## STEP 1: Information Security Framework Design

### 1.1 Overview of the Security Framework

The proposed Information Security Framework is designed to protect cloud-based enterprise environments from common security threats such as unauthorized access, data breaches, misconfigurations, and compliance violations. The framework follows a **layered security approach** and aligns with international standards such as **ISO/IEC 27001**.

The framework integrates:

- Asset classification
- Risk assessment and risk treatment
- Encryption for data protection
- Strong authentication and access control mechanisms

This structured approach ensures confidentiality, integrity, and availability (CIA triad) of cloud resources.

### 1.2 Asset Classification

Asset classification helps identify and prioritize resources that require protection based on their sensitivity and business impact.

**Asset Classification Table**

| **Asset Category** | **Asset Description** | **Classification** |
|---|---|---|
| Data Assets | Customer data, credentials, logs | Confidential |
| Application Assets | Cloud-hosted web application | Critical |
| Infrastructure Assets | Virtual machines, cloud storage | High |
| Network Assets | Firewalls, VPC, load balancers | High |
| Identity Assets | User accounts, admin credentials | Critical |

**Purpose:**

- Ensures appropriate security controls are applied
- Supports compliance with **ISO/IEC 27001 – A.8 (Asset Management)**

### 1.3 Risk Assessment Methodology

Risk assessment is conducted to identify threats, vulnerabilities, and their potential impact on cloud assets.

#### Risk Calculation Formula

*Risk = Likelihood × Impact*

#### Risk Rating Scale

| Level | Likelihood | Impact |
|---|---|---|
| Low | 1 | 1 |
| Medium | 2 | 2 |
| High | 3 | 3 |

#### Sample Risk Assessment Table

| Threat | Asset Affected | Likelihood | Impact | Risk Score | Risk Level |
|---|---|---|---|---|---|
| Data Breach | Cloud Database | 3 | 3 | 9 | High |
| Unauthorized Access | User Accounts | 3 | 2 | 6 | Medium |
| Network Sniffing | Data in Transit | 2 | 3 | 6 | Medium |
| Misconfiguration | Cloud Storage | 2 | 2 | 4 | Medium |

### 1.4 Risk Treatment Strategy

Each identified risk is handled using one of the following strategies:

| Risk | Treatment Strategy | Security Control |
|---|---|---|
| Data Breach | Mitigate | Encryption (AES, RSA) |
| Unauthorized Access | Mitigate | MFA + RBAC |
| Network Attacks | Mitigate | TLS, Firewall |
| Low Impact Risk | Accept | Monitoring |

**ISO Mapping:**

- **A.6 – Risk Assessment and Treatment**

---

### STEP 2: Encryption Mechanisms

### 2.1 Importance of Encryption in Cloud Security

Encryption ensures that sensitive data remains protected even if unauthorized access occurs. The framework uses:

- **Symmetric encryption** for data at rest
- **Asymmetric encryption** for data in transit and key exchange

---

### 2.2 Data at Rest – Symmetric Encryption

**Algorithm Used**

- **AES (Advanced Encryption Standard – 256 bit)**

**Why AES?**

- High performance
- Widely accepted industry standard
- Suitable for large volumes of cloud data

**Implementation Using OpenSSL**

```
openssl enc -aes-256-cbc -salt -in data.txt -out data.enc
```

**Explanation:**

- data.txt → original data
- data.enc → encrypted file
- AES protects stored cloud data from unauthorized access

**ISO Mapping:**

- **A.10 – Cryptographic Controls**

---

### 2.3 Data in Transit – Asymmetric Encryption

**Algorithm Used**

- **RSA (2048-bit)**

**Purpose**

- Secure key exchange
- Enable HTTPS / TLS communication
- Prevent Man-in-the-Middle (MITM) attacks

**Key Generation Using OpenSSL**

```
openssl genrsa -out private.key 2048
openssl rsa -in private.key -pubout -out public.key
```

**Explanation:**

- Public key encrypts data
- Private key decrypts data
- Used in secure cloud communication channels

---

### 2.4 Encryption Summary

| Data Type | Encryption Type | Algorithm |
|---|---|---|
| Data at Rest | Symmetric | AES-256 |
| Data in Transit | Asymmetric | RSA + TLS |

## STEP 3: Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC)

### 3.1 Authentication and Authorization in Cloud Security

In cloud-based enterprises, authentication and authorization are critical to prevent unauthorized access to sensitive systems and data. Authentication verifies the identity of a user, while authorization determines what actions the user is allowed to perform.

To strengthen access control, this framework integrates **Multi-Factor Authentication (MFA)** and **Role-Based Access Control (RBAC)**.

### 3.2 Multi-Factor Authentication (MFA)

### 3.2.1 Overview of MFA

Multi-Factor Authentication (MFA) enhances security by requiring users to provide **two or more independent authentication factors** before granting access. This reduces the risk of account compromise even if passwords are stolen.

### 3.2.2 Authentication Factors

MFA uses the following factors:

| **Factor Type** | **Example** | **Description** |
|---|---|---|
| Something you know | Password, PIN | Knowledge-based authentication |
| Something you have | OTP, Smart card, Authenticator app | Possession-based authentication |
| Something you are | Fingerprint, Face ID | Biometric authentication |

### 3.2.3 MFA Implementation Flow

1. User enters username and password
2. System sends a One-Time Password (OTP) or requests authenticator approval
3. User verifies the second factor
4. Access is granted to cloud resources

### 3.2.4 Benefits of MFA

- Prevents unauthorized access even if credentials are compromised
- Protects against phishing and brute-force attacks
- Enhances compliance with security standards

**ISO/IEC 27001 Mapping:**

- **A.9 – Access Control**

### 3.3 Role-Based Access Control (RBAC)

### 3.3.1 Overview of RBAC

Role-Based Access Control (RBAC) restricts system access based on predefined user roles. Instead of assigning permissions to individual users, permissions are assigned to roles, and users are assigned to roles.

This approach simplifies access management and improves security.

