Vulnerability Assessment Report

Job Title: *Security Officer Trainee @Accuknox*

Target: http://www.itsecgames.com/
IP Address: 31.3.96.40
Date of Assessment: 06 September 2025
Assessor: Syed Muzakkir Shah Harooni

1. Executive Summary

A reconnaissance and vulnerability assessment was performed on **itsecgames.com**, revealing that the server is hosted on IP `31.3.96.40` with multiple open services. The most notable finding is an **outdated version of OpenSSH (6.7p1)** exposed on port **22**, which is linked to multiple high-severity and exploitable vulnerabilities (CVSS up to 9.8).

The web services (ports **80/443**) are running **Apache HTTPD**, with HTTP traffic redirecting to HTTPS and another domain (`www.mmebvba.com`). The headers reveal standard configurations with no obvious security misconfigurations. No XSS, CSRF, or common HTTP-based vulnerabilities were detected via automated scans.

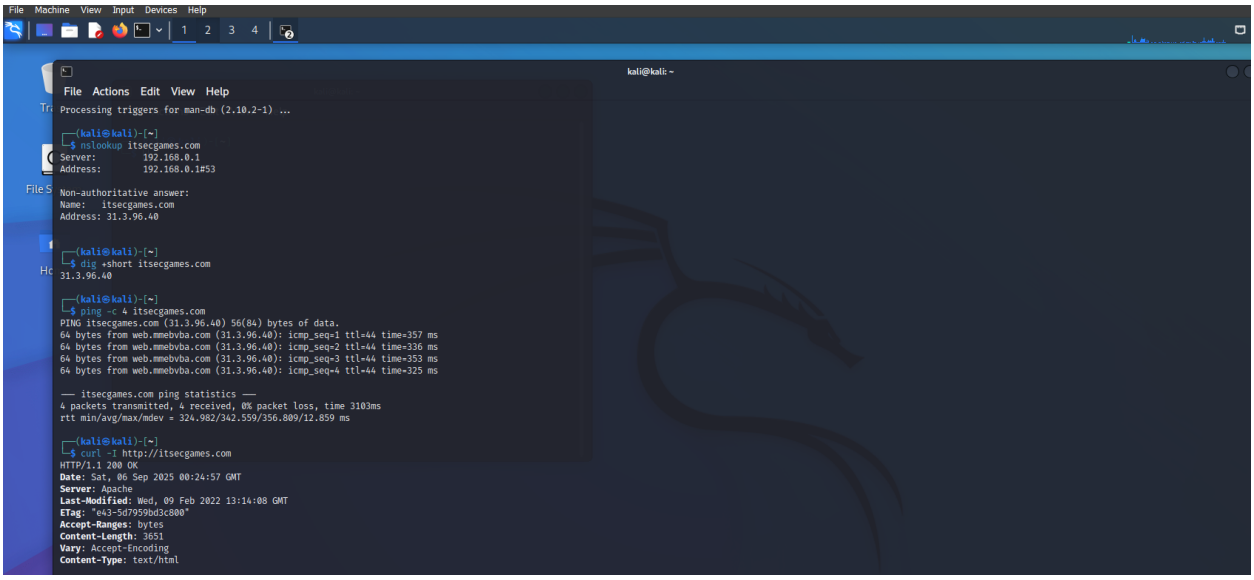
However, the outdated SSH service presents a **critical attack surface** that could allow attackers to gain unauthorized access.

