Intro to Linux

Nmap and nslookup Lab

Nmap and nslookup Materials

- Materials needed
  - Ubuntu Linux Machine
- Software Tools used
  - nmap
  - nslookup

Objectives Covered

- Linux+ Objectives (XKO-005)
  - Objective 4.2 – Given a scenario, analyze and troubleshoot network resource issues
    - Testing remote systems
      - Nmap
  - Objective 1.5 – Given a scenario, use the appropriate networking tools or configuration files
    - Name resolution
      - Bind-utils
        - nslookup

Nmap and nslookup Overview

1. Use nmap
2. Use nslookup
3. Wrap-up

Set up VM Environments

- Log into your range
- Open the Ubuntu Linux and Kali Environments
  - You should be on your Ubuntu Linux Desktop
  - You should be on your Kali Linux Desktop

ping

- The Linux ping command is a network utility used to test a host's reachability on an Internet Protocol (IP) network
- ping sends out ICMP echo request packets to the target host and waits for echo replies
- In general, the ping command has the following syntax

```
ping [options] [hostname/IP address]
```

Using the ping Command

- Open a terminal in your Ubuntu machine
- Use ping without an option (after capturing some packets, type CTRL+C)

```
ping google.com
```

- As a troubleshooting step, one can ping their host computer (CTRL+C to stop capturing)

```
ping localhost
```

- To specify how many packets to send use the –c option

```
ping -c 4 <Kali IP address>
```

Nmap

- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses
- To scan all reserved TCP ports on the machine scanme.nmap.org, use the verbose mode

```
nmap -v scanme.nmap.org
```

- Test your Kali machine for any open ports

```
nmap -sT <Kali IP address>
```

- Ask Nmap to choose 1,000 hosts at random and scan them for web servers (port 80)

```
nmap -v -iR 1000 -Pn -p 80
```

nslookup

- DNS (Domain Name Server) is a network device that will answer client queries to translate domain names into IP addresses
- nslookup is a command-line tool that can be used to get info from DNS servers including
  - The IP addresses for a specific domain
  - If a domain is associated with any other organizations
  - Who are the mail servers for the domain
  - Any extra text data included in the domain record
- Modes – nslookup can operate in Interactive or Non-Interactive Mode

Using nslookup Interactively

- To initiate the nslookup interactive mode, type the command

```
nslookup
```

- We can type a domain name to receive information about it

```
www.google.com
```

- In interactive mode, we can specify an option in a separate line before the query

```
set type=ns
google.com
```

- We can exit interactive mode

```
exit
```

Using nslookup Non-Interactively

- We can gather to same information non-interactively using

```
nslookup www.google.com
nslookup -type=ns google.com
```

- Notice the outputs are the same but we remain at the same terminal prompt rather than in the interactive mode of nslookup
- We can also check a domain's MX data with

```
nslookup -type=mx yahoo.com
```

Wrap-up

- Ping verifies basic network connectivity
- Nmap explores network topology and identifies services
- Nslookup resolves domain names to IP addresses and vice versa, aiding in DNS troubleshooting
- Together, these tools form a comprehensive toolkit for network administrators and security analysts to diagnose and manage network issues effectively.