### 3.3.2 Defined Roles in the Framework

| **Role** | **Description** | **Permissions** |
|---|---|---|
| Admin | System administrator | Full system access |
| Manager | Department manager | Read and limited write access |
| User | Regular employee | Read-only access |

### 3.3.3 RBAC Implementation Process

1. Define roles based on organizational structure
2. Assign permissions to each role
3. Assign users to roles
4. Enforce access policies in the cloud environment

### 3.3.4 Benefits of RBAC

- Prevents privilege escalation
- Reduces misconfigurations
- Simplifies access audits
- Supports least privilege principle

**ISO/IEC 27001 Mapping:**

- **A.9.1 – Business Requirements for Access Control**
- **A.9.2 – User Access Management**

### 3.4 Integration of MFA and RBAC

In the proposed framework, MFA and RBAC are integrated to provide layered access security.

**Access Flow:**

1. User authenticates using MFA
2. System verifies role using RBAC policies
3. User is granted access based on role permissions

This layered approach ensures that only authenticated and authorized users can access cloud resources.

---

### 3.5 Security Advantages of MFA + RBAC Integration

| Threat | Mitigation Control |
|---|---|
| Credential theft | MFA |
| Insider threats | RBAC |
| Privilege abuse | RBAC |
| Phishing attacks | MFA |
| Unauthorized access | MFA + RBAC |

---

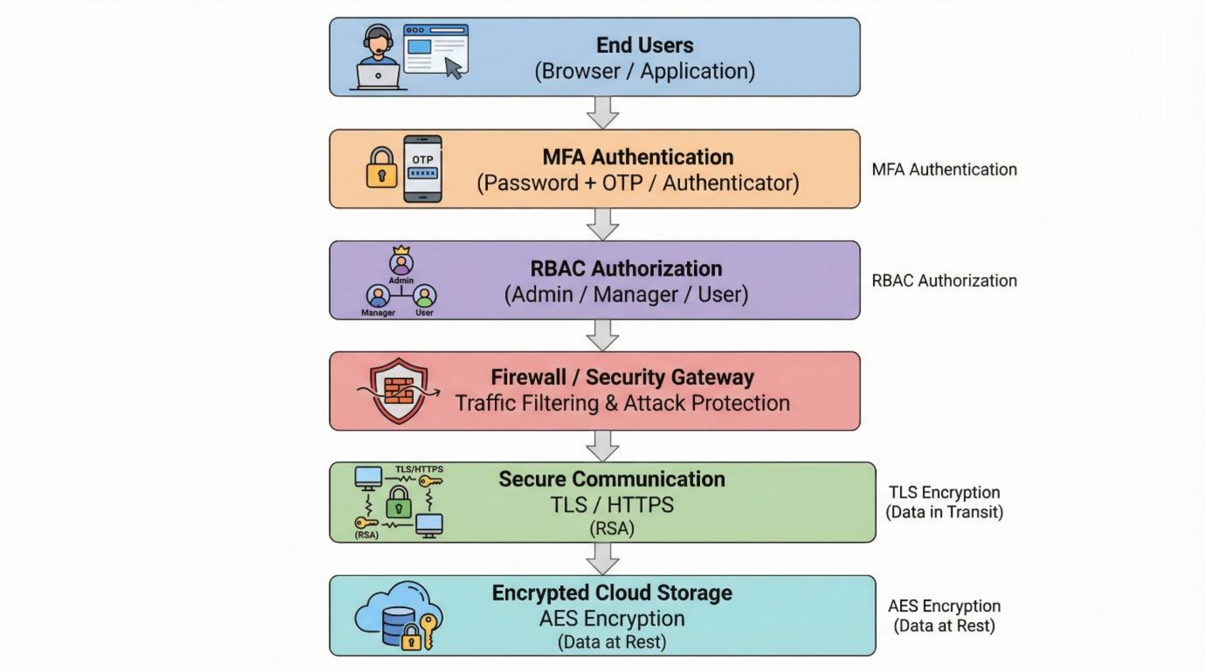
### 3.6 Summary

The integration of Multi-Factor Authentication and Role-Based Access Control significantly strengthens cloud security by ensuring that only verified users with appropriate privileges can access sensitive resources. This approach aligns with industry best practices and international security standards.

## STEP 4: Cloud Security Architecture Diagram

### 4.1 Overview of Cloud Security Architecture

The Cloud Security Architecture represents how security controls are layered within a cloud-based enterprise to protect data, applications, and infrastructure. The proposed architecture follows a **defense-in-depth approach**, ensuring security at multiple levels.



### 4.2 Components of the Architecture

**1□User Layer**

- End users access cloud services through browsers or applications
- Users must authenticate before accessing resources

---

**2□Multi-Factor Authentication (MFA)**

- Verifies user identity using password + OTP/authenticator
- Prevents unauthorized access due to stolen credentials

---

**3□Role-Based Access Control (RBAC)**

- Assigns permissions based on user roles (Admin, Manager, User)
- Ensures least privilege access

---

**4□Firewall / Security Gateway**

- Filters incoming and outgoing traffic
- Blocks unauthorized network access
- Protects against common attacks

---

**5□Secure Communication (TLS/HTTPS)**

- Encrypts data in transit
- Prevents Man-in-the-Middle (MITM) attacks

---

**6□Encrypted Cloud Storage**

- Stores sensitive data using AES encryption
- Ensures data confidentiality at rest

### STEP 5: Risk Assessment Report

### 5.1 Purpose of Risk Assessment

Risk assessment is performed to identify potential threats and vulnerabilities in a cloud-based enterprise environment and evaluate their impact on organizational assets. This process helps in selecting appropriate security controls to reduce risks to an acceptable level.

### 5.2 Identified Assets

| Asset ID | Asset Name | Asset Type |
|---|---|---|
| A1 | Cloud Database | Data |
| A2 | User Accounts | Identity |
| A3 | Cloud VM | Infrastructure |
| A4 | Network Traffic | Network |
| A5 | Cloud Storage | Storage |

### 5.3 Threats and Vulnerabilities

| Threat ID | Threat Description | Vulnerability |
|---|---|---|
| T1 | Data breach | Weak encryption |
| T2 | Unauthorized access | Weak authentication |
| T3 | Man-in-the-Middle attack | Unencrypted traffic |
| T4 | Insider misuse | Excessive privileges |
| T5 | Misconfiguration | Poor access policies |

### 5.4 Risk Evaluation Matrix

**Risk Formula:**

Risk = Likelihood × Impact

| **Threat** | **Asset** | **Likelihood** | **Impact** | **Risk Score** | **Risk Level** |
|---|---|---|---|---|---|
| Data breach | Cloud DB | 3 | 3 | 9 | High |
| Unauthorized access | User accounts | 3 | 2 | 6 | Medium |
| MITM attack | Network traffic | 2 | 3 | 6 | Medium |
| Insider misuse | Cloud VM | 2 | 3 | 6 | Medium |
| Misconfiguration | Cloud storage | 2 | 2 | 4 | Medium |

### 5.5 Risk Mitigation Controls

| **Risk** | **Mitigation Control** |
|---|---|
| Data breach | AES encryption |
| Unauthorized access | MFA + RBAC |
| MITM attack | TLS / HTTPS |
| Insider threats | RBAC + logging |
| Misconfiguration | Security policies |

### 5.6 Risk Assessment Summary

The risk assessment highlights that encryption, access control, and secure communication are critical to reducing cloud security risks. The implemented controls significantly lower the likelihood and impact of major threats.