2. Scope & Methodology

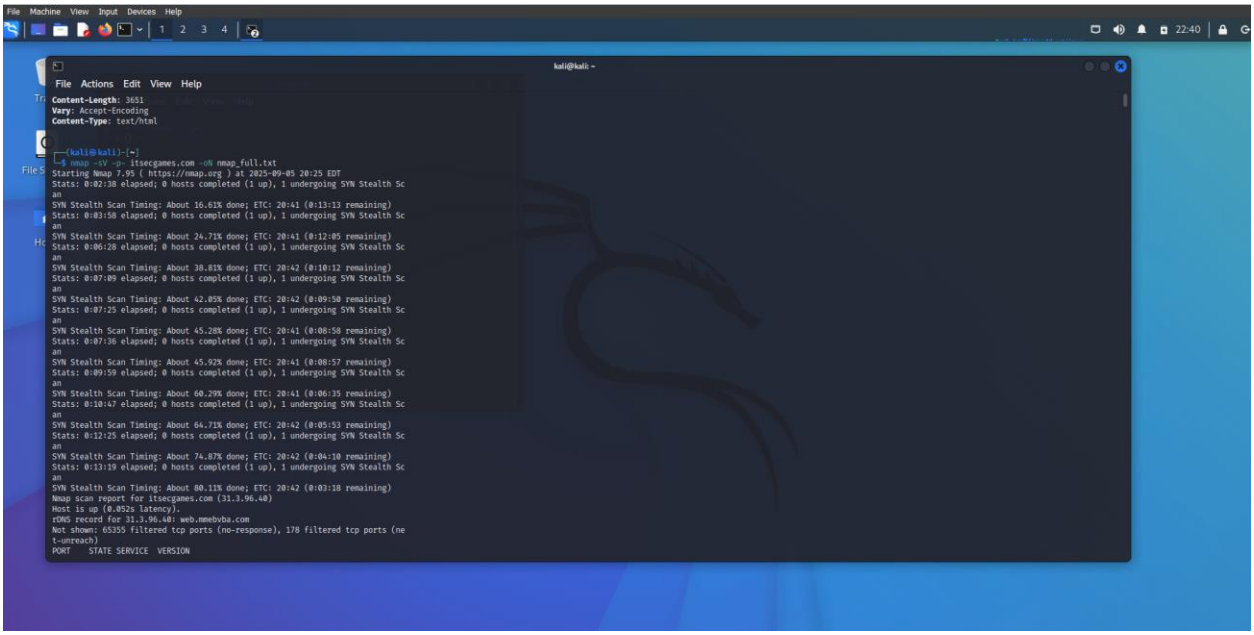
The following methodology was used:

- **Step 1: Reconnaissance**

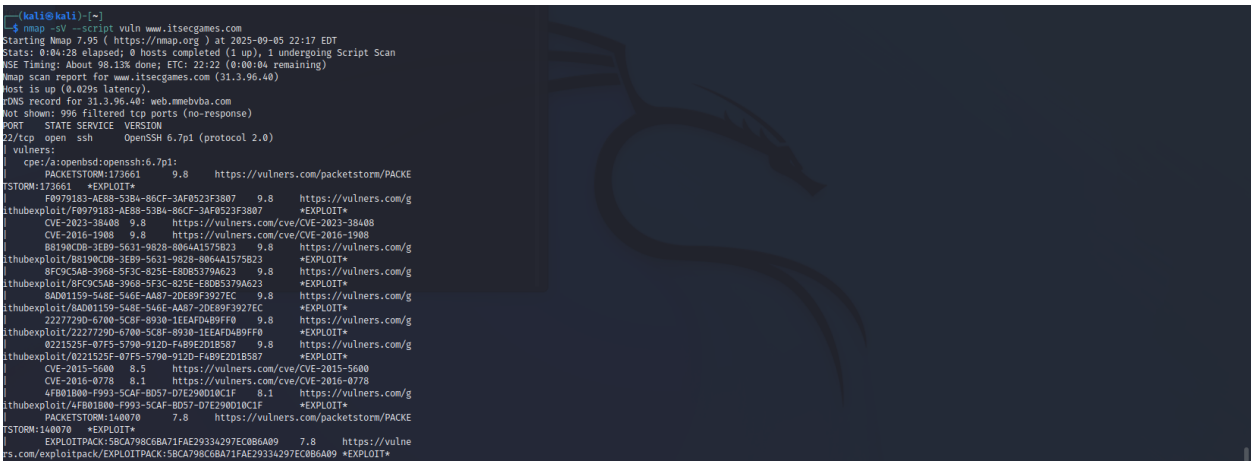
  - **DNS enumeration (nslookup, dig):** Used to identify the IP address, DNS records, and associated domains of the target. This helps map the attack surface.
  - **Network connectivity testing (ping):** Verified host availability and measured latency (round-trip time).
  - **HTTP header review (curl):** Collected server response headers to check for exposed information (e.g., software versions, missing security headers).



