DNS Enumeration and Zone Transfer Lab

Overview

This lab demonstrates basic DNS enumeration techniques using nslookup and dig. The goal was to understand how DNS records are queried, how reverse DNS works, and how misconfigured name servers can allow unauthorized zone transfers.

Tools Used

- Kali Linux
- nslookup
- dig

Part 1: DNS Enumeration

Forward DNS Lookup

Forward lookups were performed to retrieve common DNS records associated with the target domain.

nslookup -type=A example.com

nslookup -type=MX example.com

nslookup -type=NS example.com

nslookup -type=TXT example.com

These queries returned IP addresses, mail servers, authoritative name servers, and additional metadata related to the domain.

Reverse DNS Lookup

A reverse lookup was used to resolve an IP address back to a hostname. This requires first resolving the domain to an IP address.

nslookup example.com

nslookup <IP_ADDRESS>

Reverse DNS uses PTR records and is controlled by the IP owner, so results may be limited or unavailable.

Part 2: DNS Zone Transfer (AXFR)

Identifying Name Servers

Authoritative name servers for the domain were identified using:

dig example.com NS

This returned multiple name servers, including:

- ns1.example.com
- ns2.example.com

Attempting Zone Transfers

Zone transfer attempts were made against each name server.

dig @ns1.example.com example.com AXFR

dig @ns2.example.com example.com AXFR

Results

- The zone transfer from ns1.example.com was successful and returned multiple DNS records.
- The zone transfer from ns2.example.com failed with an access denied response.

Analysis

Zone transfers should be restricted to trusted servers only. The successful AXFR from ns1.example.com indicates a DNS misconfiguration. Even though ns2.example.com was correctly secured, a single misconfigured name server is enough to expose the entire DNS zone.

Conclusion

This lab shows how DNS enumeration can reveal valuable information and how improper AXFR configuration can lead to information disclosure. Proper DNS hardening requires restricting zone transfers on all authoritative name servers, not just some of them.