Ethical Hacking 1 — Final Submission (Mock Data)

Prepared for: Course Final Submission (Mock)

Environment: macOS Host (MacBook) running Parrot OS as a guest VM inside UTM. All testing performed in an isolated local lab network (Host-only + NAT where indicated). **All targets and IPs below are fictional/mock lab assets.**

Table of Contents

---

1. Environment Setup & Tools

Host: MacBook Pro (macOS 14.4) — UTM virtualization.

Guest (Attacker): Parrot Security OS 5.2 (installed in UTM) — `parrot-attacker` VM

Targets (Lab VMs):

* `lab-target-1` (Metasploitable2 mock) — 192.168.56.102
* `lab-web` (DVWA mock) — 192.168.56.103
* `lab-db` (MySQL mock) — 192.168.56.104

Network topologies used:

* UTM Host-only network: 192.168.56.0/24 (isolated between host and guest VMs)
* NAT for limited outbound updates only (attacker restricted to lab-hosted targets)

Tools installed on Parrot OS (mock evidence):

* Nmap v7.93 — `sudo apt install nmap` (Screenshot placeholder: `![screenshot: nmap-install.png]`)
* Wireshark 4.0 — `sudo apt install wireshark` and non-root capture configured (screenshot placeholder: `![screenshot: wireshark-perms.png]`)
* Metasploit Framework v6.x — `sudo apt install metasploit-framework` (screenshot placeholder)
* theHarvester — `sudo apt install theharvester` (screenshot placeholder)
* Nessus Essentials (configured on separate VM for scanning) — (screenshot placeholder)
* OWASP ZAP & Burp Suite Community — (screenshots placeholders)

Evidence of installations & basic functionality tests (mock):

* Nmap test: `nmap -v -sS 127.0.0.1` → output: `1 host up (0.0010s latency)` (screenshot placeholder)
* Wireshark test: captured host DNS query on `ut0` interface (screenshot placeholder)
* Metasploit test: `msfconsole` loads and shows banner (screenshot placeholder)

> NOTE: All screenshots in the final deliverable should be replaced with real captures from your actual lab.

---

2. Information Gathering & Reconnaissance (Passive + Active)

2.1 Scope & Ethics

* **Scope:** `lab-target-1`, `lab-web`, `lab-db` — private lab IPs only.
* **Authorization:** These are owned lab VMs. No external scanning performed.

2.2 Passive Recon (OSINT) — Mock Methodology & Findings

Tools & methods: theHarvester, Google dorking (offline mock), certificate transparency search (mock), OSINT Framework notes.

Example theHarvester command (mock):

```
theharvester -d example-lab.local -b all -l 500
```

Mock results (excerpt):

* Emails found: `admin@example-lab.local`, `devops@example-lab.local`
* Subdomains: `vpn.example-lab.local`, `dev.example-lab.local`, `web.example-lab.local`
* Linked public code references: `gitlab.example-lab.local/repos/projectX`

Documented sources: screenshots saved as `osint_theharvester_example.png`, saved CSV `theharvester_example.csv`.

2.3 Active Recon — Nmap Network Mapping

Nmap commands (mock):

* Ping scan to discover live hosts:

```
nmap -sn 192.168.56.0/24
```

Mock output (discovered hosts):

* 192.168.56.1 — UTM host
* 192.168.56.102 — lab-target-1 (up)
* 192.168.56.103 — lab-web (up)
* 192.168.56.104 — lab-db (up)

Saved evidence: `nmap_ping_scan.png`, `nmap_ping_scan.txt`.

Target profile created (see Section 4).

---

3. Scanning & Enumeration

3.1 Nmap Multi-Method Scanning (TCP, UDP, Service)

Target: 192.168.56.102 (lab-target-1) — mock

TCP SYN scan (full port range) — command:

```
nmap -sS -p1-65535 -T4 -oN nmap_tcp_full_192.168.56.102.txt 192.168.56.102
```

Mock important output (excerpt):

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
```

UDP scan (top 100 ports) — command:

```
nmap -sU --top-ports 100 -T3 -oN nmap_udp_top_192.168.56.102.txt 192.168.56.102
```

Mock UDP findings (excerpt):

```
53/udp  open  domain
123/udp open  ntp
161/udp open  snmp
```

Service/version detection:

```
nmap -sV -sC -p21,22,80,139,445,3306 192.168.56.102 -oN nmap_service_enum.txt
```

Mock output (excerpt):

```
21/tcp  ftp     vsftpd 2.3.4
22/tcp  ssh     OpenSSH 7.2p2
80/tcp  http    Apache httpd 2.4.18
3306/tcp mysql   MySQL 5.7.21
```

Screenshots & raw output files: `nmap_tcp_full_192.168.56.102.txt`, `nmap_service_enum.png`.

3.2 Service Enumeration Methods

Banner grabbing examples (Netcat):

```
nc -v 192.168.56.102 21
```

Mock banner: `220 (vsFTPd 2.3.4)` (evidence saved)

Nmap NSE scripts for further enumeration:

```
nmap -p 21 --script ftp-anon,ftp-vsftpd-backdoor 192.168.56.102 -oN nmap_ftp_nse.txt
```

Mock NSE finding: `vsftpd backdoor present (port 21)` (screenshot placeholder)

---

4. Vulnerability Analysis & Target Profile

4.1 Target Profile (Standard Template) — lab-target-1 (mock)

General:

* Hostname: `lab-target-1`
* IP: `192.168.56.102`
* MAC: `02:42:ac:38:00:66` (mock)
* Network: `192.168.56.0/24` (host-only)

Open Ports & Services:

Port	Protocol	Service	Version
21	TCP	FTP	vsftpd 2.3.4
22	TCP	SSH	OpenSSH 7.2p2
23	TCP	Telnet	telnetd (mock)
80	TCP	HTTP	Apache 2.4.18
3306	TCP	MySQL	5.7.21

OS Fingerprint (Nmap -O): Linux (Ubuntu 14.04-like) — mock

Personnel / Contacts (OSINT): admin@example-lab.local (mock)

Certificates / Web tech: Apache, PHP 5.6 (mock), CMS: none (lab app DVWA on separate host)

4.2 Vulnerability Scan Summary (Nessus Essentials — Mock Report)

Scan scope: 192.168.56.102 (authenticated scan disabled for this mock)

Top findings (mocked) — at least 3 vulnerabilities documented:

1. **CVE-2011-5539 — vsftpd 2.3.4 backdoor**

   * **Risk level:** High
   * **Description:** Backdoor in vsftpd 2.3.4 allows remote command execution when a crafted username is used.
   * **Potential impact:** Remote code execution, full system compromise.
   * **Recommendation:** Upgrade vsftpd to a patched version or remove vsftpd if not