## Conclusion & Future Enhancements

### 6.1 Conclusion

This project successfully designed and implemented a comprehensive information security framework for a cloud-based enterprise. The framework integrates asset classification, risk assessment, encryption techniques, Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC) to enhance the overall security posture.

Practical implementation using industry-standard tools such as OpenSSL, Wireshark, and Metasploit provided hands-on experience in encryption, traffic analysis, and vulnerability assessment. The framework aligns with ISO/IEC 27001 standards and effectively addresses common cloud security challenges.

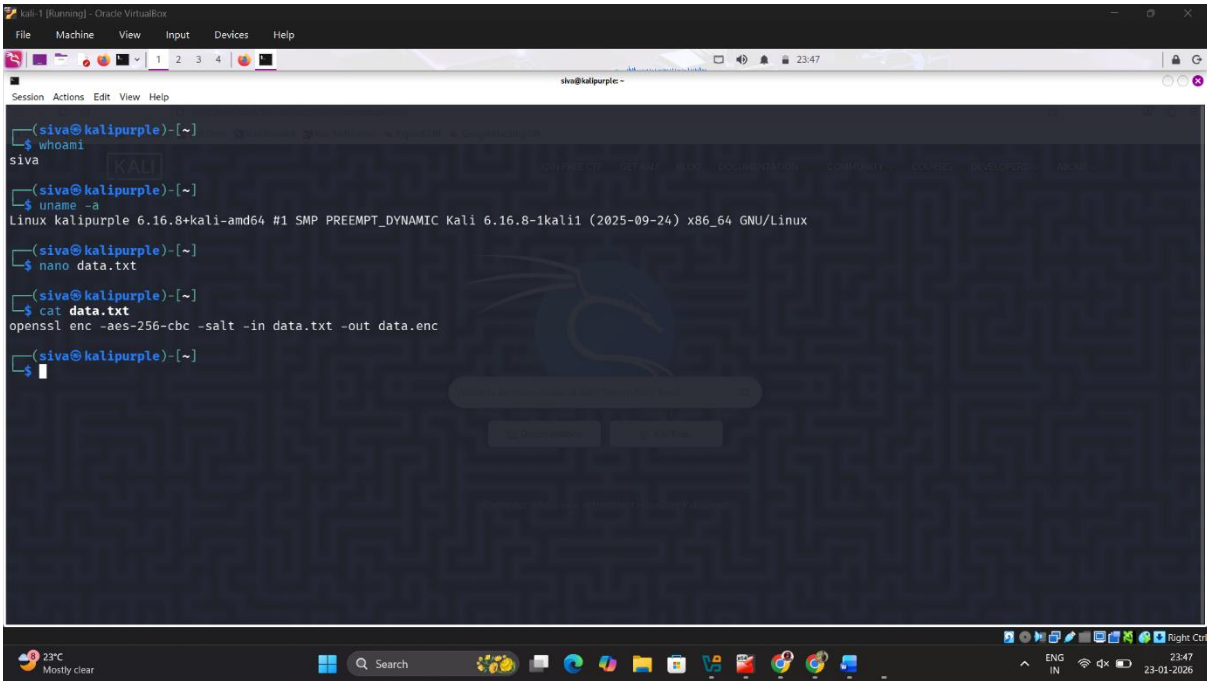
---

### 6.2 Future Enhancements

The framework can be further enhanced by:

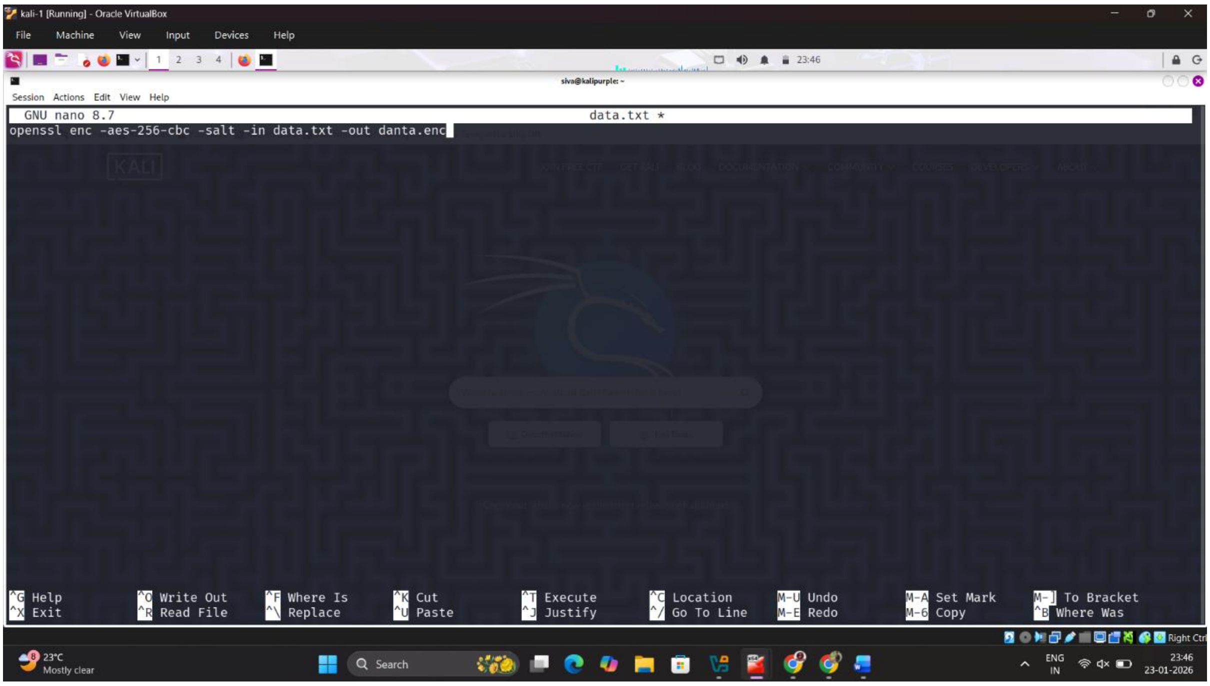
- Implementing Attribute-Based Access Control (ABAC)
- Integrating Security Information and Event Management (SIEM)
- Automating compliance monitoring
- Using AI-based threat detection
- Deploying Zero Trust Architecture