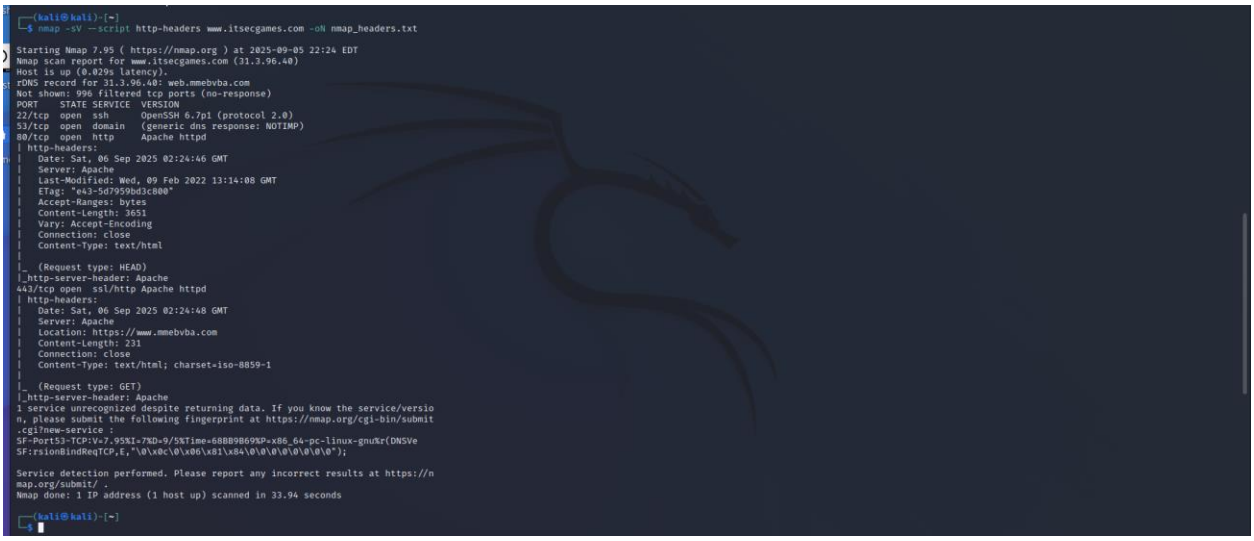
- **Step 2: Port & Service Discovery**
    - **Full TCP scan (nmap):** Scanned all 65,535 ports to identify which services are exposed to the internet.



