sdnog workshops

sdnog workshops provide hands-on training and technical sessions for network operators in Sudan, focusing on areas like network security, IPv6, routing, DNS , etc. These workshops aim to build local capacity and enhance skills among IT professionals, fostering a stronger internet infrastructure in the region.

- ISOC Chapters collaboration (Sudan & Lebanon) : DNS/DNSSEC Workshop
- HAProxy Lab Setup Guide : Multi-OS Installation
- Load Balancing Strategies: From Theory to Practice with HAProxy
- BGP Resource Management Workshop
- ICANN DNS Workshop
- Hardening a web-server for the modern internet
- DNS Workshop
- DNSSEC Workshop
- Ethical Hacking Workshop
- High Availability in LAMP Stack workshop
- How to Secure your Network Workshop
- Internet Governance Forum
- IPv6 Workshop by AFRINIC
- IPv6 Fundamentals Workshop
- IXP Best Practices
- Networks Fundamental Workshop
- Network Management and Monitoring Workshop
- Networking Best Practices Workshop
- UNIX Boot Camp
- UNIX/Linux, Networking and DNS Online Course
- Automation Tool: Ansible
- IPv6 for Services
- Network Services and Monitoring Online Course
- OpenStack Workshop

- Network Monitoring Workshop
- Security Workshop - Ethical Hacking
- Layer 2 Security Workshop
- Build your own e-mail Server
- Introduction to Git Workshop
- Automation with Ansible : The basics
- Automation with Ansible - Online Course

ISOC Chapters collaboration (Sudan & Lebanon) : DNS/DNSSEC Workshop

The Internet Society (ISOC) Chapters of Sudan and Lebanon have joined forces to strengthen regional expertise in DNS and DNSSEC technologies. This collaboration aims to foster knowledge exchange, build technical capacity, and promote best practices in secure domain name system management.

The DNS/DNSSEC Workshop serves as a platform for participants to learn from experienced trainers and peers, enhancing their skills in DNS operations, DNSSEC implementation, and overall internet security. By working together, the Sudanese and Lebanese ISOC Chapters are creating opportunities for technical advancement and regional cooperation, contributing to a safer and more resilient internet.

Workshop Level

Intermediate Level.
Anyone working with DNS in their corporate or carrier infrastructure will find this class worthwhile.
IT technicians, Systems administrators,..

Instructor

- Mohamed Alnour Hafez

Date & Time

- Date: TBD
- Time: TBD

Workshop Modules

Module 1: Introduction to DNS
Gain a solid foundation in how the Domain Name System works, including its critical role in the internet infrastructure. This module also includes practical exercises using tools like dig and drill for testing and troubleshooting DNS configurations, ensuring participants thoroughly understand DNS operations.

Module 2: DNSSEC

Understand the importance of DNS Security Extensions (DNSSEC) in ensuring the authenticity and integrity of DNS responses, protecting against attacks like DNS spoofing. This module will cover all aspects of DNSSEC, from key management to signing zones, and will include testing using tools like dig to verify DNSSEC implementation.

Module 3: Hands-on Deployment of DNSSEC
Participants will deploy DNSSEC using a real domain on provided Virtual Private Servers (VPS). This practical exercise will ensure a deep understanding of DNSSEC implementation and validation processes.

Requirements

Participants are required to meet the following:
- Stable Internet Connection
- SSH Client (PuTTY for Windows, macOS/Linux: Built-in terminal)
- Background in Linux: command line, Managing files and directories, permissions and processes, vim & nano, installing packages

HAProxy Lab Setup Guide : Multi-OS Installation

Prerequisites

- 3 VMs (or use VirtualBox/VMware Workstation to create them)
- Web browser access (for those using AFNOG infrastructure)

VM Setup

1. **VM1:** HAProxy
    - IP: 192.168.1.X
2. **VM2:** Apache Server
    - IP: 192.168.1.Y
3. **VM3:** Nginx Server
    - IP: 192.168.1.Z

Local Hosts File Configuration

Add the following entries to your local hosts file, pointing them all to the HAProxy IP (192.168.1.X):

```
192.168.1.X lb.lab.afnog.org
192.168.1.X www.lab.afnog.org
192.168.1.X nginx.lab.afnog.org
192.168.1.X apache.lab.afnog.org
```

Step 1: Install and Configure HAProxy (VM1)

Red Hat-based systems (CentOS, Fedora)

```
sudo yum update
sudo yum install haproxy
```

Debian-based systems (Ubuntu, Debian)

```
sudo apt update
sudo apt install haproxy
```

FreeBSD

```
sudo pkg update
sudo pkg install haproxy
```

Step 2: Install and Configure Apache (VM2)

Red Hat-based systems

```
sudo yum update
sudo yum install httpd
sudo systemctl start httpd
sudo systemctl enable httpd
```

Debian-based systems

```
sudo apt update
sudo apt install apache2
```

FreeBSD

```
sudo pkg update
sudo pkg install apache24
sudo sysrc apache24_enable="YES"
sudo service apache24 start
```

Create a custom index.html:

```
echo "This is the Apache Server" | tee /var/www/html/index.html
```

On FreeBSD

```
echo "This is the Apache Server" | tee /usr/local/www/apache24/data/index.html
```

Step 3: Install and Configure Nginx (VM3)

Red Hat-based systems

```
sudo yum update
sudo yum install nginx
sudo systemctl start nginx
sudo systemctl enable nginx
```

Debian-based systems

```
sudo apt update
sudo apt install nginx
```

FreeBSD

```
sudo pkg update
sudo pkg install nginx
sudo sysrc nginx_enable="YES"
sudo service nginx start
```

Create a custom index.html:

```
echo "This is the Nginx Server" |  tee /var/www/html/index.html
 # For FreeBSD:
echo "This is the Nginx Server" | tee /usr/local/www/nginx/index.html
```

HAProxy Configuration

Step 1: Basic Frontend and Backend Setup (Round-Robin)

HAProxy Configuration: Edit the HAProxy configuration file:

- **Red Hat and Debian:** /etc/haproxy/haproxy.cfg
- **FreeBSD:** /usr/local/etc/haproxy.conf

Add the following configuration:

```
global
    log         127.0.0.1:514 local1 info
    chroot      /var/empty
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon

defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 3000

frontend http-in
    bind *:80
    default_backend www_back

backend www_back
    balance roundrobin
    server nginx_server vm1.log.afnog.org:80 check
    server apache_server vm2.lab.afnog.org:80 check
```

Restart HAProxy:

```
systemctl restart haproxy
```

Step 2: Advanced Configuration with ACLs (Access Control Lists)

Updated HAProxy Configuration:

Modify the existing HAProxy configuration to include the following:

```
frontend http_front
    bind *:80
    acl url_nginx hdr(host) -i nginx.lab.afnog.org
    acl url_apache hdr(host) -i apache.lab.afnog.org
    use_backend nginx_back if url_nginx
    use_backend apache_back if url_apache
    default_backend www_back

backend www_back
    balance roundrobin
    server nginx_server 192.168.1.Z:80 check
    server apache_server 192.168.1.Y:80 check

backend nginx_back
    server nginx_server 192.168.1.Z:80 check

backend apache_back
    server apache_server 192.168.1.Y:80 check
```

To set up an active-passive configuration for your backend node, adjust the existing HAProxy configuration to include the following:

```
backend www_back
    balance roundrobin
    server nginx_server 192.168.1.Z:80 check
    server apache_server 192.168.1.Y:80 check backup
```

this setup will make node apache_server as a passive node and will not recive traffic unless node nginx_server is down

Restart HAProxy:

```
sudo systemctl restart haproxy
```

Step 3: Adding a Status Page

Final HAProxy Configuration:

Add the following configuration for the status page:

```
listen stats
    bind *:8404
    stats enable
    stats uri /
    stats refresh 5s
```

Restart HAProxy:

sudo systemctl restart haproxy

Testing the Status Page:

You can access the status page by navigating to http://192.168.1.X:8404/ in your web browser.

