PENETRATION TESTING REPORT

ALPHA VERDE
WEDNESDAY, 04 OCTOBER 2023

This Penetration Testing Report is provided in compliance with the terms outlined in Contract #2023-01-CPPT-WDX. The report encompasses the outcomes of the penetration testing engagement conducted between 2nd October 2023 and 6th October 2023. All content within this report is classified as confidential and is safeguarded by a non-disclosure agreement as stipulated in the terms of the aforementioned contract. Unauthorised disclosure or distribution of this report is strictly prohibited and may result in legal action.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 RESULTS

The comprehensive evaluation of technical risks associated with the systems and network encompassed within the designated scope has unequivocally yielded a CRITICAL assessment. It is imperative to emphasise that the attainment of a residual risk level below the HIGH threshold hinges upon the meticulous implementation of all recommended remediation strategies delineated in Section 3 of this report.

As a result of this assessment, we assert that the current state of the application, system, or network does not meet the requisite level of resilience for deployment within a production or live environment. It is imperative to address the identified critical risks and undertake the recommended remedial actions in order to enhance the system's suitability for such operational contexts. Failure to do so may expose the organisation to potential vulnerabilities and disruptions that could significantly impact its operational integrity and security. Thus, a concerted effort to mitigate these risks is of paramount importance to ensure the robustness and reliability of the systems and network in question.

The table below depict the overall result of this security assessment through the framework of cyber kill chains:

Gaining Access	Info Disclosure	Initial Exploitation	Privilege Esc
- Reverse Shell	- Version Disclosure -Flag points	- SQL Injection – Authentication Bypass - Command Injection – Admin Console	- Weak Password Policies

Regression testing is recommended following the implementation of remediation activities to validate the risk mitigation.

1.2 METHODOLOGY

The test was conducted using a combination of automated tools and manual testing techniques. The methodologies and tools used included:

- Network scanning and enumeration
- Vulnerability scanning
- Brute force username/password attacks
- Web application scanning and manual testing
- Wireless network analysis
- Exploitation frameworks

1.3 SCOPE

This security evaluation was executed from 02 OCT 2023 to 06 OCT 2023 and was limited to the review of:

a) 192.168.122.47
b) 192.168.1.1
c) 192.168.1.101
d) 192.168.1.102
e) 192.168.1.108
f) 192.168.1.109
g) 192.168.1.111
h) 192.168.1.116
i) 192.168.1.121

1.4 TECHNICAL ISSUES

No technical issues were encountered during the review. We would like to acknowledge the outstanding support of Hillard International's Trinity Team.

2 FINDINGS SUMMARY

Severity	Findings	Intranet; Development	Mitigated by remediation
CRITICAL	3.1.1 UNAUTHENTICATED REMOTE CODE EXECUTION – RCE 3.1.2 SQL Injection - Database Vulnerabilities 3.1.3 Privilege Escalation - Unauthorised Access to Admin Privileges	4	Resolved To Partial
HIGH	3.2.1 BRUTE FORCE ATTACK - INADEQUATE PASSWORD POLICY AND ENFORCEMENT	3	Resolved

Networks	*Critical*	*High*	*Medium*	*Low*	*Results*
Intranet; Development	*4*	*3*	*2*	*1*	*Fail*

* Risk rating score is based on CVSS 3.0 standard – (https://www.first.org/cvss/specification-document)
* Online calculator - https://www.first.org/cvss/calculator/3.0

3 SIGNIFICANT FINDINGS

3.1 CRITICAL

3.1.1 UNAUTHENTICATED REMOTE CODE EXECUTION – RCE

CVSS v3.0 Risk Score:

Networks	Vector	Rating
Company Intranet; Legacy	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	10.0

Component:
SOC1 - 192.168.122.102

Status:
Partially Resolved

Description:
During the security assessment of the SOC1, it was found that an unauthenticated remote code execution vulnerability was present in the '/console' location. This vulnerability allows a malicious user to inject arbitrary code directly into the running process, thereby gaining complete control over the underlying server.

