Hosting a DNS Server for Dunder Mifflin

Monday, November 18, 2024 1:24 PM

This project establishes a dedicated DNS infrastructure for Dunder Mifflin to replace reliance on external DNS services. By configuring an authoritative and recursive DNS setup, this project enables the use of symbolic names for servers, improving ease of network management and user experience.

Key Features

1. **Primary DNS Server (BIND)**:
    - Installed and configured **BIND DNS Server** on **Machine B** (dns0.dundermifflin.com) as:
        - Authoritative for the dundermifflin.com domain.
        - Providing **reverse DNS** for both the DMZ and LAN subnets.
        - Recursive for queries originating from LAN and DMZ subnets.
    - Implemented **resource records** for all servers and aliases as outlined in the provided table.
        - **A Records** for direct IP mapping.
        - **CNAME Records** for aliases and functional names.
        - TTL values: 1 hour for most records, 5 minutes for frequently updated records.
    - Configured the **SOA record** with the required specifications:
        - Master name: dns0.dundermifflin.com.
        - Administrator: the system admin.
        - TTL: Default set to 1 hour.
        - Refresh: 1 day, Retry: 1 hour, Expire: 1 week, Negative cache: 1 hour.
2. **Recursive and Restricted DNS Queries**:
    - Allowed recursive DNS resolution only for LAN and DMZ subnets.
    - Configured access controls to restrict queries from external sources to non-recursive resolution.
3. **DHCP Integration**:
    - Updated the DHCP configuration on **Machine A** to:
        - Set the **DNS server** to the newly configured Dunder-Mifflin DNS server (dns0.dundermifflin.com).
        - Ensure all Dunder-Mifflin machines use this server for DNS resolution.
4. **Secondary DNS Server (Students in 5030/5113)**:
    - Configured **Machine F** (dns1.dundermifflin.com) as a **secondary DNS server**.
    - Synchronized zones between **Machine B** and **Machine F** using BIND's built-in zone transfer mechanisms.
    - Modified configurations on all machines to use both DNS servers for fault tolerance.
5. **Reverse DNS**:
    - Implemented reverse DNS zones for both the DMZ and LAN subnets.
    - Matched the TTL values with forward DNS records for consistency.
6. **Split DNS**:
    - Configured **split DNS views**:
        - **Internal View**: Served to LAN/DMZ subnets, including both forward and reverse DNS with full record visibility.
        - **External View**: Limited to public records, excluding LAN-specific entries, and reverse DNS only for the DMZ subnet.
    - Propagated split DNS configuration to **Machine F** for secondary DNS.

This project demonstrates the ability to build a robust, scalable, and secure DNS infrastructure tailored to organizational needs while integrating advanced features like split DNS and zone synchronization.