SSL Termination on HAProxy

Generate a Self-Signed Certificate:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/haproxy.key -out /etc/ssl/certs/hapro
```

Combine the Certificate and Key:

```
cat /etc/ssl/certs/haproxy.crt /etc/ssl/private/haproxy.key |  tee /etc/ssl/certs/haproxy.pem
```

Note: For development SSL certificates, you can use the repository at https://github.com/BenMorel/dev-certificates

Update HAProxy Configuration to Use SSL:

Add the following to the `frontend http_front` section:

```
bind *:443 ssl crt /etc/ssl/certs/haproxy.pem
redirect scheme https if !{ ssl_fc }
```

Restart HAProxy:

```
sudo systemctl restart haproxy
```

Example for Layer 4 Load balancing , DB port :

```
frontend mysql
 mode tcp
 bind :3306
 default_backend mysql_servers
```

```
backend mysql_servers
 mode tcp
 balance leastconn
 server s1 192.168.0.10:3306 check
 server s2 192.168.0.11:3306 check
```

Configure Syslog for HAProxy Logging

1. Open the syslog configuration file for editing:

```
vi /etc/syslog.conf
```

1. Add the following lines to configure logging:

```
*.err;kern.warning;auth.notice;mail.crit                /dev/console
local1.*                                                /var/log/haproxy.log
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err   /var/log/messages
```

1. Create the HAProxy log file:

```
touch /var/log/haproxy.log
```

1. Set the appropriate ownership for the log file:

```
chown haproxy:haproxy /var/log/haproxy.log
```

1. Update the syslogd flags to bind to localhost and run in compatibility mode:

```
sysrc syslogd_flags="-b localhost -C"
```

1. Restart the syslog service to apply changes:

```
service syslogd restart
```

Testing

Using `web browser`:

1. Test round-robin for `www.lab.afnog.org`:
2. Repeat the command several times to see alternating responses from Nginx and Apache.

- Test Nginx backend:

```
 nginx.lab.afnog.org
# This should consistently return the Nginx server response.
```

- Test Apache backend:

```
 apache.lab.afnog.org
# This should consistently return the Apache server response.
```

- Test SSL termination:

```
 https://www.lab.afnog.org
# This should return responses over HTTPS, with round-robin load balancing between Nginx and Apache.
```

Troubleshooting: Common Issues and Solutions

HAProxy not starting:

- Check the configuration file for syntax errors:

```
haproxy -c -f /etc/haproxy/haproxy.cfg
```

- Verify that the ports HAProxy is trying to bind to are not in use by other services.

Backend servers not responding:

  - Ensure that Apache and Nginx are running on their respective VMs.
  - Check firewall rules to allow traffic between HAProxy and backend servers.
  - Verify the IP addresses and ports in the HAProxy configuration.

SSL certificate issues:

  - Double-check the path to the SSL certificate and key in the HAProxy configuration.
  - Ensure the combined PEM file has the correct permissions.

ACLs not working as expected:

  - Verify that your local hosts file is correctly configured.
  - Use `tcpdump` or `wireshark` to inspect the HTTP headers and ensure the correct `Host` header is being sent.

Performance Tuning: Optimizing HAProxy

Increase maximum connections:

  - Adjust the `maxconn` parameter in the `global` section based on your server's capacity.

Enable kernel TCP splicing:

- Add `option tcpka` to the `defaults` section for keep-alive connections.

Use HTTP/2:

- Update your SSL binding to support HTTP/2:

```
bind *:443 ssl crt /etc/ssl/certs/haproxy.pem alpn h2,http/1.1
```

Implement caching:

- Consider adding a caching layer with Varnish in front of HAProxy for static content.

Optimal Configuration Options for Web-Based Frontends

It's crucial to customize the following according to your application's specific requirements.

```
frontend http-in
bind *:80
bind *:443 ssl crt /etc/haproxy/certs/cert.pem no-sslv3
mode http
option httplog
log global

# Redirect HTTP to HTTPS (enforce HTTPS for all traffic)
http-request redirect scheme https code 301 if !{ ssl_fc }

# Set default security headers for responses
# Enforce HSTS for HTTPS (1 year, include subdomains, preload)
http-response set-header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"

# Clickjacking protection, allow only the same origin to embed this site
http-response set-header X-Frame-Options "SAMEORIGIN"

# XSS filtering enabled in browsers, block if an attack is detected
http-response set-header X-XSS-Protection "1; mode=block"

# Prevent MIME type sniffing (force browser to honor content type declared by the server)
http-response set-header X-Content-Type-Options "nosniff"

# Add Content Security Policy to mitigate XSS and data injection attacks
http-response set-header Content-Security-Policy "default-src 'self'; script-src 'self'; object-src 'none'"

# Disable referrer information leakage when navigating to a different origin
http-response set-header Referrer-Policy "no-referrer-when-downgrade"

# Prevent browsers and proxies from caching sensitive data
http-response set-header Cache-Control "no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0"

# Set secure cookies (only for HTTPS, HttpOnly, and prevent cross-site requests)
```

```
acl secure_cookie hdr_sub(cookie) Secure
http-response set-header Set-Cookie %[res.hdr(Set-Cookie)] if secure_cookie
http-response set-header Set-Cookie Secure; HttpOnly; SameSite=Strict if secure_cookie

# Forward client's original IP in X-Forwarded-For header
http-request add-header X-Forwarded-For %[src]

# Forward the protocol used by the client (HTTP/HTTPS) in X-Forwarded-Proto header
http-request add-header X-Forwarded-Proto https if { ssl_fc }
http-request add-header X-Forwarded-Proto http if !{ ssl_fc }

# Preserve the original Host header
http-request add-header X-Forwarded-Host %[req.hdr(host)]

default_backend servers
```

Security Considerations

1. Regularly update HAProxy and backend servers
2. Implement strong SSL/TLS configurations
3. Use IP whitelisting for the HAProxy stats page
4. Consider implementing Web Application Firewall (WAF) rules in HAProxy
5. Regularly audit your HAProxy configurations and access logs

This guide provides a comprehensive setup process for HAProxy, starting from a basic configuration and progressing to more advanced setups with ACLs, SSL termination, and performance optimization. Always ensure to test thoroughly in a staging environment before applying changes to production systems.

Author

Manhal Mohamed , sdnog team

Load Balancing Strategies: From Theory to Practice with HAProxy

Date & Time

- Event: Africa Internet Summit - AIS 2024
- Date: September 5, 2024
- Time: 13:00 - 15:30

Intended Audience

This workshop is specifically designed for Senior Systems Engineers who are looking to deepen their understanding of load balancing and HAProxy configuration.

Description

This workshop is a comprehensive 2-hour session that includes both theoretical concepts and practical hands-on labs, with a short break. The session covers the following topics:

Agenda

Introduction (5 minutes)

- Brief overview of load balancing concepts
- Importance of load balancing in modern infrastructure

Load Balancing Fundamentals (15 minutes)

- Types of load balancers:

```
  * Layer 4 (L4) vs. Layer 7 (L7)
```

- Common load balancing algorithms:

```
  * Round Robin
  * Least Connections
  * IP Hash
```

- Health checks and failure handling

Introduction to HAProxy (10 minutes)

- Overview of HAProxy and its key features
- Architecture and components of HAProxy

HAProxy Configuration Basics (20 minutes)

- Structure of the HAProxy configuration file
- Key sections:

```
* Frontend
* Backend
```

- Access Control Lists (ACLs) and `use_backend` rules

Advanced HAProxy Features (20 minutes)

- SSL termination
- Sticky sessions
- HTTP rewriting and redirection
- Logging and monitoring

Live Demo: Setting up HAProxy (30 minutes)

- Installing HAProxy
- Configuring a basic load balancer
- Testing and verifying the setup
- Demonstration of advanced features

Best Practices and Performance Tuning (10 minutes)

- Optimization of HAProxy configuration
- Security considerations
- Scaling HAProxy

Session Hands-On

- Slides "click here"
- HAProxy Lab Setup Guide - Multi-OS Installation

Lead Instructor

- **Manhal M. Mokhtar**

BGP Resource Management Workshop

The IRR system is a global databases where network operators publish their routing policies and announcements in order for other interested network operators to use that data, for ease of interconnecting and working together. In this workshop we will discuss in details the IRR system and to use it to manage your resources. Attendees will learn how to use common automation techniques to use the IRR easily and efficiently to perform network management.

Special Thanks To Our Sponsors

We Would like to Thanks our wonderful sponsors! without whom our workshop would not be possible:

- **Infrastructure Provider** : INX-ZA
- **Meeting Platform Support**: Global NOG Alliance
- **Supporting Organization** : Packet Clearing House

Objectives

By the end of this workshop you will be able to :

- Understand the Internet Routing Registry system
- Understand the importance of Registering IRR Objects
- Know how to confirm that your resources are accurately registered (and fix shortcomings)
- Learn how to automate your network filtering.
- Know what is RPKI and How to get a ROA

Workshop Level

Intermediate Level

Who should attend

Individuals involved in BGP, BGP network filtering.

Requirements

- You should have some idea of how Internet peering and transit works

- You should have conceptual BGP skills
- You should know how to manipulate objects in a WHOIS database

Date & Time

- Date: Sunday, 27 March 2022
- Time: 08:00 - 11:00 UTC (10:00 - 13:00 Sudan Time)

Instructors

- Alkhansaa Abdalla - IP Number Resource Analyst (AFRINIC)
- Dibya Khatiwada - Global Peering Coordinator (Packet Clearing House)
- Edd
- Hiba Abbas
- Nishal Goburdhan

Fees

Free :-)

Materials

You can download the slides from here

Reference

Some useful reading material

- AFRINIC’s Internet Routing Registry (IRR)
- A Quickstart Guide to Documenting Your Prefixes with IRR

ICANN DNS Workshop

Domain Name System "DNS" is one of the core services in the Internet, it translates domain names to IP addresses. This is a 3-days, online theoretical workshop in collaboration with ICANN. You’ll get a comprehensive overview of DNS operations, abuse and security.

Objectives

By the end of the workshop, attendees will know what is DNS? how it works? how to prevent DNS abuse and how to secure it?

Workshop Level

Beginner Level

Prerequisites

- Good understanding of network basics (IP networking)

Date & Time

- Day 1 : DNS Operations: 16 February 2021, 10:00 AM - 11:30 AM (KRT Time)
- Day 2 : DNS Abuse: 17 February 2021, 10:00 AM - 12:00 PM (KRT Time)
- Day 3 : DNSSEC: 18 February 2021, 10:00 AM - 11:00 AM (KRT Time)

Trainers

This online workshop will be delivered by

- Paul Muchene
- Yazid Akanho

Agenda

Day 1: DNS Operations

1. What is DNS?
2. Some common DNS records
3. DNS resolution process
4. Caching
5. Some best practices

Day 2: DNS Abuse

1. What is abuse of DNS?
2. Categories of DNS abuse
3. Solutions overview
4. Recommendations

Day 3: DNSSEC

1. Why DNSSEC ?
2. What does DNSSEC protect and what doesn’t it protect?
3. DNSSEC deployment status around the world and in the region.
4. Who can implement DNSSEC?
5. Overview of DNSSEC concepts and new resource records.

Offline Materials

- DNS Operation
- DNSSEC
- DNS Abuse

Hardening a web-server for the modern internet

Introduction

Hands on how to secure your network Three day course – Philip Paeps

Objectives

By the end of the workshop, everyone should know how to run secure services in jails on FreeBSD and use the pf firewall to keep malicious people on the internet out of their jails.

Prerequisites

Participants should be familiar with Unix-style operating systems. The course is taught on FreeBSD but the environment will be familiar to people with a systems administration background on Linux or Solaris. Participants should bring their own laptops.

Participants

Systems administrators and network operators who are running Network services in their organization.

Workshop Requirements

- Knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- All participants will need to bring a laptop with WiFi access. You cannot use a tablet for this workshop.

Instructors

Philip Paeps

Agenda

Time	Day 1: Sunday 14 August	Day 2: Monday 15 August	Day 3: Tuesday 16 August
08:30 – 09:15 (45 minutes)	Registration and coffee	Registration and coffee	Registration and coffee

09:15 – 11:15 (120 minutes)	• Installing FreeBSD in a VM • Where to find installation media • Which installation to choose •Installing on a clean machine	• Advanced jails • Installing a jail from scratch • Isolating jails with pf • Nested jails	• Jailing the Postfix mailserver • Installing Postfix from a package • Configuring a basic Postfix in a jail • letsencrypt.org certificate for SMTP
11:15 – 11:30 (15 minutes)	Coffee break	Coffee break	Coffee break
11:30 – 13:00 (90 minutes)	• FreeBSD is not Linux • Filesystem overview • init(8) and rc(8) (NO SYSTEMD!) •Starting and stopping processes • Package management with pkg(8)	• Using ezjail for easier management • Installing a dozen jails in two minutes •Upgrading jails • Deleting and archiving jails • Package management across many jails	• Hardening Postfix against spammers • DNS blacklists and whitelists •Sender and recipient restrictions •Fun tricks with multiple IP addresses
13:00 – 14:00 (60 minutes)	Lunch	Lunch	Lunch
14:00 – 15:30 (90 minutes)	• pf: the BSD firewall • Default-deny ruleset • Allowing services • NAT and port forwarding	• Jailing and securing nginx • Installing nginx in a fresh jail • Tuning nginx for maximum security •Obtaining and managing letsencrypt.org certificates •Online tools for confirming webserver security	• Building your own custom packages • Introduction to Poudriere • Installing Poudriere in a jail
15:30 – 15:45 (15 minutes)	Coffee break	Coffee break	Coffee break
15:45 – 16:30 (45 minutes)	•Introduction to jails • Lightweight virtualisation • Jails vs. virtual machines • Mention bhyve	•Exercises with nginx • Reverse proxies across multiple jails •Dodgy services locked up in nested jails	• Putting it all together • ezjail, poudriere, nested jails •Mostly automated installations •Using multiple package repositories

DNS Workshop

The Domain Name System is one of those topics in IT that you hope is simple and straightforward even though you know everything in IT is complicated. And guess what? DNS is much more complex than first meets the eye! In this hands on focused class we start with the basics and work our way through all of the DNS complexity. The goal of the workshop is to enable the participants to understand the basics of DNS , How to build and activate a caching/authoritative DNS Server and also to understand the role of DNS on the Internet. This workshop is suitable Systems administrators and network operators responsible for the DNS services in their organization.

Workshop Level

Intermediate Level.
Anyone working with DNS in their corporate or carrier infrastructure will find this class worthwhile.
IT technicians, Systems administrators,..

Instructor

- Mohamed Aymen
- Abdelrahman Mohamed Hassan
- Sara Mohammed

Requirements

- A good understanding of core TCP/IP concepts is a requirement.
- Basic knowledge of Unix/Linux systems
- Students should have a reasonably solid understanding of LAN/WAN networking.
- Laptop with Wireless card working and minimal of 4G RAM

Date & Time

- Date: Saturday, x.x.x.x
- Time: 9:30AM - 4:30PM

What you will learn

- Learn the details of how DNS operates. Gain real world, practical DNS deployment and troubleshooting skills.
- Comprehend Basic concepts of DNS
