Penetration Testing

1.1 - Planning

Target

- A personal web application
  - → login page
  - → contact form
  - → user dashboard

1.1.2 - Plan

- Gray Box Testing
  - ↳ partial knowledge of system
    (practice insider)

Tools

- nmap → Port scanning
- Ping
- whois ...
- Burpsuite

1.2 - Enumeration

```
nmap -sS -sV -T4 192.168.0.1
```

Findings from Scan

Port 20 (SSH) → Open
port 80 (HTTP) → open
port 3306 (MySQL) → Filtered (potential for misconfiguration

Can also manually inspect the website

1.3 Exploitation

SQL injection → ' or '1'='1 to bypass login

XSS
↳ <script> alert(1) </script>

1.4 Escalation

After bypassing login
- Accessed admin panel
- Downloaded files
- Gained limited shell access

1.5 Reporting

Exec Summary
- Risk
- vulnerabilities
- Impact

Methodology

Gray Box
Nmap
Ping
whois
etc...

Findings (more detailed)

SQL
XSS
Files

Risk Analysis

- impact in real scenario
- How access escalated

Recommendations

Fix SQL
Sanitisation

Forensics Report

Identify	5W1H	FTK Imager for Disk Acquisition
Collect	what	Autopsy → MFT and Artefact Analysis
Acquire	when	Event Viewer → System logs
Preserve	why	Registry Explorer for keys/Hives.
Analyse	how	
Interpret	who	
Report.	where	

VID → Vendor ID, identifies Manufacturer

PID → Product ID, specific Model

↑ Stored in HKEY

Summary

Background

Scope

- Devices analysed
- Data types examined
- MFT (Master File Table)

Tools and Methodology

Findings

a) File creation/modification/Accessed

prefetch analysis

- Stuff like when was word opened compared to the documents.

Recycle Bin Artifacts

$I : metadata (can tell location of file)

$R : Recycle Bin.

Registry Evidence

- RecentDocs and Userassist

Userassist is in ROT13

Link files

- Found in Recent folder shows target path and timestamp matching access time

Event logs

SID → Unique identifier assigned to every group
e.g S-1-5-21

Interpretation

Conclusion

GUID → Globally Unique Identifier, identifies devices

Recommendations