## SCREENSHOTS:



kali-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:47
siva@kalipurple: ~
Session Actions Edit View Help
23°C
Mostly clear
Search
ENG
IN
23:47
23-01-2026

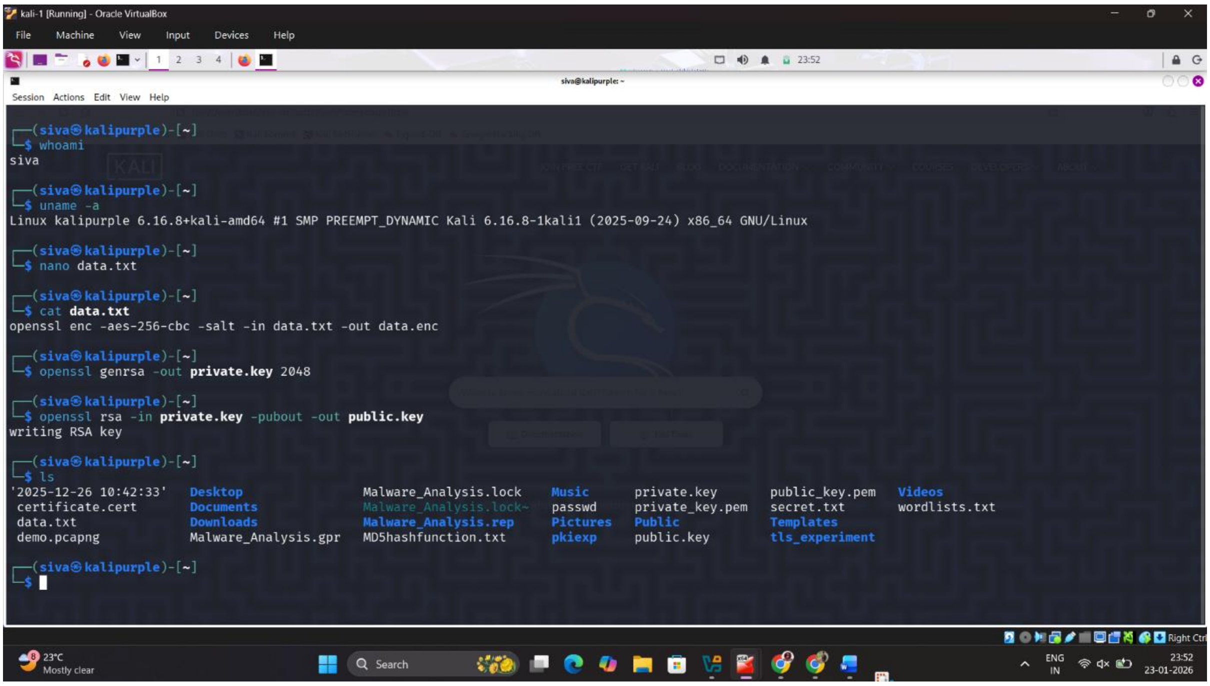
```
┌──(siva㉿kalipurple)-[~]
└─$ whoami
siva

┌──(siva㉿kalipurple)-[~]
└─$ uname -a
Linux kalipurple 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64 GNU/Linux

┌──(siva㉿kalipurple)-[~]
└─$ nano data.txt

┌──(siva㉿kalipurple)-[~]
└─$ cat data.txt
openssl enc -aes-256-cbc -salt -in data.txt -out data.enc

┌──(siva㉿kalipurple)-[~]
└─$ 
```



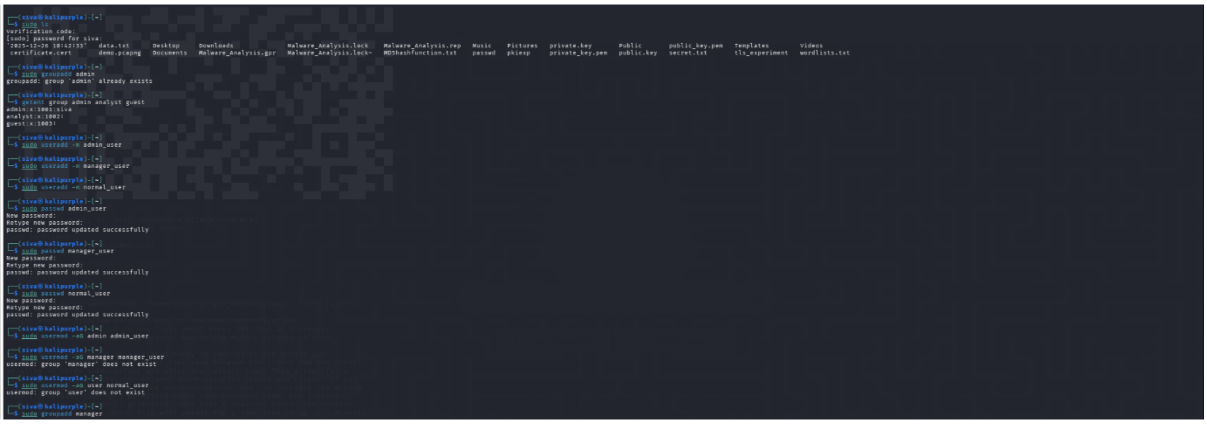
kali-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:46
siva@kalipurple: ~
Session Actions Edit View Help
23°C
Mostly clear
Search
ENG
IN
23:46
23-01-2026

```
  GNU nano 8.7                                 data.txt *
openssl enc -aes-256-cbc -salt -in data.txt -out danta.enc

^G Help       ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^B Where Was
```

