Welcome to Day 9

Day 9

- Introduction
- What is OpenSSH
- Installing OpenSSH
- Basic Configuration
- Key Based Authentication
- Analyzing SSH logs
- Storing Logs
- Monitoring Logs

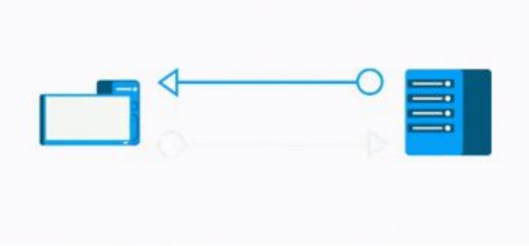
01

Introduction

Configuring and Securing OpenSSH on Linux

OpenSSH

It provides encrypted communication between clients and servers.



02

OpenSSH

What is OpenSSH on Linux

OpenSSH is a suite of secure networking tools based on the SSH protocol.

OpenSSH

Key Components

SSH

Secure client for remote login.

SSHD

Server daemon that handles incoming connections.

SCP

Secure file copy.

Key Components

SSH-keygen

Tool for generating authentication keys.

sftp

Secure file transfer protocol.

Why secure OpenSSH?

- Prevent Unauthorized Access: Protect sensitive data and system integrity.
- Ensure Confidentiality: Encrypt communication to prevent eavesdropping.
- Maintain System Integrity: Only authorized users can make changes to the system.

Common Security Measures

- Disable root login to reduce the risk of system compromise.
- Use key-based authentication for stronger security.
- Change default SSH port to avoid automated attacks.
- Employ tools like Fail2Ban to block suspicious activities.

03

OpenSSH

Installing OpenSSH on Linux

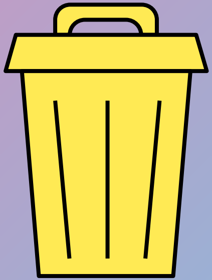
Installing OpenSSH

```
sudo apt-get install openssh-server
sudo systemctl start sshd
sudo systemctl enable sshd
```

04

Configs

Basic Configuration



Basic Configuration

- Configuration File: /etc/ssh/sshd_config
- Key Parameters:
  - Port 22: Default SSH port
  - PermitRootLogin no: Disable root login
  - PasswordAuthentication no: Disable password authentication, use key-based authentication
  - AllowUsers user1 user2: Restrict users who can log in

05

Key Based

Key Based Authentication

Key Based Authentication

- Generating Keys:

```
ssh-keygen -t rsa -b 4096
```

- Copying Public Key to Server:

```
ssh-copy-id user@server
```

- Disabling Password Authentication:
  - Edit /etc/ssh/sshd_config
  - Set PasswordAuthentication no
  - Restart SSH: sudo systemctl restart sshd

06

Analyzing

SSH Logs

Location of Logs

Debian / Ubuntu

/var/log/auth.log

RHEL / CentOS

/var/log/secure

Important Log Entries:

1) Successful Logins

2) Failed login attempts

3) Key-based authentication attempts

07

Storing

SSH Logs

Storing Logs

- Centralized Logging Solutions:
  - Syslog: Standard for logging
  - Rsyslog: Enhanced syslog
  - Logrotate: Manage log file sizes
- Configuring Rsyslog:
  - Edit /etc/rsyslog.conf
  - Enable and configure remote logging

08

Monitoring

SSH Logs

Tools For Monitoring

tail -f /var/log/auth.log

Real-time monitoring

Log watch

Summarizes log entries

ELK Stack

Elasticsearch, Logstash, Kibana Powerful log analysis and visualization

Hands-on

OpenSSH Commands

Steps for OpenSSH

```
sudo apt update
sudo apt install openssh-server
```

```
sudo systemctl status ssh
```

```
sudo systemctl start ssh
```

```
sudo systemctl enable ssh
```

```
sudo nano /etc/ssh/sshd_config
```

Common configurations include changing the default port (Port 22), disabling root login (PermitRootLogin no), and specifying allowed users.

```
sudo systemctl restart ssh
```

Steps for OpenSSH - Firewall

```
sudo ufw allow 2222/tcp
```

```
ssh username@hostname -p 2222
```

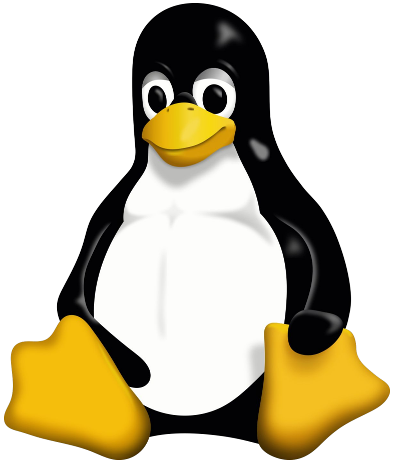
Steps for OpenSSH - Key Gen

```
ssh-keygen -t rsa -b 4096

ssh-copy-id -i ~/.ssh/id_rsa.pub -p 2222 username@hostname
```

Q/A Session

Thank you !



End of Day 9 & The Linux Week!