BBC BANK UGANDA LIMITED

Information Security and Auditing (BUC3126) Capstone

VAPT LAB GUIDE

Area 9: Vulnerability Assessment and Penetration Testing

1. Purpose and Context

The Board Audit and Risk Committee wants assurance that the servers exposed in the BBC Bank network perimeter are hardened. As part of the audit, your team performs a vulnerability assessment and penetration test (VAPT) against a representative server in the bank's demilitarised zone (DMZ).

Important framing. The target VM is a generic Linux server that stands in for a DMZ host at BBC Bank. It is NOT the Finacle core banking application, which is never exposed for direct testing. Treat your findings as indicative of the bank's server hardening and patch management, and link them to the wider audit (for example, weak password and patch controls seen elsewhere in the evidence).

2. Rules of Engagement (read before you start)

- **Authorised target only.** You may scan and exploit ONLY the provided vulnerable VM on your own machine. Testing any other system, network, website or person is illegal under the Computer Misuse Act, 2011 (as amended, 2022) and will earn zero marks and disciplinary action.
- **Isolated network only.** The target must run on a Host-Only or Internal network. It must never touch the campus network or the internet. Configure this before you power the target on.
- **Sign the authorisation.** Complete the Authorisation to Test statement in Appendix A and include it in your report. In real audits, testing without written authorisation is itself a serious finding.
- **Do no harm beyond scope.** Do not attempt denial-of-service that could corrupt the VM before you have finished evidence gathering. Snapshot the VM first.
- **Evidence discipline.** Save all scan outputs and screenshots with timestamps. These go into your working-papers ZIP.

3. What You Will Build

A small two-machine lab that runs entirely offline on one laptop:

Machine	Role	Login
Kali Linux	Attacker (your tools)	kali / kali
Metasploitable 2	Target (BBC DMZ server)	msfadmin / msfadmin
Network	VirtualBox Host-Only adapter	Isolated, no internet

Minimum hardware: a 64-bit laptop with virtualization enabled in BIOS, 8 GB RAM (4 GB works if you give Kali 2.5 GB and the target 512 MB), and about 30 GB free disk. If your machine cannot run both, pair up with a group member whose machine can, or use a lab PC.

4. Download the Tools (all free)

Download these once, ideally on campus wifi, then work offline. Verify the checksum where one is provided.

Tool	Purpose	Official download
Oracle VirtualBox	Runs the virtual machines	virtualbox.org/wiki/Downloads
Kali Linux (VirtualBox image)	Attacker box with tools preinstalled	kali.org/get-kali (Virtual Machines)
Metasploitable 2	The vulnerable target VM	sourceforge.net/projects/metasploitable
OWASP Juice Shop (optional)	Vulnerable web app (internet banking angle)	owasp.org/www-project-juice-shop

Direct links:

- Oracle VirtualBox https://www.virtualbox.org/wiki/Downloads
- Kali Linux (prebuilt VM) https://www.kali.org/get-kali/#kali-virtual-machines
- Metasploitable 2 (SourceForge, Rapid7) https://sourceforge.net/projects/metasploitable/
- OWASP Juice Shop https://owasp.org/www-project-juice-shop/

Tools you will use on Kali (already installed): Nmap, OpenVAS/Greenbone or Nessus Essentials, Metasploit Framework, Nikto, dirb/gobuster, Hydra, John the Ripper, Wireshark.

5. Build the Lab, Step by Step

5.1 Install VirtualBox and import Kali

1. Install VirtualBox on your laptop and reboot.
2. Import the Kali VirtualBox image (File > Import Appliance), give it 2.5 to 4 GB RAM, and start it. Log in with kali / kali.

5.2 Import the target

3. Unzip the Metasploitable 2 download. You will get a folder with a .vmdk disk.
4. In VirtualBox, create a new VM: type Linux, version Ubuntu (64-bit or 32-bit). At the disk step, choose "Use an existing virtual hard disk file" and select Metasploitable.vmdk.
5. Do NOT power it on yet. First set the network (5.3).

5.3 Isolate the network (critical)

6. For BOTH VMs, open Settings > Network > Adapter 1 and set "Attached to: Host-Only Adapter" (vboxnet0). Create the host-only network first under File > Tools > Network Manager if none exists.
7. Confirm neither VM has a NAT or Bridged adapter enabled. This keeps the vulnerable box off the internet and off the campus LAN.
8. Power on both VMs. On the target, log in msfadmin / msfadmin.