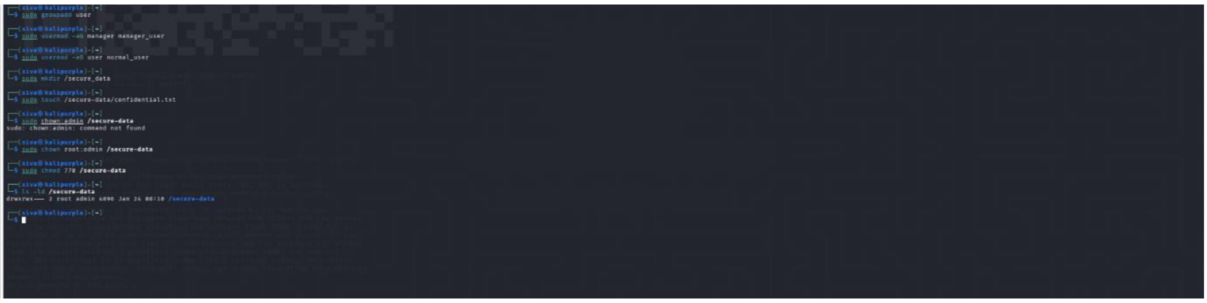
MFA, RBAC CREATION:


kali-1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
siva@kalipurple: ~
Session Actions Edit View Help
23°C
Mostly clear
Search
Right Ctrl
ENG
IN
23:52
23-01-2026

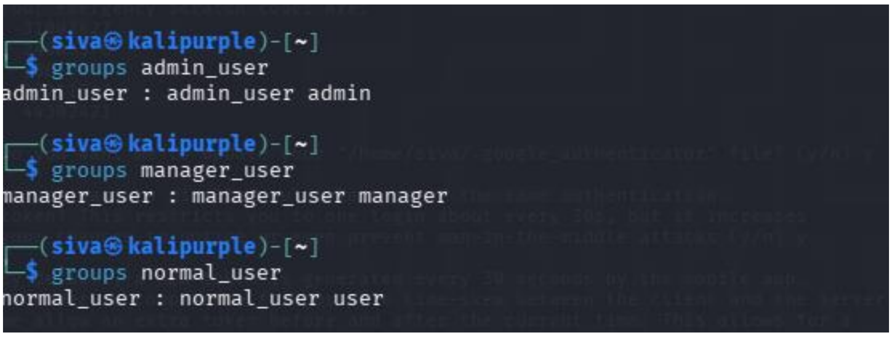
```
┌──(siva㉿kalipurple)-[~]
└─$ whoami
siva

┌──(siva㉿kalipurple)-[~]
└─$ uname -a
Linux kalipurple 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64 GNU/Linux

┌──(siva㉿kalipurple)-[~]
└─$ nano data.txt

┌──(siva㉿kalipurple)-[~]
└─$ cat data.txt
openssl enc -aes-256-cbc -salt -in data.txt -out data.enc

┌──(siva㉿kalipurple)-[~]
└─$ openssl genrsa -out private.key 2048

┌──(siva㉿kalipurple)-[~]
└─$ openssl rsa -in private.key -pubout -out public.key
writing RSA key

┌──(siva㉿kalipurple)-[~]
└─$ ls
'2025-12-26 10:42:33'   Desktop               Malware_Analysis.lock    Music       private.key       public_key.pem   Videos
 certificate.cert       Documents             Malware_Analysis.lock~   passwd      private_key.pem   secret.txt       wordlists.txt
 data.txt               Downloads             Malware_Analysis.rep     Pictures    Public            Templates
 demo.pcapng            Malware_Analysis.gpr  MD5hashfunction.txt      pkiexp      public.key        tls_experiment

┌──(siva㉿kalipurple)-[~]
└─$ 
```



```
┌──(siva㉿kalipurple)-[~]
└─$ sudo ls
Verification code:
[sudo] password for siva:
'2025-12-26 10:42:33'   data.txt      Desktop     Downloads              Malware_Analysis.lock    Malware_Analysis.rep   Music    Pictures   private.key       Public       public_key.pem   Templates        Videos
 certificate.cert       demo.pcapng   Documents   Malware_Analysis.gpr   Malware_Analysis.lock~   MD5hashfunction.txt    passwd   pkiexp     private_key.pem   public.key   secret.txt       tls_experiment   wordlists.txt

┌──(siva㉿kalipurple)-[~]
└─$ sudo groupadd admin
groupadd: group 'admin' already exists

┌──(siva㉿kalipurple)-[~]
└─$ getent group admin analyst guest
admin:x:1001:siva
analyst:x:1002:
guest:x:1003:

┌──(siva㉿kalipurple)-[~]
└─$ sudo useradd -m admin_user

┌──(siva㉿kalipurple)-[~]
└─$ sudo useradd -m manager_user

┌──(siva㉿kalipurple)-[~]
└─$ sudo useradd -m normal_user

┌──(siva㉿kalipurple)-[~]
└─$ sudo passwd admin_user
New password:
Retype new password:
passwd: password updated successfully

┌──(siva㉿kalipurple)-[~]
└─$ sudo passwd manager_user
New password:
Retype new password:
passwd: password updated successfully

┌──(siva㉿kalipurple)-[~]
└─$ sudo passwd normal_user
New password:
Retype new password:
passwd: password updated successfully

┌──(siva㉿kalipurple)-[~]
└─$ sudo usermod -aG admin admin_user

┌──(siva㉿kalipurple)-[~]
└─$ sudo usermod -aG manager manager_user
usermod: group 'manager' does not exist

┌──(siva㉿kalipurple)-[~]
└─$ sudo usermod -aG user normal_user
usermod: group 'user' does not exist

┌──(siva㉿kalipurple)-[~]
└─$ sudo groupadd manager
```

