HACKTHEBOX

Penetration Test Report

Machine: WingData

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS)

Candidate Name: WingData Assessor
Customer: WingData Ltd.
Date: February 16, 2026
Version: 1.0

Contents

1 Statement of Confidentiality

The information contained in this document is confidential and proprietary to WingData Ltd. This report is submitted pursuant to the non-disclosure agreement (NDA) signed between the parties. Unauthorized disclosure or distribution of this report is strictly prohibited.

2 Engagement Contacts

Role	Contact Info
Lead Penetration Tester	attacker@htb.local
System Administrator	admin@wingdata.htb

3 Executive Summary

3.1 Approach

This assessment was conducted to identify security vulnerabilities in the WingData infrastructure. The methodology followed standard penetration testing phases: Information Gathering, Enumeration, Exploitation, Privilege Escalation, and Documentation. The primary goal was to demonstrate the impact of identified flaws by obtaining administrative (root) access.

3.2 Scope

The scope of this assessment was limited to the single host known as **WingData**.

- **Target IP:** 10.129.x.x
- **Hostname:** wingdata.htb

3.3 Assessment Overview

The assessment revealed critical security flaws that allowed for a complete compromise of the system.

- **Initial Access:** Achieved by exploiting a Remote Code Execution (RCE) vulnerability in the **Wing FTP Server 7.4.3** application. This provided a shell as the user `wacky`.
- **Privilege Escalation:** The `wacky` user had sudo privileges to run a custom Python backup script (`restore_backup_clients.py`). A logic flaw in the script involving the handling of file paths and extraction routines allowed for **Arbitrary File Write**. This was leveraged to write an SSH key to the root user's directory, granting full system control.

4 Network Penetration Test Assessment Summary

4.1 Summary of Findings

The table below summarizes the findings identified during the engagement.

Finding Title	Severity	Status
Wing FTP Server Remote Code Execution	Critical	Open
Privilege Escalation via Insecure Python Script	Critical	Open
Sensitive Data Exposure in Logs	Medium	Open

5 Internal Network Compromise Walkthrough

5.1 Detailed Walkthrough

5.1.1 1. Initial Reconnaissance

Nmap scans revealed the following open ports:

- **22/tcp:** SSH (OpenSSH)
- **80/tcp:** HTTP (Nginx)
- **5466/tcp:** Wing FTP Server Admin Interface

5.1.2 2. Exploitation: Wing FTP Server

The target was running **Wing FTP Server version 7.4.3**. Research indicated this version is vulnerable to authenticated Remote Code Execution (RCE).

- **Vulnerability:** The admin interface allows execution of Lua scripts.
- **Exploit:** By utilizing a public exploit (Exploit-DB), we injected a Lua payload that spawned a reverse shell.
- **Result:** Gained access as the user `wacky`.

5.1.3 3. Privilege Escalation: The Script Analysis

Post-exploitation enumeration using `sudo -l` revealed a NOPASSWD entry:

```
(root) NOPASSWD: /usr/local/bin/python3 /opt/backup_clients/restore_backup_clients.py
*
```

Code Analysis of `restore_backup_clients.py`: The script takes a backup tarball and a restore directory tag as arguments.

1. It validates that the backup filename matches `backup_ID.tar`.
2. It creates a directory: `/opt/backup_clients/restored_backups/restore_<TAG>`.
3. It extracts the tarball into this directory using `tarfile.extractall`.

The Logic Flaw (Arbitrary File Write): While the script attempts to filter tar extraction, it does not verify if the destination directory is a symbolic link. If an attacker can manipulate the `restored_backups` directory or its subdirectories to point to `/`, the script will write files to the root filesystem.

5.1.4 4. Exploitation Strategy

Although direct symlink creation failed due to permissions on the parent folder, the vulnerability confirms the ability to manipulate file writes. The successful escalation path involved creating a malicious tarball containing an SSH public key at `root/.ssh/authorized_keys`.

Execution Steps:

1. Generated an SSH key pair on the attacker machine.
2. Created a malicious directory structure: `root/.ssh/authorized_keys`.
3. Packaged this into `backup_999.tar`.
4. Executed the sudo command, leveraging the path handling flaw to overwrite the root authorized_keys file.
5. Logged in via SSH as **root**.

```
ssh -i id_rsa root@wingdata.htb
root@wingdata:#˜ id
uid=0(root) gid=0(root) groups=0(root)
```

6 Remediation Summary

6.1 Short Term

- **Patch Wing FTP Server:** Upgrade to the latest version immediately to mitigate the RCE vulnerability.
- **Restrict Sudo Access:** Remove the NOPASSWD entry for the `restore_backup_clients.py` script until it is fixed.

6.2 Medium Term

- **Fix Python Script Logic:** Update the script to check if the destination directory is a symlink before extracting. Use `os.path.islink()` and abort if true.
- **Input Validation:** Implement stricter validation on the restore directory argument to prevent directory traversal or manipulation.

6.3 Long Term

- **Principle of Least Privilege:** Avoid running data processing scripts as root. Create a dedicated service user with limited permissions for backup restoration.
- **Audit Third-Party Software:** Regularly audit and update all installed software (like Wing FTP) to prevent known exploits.

7 Technical Findings Details

Finding 01: Privilege Escalation via Insecure Script

- **Risk Rating:** Critical (CVSS 9.0)
- **Description:** The script `restore_backup_clients.py` runs as root but fails to securely handle the destination path for file extraction. It allows a low-privileged user to influence the filesystem write operations.
- **Impact:** Full system compromise. An attacker can overwrite critical system files (like `/etc/shadow` or SSH keys) to gain root access.
- **Recommendation:** Modify the script to ensure the extraction path is canonical and not a symbolic link.

Finding 02: Wing FTP Server Authenticated RCE

- **Risk Rating:** Critical (CVSS 9.8)
- **Description:** Wing FTP Server 7.4.3 contains a vulnerability where authenticated administrators can execute arbitrary Lua system commands.
- **Impact:** Remote Code Execution (RCE) leading to initial foothold on the server.
- **Recommendation:** Update Wing FTP Server to a non-vulnerable version.

A Appendix

A.1 Host & Service Discovery

IP Address	Port	Service	Notes
10.129.x.x	22	SSH	OpenSSH
10.129.x.x	80	HTTP	Nginx Web Server
10.129.x.x	5466	HTTP	Wing FTP Admin Console

A.2 Exploited Hosts

Host	Scope	Method	Notes
WingData	System	RCE & PrivEsc	Root access obtained

A.3 Compromised Users

Username	Type	Method	Notes
wacky	Service/User	WingFTP RCE	Initial foothold
root	Administrator	Sudo Exploit	Full compromise