Vulnerability Assessment Report

Objective :
Import the provided OVA into VirtualBox (host-only network), identify and exploit vulnerabilities to demonstrate impact, and produce a short, clear report of steps and findings.

Environment

- Attacker VM: Kali Linux (host-only) — example IP 192.168.56.102
- Target VM: Imported OVA (Ubuntu 14.04 in this exercise) — example IP 192.168.56.101
- Tools used: nmap, msfconsole (Metasploit), a web browser, and standard Linux shell commands.

Summary of actions

1. Performed host discovery to find the target VM on the host-only network (e.g., nmap -sn 192.168.56.0/24).
2. Ran service and version enumeration (nmap -sV -O 192.168.56.101) to list open ports and services.
3. Inspected the web root in a browser (http://192.168.56.101) and noted accessible web applications and directory listing.
4. Researched an observed service (ProFTPD 1.3.5) and identified the known mod_copy vulnerability (CVE-2015-3306).
5. Used Metasploit (exploit/unix/ftp/proftpd_modcopy_exec) with a reverse-shell payload to upload and trigger a web payload, resulting in a remote shell as www-data.
6. Enumerated /var/www/html and confirmed presence of web apps (Drupal, phpMyAdmin, payroll_app, chat).

Findings

- **Critical:** ProFTPD 1.3.5 with mod_copy enabled allowed arbitrary file copy which was used to upload a web payload and obtain remote code execution as www-data.
- **High:** Web applications (Drupal, phpMyAdmin, payroll app) accessible in webroot — increase attack surface and risk of data exposure.
- **High:** MySQL is reachable on the network and could be abused if credentials are weak.
- **Medium:** Directory listing was enabled, revealing application files and structure. Overall, the target was effectively compromised at the web-server level.

Impact
An attacker can run arbitrary commands in the web server context, modify or upload web

content, and potentially access application databases — effectively full compromise of web services.

Simple recommendations (priority order)

1. Patch or remove the vulnerable ProFTPD or disable mod_copy immediately.
2. Remove FTP write access to the webroot; ensure services cannot write to publicly accessible directories.
3. Disable directory listing and restrict access to admin panels (phpMyAdmin/Drupal) via IP restrictions or additional authentication.
4. Restrict MySQL to localhost or trusted hosts and enforce strong passwords.
5. After remediation, rotate credentials for any potentially exposed accounts and scan for backdoors/uploads.

Conclusion
The imported VM contained a known, exploitable FTP vulnerability which allowed uploading a web payload and obtaining a shell. Combined with exposed web applications and database access, this led to a high-impact compromise. Applying the prioritized fixes above will remove the immediate attack vector and significantly reduce risk.