# Penetration Testing Report: Easy Peasy

### Executive Summary

A comprehensive penetration test was conducted on the target system with the IP address 10.10.47.153. The objectives were to identify open ports, vulnerable services, and to exploit these vectors to gain unauthorized access. The testing was performed in a controlled environment with authorized access.

### Methodology and Findings

### Network Scanning

1. **Initial Nmap Scan:**
    - Command: **nmap -A 10.10.47.153**
    - Found open HTTP port (80/tcp) running Nginx 1.16.1.
2. **Extended Nmap Scan:**
    - Command: **nmap -A -p- 10.10.47.153**
    - After 20 minutes, additional open ports were discovered:
        - 80/tcp (HTTP) running Nginx 1.16.1.
        - 6498/tcp (SSH) running OpenSSH 7.6p1 Ubuntu.
        - 65524/tcp (HTTP) running Apache httpd 2.4.43 (Ubuntu).

### Web Enumeration

1. **GoBuster Directory Search:**
    - Command: **gobuster dir -u http://10.10.47.153 -w /usr/share/wordlists/dirb/common.txt**
    - Identified a hidden directory **/hidden** with a suspicious image.
2. **Further GoBuster on Hidden Directory:**
    - Command: **gobuster dir -u http://10.10.47.153/hidden -w /usr/share/wordlists/dirb/common.txt**
    - Discovered another directory **/whatever**.

### Cryptanalysis and Flag Recovery

1. **Steganalysis of Downloaded Images:**
    - No findings on initial image.
    - Second image contained a Base64 encoded string.

2. **Base64 Decoding:**
    - Decoded to reveal the first flag: **flag{f1rs7_fl4g}**.
3. **MD5 Hash Identification:**
    - Analyzed the user-agent string in **/robots.txt** on port 65524.
    - Decoded to reveal the second flag via md5hashing.net.
4. **Password Enumeration with Text File:**
    - Utilized a list of potential passwords named **easypeasy** for further attacks.

**Exploitation of Web Service**

1. **Discovery of Encoded Directories:**
    - A Base62 encoded string revealed a directory: **/n0th1ng3ls3m4tt3r/**.
2. **Matrix Screen Analysis:**
    - Found a GOST hash and another image to investigate.

**Password Cracking and Steganalysis**

1. **GOST Hash Cracking:**
    - Cracked using John the Ripper with the **easypeasy** password list.
    - Obtained a password: **mypasswordforthatjob**.
2. **Steghide Extraction:**
    - Extracted **secrettext.txt** using the cracked password.
    - Retrieved credentials with a binary-encoded password.

**SSH Access and Flag Acquisition**

1. **SSH Access with Enumerated Credentials:**
    - Accessed SSH on port 6498 with username **boring**.
    - Found a user flag that appeared to be ROT-13 encoded.
2. **ROT-13 Decoding:**
    - Decoded to obtain the user flag: **flag{n0wits33msn0rm4l}**.

**Privilege Escalation and Root Flag Recovery**

1. **Cron Job Exploitation:**
    - Located a writable cron job script owned by the user.
    - Inserted a reverse shell payload pointing back to the penetration tester's machine.

2. **Root Access and Final Flag:**
    - Gained a root shell via the reverse shell.
    - Navigated to the root directory to find the final flag.

**Recommendations**

- Update and patch services, especially Nginx and OpenSSH, to the latest versions to mitigate known vulnerabilities.
- Secure web directories and implement proper access control to prevent unauthorized access to sensitive areas.
- Implement stronger password policies and use multi-factor authentication where possible.
- Conduct regular security audits and scans to detect and remediate misconfigurations or vulnerabilities.
- Limit write access to essential files and directories, especially those executed by cron jobs, to prevent privilege escalation.

**Conclusion**

The test revealed several security vulnerabilities that were successfully exploited. Critical data was accessed, including multiple flags indicative of potential real-world sensitive information. Immediate and long-term security measures are recommended to enhance the security posture and resilience against attacks.