Impact:
A malicious actor, upon gaining access to the company intranet, can exploit the vulnerability present in the '/console' location. This exploitation allows them to attain full terminal access to the target server, leading to a complete compromise of the system's confidentiality, integrity, and availability. Notably, the malicious code injection occurs directly into memory, effectively bypassing anti-virus software. It's essential to recognize that this specific exploit served as the entry point that facilitated unauthorised access to the entire subnet, posing a significant threat to network security.

Technical fix:
This risk can be mitigated through input validation, security patch, access control, monitoring and intrusion detection, and regular updates.

Remediation:
To remediate the vulnerability in '/console,' Hillard International's security team isolated the component, deployed an urgent security patch, implemented input validation, enhanced access control, set up monitoring and intrusion detection, conducted regular security audits, maintained documentation, verified remediation through testing, and ensured ongoing monitoring for vulnerabilities.

Technical Details:
During the assessment, a vulnerability was identified in the SOC1, stemming from the compromise of the PFSense firewall. This breach facilitated unauthorised port forwarding, ultimately resulting in the establishment of a reverse shell.

3.1.2 SQL INJECTION - DATABASE VULNERABILITIES

CVSS v3.0 Risk Score:

Networks	Vector	Rating
Company Intranet; Legacy	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	10.0

Component:
SOC1 - 192.168.122.102

Status:
Resolved

Description:
During the security assessment of the SOC1, it was found that an unauthenticated remote code execution vulnerability was present in the '/console' location. This vulnerability allowed our attackers to inject malicious SQL code thereby gaining complete control over the underlying component.

Impact:
Upon the SQL injection our attackers were granted access to the intranet. This sophisticated attack vector grants them full terminal access to the target server, resulting in a complete compromise of the system's confidentiality, integrity, and availability. Notably, the SQL injection occurs directly in memory, allowing it to circumvent anti-virus software. It's crucial to emphasise that this specific SQL injection exploit served as the initial entry point, enabling unauthorised access to the entire subnet and presenting a grave menace to network security.

Technical fix:
This risk can be mitigated through input validation, security patch, access control, monitoring and intrusion detection, and regular updates.

Remediation:
To remediate the vulnerability in '/console,' Hillard International's security team isolated the component, deployed an urgent security patch, implemented input validation, enhanced access control, set up monitoring and intrusion detection, conducted regular security audits, maintained documentation, verified remediation through testing, and ensured ongoing monitoring for vulnerabilities.

Technical Details:

In the scenario involving the '/console' location, our attackers exploited a critical SQL injection vulnerability within the application. They manipulated the input fields to inject malicious SQL code directly into the database query. For instance, they may input '1' OR '1'='1' --' as the username, which effectively comments out the rest of the query and always returns 'true.' This resulted in the system executing unintended database actions, revealing sensitive data, and giving our attackers unauthorised access. In this case, the attacker's input directly interferes with the SQL

query, bypassing security measures and showcasing the significance of addressing SQL injection vulnerabilities to prevent such unauthorised actions.

3.1.3 Privilege Escalation - Unauthorised Access to Admin Privileges

CVSS v3.0 Risk

Networks	Vector	Rating
Company Intranet; Legacy	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	9.4

Component:
SOC1 – 192.168.122.102
SOC2 - 192.168.122.111
SOC6 - 192.168.1.101

Status:
Partially Resolved

Description:
Once entrance was made into the subnet of 192.168.122.47, pivoting allowed the attacker to access different systems throughout the subnet. Once in the systems the attacker was able to gain root access through privilege escalation.

Impact:
Attackers with admin access can exert full control over the system, allowing them to make unauthorised changes to configurations, install malicious software, or manipulate critical settings. This can lead to data breaches, service disruption, and malware deployment.

