DNS training in Rwanda - 27 Feb to 03 March 2023

Introduction:

The information technology industry is experiencing a new industrial and technological revolution. ICT industry has got the ever-changing needs including the Domain Name System (DNS), Peering, core IP Engineering as well as integrating the real-world use and impact of IP Technologies. Domain Name System (DNS) is like the Internet's phone book. It allows computers to convert human-readable domain names into numerical Internet Protocol (IP) addresses that they need to communicate since core networking protocols use IP addresses, not hostnames.

The proper functioning of the Internet is critically dependent on the Domain Name System (DNS). Every web page visited, every email sent, every picture retrieved from social media: all those interactions use the DNS to translate human-friendly domain names to the IP addresses needed by servers, routers, and other network devices to route traffic across the Internet to the proper destination.

RICTA and ICANN will organize a DNS training to meet the needs of the Rwanda Internet Community by;

- ☐ Addressing the current technological changes in the DNS Ecosystem with the required technical skills.
- ☐ Discussing on a wide range of issues of the Internet including the current and newest trends in DNS Ecosystem.
- ☐ Discussing DNSSEC deployment processes, challenges and benefits on the Internet Ecosystem.

Objectives:

The Objectives of the training are:

- ☐ To train Engineers with sustainable technical skills in support of the very rapidly changing DNS Ecosystem.
- ☐ To empower Engineers with technical expertise on how DNS works, how different DNS components interact with each other and DNSSEC deployment processes.
- ☐ To build a network of tech community that can easily interact and support each other in running a smooth DNS Ecosystem.

Proposed dates:

- Day 0: 27 February
- Day 1 to 3: 01 to 03 March 2023.

Location: UR-College of Science and Technology Kigali, Rwanda

Local host: RICTA

Role and responsibilities:

- Promote the event in the local community,
- Coordinate participants registration
- Provide logistics and venue,
- Provide lunch and coffee breaks
- Provide training facilitator: Assist the on-site trainer in all issues and needs.

Partner: ICANN

Role and responsibilities:

- Provide trainer(s)
- Provide training material and content: courses, labs, lab platform
- Provide training survey to allow participants share their feedback

Expected Outcomes:

- ☐ 35 Engineers trained in the Domain Name System functions.
- ☐ Strong Rwandan Internet Community with the Experts in DNS operations that can help each other in solving their daily challenges not only at their workplace but as well as in the entire Ecosystem.

Content and Prerequisites:

High level overview

Day 0 : DNS for beginners

1. Prerequisite: None
2. Duration: 8 hours
3. Audience: newcomers and junior staff with technical background in IP networks (ICT university students or graduate students, junior ICT engineers: network, admin, developer, cybersecurity, etc.), policy makers, ICT managers, general public.
4. Engineers will bring their own Laptops

Day 1, 2 and 3: advanced DNS

1. Prerequisite: before attending these three days class, participants must:
    a. Be familiar with the UNIX/Linux command line environment.
    b. attend day 0 courses and/or have at least basic practical experience in DNS configuration and DNS ecosystem: this course is not an introduction.
    c. Basic knowledge of TCP/IP networking
2. Duration: 8 hours each day
3. Audience: Network/systems administrators and engineers from ISP/REN/Universities or corporations, who are responsible for DNS service, and operating authoritative and/or recursive DNS installations, cybersecurity engineers, DevOps engineers, ICT operations managers, etc.

Course Outline

Day 0: ICANN's technical mission and DNS 101 (Introduction to Domain Name System).

Course: ICANN's technical mission

Description: This course will provide an overview of ICANN's technical mission. Beyond the policy development coordination role for the community, ICANN plays a significant role coordinating the technical aspects of the Internet's unique identifier system.

Outline:

- ICANN Ecosystem
- Introduction to Internet's Unique Identifiers
- Numbers: IANA function & the RIR System
- Protocol Parameters: IANA function and The IETF
- Names: DNS, DNS Resolution, Root Server System
- The Registry/Registrar/Registrant model
- Security, Stability, and Resiliency: DNSSEC, Compliance, OpSec
- Policy Development Processes and Stakeholder Engagement

Course: DNS 101 (DNS for beginners)

Description: This course will provide participants with basic knowledge of how DNS works and how the different DNS components interact with each other.

Outline:

- Brief History of DNS
- The Name Space, Delegation, Zones
- Components for the DNS: Authoritative Servers, Resolvers (Stub & Recursives)
- DNS Data: Zone Files, RR Types, Glue
- Root Server System overview

- DNS software overview
- demos

Day 1 and 2: deploy and secure your DNS infrastructure

Description: This course will discuss the DNS configurations, operations, and security in detail.

Note: Participants will be provided **virtual machines to practice lab exercises using various DNS software such as BIND, Unbound and NSD**.

Outline:

- Refresher DNS 101: name space, zones, delegations, components of DNS infrastructure
- Reverse DNS
- hardening your DNS with ACLs, TSIG (secure zone transfers), logging
- DNSSEC: signature and validation overview
- Open vs. Closed Resolvers
- DoH and DoT
- Hyperlocal
- DNS Operations monitoring & troubleshooting
- RPKI (Routing security) introduction
- KINDNS
- demos

Labs:

- configure authoritative servers: forward and reverse DNS
- configure zone transfers
- DNS security: ACLs, TSIG, logging
- configure recursive resolvers
- configure and test DNSSEC validation

Day 3: DNS ecosystem threats and security best practices

Description: This course will provide a comprehensive discussion on how adversaries abuse and leverage the DNS and domain registration services to carry out different types of attacks. The course will end up with the best practices that can be deployed to secure the overall DNS ecosystem.

Outline:

- DNS Threats & Abuses Overview
- Investigating DNS Threats & Abuses: Tools and Techniques
- Security Considerations: SSH, DNSSEC, SPF, DMARC, DKIM, etc.

- Common Attacks: Cache Poisoning, Fast Flux, Homographic Attacks, Emojis, IoT, etc.
- Mitigation with DNSSEC, RPKI, DMARC, SPF, or DKIM
- Mitigation with encryption
- Enhance collaboration