- Learn how to host, dig, and nslookup
- Comprehend Domain name registration
- Comprehend Root zones
- Comprehend BIND 9 installation from source code

- Configure caching-only name server
- Comprehend DNS (Domain Name System) administration
- Set up Master DNS server and Slave DNS server
- arpa zones
- Delegate zones to other DNS servers
- Comprehend Resource Records
- Understand named logging
- Comprehend DNS zones
- Comprehend Techniques of DNS troubleshooting
- Comprehend Common BIND error messages

Registration

Registration link will be here

Workshop materials

you can find this workshop materials at:

https://drive.google.com/open?id=1eI9PeE5KBad8Y_BAPdal6QyaCmipk2Xp

DNSSEC Workshop

Introduction

Hands on DNS and DNSSEC Three day course – Philip Paeps

Objectives

At the end of this course, participants will be familiar with the Domain Name System and Security Extensions to the Domain Name System (DNSSEC). The course is taught "hands-on" in a virtualised FreeBSD environment. Participants will configure authoritative and recursive domain name servers and will learn to analyse and debug common misconfigurations and bugs

Prerequisites

Participants should be familiar with Unix-style operating systems. The course is taught on FreeBSD but the environment will be familiar to people with a systems administration background on Linux or Solaris. Participants should bring their own laptops. The virtualised lab environment is hosted on a server in Germany. Reliable internet connectivity with reasonable latency is required

Participants

Systems administrators and network operators responsible for the DNS services in their organisation.

Workshop Requirements

- Some understanding of DNS is required (for example, operational experience managing DNS servers is useful)
- Some knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- All participants will need to bring a laptop with WiFi access. You cannot use a tablet for this workshop.

Instructors

Philip Paeps

Agenda

Time	Day 1: Sunday 23 August	Day 2: Monday 24 August	Day 3: Tuesday 25

08:30 – 09:15 (45 minutes)	Registration and coffee	Registration and coffee	Registration and coffee
09:15 – 11:15 (120 minutes)	• Introduction to DNS • Resource records • Delegation • Queries, responses and flags	•Configuring authoritative nameservers • Setting up DNS zonefiles • Delegating authority • Debugging common zonefile problems	• Introduction to DNSSEC • New resource records and flags in DNSSEC • Validating a domain from the root step by step
11:15 – 11:30 (15 minutes)	Coffee break	Coffee break	Coffee break
11:30 – 13:00 (90 minutes)	• DNS packet analysis • DNS data flow • DNS vulnerabilities	• Very brief introduction to cryptography •Using TSIG to secure queries	• Key management: ZSKs and KSKs • Theory of key rollover and best practices
13:00 – 14:00 (60 minutes)	Lunch	Lunch	Lunch
14:00 – 15:30 (90 minutes)	• Tools: dig, drill, host, nslookup, tcpdump • Tools exercises • Resolving a domain from the root by hand	• Configuring secondary nameservers • Configuring TSIG to secure zone transfers • Debugging common zone transfer issues	• Manually signing a zone with BIND 9 • Configuring automatic DNSSEC with BIND 9 • Brief introduction to OpenDNSSEC
15:30 – 15:45 (15 minutes)	Coffee break	Coffee break	Coffee break
15:45 – 16:30 (45 minutes)	• Introduction to the lab environment • Discussion and Q&A	• Configuring unbound as a recursive resolver • Discussion and Q&A	• Configuring unbound with trust anchors • Demo with SSHFP and TLSA • Discussion and Q&A

Ethical Hacking Workshop

One Day workshop about Ethical Hacking and Information Security that will introduce a general background for students to know how to scan, test, hack and protect their own systems and gives each student in-depth knowledge and practical experience about the current essential security systems. It will also help them to understand how to secure and protect their networks.
The goal of this course is to help participants to master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation and its techniques.
This workshop is suitable for Network Engineers, Network Security Engineer, network administrators and for those who have strong interests in information security and hacking.

Workshop Level

Intermediate Level

Instructor

- Farah almohager
- Mohaund Altayib

Requirements

- Participants must have a good knowledge about networking and IP addressing; also know the basic commands of Linux and how to work in UNIX systems.
- Participants should bring a laptop computer to participate in the lab, with 4GB RAM as minimum.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:30AM - 5:30PM

Outline

- Introduction CHE
- Foot printing
- Scanning network
- Enumeration
- System hacking

- Social Networking
- Web hacking
- Metasploit
- Web application attack
- Kali installation and configuration network.

Registration

Paste registration link here

High Availability in LAMP Stack workshop

The workshop will show how to deploy LAMP Stack web application in a high availability environment to avoid single point of failure by utilizing different tools and technologies such as load balancer, clustering and distributed storage.

Workshop Level

Intermediate Level

Instructor

Samir Abdullatif

Requirements

- Knowledge about LAMP Stack
- Ability to install software in Linux
- Basic networking knowledge

OS, Software and tools used

Ubuntu 16.04 LTS,

- HAProxy
- Keepalived
- GlusterFS
- Percona XtraDB Cluster

Date & Time

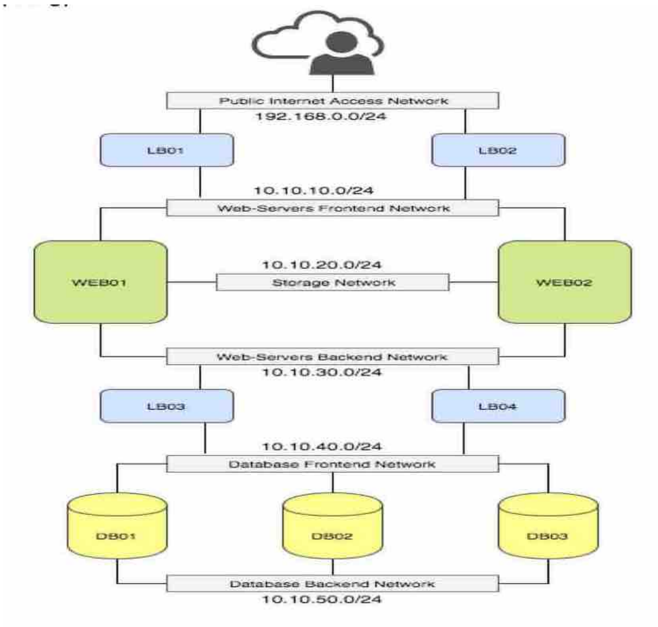
- Date: Saturday, x.x.x
- Time: 9:00AM - 4:30PM

Outline

- LAMP Stack
- Single Server Architecture vs. Multi-tier Architecture
- High Availability and Scaling

- Load balancing
- Floating IP
- Shared Storage
- Database Clustering

Lab topology



Registration

paste registration link here

How to Secure your Network Workshop

Introduction

Hands on how to secure your network Three day course – Philip Paeps

Objectives

At the end of this course, participants will be familiar with new ways and methods to help them to secure their networks. The course is taught "hands-on" in a virtualised FreeBSD environment. Participants will configure some tasks and will learn to analyze and debug common mis-configurations and bugs

Prerequisites

Participants should be familiar with Unix-style operating systems. The course is taught on FreeBSD but the environment will be familiar to people with a systems administration background on Linux or Solaris. Participants should bring their own laptops.

Participants

Systems administrators and network operators who are running Network services in their organization.

Workshop Requirements

- Some knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- All participants will need to bring a laptop with WiFi access. You cannot use a tablet for this workshop.

Instructors

Philip Paeps

Agenda

Time	Day 1: Sunday 14 August	Day 2: Monday 15 August	Day 3: Tuesday 16 August

08:30 – 09:15 (45 minutes)	Registration and coffee	Registration and coffee	Registration and coffee
09:15 – 11:15 (120 minutes)	• Introduction to security • Network layers • Defence in depth •Basic physical layer security	• Firewalls • Inclusive and exclusive policies • Simple ACLs	• Securing websites: HTTP and HTTPS • Configuring Apache and nginx
11:15 – 11:30 (15 minutes)	Coffee break	Coffee break	Coffee break
11:30 – 13:00 (90 minutes)	• Layer 1 and layer 2 • Ethernet: VLANS • Wireless basics	• Statefull firewalls •pf: the BSD packet filter	• Introduction to cryptography • PKI, basics of letsencrypt.org
13:00 – 14:00 (60 minutes)	Lunch	Lunch	Lunch
14:00 – 15:30 (90 minutes)	• Wireless: WEP, WPA, WPA2? • Captive portals • Ethernet 802.1x	• Securing higher layers (applications) • E-mail: what about spam? • Sensible outbound filtering	• Generating letsencrypt.org certificates • Configuring nginx and Apache with HTTPS • Using SSL in other applications
15:30 – 15:45 (15 minutes)	Coffee break	Coffee break	Coffee break
15:45 – 16:30 (45 minutes)	•Introduction to firewalls (more tomorrow!) • Discussion and Q&A	•Configuring postfix and dovecot to protect against spam (abuse) • Discussion and Q&A	• Mitigation: what if it all goes wrong? • Discussion and Q&A