Technical fix:
Enforce strong password policies, including complexity requirements, regular password changes, and password storage best practices (e.g., hashing and salting). Implement multi-factor authentication (MFA) to strengthen user authentication. Require multiple forms of verification, such as passwords, tokens, or biometrics, to access admin accounts.

Remediation:
Hillard International's cyber team implemented strong authentication measures, including MFA for admin accounts. We then confirm the successful implementation of MFA to resolve this finding.

Technical Details:
Following an initial breach into the network subnet at 192.168.122.47, the attacker proceeded to employ a series of sophisticated tactics, techniques, and procedures (TTPs) to traverse and infiltrate various systems within the subnet. Leveraging their initial foothold, the attacker engaged in lateral movement, actively exploring and probing the network's internal architecture.

Through meticulous reconnaissance, the attacker identified vulnerable systems and applications, capitalising on misconfigurations and security weaknesses. Exploiting these vulnerabilities, the attacker successfully infiltrated multiple hosts, spanning both servers and workstations.

To achieve complete control and escalate their privileges, the attacker executed a combination of privilege escalation tactics. This involved exploiting known vulnerabilities, misconfigured permissions, or flawed access control mechanisms on compromised systems. As a result, the attacker obtained root-level access on these systems, granting them unrestricted control over critical system resources and configurations.

It is essential to note that throughout this process, the attacker operated discreetly to avoid detection, often utilising techniques such as stealthy lateral movement, obfuscation, and evasion of intrusion detection systems.

The combination of these actions represents a multi-faceted and highly orchestrated intrusion that not only compromised the integrity and confidentiality of the affected systems but also posed a significant security risk to the entire network infrastructure. This comprehensive security breach underscores the critical importance of implementing robust defensive measures and proactive security practices to safeguard against such sophisticated threats.

3.2 HIGH

3.2.1 BRUTE FORCE ATTACK - INADEQUATE PASSWORD POLICY AND ENFORCEMENT

CVSS v3.0 Risk Score:

Networks	Vector	Rating
Company Intranet; Legacy	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.4

Component:
Every component in the scope.

Status:
Resolved

Description:
During the penetration test, our red team successfully executed brute force attacks, enabling them to gain unauthorised access to numerous accounts and directories.

Impact:
Weak password policies can lead to: unauthorised access, data breaches, privilege escalation, compromised user identities, and/or disruption of services.

Technical fix:
This issue can be mostly fixed through: password complexity requirements, password expiration, account lockout policies, password history, mfa, password recovery processes, user education, password management tools, regular security audits, and/or monitoring and alerting.

Remediation:
The purple team (attackers and defence team) implemented many measures to attempt to make this issue irrelevant. This included the enforcement of robust password complexity requirements, setting up password expiration policies, and implementing account lockout mechanisms to deter brute-force attacks. Additionally, we advocated for the adoption of MFA across the network, as it proved to be an effective defence against unauthorised access. Lastly, we recommended regular security audits and assessments to continuously monitor and improve password security. These measures collectively aimed to enhance the organisation's cybersecurity posture by strengthening its defences against weak password practices and reducing the risk of unauthorised access."

Technical Details:
For our penetration testing efforts, we utilised Hydra, a potent and versatile password-cracking tool, in combination with the 'rockyou.txt' wordlist, to systematically conduct brute force attacks on multiple accounts across various computer systems. Leveraging its flexibility and extensibility, we crafted custom scripts and configurations to target weak password policies within the organisation's infrastructure. Hydra allowed us to automate login attempts across a range of services and protocols, systematically testing different username and password combinations using the extensive 'rockyou.txt' wordlist. This comprehensive

approach highlighted the stark vulnerabilities associated with weak passwords and illustrated the potential for unauthorised access to critical systems.