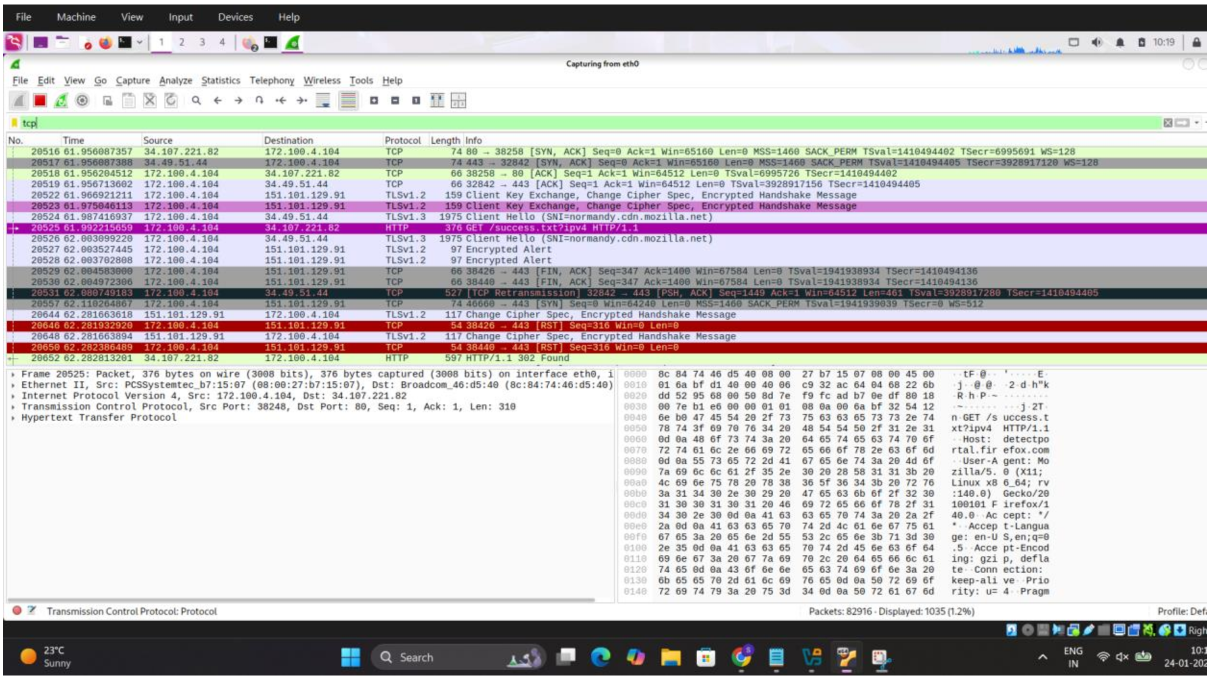


```
┌──(siva㉿kalipurple)-[~]
└─$ sudo groupadd user

┌──(siva㉿kalipurple)-[~]
└─$ sudo usermod -aG manager manager_user

┌──(siva㉿kalipurple)-[~]
└─$ sudo usermod -aG user normal_user

┌──(siva㉿kalipurple)-[~]
└─$ sudo mkdir /secure_data

┌──(siva㉿kalipurple)-[~]
└─$ sudo touch /secure-data/confidential.txt

┌──(siva㉿kalipurple)-[~]
└─$ sudo chown:admin /secure-data
sudo: chown:admin: command not found

┌──(siva㉿kalipurple)-[~]
└─$ sudo chown root:admin /secure-data

┌──(siva㉿kalipurple)-[~]
└─$ sudo chmod 770 /secure-data

┌──(siva㉿kalipurple)-[~]
└─$ ls -ld /secure-data
drwxrwx--- 2 root admin 4096 Jan 24 00:10 /secure-data

┌──(siva㉿kalipurple)-[~]
└─$ 
```



```
┌──(siva㉿kalipurple)-[~]
└─$ groups admin_user
admin_user : admin_user admin

┌──(siva㉿kalipurple)-[~]
└─$ groups manager_user
manager_user : manager_user manager

┌──(siva㉿kalipurple)-[~]
└─$ groups normal_user
normal_user : normal_user user
```

**Network traffic captured using Wireshark showing TLS-encrypted communication over TCP (HTTPS), demonstrating secure data transmission:**



File Machine View Input Devices Help
1 2 3 4
10:19
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
23°C
Sunny
Search
ENG
IN
24-01-202