5.4 Confirm connectivity

9. On the target, run ifconfig and note its IP (for example 192.168.56.101).
10. On Kali, run ip a to see your IP on the same host-only subnet, then ping the target.

```
msfadmin@metasploitable:~$ ifconfig
eth0  inet addr:192.168.56.101  Mask:255.255.255.0

kali@kali:~$ ping -c3 192.168.56.101
```

11. Snapshot both VMs now (Machine > Take Snapshot) so you can roll back after exploitation.

6. VAPT Methodology

Follow a recognised methodology. This guide uses the phases of NIST SP 800-115 and the Penetration Testing Execution Standard (PTES). Document each phase.

Phase	What you do	Primary tools
1. Planning and scoping	Define target, rules, authorisation	Appendix A
2. Discovery	Host and port discovery, service and version enumeration	Nmap
3. Vulnerability assessment	Automated scan, rank findings by CVSS	OpenVAS / Nessus, Nikto
4. Exploitation	Safely confirm selected vulnerabilities	Metasploit, Hydra
5. Post-exploitation	Show business impact (data access, privilege)	Kali shell
6. Reporting	CVSS-rated findings, business impact, remediation	VAPT report template

6.1 Discovery with Nmap

```
# Full TCP service and version scan
kali@kali:~$ nmap -sS -sV -O -p- 192.168.56.101 -oN nmap_full.txt

# Default vulnerability scripts
kali@kali:~$ nmap -sV --script vuln 192.168.56.101 -oN nmap_vuln.txt
```

Expected: over 20 open TCP ports, including FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), SMB (139/445), MySQL (3306) and more. Record every open port and its version.

6.2 Vulnerability assessment

12. Run an OpenVAS/Greenbone (or Nessus Essentials) authenticated and unauthenticated scan against the target.
13. Export the report. For each vulnerability, record the CVE, the CVSS v3.1 base score, and the severity band (Critical 9.0-10, High 7.0-8.9, Medium 4.0-6.9, Low 0.1-3.9).
14. Run Nikto against the web service: nikto -h http://192.168.56.101

6.3 Controlled exploitation (confirm, do not destroy)

Confirm at least three vulnerabilities of different types. Examples you can safely demonstrate on this target:

- vsftpd 2.3.4 backdoor (CVE-2011-2523) to gain a root shell.
- UnrealIRCd backdoor (CVE-2010-2075).
- Weak or default credentials over SSH or Telnet using Hydra.
- Open, world-readable MySQL with a blank root password.

```
kali@kali:~$ msfconsole
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > set RHOSTS 192.168.56.101
msf6 > run

# On success you get a shell:
id
uid=0(root) gid=0(root)
```

Grading note: you are graded on method, evidence and analysis, not on whether every exploit succeeds. A well-documented failed attempt with reasoning scores well.

6.4 Post-exploitation and business impact

15. For each confirmed exploit, show what an attacker could reach: read /etc/passwd and /etc/shadow, list databases, or read application files.
16. Translate this into BBC Bank business impact. Example: root on a DMZ server could let an attacker pivot toward the core banking network, breaching confidentiality and integrity of customer data and the BoU Cyber and Technology Risk Management Guidelines, 2024.

7. Linking VAPT to the Audit

Your VAPT is not a standalone exercise. In your report, connect it to the rest of the engagement:

- Unpatched services on the target mirror weak patch and change management seen in the change register.
- Default and weak credentials mirror the password configuration findings across AD, Finacle and AgentConnect.
- Excessive open services echo the least-privilege and hardening gaps in the ICT Policy.
- Recommend threat-led penetration testing, which the BoU guidelines now expect of supervised financial institutions.

8. Deliverables for Area 9

- A VAPT section in the final report (about 2 to 3 pages) built from the VAPT report template.
- A CVSS-rated findings table with at least eight vulnerabilities, three of them confirmed by exploitation.
- Raw evidence in the working-papers ZIP: nmap outputs, the scanner report (PDF or export), Nikto output, and exploitation screenshots with timestamps.
- The signed Authorisation to Test (Appendix A).

Appendix A: Authorisation to Test

Complete, sign and include this in your report.

Field	Entry
Group number and name	
Members (names and reg. numbers)	
Authorised target	Metasploitable 2 VM running on group member's laptop
Target IP and network	Host-Only, isolated
Testing window (dates)	
We confirm we tested only the authorised target on an isolated network, in line with the Rules of Engagement and the Computer Misuse Act.	
Signatures / date	

Supervisor authorisation (lecturer): _____ Date: _____