Internet Governance Forum

This is a half-day workshop. An introductory workshop about Internet Governance which focus on Internet ecosystem, key players, key issues and how Internet is governed? how we can take part? how it is affecting our life?

Objectives

- Provide a safe and accommodating environment for new entrants to the field and increase their knowledge on IG.
- Bring together people from government, civil society, business and other stakeholder groups to interact and build common ground around a public interest-oriented approach to IG

Workshop Level

Basic Level

Instructor

Hiba Abbas

Requirements

- Participants must have a good knowledge about networking.

Date & Time

- Date: Saturday, x.x.x
- Time: 10:30AM - 2:30PM

Registration

Paste registration link here

IPv6 Workshop by AFRINIC

Introduction

This is the keystone foundation module for all our technical workshops. It gives the participants a solid understanding of IPv6's core concepts and is required for understanding all other IPv6 topics.

Objectives

- Identify, write and shorten IPv6 addresses
- List the types of IPv6 addresses and their unique characteristics
- Create an IPv6 address plan for a network
- Identify and list the equivalent IPv4 key protocols in IPv6
- Describe how NDP is used to deliver key IPv6 functions
- Configure and verify basic IPv6 on hosts and routers

for more details check: http://learn.afrinic.net/en/course/ipv6/foundation

Registration

The registration is closed.

- Please note there will be a selection process, and selected candidates will be contacted to confirm their participation.

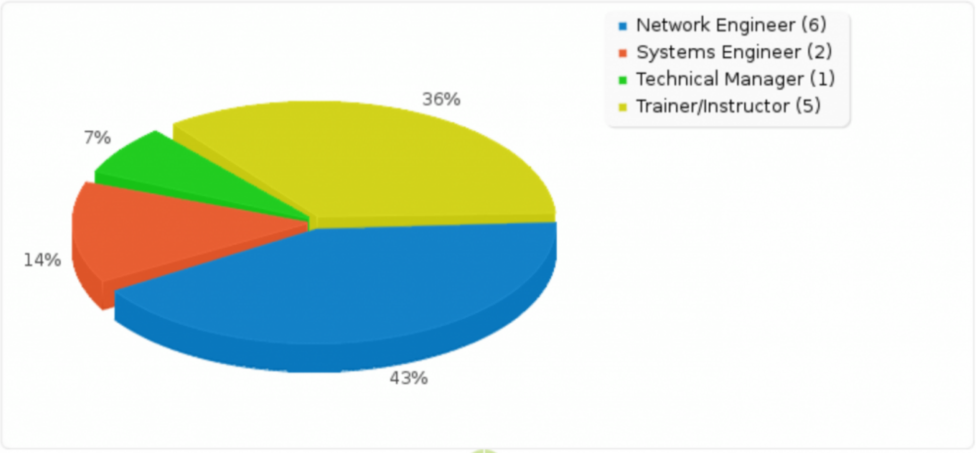
Instructors

- Stephan Musa
- Olatunde Awobuluyi

Feedback from Mr.Musa

> Hello SdNOG, We had a great time thanks to you in Khartoum last week.
>
> On behalf of us all at AFRINIC, we thank you for joining us on this mission to
>
> ensure that no network engineer gets left behind on the skills required to build and run IPv6 networks.
>
> We rate our workshops using the Net Promoter System which has a range of -100 → 100.
>
> - International benchmark for IT Training is 70
>
> - On this workshop the score was 77.

more info at: AFRINIC blog



IPv6 Fundamentals Workshop

Ready or not, IPv6 is here!

IPv6 was developed more than a decade ago, but now is being implemented by both service providers and companies alike primarily due to the lack of IPv4 addresses. This one day hands-on will cover IPv6 concepts, IPv6 Address Basics, and IPv6 basic configuration in a Cisco infrastructure. This workshop is suitable for network engineers, network operators or Systems/IT admin who are responsible about network operation in their organization.

Objectives

This workshop will help to :

- Understand the differences and similarities between IPv4 and IPv6
- Know that deploying IPv6 will enable continued IP networking growth
- Understand the implications of running out of available IPv4 address space
- also to remove some of the fear related to IPv6 deployment and to enable it

Workshop Level

Intermediate Level

Instructor

- Sara Alamin Mohamed
- Salih Shihab Aldeen

Requirements

- It is assumed you are familiar with common IP terminology and have practical knowledge of running an IP network.
- Participants should bring a laptop computer to participate in the lab, with 2GB RAM as minimum.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:00AM - 4:30PM

Outline

- Internet Ecosystem
- IPv4 Exhaustion
- IPv6 Address Basics > notation, shortening rules
- IPv6 Address Types
- IPv6 vs IPv4
- transition mechanism
- Basic Configuration

Registration

Paste registration link here

IXP Best Practices

Introduction

As at July 2015, there are known shortcomings to how the SIXP operates. With the assistance of PCH, the SdNOG team will host this workshop on IXP best practices as a pre-cursor to the sdnog-2 event. It is intended that the event will attract the key stakeholders for the SIXP, as well as the relevant participants from the NTC and NIC.

Layout

The workshop is intended to be a one day event, split between, an understanding of the economic elements, and strategic objectives of an IXP; it's role in the local Internet economy, and technical and operational management. The table below has a suggested overview of the topics that would be addressed.

Day 3 : 25 August 2015	Topic
Session 1	Internet Economics; the value of peering and the role of the IXP in the Internet economy Discussion: Strategies for IXP development.
Session 2	Regulatory best practices for economic growth Total Internet security of a country.
Session 3	Technical operations and management
Session 4	

Instructor List

Nishal Goburdhan, PCH

Networks Fundamental Workshop

A strong foundation of basic networking concepts is fundamental to have a successful career in information technology. This Workshop will help you understand Networking Fundamentals. By the end of this Workshop, you will gain real-world practical skills necessary for Networking
This workshop is suitable for BSc Students, fresh graduate and for those who have strong interests in networking

Workshop Level

Basic Level

Instructor

- Mohaund Adil
- Jadallah Mohamed

Requirements

- Participants must have a good knowledge about networking and IP addressing; also know the basic commands of Linux and how to work in UNIX systems.
- Participants should bring a laptop computer to participate in the lab, with 4GB RAM as minimum.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:30AM - 5:30PM

Outlines

1.Basics of Networking

- What is networking?
- Types of Networks
- Usefulness of networks
- Types of network
- OSI Protocol description

2.Network Devices
3.IP Addressing

- IPv4
- IPv6
- IPv4 Vs. IPv6
- Understanding VLSM technology

4.Overview about Switching
5.Overview about Routing

Registration

paste registration link here

Network Management and Monitoring Workshop

Introduction

This workshop is designed for engineers and system staffs at ISPs and large networks including academic networks who are involved with system management, network monitoring and management and problem response. The course is for those who need to manage diverse Network and NOC operations. There will be hands-on for three days.

Objectives

By the end of this course you will be able to: Distinguish between network management and monitoring.

- Determined what should be monitored.
- Install various network management/monitoring tools.
- Track the changed on the network device's configurations.
- Use SNMP protocol and log management.

Requirements

- laptop with wireless capability.
- IPv4 addressing and general network concepts.
- Knowledge of Linux.

Instructors

- Salih Shihab
- Patrick Okui

Agenda

Time	Day 1: Sunday 14 August	Day 2: Monday 15 August	Day 3: Tuesday 16 August
09:00 – 11:00	Welcome, Introductions, Workshop Details	Cacti software	Nagios3 Software
11:00 – 11:30	Coffee break	Coffee break	Coffee break

11:30 – 13:00	Introduction to Network Monitoring & Management	Smokeping software	LOG Management
13:00 – 14:00	Lunch	Lunch	Lunch
14:00 – 16:30	Cisco Configuration Basics and SNMP	LimbreNMS software	Version control RANCID / WebSVN and NetFlow / NfSen

Networking Best Practices Workshop

Introduction

This tutorial is aimed at teaching Best Practices in network deployment. The intent is to sensitise operators, and participants to things that they should be aware of, from a macro level, and to stimulate discussion, interest, and knowledge in the mechanisms for operation. It is not intended for this to be extremely low level.

Layout

The key ideas would be to talk about issues that operators should be engaged in already, in a 90min slot. Some topics for discussion could be:

- the proper use of NMS systems
- configuration management
- IGP and EGP configuration and setup
- routing and Switching
- scaling virtualisation deployments

Since this would be tutorial style, it's intended for the discussions to be as interactive as possible, and, where possible, include hands-on practical sessions. It is also intended to be an introductory/refresher tools that we can use to gauge interest, and competency, that will allow us to plan for future workshops.

