_checksums.sha256
```

F. Containment (after evidence saved)
Block attacker IP or stop service (choose one; preserve evidence first):

```
# Block IP (temporary)
sudo iptables -A INPUT -s <attacker-ip> -j DROP
# Or stop web service
sudo systemctl stop apache2
# To undo block: sudo iptables -D INPUT -s <attacker-ip> -j DROP
```