4 APPENDIX

4.1 TEST SUMMARY

In this comprehensive security assessment, we conducted a thorough evaluation of the organisation's cybersecurity posture, encompassing a range of critical findings and assessments. We initiated our engagement by performing a detailed analysis of the company's network and systems, employing a variety of tools and methodologies. Notably, we utilised 'Hydra,' 'Metasploit,' and 'Dirb,' in combination with the 'rockyou.txt' wordlist, to conduct extensive brute force attacks on multiple accounts across diverse computer systems and to identify existing web directories on web servers. This approach effectively exposed vulnerabilities associated with weak password policies, resulting in unauthorised access to numerous accounts and directories.

Additionally, our assessment unveiled significant vulnerabilities, including unauthenticated remote code execution (RCE) in the '/console' location and SQL injection vulnerabilities within the application. These findings highlight the potential for attackers to gain full control over the targeted systems, compromising confidentiality, integrity, and availability.

Furthermore, we identified privilege escalation tactics, which underscored the critical need for robust access controls and strong authentication measures to prevent unauthorised access to administrative privileges. The attacker's lateral movement throughout the network demonstrated a high level of sophistication, emphasising the importance of proactive security practices.

To address these findings, our remediation efforts included deploying security patches, implementing input validation, enhancing access controls, enabling monitoring and intrusion detection, conducting regular security audits, and advocating for the adoption of multi-factor authentication (MFA). These measures collectively aimed to strengthen the organisation's cybersecurity defences and reduce the risk of unauthorised access and data breaches.

Throughout this engagement, we meticulously documented our testing methodology, tool usage, and findings, providing the organisation with a comprehensive assessment of their security posture and actionable recommendations for improvement

4.2 FLAGS

SOC2:

```
File  Actions  Edit  View  Help
./new.txt: line 20: syntax error near unexpected token `(
./new.txt: line 20: `root       ALL=(ALL:ALL) ALL'
lhillard@SOC2:~$ sudo su
[sudo] password for lhillard:
root@SOC2:/home/lhillard# find / -name flag.txt
/home/rbarry/Desktop/flag.txt
root@SOC2:/home/lhillard# cd ..
root@SOC2:/home# ls
gns3  lhillard  rbarry
root@SOC2:/home# cd rbarry
root@SOC2:/home/rbarry# cd Desktop
root@SOC2:/home/rbarry/Desktop# ls
flag.txt
root@SOC2:/home/rbarry/Desktop# cat flag.txt
SOC2:RBARRY:15POINTS
root@SOC2:/home/rbarry/Desktop# cd
root@SOC2:~# cd
root@SOC2:~# find / -name root.txt
/home/lhillard/Desktop/root.txt
root@SOC2:~# cd home
bash: cd: home: No such file or directory
root@SOC2:~# pwd
/root
root@SOC2:~# cd /home
root@SOC2:/home# cd lhillard
root@SOC2:/home/lhillard# cd Desktop
root@SOC2:/home/lhillard/Desktop# ls
root.txt
root@SOC2:/home/lhillard/Desktop# cat root.txt
SOC2:LHILLARD:30POINTS
root@SOC2:/home/lhillard/Desktop#
```