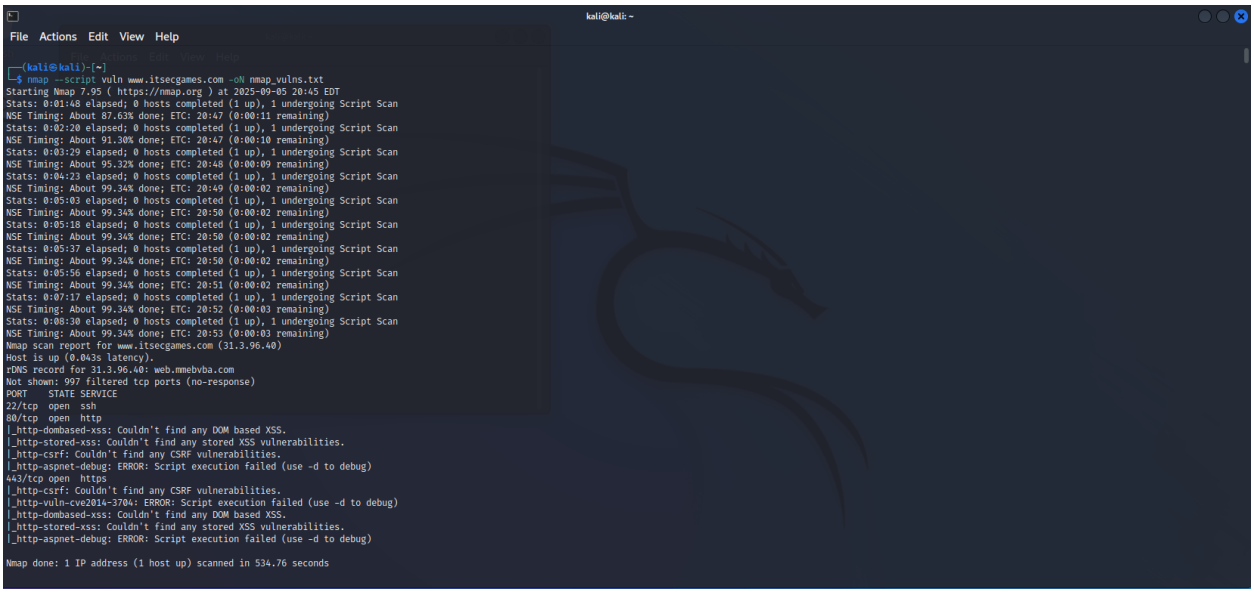
    - **Service version detection (nmap -sV):** Determined the version of running services (e.g., OpenSSH 6.7p1, Apache HTTPD) for vulnerability matching.



- **Header collection (nmap --script http-headers):** Gathered additional HTTP header information for misconfiguration analysis.



- **Step 3: Vulnerability Assessment**
  - **Automated script scan (nmap --script vuln):** Ran Nmap's NSE vulnerability scripts to check for common CVEs (e.g., XSS, CSRF, outdated services).
  - **CVE mapping (vulners database):** Cross-referenced service versions (like OpenSSH 6.7p1) against known CVEs to assess severity and exploit availability.



3. Findings

3.1 Network & DNS Information

- **Domain:** itsecgames.com
- **Resolved IP:** `31.3.96.40`
- **Reverse DNS:** `web.mmebvba.com`
- **Latency:** ~325–356 ms average RTT
- **Availability:** Host responds consistently to ICMP

3.2 Open Ports & Services

Port	State	Service	Version	Notes
22	Open	SSH	OpenSSH 6.7p1 (protocol 2.0)	**Outdated**, multiple critical CVEs
53	Open	DNS	Generic DNS (TCP)	Returns NOTIMP response
80	Open	HTTP	Apache HTTPD	Responds with `200 OK`, static content
443	Open	HTTPS	Apache HTTPD	Redirects to `https://www.mmebvba.com`

3.3 HTTP Headers (Port 80)

```
Date: Sat, 06 Sep 2025 00:24:57 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022
ETag: "e43-5d7959bd3c800"
Content-Length: 3651
Content-Type: text/html
```

Nikto web server scan: Checked for misconfigurations, outdated components, and missing security headers.
(nikto -h http://www.itsecgames.com -output nikto_report.txt) confirmed the absence of key security headers such as HSTS, X-Frame-Options, and Content-Security-Policy, consistent with the manual header review.

- No `Strict-Transport-Security` (HSTS) header detected.
- No `X-Frame-Options`, `X-XSS-Protection`, or `Content-Security-Policy` headers observed.
- Site still accessible via **plain HTTP** → vulnerable to MITM.

3.4 Vulnerability Assessment

SSH (Port 22 - OpenSSH 6.7p1)

- Multiple **critical vulnerabilities** identified:
  - **CVE-2023-38408** (CVSS 9.8) – Remote code execution in OpenSSH.
  - **CVE-2016-1908** (CVSS 9.8) – Privilege escalation.
  - **CVE-2015-5600** (CVSS 8.5) – Keyboard-interactive authentication brute force.
  - **CVE-2020-15778** (CVSS 7.8) – Command injection via scp.
  - Several enumeration and information disclosure flaws.

