Network Monitoring and Security

Understanding DNS, Wireshark, and Network Scanning

Introduction to DNS

What is DNS?

- DNS translates domain names to IP addresses, functioning like the internet's phonebook.

DNS Resolution Process

1. **User Input**: User enters a domain name.
2. **Local Cache Check**: Operating system checks its cache to find the IP.
3. **Resolver Query**: Queries the configured DNS server if cache miss occurs.
4. **Recursive Search**: Server queries other DNS servers if needed.
5. **IP Address Returned**: Final IP address is returned to the client.

Common DNS Records

Types of DNS Records

- **A Record**: Links a domain to an IPv4 address.
- **AAAA Record**: Links a domain to an IPv6 address.
- **CNAME Record**: Alias of one domain to another.
- **MX Record**: Directs mail to an email server.
- **TXT Record**: Provides textual information about a domain.

Introduction to Wireshark

What is Wireshark?

- Wireshark is a network protocol analyzer used for network troubleshooting, analysis, and software development.

Installing Wireshark

How to Install

- Arch Linux (`sudo pacman -S nmap`),
- Windows/ macOS (download from wireshark.org).

Key Features of Wireshark

- **Real-Time Capture**: Capture and analyze network traffic as it happens.
- **Advanced Filtering**: Filter traffic by protocol, IP address, port, etc.
- **Graphical Packet Analysis**: Visualize packet flow and protocol relationships.

Wireshark Interface Overview

Key Areas

- **Menu Bar and Toolbar**: Access tools and apply filters.
- **Packet List Pane**: Displays packets in real-time.
- **Packet Details Pane**: Examines details of the selected packet.
- **Packet Bytes Pane**: View packet data at the byte level.

Capturing HTTP Traffic in Wireshark

Command to Filter HTTP Traffic

- Filter expression: `http`
- This command isolates all HTTP traffic, showing only packets related to HTTP transactions.

Packet Capture Process in Wireshark

Steps for Capturing Packets

1. **Open Wireshark**: Launch the application.
2. **Select Network Interface**: Choose which network interface to monitor.
3. **Start Capture**: Click the start button to begin capturing packets.
4. **Stop Capture**: Click the stop button once you've captured the necessary data.

Analyzing Packet Layers in Wireshark

Examination of Layers

- **Ethernet Layer**: View MAC addresses involved in packet transmission.
- **IP Layer**: Shows source and destination IP addresses.
- **TCP/UDP Layer**: Details source and destination ports.
- **HTTP Layer**: Inspects HTTP request and response headers.
- **Data Layer**: Analyze payload data within the packet.

Network Scanning with Nmap

Overview of Nmap

- Nmap is used for network discovery and security auditing.

Basic Nmap Commands

Scanning Commands

- **Scan All Ports**: `nmap -p- target`
- Scans all 65535 ports of the target system.
- **Fast Scan**: `nmap -F target`
- Scans only the 100 most common ports, faster than a full scan.
- **OS Detection**: `nmap -A target`
- Attempts to identify the target's operating system and services.

Advanced Nmap Techniques

Decoy Scanning and Service Enumeration

- **Decoy Scanning**: `nmap -D decoy1,decoy2 target`
- Uses fake IPs to hide the scanner's origin.
- **Service Enumeration**: `nmap -sV target`
- Detects service versions on open ports.

Practical Exercise: Network Scanning

Hands-On Activity

1. **Start Nmap**: Use the provided commands to scan a test network.
2. **Analyze Results**: Review the output to identify open ports and running services.
3. **Report Findings**: Document potential security vulnerabilities.

DNS Security

DNS Security Threats

- DNS Spoofing: Falsifying DNS data to redirect traffic.
- DNS Amplification: Using small queries to generate large responses, overwhelming the target.

DNSSEC

- **DNSSEC (DNS Security Extensions)**: Protects against unauthorized DNS data modifications.
- **How It Works**: Adds digital signatures to DNS data to verify its authenticity.

Practical DNS Troubleshooting

Using `dig` and `nslookup`

- **Example Command**: `dig @1.1.1.1 example.com`
- Queries the DNS server at 1.1.1.1 for records of example.com.
- **Example Command**: `nslookup -type=mx example.com`
- Fetches mail exchange records for example.com.

Custom Filters in Wireshark

Creating Custom Filters

- **Example**: Filter by IP range: `ip.addr >= 192.168.0.1 and ip.addr <= 192.168.0.255`
- **Example**: Filter TCP traffic from a specific port: `tcp.port == 80`

Analyzing Network Performance with Wireshark

Identifying Network Issues

- **Latency Problems**: Look for large time gaps between packets.
- **Retransmissions**: Filter for `tcp.analysis.retransmission` to find dropped packets.

Wireshark Graphs

- Use `Statistics > IO Graphs` to visualize traffic patterns and identify spikes or drops.

Using Hping for Advanced Scanning

Command Examples

- **Ping Sweep**: `hping3 -S -p 80 -c 1 192.168.0.0/24`
- Sends SYN packets to port 80 across the subnet.
- **Traceroute**: `hping3 --traceroute -V -1 example.com`
- Detailed traceroute using ICMP packets.

DNS Query Analysis Exercise

Capturing DNS Traffic

- Start capture with filter `dns`
- Analyze request and response details: transaction IDs, query type, etc.

Advanced Nmap Scripting

Nmap Scripting Engine

- **Example**: `nmap --script=http-title 192.168.1.0/24`
- Scans network and lists the titles of web pages hosted on HTTP servers.

Case Study: Network Attack Prevention

Using Tools for Defense

- Discuss a DDoS attack scenario.
- Role of network monitoring tools like Wireshark and protective scans with Nmap.

Appendix: Examples of Network Tools

DNS Tools

- **Check DNS Records**: `dig +short MX example.com`
- **Verify DNSSEC**: `dig +dnssec example.com`

Wireshark Examples

- **Filter SSL Traffic**: `ssl`
- **Analyze DHCP Traffic**: `bootp.type == 2`

Appendix Cont.: Examples of Network Tools

Nmap Examples

- **Detect Live Hosts**: `nmap -sn 192.168.1.0/24`
- **Version Detection**: `nmap -sV 192.168.1.105`

Hping Examples

- **Firewall Testing**: `hping3 -S -p 80 -c 3 192.168.1.1`
- **ARP Ping**: `hping3 -2 -c 4 -p 5060 192.168.1.1`

References

- Wireshark Official Website
- Nmap Documentation
- DNS Overview