15 point and 30 point flag respectively

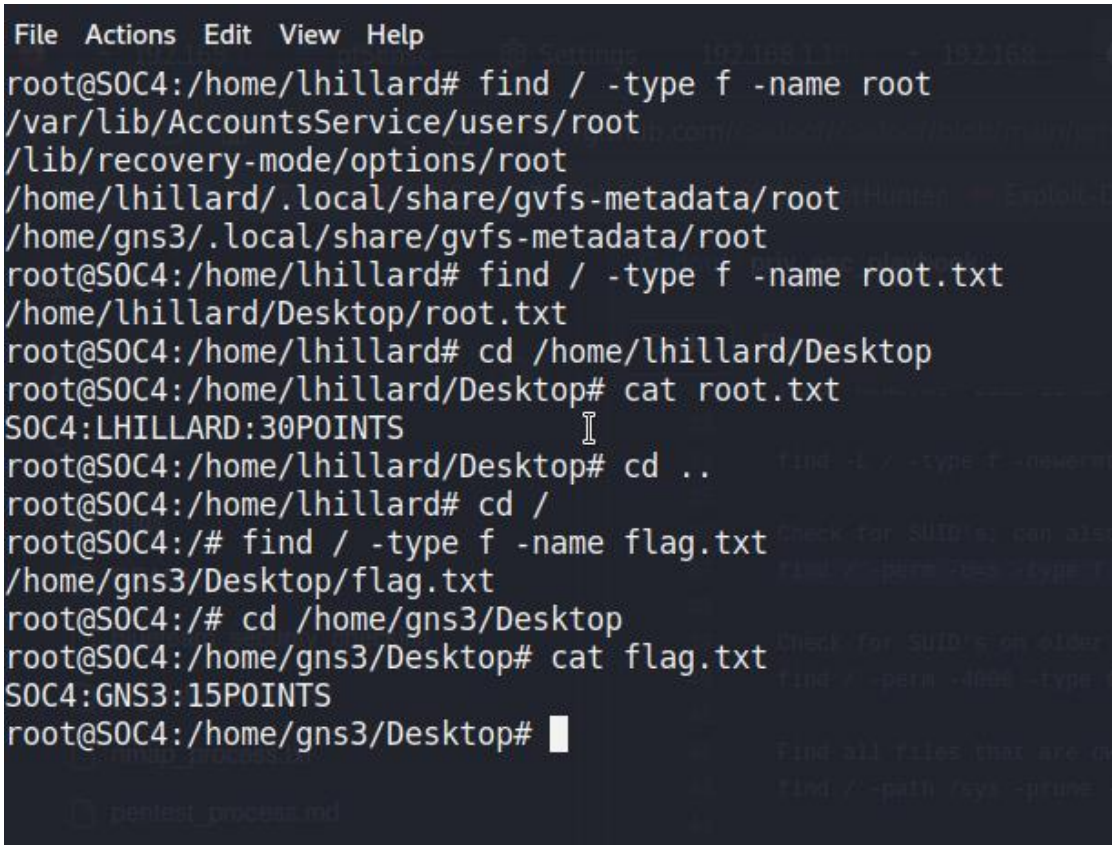
SOC3:

```
C:\Users\rbarry\Desktop>flag.txt
flag.txt

C:\Users\rbarry\Desktop>more flag.txt
more flag.txt
SOC3:RBARRY:15POINTS
```

