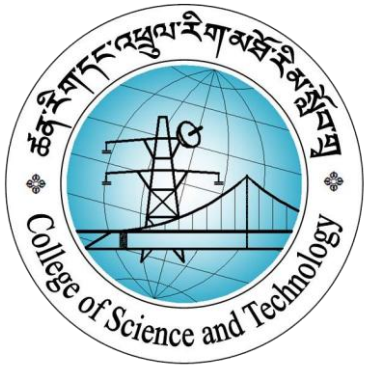

DNS

More on DNS : Risk of Misconfigured DNS

Understanding DNS Misconfigurations and Their Causes

- **Incorrect or Outdated DNS Records:**
  - Old, outdated records or records with typos can lead to disruptions or unintentional traffic redirection.
- **Open DNS Resolvers:**
  - While you want your public website to remain accessible and reliable, the same is not true of your DNS server. An open DNS resolver responds to requests from anyone, not just trusted users, and malicious actors can use your DNS to amplify Distributed Denial of Service (DDoS) attacks.
- **Lack of DNSSEC Implementation:**
  - Without DNS Security Extensions (DNSSEC), attackers can forge DNS responses (e.g., pointing login.bank.com to a fake IP), enabling phishing, man-in-the-middle attacks, and cache poisoning.

Understanding DNS Misconfigurations and Their Causes

- **Improper Forwarding Configurations:**
  - Forwarding DNS queries to untrusted or external servers can leak sensitive internal domain info (like server names or file shares), exposing your network to reconnaissance and targeted attacks.
- **Incorrect Zone File Settings:**
  - Bad records or syntax errors (like wrong IPs, orphaned subdomains, or missing SPF/DKIM entries) can break security protections, misroute traffic, or enable subdomain takeovers and email spoofing.

How to Prevent DNS Misconfigurations?

- **Follow DNS Configuration Best Practices**
  - Be sure to double-check all DNS records (A, CNAME, MX, TXT, etc.) for typos or incorrect values. Additionally, avoid pointing DNS records to internal IP addresses (e.g., RFC1918 ranges) in public zones.
- **Implement Access Controls**
  - As a best practice, you should limit who can view or edit DNS records. Require multi-factor authentication (MFA) to secure any administrator accounts and keep registrar and DNS provider credentials separate from other infrastructure accounts.
- **Audit DNS Zones Regularly:**
  - Be sure to remove any old, stale, or orphaned records (e.g., subdomains pointing to decommissioned services).

How to Prevent DNS Misconfigurations?

- **Avoid Manual Entry When Possible**
  - Mistakes happen, and manual entry is one of the easiest ways to introduce errors into your DNS settings. Whenever possible, use templates or automation to enforce consistent record structure and reduce the risk of human error.

- **Work with a Reliable DNS Provider**
  - A DNS service provider plays a crucial role in ensuring DNS records are properly created, propagated, and secured. By leveraging a DNS service, organizations can minimize the risk of DNS misconfiguration.

REAL LIFE INCIDENTS…Major incidents examples

MasterCard's five-year misconfiguration:

- A security researcher discovered that MasterCard's DNS settings had a major vulnerability for nearly five years. An unused domain name associated with the company was misconfigured in a way that could have allowed an attacker to intercept traffic. The researcher had to pay to register the domain to prevent it from being taken over by malicious actors.

MikroTik botnet:

- A large global botnet was built using compromised MikroTik routers. A key factor was misconfigured DNS records, specifically permissive SPF records on thousands of legitimate domains. This mistake allowed attackers to spoof these domains, making their phishing emails look authentic and bypass security checks.

Sea Turtle group's DNS hijacking:

- This threat actor group compromised various DNS registrars and registries to redirect users of certain Dutch IT and telecom companies to their malicious servers. By manipulating DNS responses, they were able to harvest credentials by making it seem like users were visiting legitimate sites, a technique made possible by poor DNS hygiene on the part of the victim companies.