Note: sdnog-1 attendance showed us a significant student population attending, so we expect that this workshop would be more appealing to them, vs. a more low-level, specific workshop on a particular topic.

A suggestion for the tutorial scheme could be:

	Day 1	**Day 2**	**Day 3**
Session 1	IP address space design and planning	Routing - IGP and EGP best practices	DNS
Session 2	IPv6 and its role in your network	BCP 38 and routing sanity	Configuration management
Session 3	Designing a switching environment	Network management systems	RIPE ATLAS Tutorial

Session 4	Designing a switching environment (cont)	Network management systems	Open Q&A

Instructor List

It is desirable that the instructor be experts in their respective areas of presentation, and have significant experience in the topics that they are presenting. Additionally, a good mix of local, and foreign expertise would be desirable, to allow for different points of perspective.

- Christian Teuschel
- Daniel Shaw
- Hiba Abbas
- Nishal Goburdhan
- Patrick Okui
- Sirag Aldeen Mahgoob

UNIX Boot Camp

This 'boot-camp' is intended to provide the participant a basic overview of essential Unix/Linux commands that will allow them to navigate a file system and move, copy, edit files. It will also introduce a brief overview of some 'Network' commands in UNIX.
This workshop is suitable for BSc Students, fresh graduate and for those who have strong interests to learn Linux.

Workshop Level

Basic Level

Instructor

- Mohamed Alhafez Alnour
- Mohamed Yusuf
- Saad Awad

Tutors

- Ahmed Hassan
- Khansaa Abdallah

Requirements

- Participants should bring a laptop to participate in the lab.

Date & Time

- Date: Saturday, x.x.x.x
- Time: 9:30AM - 4:30PM

Outlines

- UNIX Operating System Overview
- How to install (Ubuntu, Red hat, Centos...)
- Linux Commands
- Directory Structures

- Disk Partitioning Schemes
- Privileges
- Vi and vim Editor Usage
- Network Layers
- Network Configuration

Registration

Registration link will be here

UNIX/Linux, Networking and DNS Online Course

The Internet Society invites engineers from Africa to participate in an intensive online course titled "Introduction to Network Operations: UNIX/LINUX, Networking and DNS" This is an introductory course targeted at novice/entry-level UNIX/Linux users pursuing careers in Network or System Administration. This course provides the necessary skills to progress to more advanced topics in the future. This course is practically oriented and provides step-by-step guidance on how to configure a UNIX/Linux server and then run a Caching Domain Name System (DNS) server in a virtualized environment. The techniques covered in the course are applicable in real-world environments to set up Internet-ready caching DNS servers.

Trainees who complete the course will be awarded with a **Certificate of Completion.**
Trainees will also be provided a remote server to carry out the hands on parts of the course and the exercises.

More info at: https://www.internetsociety.org/inforum/network-operations/

Course objectives

The course follows the following schedule:

- Learn about and operate a UNIX/Linux operating system in a virtualized environment.
- Develop competences in key networking topics: IPv4 and IPv6.
- Install third-party software on a UNIX or Linux platform using common software management tools.
- Work with the UNIX/Linux shell and become comfortable with the command line interface.
- Edit files in UNIX/Linux environments without Graphical User Interfaces (GUI).
- Understand the role of the Domain Name System (DNS) in the operation of the Internet.
- Build and activate a caching Domain Name System (DNS) server.
- Learn about the Internet Engineering Task Force (IETF) and the Request for Comments (RFC) process

Who Should Attend

Novice/entry level network engineers and system administrators (from Africa) who are interested in learning about UNIX/Linux, Networking and DNS.
The course is targeted at upcoming network engineers and system administrators from Research Education Networks (RENs), Network Operator Groups, Universities, ccTLD registries or Internet Service Providers (in Africa).

Our Certified Participants

Meet our certified Participants who complete the online course successfully. □

Participants' Feedback

What former participants say about the courses.

Language

Language of instruction will be English.

Moderation and Online Support

This course will be moderated by **Eng. Manhal Mohamed**. and assisted by **Eng. Abdulrahman Mohammed Hassan**.
Online remote support is available via Email or Telegram and also via Jitsi meet

Offline Content

Offline training materials are available and are frequently updated.

Registration Form

https://docs.google.com/forms/d/e/1FAIpQLSd7MR1UkX4NoTS0OnHYeJCFCUxarBzuzIz3xpMxkawevBCQIg/viewform?usp=sf_link

Automation Tool: Ansible

Hands-on how to use automation in your network. Three day course

Objectives

By the end of the workshop, attendees will know how to use automation with Ansible to ease the burden of consistent configuration of servers and network devices and how to choose what/when to automate.

Workshop Level

Advance Level

Prerequisites

- Participants should be familiar with Unix-style operating systems. The course is taught on Linux (Ubuntu or CentOS) but the environment will be familiar to people with a systems administration background on FreeBSD or Solaris.
- Knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- All participants will need to bring a laptop with WiFi access.

Participants

System administrators,Network engineers and Network technicians who are running network devices like servers, routers and switches in their organization.

Date & Time

- Date: Sunday 30 Sep - Tuesday 2 Oct 2018
- Time: 8:30AM - 4:00PM

Instructors

Sander Steffann

Agenda

- Benefits of automation
- What to automate?
- What not (yet) to automate?

- Available automation tools (Ansible, Puppet, Salt etc)
- What is Ansible?
- Installing Ansible
- How Ansible Works and its Key Components
- Playbook Basics
- Organising your roles
- Combining Ansible with other tools (bgpq3 etc)
- Sharing playbooks and revision management (git etc)

IPv6 for Services

hands-on workshop to teach the concept of IPv6 protocol on most common services expected of any network

Objectives

by end of this workshop participants will be able to verify any application for IPv6 capability and Configure and test an dual stack DNS, HTTP and DHCP server.

Workshop Level

Intermediate Level

Prerequisites

- Participants should be familiar with Unix-style operating systems.
- Participants should have a good knowledge about IPv6 protocol architecture.
- Participants should have a good knowledge about Network services like DNS, HTTP,...
- Participants should bring their own laptops with WiFi access

Participants

System administrators,Network engineers and Network technicians who are running Network services in their organization. The course is taught on FreeBSD but the environment will be familiar to people with a systems administration background on Linux.

Date & Time

- Date: Sunday 30 Sep - Tuesday 2 Oct 2018
- Time: 8:30AM - 4:00PM

Instructors

- Mohamed Alhafiz - Canar Telecom
- Khansaa Abdallah - Canar Telecom
- Rawan Shareef - MTN

Agenda

- IPv6 refresher
- FreeBSD refresher
- IPv6 Network Setup
- Packet berkeley filter overview
- DNS for IPv6 / DNS troubleshooting
- DHCP for IPv6
- HTTP, SSH and SFTP for IPv6
- Network Tools for troubleshooting

Network Services and Monitoring Online Course

Background

This is an intermediate level course for network and system engineers/administrators aiming to get operational experience with IPv6 with a focus on specific Internet services provided by Internet Society. The course covers the following main areas:

- Authoritative DNS
- Introduction to Email
- Network Monitoring

The course is strictly 3 weeks long. Each trainee will be assigned a virtual server and will be required to build working services as mentioned above to provide services on an IPv6 address. The course is lab intensive (70%) with trainees provided with theory materials that they can read. Trainees are also encouraged to do their own research in order to cover the concepts in the course.

Course Timetable

The course follows the following schedule:

```
 Week 1:
    - Introduction to DNS
    - DNS Resolvers
    - DNS Authoritative
    - LAB ASSIGNMENT 1: install BIND
    - LAB ASSIGNMENT 2: Zone set up
    - LAB ASSIGNMENT 3 : Zone file creation

Week 2:
    - Email introduction
    - Postfix Dovecot Introduction
    - LAB ASSIGNMENT 4: create MX record for your mail server
    - LAB ASSIGNMENT 5: Install Postfix and Dovecot
    - LAB ASSIGNMENT 6: Setup Postfix and Dovecot

  Optional Part - Securing mail system :
  -------------------------------------□
    - LAB ASSIGNMENT 7 SENDING EMAILS
    - LAB ASSIGNMENT 8 Apache setup
    - LAB ASSIGNMENT 9 letsencrypt Part01
    - LAB ASSIGNMENT 10 letsencrypt Part02
```

- LAB ASSIGNMENT 11 Configure Dovecot
- LAB ASSIGNMENT 12 Configure Squirrel-mail

Week 3:

- Nagios Introduction
- LAB ASSIGNMENT 13 Installing Nagious
- LAB ASSIGNMENT 14 monitor DNS on localhost

Pre-Requisites to attend

- Completion of the Introduction to UNIX/Linux and Networking Course.
- A Computer system with at least 2 browsers (Chrome and Firefox preferred.
- Good Internet Connectivity.

Our Certified Participants

Meet our certified Participants who complete the online course successfully.

Participants' Feedback

What former participants say about the courses.

Language

Language of instruction will be English.

Moderation and Online Support

This course will be moderated by **Eng. Manhal Mohamed** & assisted by **Eng. Abdulrahman Mohammed Hassan**.
Online remote support is available via Email or Telegram.

Offline Content

Offline training materials are available and are frequently updated.

Registration Form

https://docs.google.com/forms/d/e/1FAIpQLSejyyI1yVwFjOFqNAjTUwr4irmh0YY5hv1Dv3HmOY2L24dCsw/viewform?usp=sf_link

OpenStack Workshop

OpenStack is a set of software tools for building and managing cloud computing platforms for public and private clouds. Backed by some of the biggest companies in software development and hosting, as well as thousands of individual community members, many think that OpenStack is the future of cloud computing.
This workshop will help the participants to assess the architectures, components, operation and tools of OpenStack.
Participate will have a hands-on labs showing how to build, use, and deploy an OpenStack Platform.

Workshop Level

Intermediate Level

Instructor

- Mohamed Ibrahim Oshari

Requirements

- Participants must have a good knowledge about networking and IP addressing;
- also know the basic commands of Linux and how to work in UNIX systems;
- also Participants should know basic knowledge about Virtualization Techniques.
- Participants should bring a laptop computer to participate in the lab, with 4GB RAM as minimum.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:30AM - 5:30PM

Outline

- Whats OpenStack and its Present and Future
- Learn about the individual OpenStack components
- Learn about the OpenStack architecture.

Registration

Registration link will be here

Network Monitoring Workshop

Introduction

This workshop is designed for engineers and system staffs at ISPs and large networks including academic networks who are involved with system management, network monitoring and management and problem response. The course is for those who need to manage diverse Network and NOC operations. There will be hands-on for four days.

Objectives

By the end of this course you will be able to: Distinguish between network management and monitoring.

- Determined what should be monitored.
- Install various network management/monitoring tools.
- Track the changed on the network device’s configurations.
- Use SNMP protocol and log management.

Workshop Level

Intermediate level

Requirements

- laptop with wireless capability.
- IPv4 addressing and general network concepts.
- Knowledge of Linux.

Date & Time

- Date: Sunday 27 Oct - Wednesday 30 Oct 2019
- Time: 8:30AM - 3:30PM

Workshop Fees

200SDG

Instructors

- Salih Shihab

Agenda

- Introduction to Network Monitoring & Management
- Cisco Configuration Basics and SNMP
- Cacti software
- Smokeping software
- LibreNMS software
- Nagios3 Software
- LOG Management
- {PHP}IPAM
- Version control RANCID / WebSVN and NetFlow / NfSen

Security Workshop - Ethical Hacking

Introduction

This workshop is designed for system administrators, network administrators, auditors and web developers to gain knowledge about the security assessment and penetration testing processes. In addition, it will help to improve network and systems by analyzing the existing vulnerabilities to defend systems against attacks.

Objectives

By the end of this course you will be able to:

- Define Ethical Hacking concepts
- Determine different threats.
- Apply techniques and use penetration testing tools
- Provide defence against different types of attack.

Workshop Level

Intermediate level

Requirements

- Laptop with wireless capability.
- Good Network concepts.
- System concepts
- Basic/intermediate Linux Knowledge.

Date & Time

- Date: Sunday 27 Oct - Wednesday 30 Oct 2019
- Time: 8:30AM - 3:30PM

Workshop Fees

200SDG

Instructors

- Hiba Alamin

Agenda

- Introduction to Ethical Hacking
- Foot-printing and Reconnaissance
- Scanning Networks & Enumeration
- System Hacking
- Sniffing
- Social Engineering
- Denial-of-Service
- Overview about other security fields
- Security polices and Recommendations

Layer 2 Security Workshop

LAN network protection is generally neglected, which is a high risk to the organization or company This Workshop will help you understand L2 vulnerabilities. By the end of this Workshop, you will gain real-world practical skills necessary for LAN security, this workshop is suitable for all interested in cybersecurity, Network Security and Penetration Testing.

Workshop Level

Intermediate level

Instructor

Mohanned Adil Omer

Requirements

- Participants must have a good knowledge about networking, TCP/IP and IP addressing; also know the basic knowledge of Linux.
- Participants must have a Good understanding of switching behavior and protocols.
- Participants should understanding network services (DHCP, DNS, AD ... etc.).
- Participants should bring a laptop computer to participate in the lab, with 4GB RAM as minimum.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:00 to 15:30

Outlines

1. Why L2 Security.
2. Switching review.
    - How switch work?
    - Switch weakness.
3. Sniffing Techniques
    - Packet Sniffers
    - PCAP and promiscuous mode.
    - Sniffing Tools.
    - Active and Passive Sniffing.
4. L2 Attacks and Defenses
    - Mac table Flooding.
    - ARP attack.

   1. Introduction.
   2. When ARP is used?
   3. Types of ARP message.
   4. Example use of ARP.
   5. ARP cache.
   6. RARP.
   7. ARP Types.
   8. ARP Attacks.
   9. ARP Spoofing.
   10. ARP Denial of Service.
   11. Defenses.
   12. S-ARP.
   13. Conclusion.
5. DHCP attack
   - How DHCP Work.
   - DHCP Spoofing Attack.
   - DHCP Starvation Attack.
   - Defenses.
   - Conclusion.
6. Some Guides to Minimum Security Baseline for any organization.

Build your own e-mail Server

This workshop is designed for engineers and system staffs at ISPs and large networks including academic networks who are involved with system management, system administration and operations and problem response. The workshop is for those who need to manage mail servers and systems. Anyone working with mail system in their corporate or carrier infrastructure will find this class worthwhile. this one day workshop describes how to setup a local Email with best practices using Postfix, Dovecot And Squirrelmail.