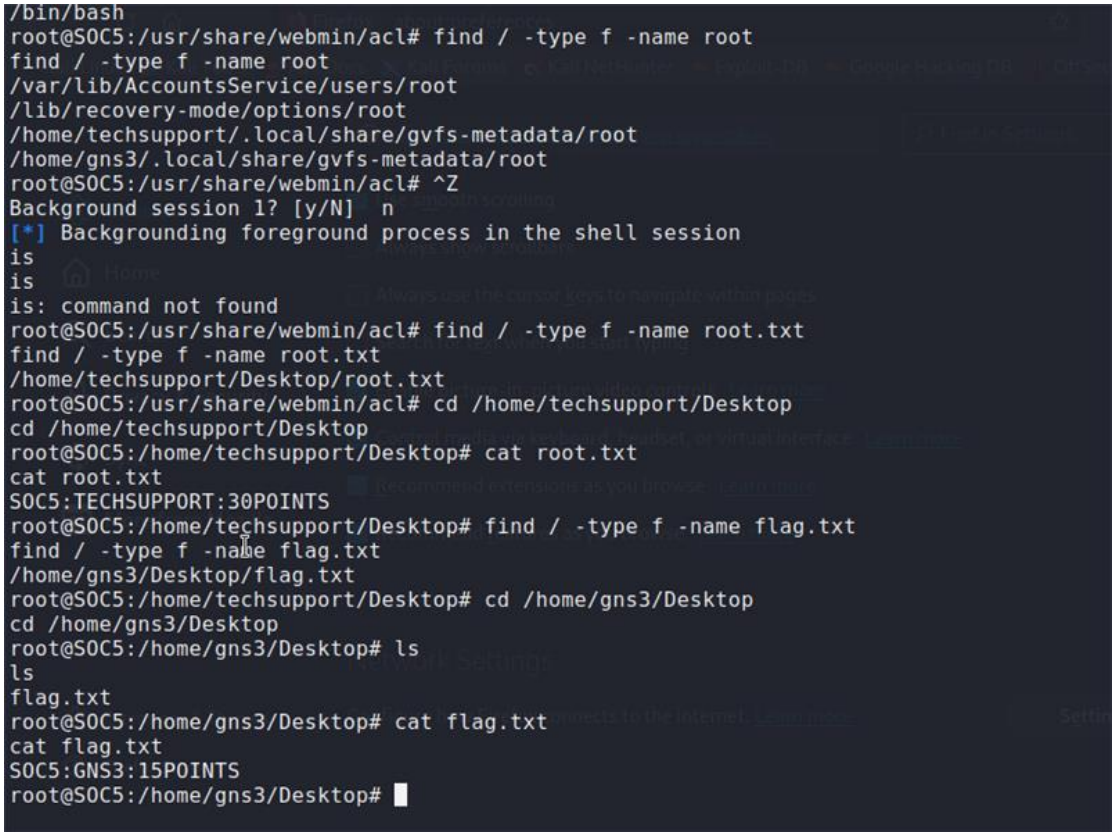
15 point flag

SOC4:



