DNS Poisoning

And Mitigation

Adithya Nair - AID23002
Avighna Reddy - AID23005
P.Ananthapadmanabhan Nair - AID23036

Group-2

Agenda

- Introduction
- Attack Environment
- Tools Used
- Attack Steps Overview
- What Happens During the Attack?
- Defense Mechanisms
- Conclusion

Back to Agenda Page

Introduction

DNS spoofing is a cyber attack where DNS responses are manipulated to redirect users to malicious sites. This demonstration uses virtual machines to simulate a DNS spoofing attack.

Back to Agenda Page

Attack Environment

- Kali Linux VM: Used to launch the attack and run tools like dnsmasq.
- Victim: Any device in the local network attempting DNS resolution.
- Poisoned Domain: A domain (grouptwo.com) is redirected to a malicious IP.

Software Used

Back to Agenda Page

- dnsmasq: A lightweight DNS server used to serve poisoned DNS records..
- IP Tables: CLI that’s configured to redirect DNS traffic and modify packet attributes.
- ettercap: Tool for ARP spoofing and network monitoring.

Attack Steps Overview

1. Set up dnsmasq to serve poisoned DNS records.

2. Perform ARP spoofing to become the default gateway.

3. Enable IP forwarding to maintain network functionality.

4. Configure IP tables to redirect DNS traffic to dnsmasq.

5. Launch ARP spoofing and monitor traffic using ettercap.

Back to Agenda Page

What Happens During the Attack?

- User requests access to a domain
- Request is intercepted by the Kali VM
- dnsmasq responds with poisoned DNS records.
- User is redirected to a malicious site controlled by the attacker.

Defense Mechanisms

- Implement static ARP entries where feasible.
- Use ARP poisoning detection tools (e.g., arpwatch).
- Restrict access to DNS servers and monitor traffic.

Back to Agenda Page

Conclusion

Thank you!