Exploits for these vulnerabilities are publicly available (ExploitDB, GitHub, PacketStorm).

HTTP / HTTPS (Ports 80/443 – Apache HTTPD)

- Server header exposed → version fingerprinting possible.
- **Redirects traffic from 443 → www.mmebvba.com** (external domain).
- No critical vulnerabilities detected by Nmap.
- No stored/DOM-based XSS or CSRF found in automated scans.
- Missing security headers as mentioned above.

DNS (Port 53)

- Open TCP but limited functionality (`NOTIMP` response).
- No active exploitation observed.

4. Risk Assessment

Risk	Affected Service	Severity	Description
Outdated OpenSSH 6.7p1	SSH (22/tcp)	🔴 **Critical**	Multiple RCE & privilege escalation vulnerabilities, public exploits available.
Missing Security Headers	HTTP/HTTPS	🟠 Medium	Increases risk of clickjacking, XSS, MITM attacks.
Plain HTTP access	HTTP (80/tcp)	🟠 Medium	No enforced HTTPS, susceptible to session hijacking.
Information Disclosure	Apache, DNS	🟢 Low	Server headers and DNS info exposed, useful for attackers in recon.

5. Recommendations

1. **Patch SSH Immediately**
    a. Upgrade OpenSSH to the latest stable version.
    b. Restrict SSH access to trusted IPs only (via firewall).
    c. Enforce key-based authentication and disable password logins.
2. **Enforce HTTPS Strictly**
    a. Redirect all HTTP traffic to HTTPS.
    b. Enable HSTS (Strict-Transport-Security).
3. **Harden Web Server Security Headers**
    a. Add `X-Frame-Options: DENY`
    b. Add `Content-Security-Policy`
    c. Add `X-Content-Type-Options: nosniff`
4. **Limit Information Disclosure**
    a. Remove or obfuscate `Server: Apache` header.
    b. Configure DNS to minimize leakage.
5. **Ongoing Security Practices**
    a. Regular vulnerability scanning and patch management.
    b. Intrusion Detection / Prevention monitoring for SSH brute force attempts.
    c. Web Application Firewall (WAF) for added HTTP protection.

6. Conclusion

The assessment of **itsecgames.com** revealed a **high-risk security posture**, primarily due to an outdated SSH service with known exploits. While the web services did not show major vulnerabilities during automated scans, missing best-practice security headers and lack of HTTPS enforcement expose users to potential MITM and client-side attacks.

7. Appendix

7.1 Tools Used (Linux Environment)

- **Nmap** → Network scanning, port & service discovery, vulnerability scripts
- **Nikto** → Web server vulnerability scanner
- **cURL** → Manual HTTP header inspection
- **OpenSSL** → SSL/TLS certificate review
- **Ping / Dig / Nslookup** → Basic reconnaissance and DNS enumeration

7.2 Commands Executed

Reconnaissance

```
# Check domain resolution
nslookup itsecgames.com

# Alternative DNS lookup
dig itsecgames.com

# Test host connectivity
ping -c 4 itsecgames.com
```

HTTP Header Review

```
curl -I http://www.itsecgames.com
```

Port & Service Discovery

```
# Full TCP scan
nmap -p- itsecgames.com
```

```
# Service version detection
nmap -sV itsecgames.com

# Collect HTTP headers
nmap --script http-headers -p 80,443 itsecgames.com
```

Vulnerability Assessment

```
# Run vulnerability scripts
nmap --script vuln -oN nmap_vulns.txt itsecgames.com

# Web server scan with Nikto
nikto -h http://www.itsecgames.com -output nikto_report.txt
```

SSL/TLS Testing

```
openssl s_client -connect www.itsecgames.com:443
```

Webpage View