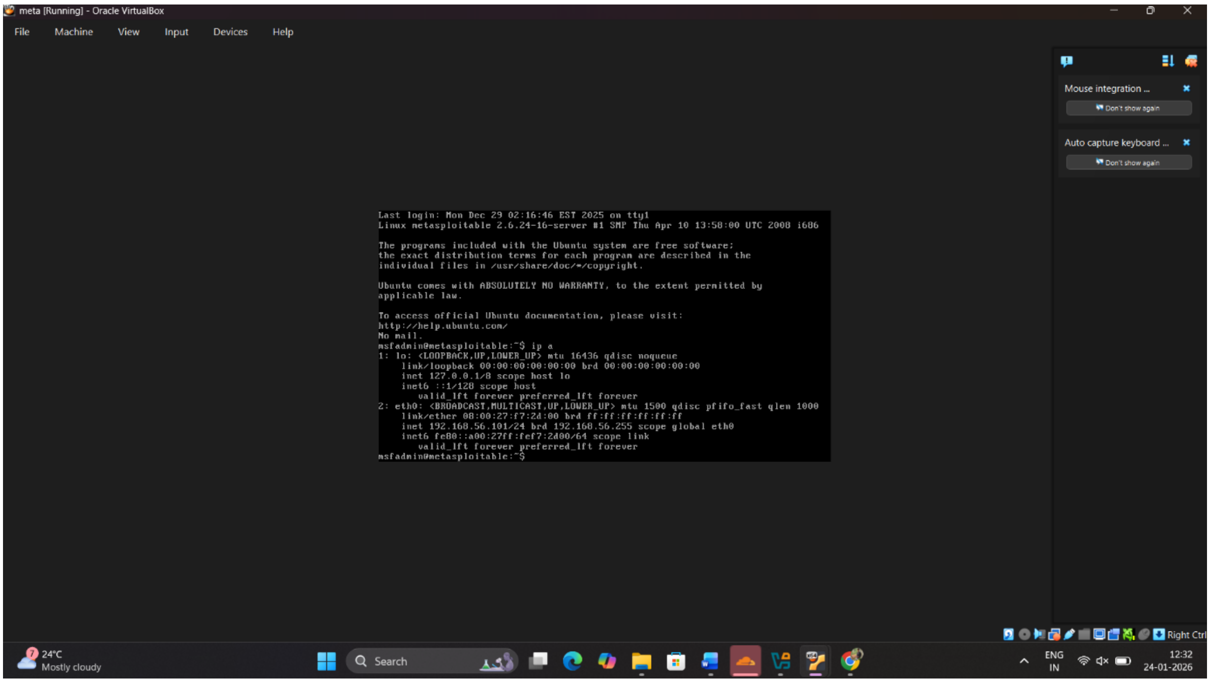
```
No.   Time           Source           Destination      Protocol Length Info
 20516 61.956087357  34.107.221.82    172.100.4.104    TCP        74 80 → 38258 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1410494402 TSecr=6995691 WS=128
 20517 61.956087388  34.49.51.44      172.100.4.104    TCP        74 443 → 32842 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1410494405 TSecr=3928917120 WS=128
 20518 61.956204512  172.100.4.104    34.107.221.82    TCP        66 38258 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=6995726 TSecr=1410494402
 20519 61.956713602  172.100.4.104    34.49.51.44      TCP        66 32842 → 443 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=3928917156 TSecr=1410494405
 20522 61.966921211  172.100.4.104    151.101.129.91   TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 20523 61.975046113  172.100.4.104    151.101.129.91   TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 20524 61.987416937  172.100.4.104    34.49.51.44      TLSv1.3  1975 Client Hello (SNI=normandy.cdn.mozilla.net)
 20525 61.992215659  172.100.4.104    34.107.221.82    HTTP      376 GET /success.txt?ipv4 HTTP/1.1
 20526 62.003099220  172.100.4.104    34.49.51.44      TLSv1.3  1975 Client Hello (SNI=normandy.cdn.mozilla.net)
 20527 62.003527445  172.100.4.104    151.101.129.91   TLSv1.2    97 Encrypted Alert
 20528 62.003702808  172.100.4.104    151.101.129.91   TLSv1.2    97 Encrypted Alert
 20529 62.004583000  172.100.4.104    151.101.129.91   TCP        66 38426 → 443 [FIN, ACK] Seq=347 Ack=1400 Win=67584 Len=0 TSval=1941938934 TSecr=1410494136
 20530 62.004972306  172.100.4.104    151.101.129.91   TCP        66 38440 → 443 [FIN, ACK] Seq=347 Ack=1400 Win=67584 Len=0 TSval=1941938934 TSecr=1410494136
 20531 62.080749183  172.100.4.104    34.49.51.44      TCP       527 [TCP Retransmission] 32842 → 443 [PSH, ACK] Seq=1449 Ack=1 Win=64512 Len=461 TSval=3928917280 TSecr=1410494405
 20557 62.110264867  172.100.4.104    151.101.129.91   TCP        74 46660 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1941939039 TSecr=0 WS=512
 20644 62.281663618  151.101.129.91   172.100.4.104    TLSv1.2   117 Change Cipher Spec, Encrypted Handshake Message
 20646 62.281932920  172.100.4.104    151.101.129.91   TCP        54 38426 → 443 [RST] Seq=316 Win=0 Len=0
 20648 62.281663894  151.101.129.91   172.100.4.104    TLSv1.2   117 Change Cipher Spec, Encrypted Handshake Message
 20650 62.282386489  172.100.4.104    151.101.129.91   TCP        54 38440 → 443 [RST] Seq=316 Win=0 Len=0
 20652 62.282813201  34.107.221.82    172.100.4.104    HTTP      597 HTTP/1.1 302 Found
```

```
› Frame 20525: Packet, 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface eth0, i
› Ethernet II, Src: PCSSystemtec_b7:15:07 (08:00:27:b7:15:07), Dst: Broadcom_46:d5:40 (8c:84:74:46:d5:40)
› Internet Protocol Version 4, Src: 172.100.4.104, Dst: 34.107.221.82
› Transmission Control Protocol, Src Port: 38248, Dst Port: 80, Seq: 1, Ack: 1, Len: 310
› Hypertext Transfer Protocol
```

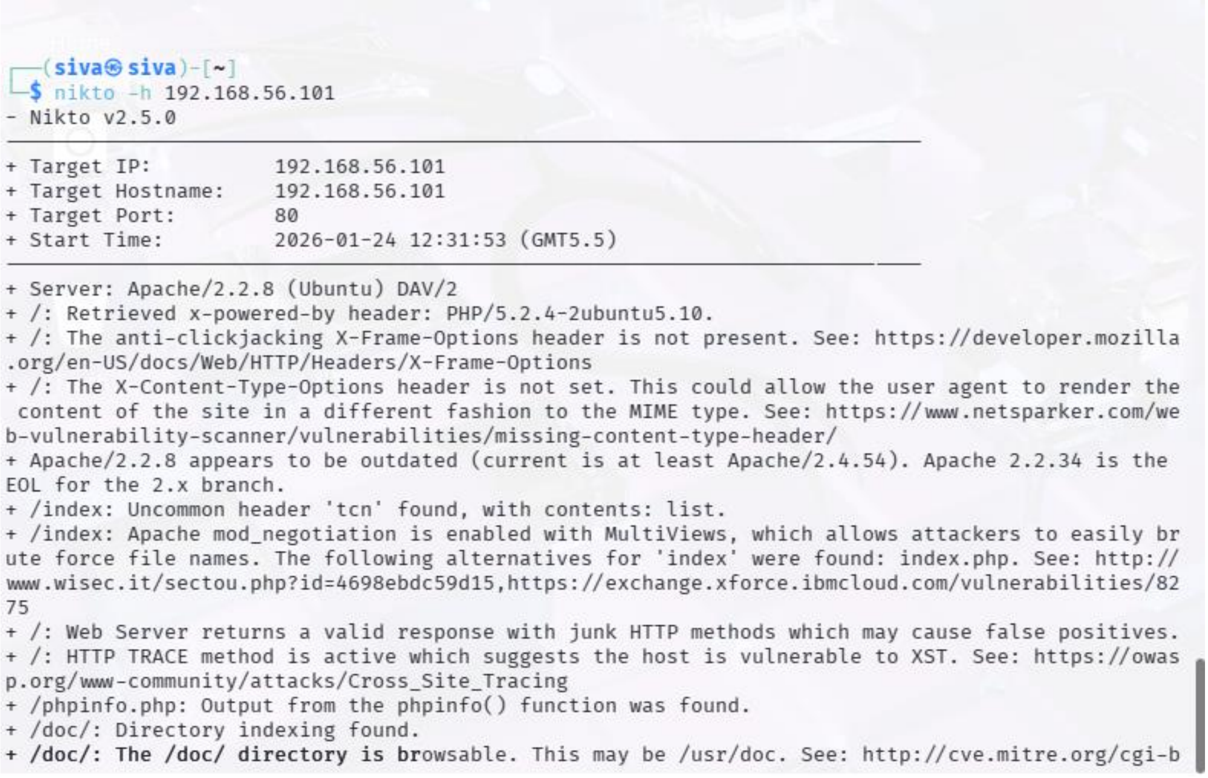
```
0000  8c 84 74 46 d5 40 08 00  27 b7 15 07 08 00 45 00   ··tF·@·· '·····E·
0010  01 6a bf d1 40 00 40 06  c9 32 ac 64 04 68 22 6b   ·j··@·@· ·2·d·h"k
0020  dd 52 95 68 00 50 8d 7e  f9 fc ad b7 0e df 80 18   ·R·h·P·~ ········
0030  00 7e b1 e6 00 00 01 01  08 0a 00 6a bf 32 54 12   ·~······ ···j·2T·
0040  6e b0 47 45 54 20 2f 73  75 63 63 65 73 73 2e 74   n·GET /s uccess.t
0050  78 74 3f 69 70 76 34 20  48 54 54 50 2f 31 2e 31   xt?ipv4  HTTP/1.1
0060  0d 0a 48 6f 73 74 3a 20  64 65 74 65 63 74 70 6f   ··Host:  detectpo
0070  72 74 61 6c 2e 66 69 72  65 66 6f 78 2e 63 6f 6d   rtal.fir efox.com
0080  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0090  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
00a0  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00b0  3a 31 34 30 2e 30 29 20  47 65 63 6b 6f 2f 32 30   :140.0)  Gecko/20
00c0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 31   100101 F irefox/1
00d0  34 30 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   40.0··Ac cept: */
00e0  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *··Accep t-Langua
00f0  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0100  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
0110  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0120  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te··Conn ection:
0130  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 50 72 69 6f   keep-ali ve··Prio
0140  72 69 74 79 3a 20 75 3d  34 0d 0a 50 72 61 67 6d   rity: u= 4··Pragm
```

```
Transmission Control Protocol: Protocol          Packets: 82916 · Displayed: 1035 (1.2%)          Profile: Def
```

