IEEE-IC: STANDARDS HACKATHON

Problem Statements

Problem Statement No. # 1

Problem Statement: Designing a Tool for Querying DNS Resolver Information

Problem Statement Description: DNS clients often have limited visibility into the features or policies of the DNS resolver they are using. The self-publication mechanism outlined in RFC 9606 allows DNS resolvers to make this information accessible.

Objective:

Develop a tool that queries DNS resolvers for their self-published information, such as:

- Supported DNSSEC capabilities
- Privacy policies (e.g., support for QNAME minimization)
- Caching and filtering behaviour

Deliverables:

A tool that can send DNS queries for resolver information based on RFC 9606 and return human-readable summaries of the resolver's capabilities and policies. The tool should be capable of comparing multiple resolvers for feature selection.

Reference:

RFC 9606: "DNS Resolver Information" defines mechanisms for DNS resolvers to publish information about their capabilities, policies, and configurations. This allows clients, network administrators, or other systems to query resolvers for self-published information, improving transparency, trust, and optimizing resolver selection based on features.

Published: June 2024

https://datatracker.ietf.org/doc/rfc9606/

Problem Statement No. # 2

Problem Statement: Automating Service Binding Discovery for Multi-Service Environments

Problem Statement Description: In large networked environments, services like web hosting, mail, and databases often reside on different servers. Service Binding (SVCB/HTTPS) allows for dynamic discovery of which servers handle specific services, simplifying configuration and reducing hard-coded dependencies.

Objective:

Develop a tool or library that automatically queries DNS servers to discover service bindings for different services (e.g., web, email, database) in multi-service environments.

Key Challenges:

- Implement support for querying SVCB and HTTPS records from DNS servers.
- Automatically determine the appropriate server and protocol for each service.
- Provide fallback mechanisms when service bindings are unavailable or misconfigured.

Deliverables:

A tool that can dynamically discover service bindings in a given network or domain, configure client applications, and provide error handling and fallback mechanisms.

Reference:

RFC 9461: "Service Binding Mapping for DNS Servers": It defines a mechanism for mapping services to DNS servers using Service Bindings. It provides a standardized way for clients to discover the appropriate server for a service, along with necessary parameters, such as transport protocols, security settings, and resource locations.

Published: November 2023

https://datatracker.ietf.org/doc/rfc9461/

Problem Statement No. # 3

Problem Statement: Intrusion Detection/Prevention System (IDS/IPS) Throughput and Latency Benchmarking

Problem Statement Description: IDS/IPS devices are used to detect and prevent security threats, but their performance can vary with traffic volume, packet sizes, and the complexity of signatures used.

Objective: Develop a benchmarking solution to evaluate the throughput and latency performance of an IDS/IPS device. The solution should support:

Different traffic profiles (e.g., regular traffic vs. attack traffic)

Signature complexity impact

Latency and packet drop measurements during high-traffic loads

Deliverables: A tool that benchmarks IDS/IPS devices based on throughput, latency, and detection accuracy under various conditions. The tool should visualize performance degradation as traffic increases.

Reference:

RFC 9411: "Benchmarking Methodology for Network Security Device Performance" It provides guidelines for evaluating the performance of network security devices (NSDs) such as firewalls, intrusion detection/prevention systems (IDS/IPS), and other security appliances. The goal is to create a standardized method for benchmarking NSDs to ensure that performance is measured consistently and accurately across different implementations.

Published: March 2023

https://datatracker.ietf.org/doc/rfc9411/

Problem Statement No. # 4

Problem Statement: Stateful vs. Stateless Filtering Performance Comparison

Problem Statement Description: Stateful and stateless filtering are two core functionalities of network security devices. Their performance can vary significantly, and understanding the differences can help in optimizing network security setups.

Objective:

Design a benchmarking tool that compares the performance of stateful vs. stateless filtering in terms of:

- Latency introduced by maintaining stateful connections
- Throughput under different types of traffic (e.g., short-lived vs. long-lived connections)
- CPU and memory usage by stateful vs. stateless filtering

Deliverables:

A comparison report generated by a tool that benchmarks a device's performance in both modes, highlighting the trade-offs between stateful and stateless filtering

Reference:

RFC 9411: "Benchmarking Methodology for Network Security Device Performance" It provides guidelines for evaluating the performance of network security devices (NSDs) such as firewalls, intrusion detection/prevention systems (IDS/IPS), and other security appliances. The goal is to create a standardized method for benchmarking NSDs to ensure that performance is measured consistently and accurately across different implementations.

Published: March 2023

https://datatracker.ietf.org/doc/rfc9411/

Problem Statement No. # 5

Problem statement: Measurement of Power Consumption in NSDs During High Load Traffic

Problem Statement Description: Network security devices may consume more power when under heavy load, especially when processing complex traffic or encrypted packets.

Objective:

Create a test environment that benchmarks the power consumption of a security device while processing different traffic volumes and types. The system should measure:

- Power consumption at idle, low, medium, and high traffic loads
- Correlation between encryption type, packet size, and power usage
- Power efficiency per processed packet

Deliverables:

A power benchmarking report and a tool that visualizes how power consumption changes with different traffic conditions. This will help understand the energy efficiency of security devices under various loads

Reference:

RFC 9411: "Benchmarking Methodology for Network Security Device Performance" It provides guidelines for evaluating the performance of network security devices (NSDs) such as firewalls, intrusion detection/prevention systems (IDS/IPS), and other security appliances. The goal is to create a standardized method for benchmarking NSDs to ensure that performance is measured consistently and accurately across different implementations.

Published: March 2023

https://datatracker.ietf.org/doc/rfc9411/