Objectives

By the end of this workshop you will be able to:

- Understand the concept of the SMTP and electronic mail
- Overview of common terms and protocols
- How the mail system works
- building a mail server using Postfix, Dovecot And Squirrelmail
- knowing best practices on securing and setting your mail server

Workshop Level

Intermediate Level

Requirements

- laptop with wireless capability , 64 bit OS , minimum 4G RAM "with enabled virtualization technology"
- IPv4 addressing and general network concepts.
- Good Knowledge of Linux.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:30AM - 4:30PM

Instructors

Manhal Mohammed Mokhtar

Content

- SMTP concept
- Mail System terms
- How mail system works
- Setup and configure Postfix, Dovecot And Squirrelmail
- Mail system security

Registration

Registration link will be published here

Workshop materials

you can find this workshop materials at:

https://drive.google.com/drive/folders/1OnHplRXTB59VAgPi9pl_fIZyX9tkB78A?usp=sharing

Introduction to Git Workshop

This workshop is an introduction to version control systems with Git. Version control systems are tools that keep track of the changes made on a document, and help version and merge files. They allow the user to decide which changes make up the next version, and keep useful data about them. Version control systems are usually used by developers and people who write code, but are very useful also for people working with documents in general. It is especially helpful for collaborative work with more than one person working on the same file.

Objectives

This workshop is designed for people who have never used Git or a version control system before to :

- Learn more about what version control systems can do for them and their research.
- Help a team of people to work together, all using the same files.
- Helps the team cope with the confusion that tends to happen when multiple people are editing the same files.

Who should attend?

From web developers to system administrators, Git is useful to anyone who writes code, configuration files, scripts, and text documentation.

Workshop Level

Basic Level

Requirements

laptop with wireless capability , 64 bit OS , minimum 4G RAM

Date & Time

- Date: Saturday, x.x.x
- Time: 9:30AM - 4:30PM

Instructors

Sara Mohammed Abdulraheem

Content

1. What is Git and Gitlab?
    - History of Git
    - Design Principles
    - Distributed Version Control
2. Installing Git
3. Git File Management
    - Common Git Commands
    - Configuring Git
    - Creating Repositories
    - Creating a Commit
4. Branching
    - Visualizing Branches
    - Branch Naming Conventions
    - Creating a new Branch
    - Handling Merge Conflicts

Registration

Registration link will be published here

Workshop materials

you can find this workshop materials at:

https://drive.google.com/open?id=12vGnb0TdEbxHif_ywp-AQsTsG2agKFgM

Automation with Ansible : The basics

Introduction

Ansible is an open-source software provisioning, configuration management, and application-deployment tool to automate all your system work. this is one-day , hands-on workshop. You'll get a comprehensive overview of Ansible and then dive into Ansible Roles and playbooks.

Objectives

By the end of the workshop, attendees will know how to use automation with Ansible to ease the burden of consistent configuration of servers and network devices and how to choose what/when to automate.

Workshop Level

intermediate Level

Prerequisites

- Participants should be familiar with Unix-style operating systems. The course is taught on Linux (Ubuntu or CentOS) but the environment will be familiar to people with a systems administration background on FreeBSD or Solaris.
- Knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- All participants will need to bring a laptop with WiFi access.

Date & Time

- Date: Saturday 14 March 2020
- Time: 9:30AM - 4:30PM

Instructors

- Manhal Mohamed
- Sara Alamin

Agenda

- Introduction to Ansible
- Installing and Configuration
- Configuring Clients
- ad-hoc commands
- Ansible Playbook
  - Format& Function
  - Handlers
  - Variables
  - Conditions
  - Loops
- Ansible Templates
- Ansible Roles

Registration

Registration link will be published here

Workshop materials

you can find this workshop materials at:

https://drive.google.com/open?id=1OV4fWCRiLWAz4WQ-ohdT3msUXXY1EDPd

Automation with Ansible - Online Course

Introduction

Ansible is an open-source software provisioning, configuration management, and application-deployment tool to automate all your system work. this is 10-days , hands-on online workshop. in this online workshop You'll get a comprehensive overview of Ansible and then dive into Ansible Roles and playbooks.

- this is a 10-days , hands-on online Workshop .
- Each trainee will be assigned a virtual server and will be required to build working services using Ansible tool
- The Online Workshop is lab intensive (70%) with trainees provided with theory materials that they can read

Objectives

By the end of the workshop, attendees will know how to use automation with Ansible to ease the burden of consistent configuration of servers and network devices and how to choose what/when to automate.

Workshop Level

intermediate Level

Prerequisites

- Participants should be familiar with Unix-style operating systems. The workshop is taught on UNIX "FreeBSD" but the environment will be familiar to people with a systems administration background on Debian or RedHat.
- Knowledge of Linux/UNIX command line
- Good understanding of network basics (IP networking)
- Each participant will be assigned a virtual server to work on it , you only need a laptop with an internet connection for remote access to the server

Date & Time

- Round One: 10 days. from 11 April 2020 to 21 April 2020
- Round Two: 10 days. from 20 to 31 May 2021
- Round Three: TBD

Moderation and Online Support

This online workshop will be moderated by:

- Manhal Mohammed
- Sara Alamin
- Abdulrahman Mohammed
- Shimaa babiker
- Mohamed Ayman

Online remote support is available via **Telegram Group only** " group link will be sent to selected participates"

Agenda

Day (1 & 2) : Introduction to Ansible

1. Module-01: Introduction to Automation
2. Assignment 01 : Introduction to Automation
3. LAB01 : deploying Ansible
4. Assignment 02: Ansible Ad-Hoc
5. Quiz #1

Day (3 & 4): Ansible Playbook

1. Module-02: Ansible Play and Play-books
2. LAB02: play book to install pkg
3. LAB03: show uptime of remote servers
4. LAB04 : Ansible Variables
5. LAB05: working with ansible loops

Day (5 & 6) : Ansible detailed Playbooks

1. Module-03: Ansible detailed Playbooks
2. LAB06: working with ansible loops-2
3. LAB07: Ansible conditions
4. Assignment 03 : Implementing Ansible Playbooks using templates

Day (7 & 8) : Ansible Roles

1. Module-04: Ansible Roles
2. LAB08: working with Ansible roles

Day (9 & 10): final Project

Participants

Participants who complete this online course successfully. □

Offline Materials

You can find the offline contents for this online course here