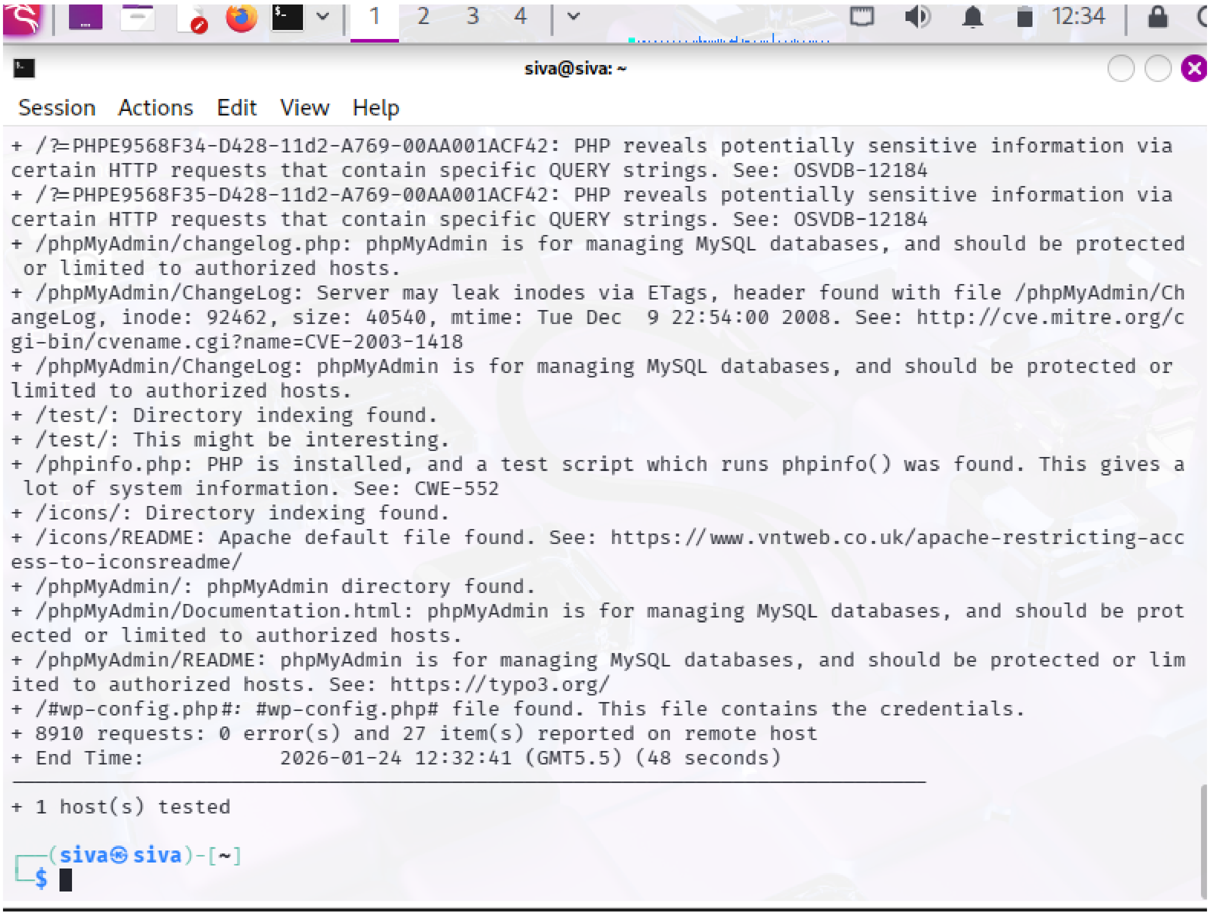
## Metasploitable Virtual Machine Setup and Target Identification:



```
Last login: Mon Dec 29 02:16:46 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:f7:2d:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fef7:2d00/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```



```
┌──(siva㉿siva)-[~]
└─$ nikto -h 192.168.56.101
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2026-01-24 12:31:53 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the
 content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/we
b-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the
EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily br
ute force file names. The following alternatives for 'index' were found: index.php. See: http://
www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/82
75
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owas
p.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-b
```



```
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected
 or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Ch
angeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 22:54:00 2008. See: http://cve.mitre.org/c
gi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or
limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a
 lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-acc
ess-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be prot
ected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or lim
ited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2026-01-24 12:32:41 (GMT5.5) (48 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(siva㉿siva)-[~]
└─$ 
```