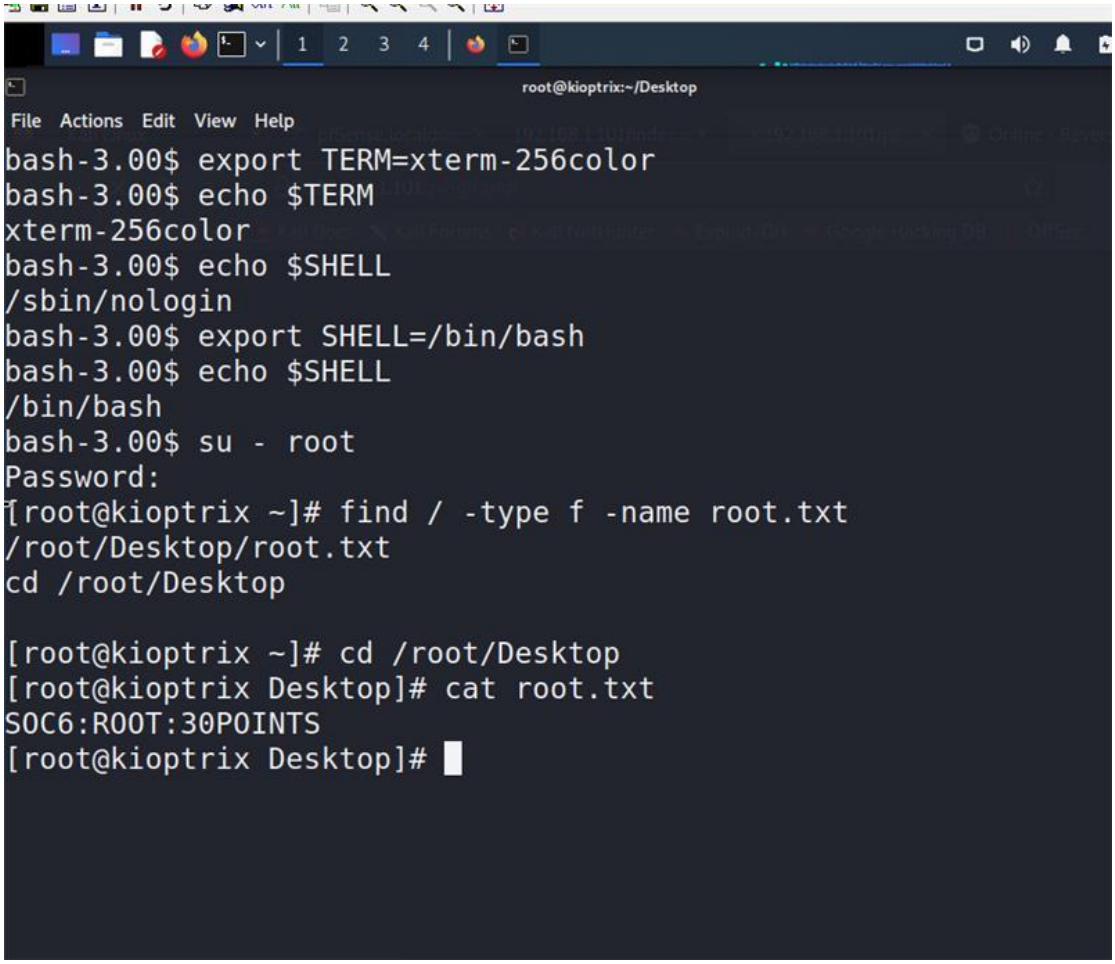
30 point and 15 point flag respectively

SOC:5

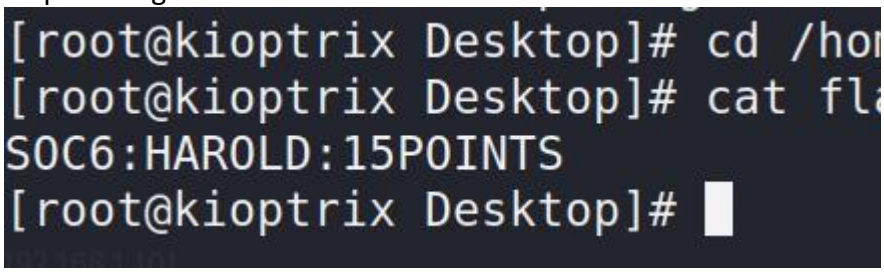


30 point and 15 point flag respectively TOTAL: 45 points

SOC6:



30 point flag



15 point flag

Risk Calculation Metrics

4.2.1 CVSS 3.0 Scale

CVSS 3.0 Scale	
None	0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

4.2.2 Remediation Metrics

Mitigated without code change	Mitigated with code change
Configuration Change	Code change / patch
Network segmentation	Addition of new module/component
Removing component	
Disabling a service	

4.2.3 Evaluation Report State

Evaluation Report State			
	Critical (unresolved)	High (unresolved)	Medium (unresolved)
Sufficiently resilient	0	less than 2	less than 4
Not Sufficient	1 or more	2 or more	4 or more
1 Critical = 2 High ; 1 High = 2 Medium ; 1 Medium = 4 Low			

Conclusion:

The penetration test identified several vulnerabilities and risks within Hillard International's network and applications. It is crucial to address these issues promptly to improve security and reduce the risk of cyberattacks. Regular security assessments and proactive measures are recommended to maintain a strong security posture.

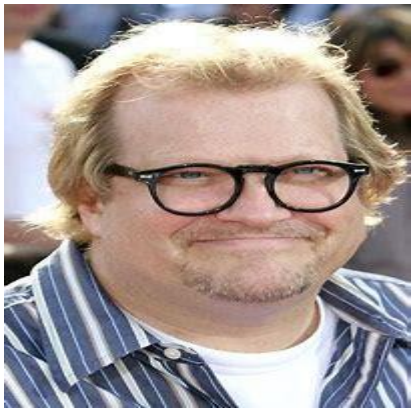
Group Alpha appreciates the opportunity to perform this penetration test and is available for any further assistance or clarification.

Sincerely,
Matthew Worthen
Alpha Verde

Meet Our Team

Our Red Team:

Joshua Godfrey



Steve Vineyard

Andrew Vinson

Media and Reporting Team:

Matthew Worthen