Command Line Networking Basics Worksheet

1. Ping: Testing Connectivity

Objective: Use `ping` to test network connectivity between your system and a remote host.

Key Concepts: - The `ping` command sends Internet Control Message Protocol (ICMP) echo requests to a target to check connectivity. - It is commonly used to troubleshoot network issues.

Basic Command: `ping [hostname or IP address]`

Exercises: 1. Use `ping google.com` to test your internet connection. What does the output tell you? 2. Use `ping -c 5 google.com` to send exactly 5 ping requests. How does this differ from the default behavior? 3. Try pinging a local device (e.g., another computer or router) on your network using its IP address. What is the response time?

Challenge: - Use `ping -i 2 google.com` to send a ping request every 2 seconds. Observe the output and explain when this might be useful.

---

2. Traceroute: Tracking Packet Paths

Objective: Use `traceroute` to map the route packets take to reach a destination.

Key Concepts: - `traceroute` shows the path packets take from your machine to the destination, revealing any bottlenecks or hops in between. - It is helpful for diagnosing routing issues.

Basic Command: `traceroute [hostname or IP address]`

Exercises: 1. Use `traceroute google.com` to see the route packets take to reach Google's servers. How many hops are there? 2. Identify the IP addresses or hostnames of the routers between your system and Google. Are any of them in private IP ranges (e.g., `192.168.x.x`)? 3. Run `traceroute` on a local device within your network. Compare the output to your internet-based `traceroute`.

Challenge: - Use `traceroute -I google.com` to use ICMP instead of the default UDP packets. How does the result compare to a standard `traceroute`?

---

3. Curl: Retrieving Web Content

Objective: Use `curl` to interact with web servers and retrieve content.

Key Concepts: - `curl` is a versatile tool that can fetch data from URLs. It supports various protocols, including HTTP, HTTPS, FTP, and more. - It's often used to test and troubleshoot web servers and APIs.

Basic Command: `curl [URL]`

Exercises: 1. Use `curl http://example.com` to fetch the content of the example website. What does the output look like? 2. Use `curl -I http://example.com` to retrieve only the HTTP headers of the website. 3. Use `curl -o page.html http://example.com` to save the website content to a file. Open the file using a text editor or web browser.

Challenge: - Use `curl -L http://example.com` to follow any redirects. Explain when and why websites might use redirects.

Here's the updated worksheet with a detailed description of the DNS record types in the **Dig** section:

Command Line Networking Basics Worksheet

4. Dig: Querying DNS Information

Objective: Use `dig` to query DNS servers and retrieve domain-related information.

Key Concepts: - `dig` is a DNS lookup utility that queries the Domain Name System (DNS) to resolve domain names to IP addresses. - DNS is like the "phone book" of the internet, translating domain names into IP addresses so devices can communicate. - `dig` is helpful for troubleshooting DNS-related issues and gathering domain information.

Basic Command: `dig [domain]`

Exercises: 1. Use `dig google.com` to query the DNS records for Google. What is the IP address for Google in the output? 2. Use `dig +short google.com` to see only the IP addresses returned by the DNS query. 3. Use `dig google.com MX` to query the Mail Exchange (MX) records for Google. 4. Explore different DNS record types using the command `dig [domain] [record type]`.

DNS Record Types: - **A Record** (Address Record): Maps a domain name to an IPv4 address. - Example: `dig google.com A` returns the IPv4 address associated with Google's domain. - **AAAA Record** (IPv6 Address Record): Maps a domain name to an IPv6 address. - Example: `dig google.com AAAA` returns the IPv6 address associated with Google's domain. - **MX Record** (Mail Exchange): Specifies the mail servers responsible for receiving emails for a domain. - Example: `dig google.com MX` returns the mail servers for Google, each with a priority level. - **CNAME Record** (Canonical Name): Maps one domain name to another (alias). - Example: `dig www.example.com CNAME` might show that `www.example.com` is an alias for `example.com`. - **NS Record** (Name Server): Specifies the authoritative name servers for a domain. - Example: `dig example.com NS` returns the name servers for `example.com`, which are responsible for handling DNS queries for that domain. - **TXT Record** (Text Record): Used to store arbitrary human-readable or machine-readable text, often for purposes like verifying domain ownership or providing SPF (Sender Policy Framework) records for email. - Example: `dig example.com TXT` might show verification details for services like Google or AWS. - **SOA Record** (Start of Authority): Provides information about the domain's DNS zone, including the primary name server and zone management details. - Example: `dig example.com SOA` returns the DNS zone's version and authoritative server information. - **PTR Record** (Pointer Record): Maps an IP address to a domain name (reverse lookup). - Example: `dig -x [IP address]` performs a reverse DNS lookup to find the domain name associated with an IP address.

Challenge: - Use `dig google.com ANY` to query all available DNS records. Identify the different record types (A, AAAA, MX, NS, etc.) in the output. Explain how each type is used for managing domain resources.

---

5. IP Route: Viewing and Modifying Routing Tables

Objective: Use `ip route` to view and manage the system's routing table.

Key Concepts: - The `ip route` command shows the system's routing table, which determines how packets are routed within and outside your network. - You can also use it to add or delete routes.

Basic Command: `ip route`

Exercises: 1. Use `ip route` to view the routing table on your system. What is the default gateway? 2. Identify the route that packets will take to reach external networks (i.e., the internet). 3. Use `ip route get 8.8.8.8` to see the route that will be used to reach Google's public DNS server.

Challenge: - Research how to add a static route using `ip route add`. Write the command to add a route to a network `192.168.1.0/24` through gateway `192.168.0.1` and verify it using `ip route`.

---

6. Nmap: Network Scanning

Objective: Use `nmap` to scan networks and discover hosts and services.

Key Concepts: - `nmap` is a powerful network scanning tool that can be used to discover devices, services, and vulnerabilities on a network. - It is often used by network administrators for security audits and troubleshooting.

Basic Command: `nmap [options] [target]`

Exercises: 1. Use `nmap localhost` to scan your local machine. What open ports and services are detected? 2. Use `nmap 192.168.1.0/24` to scan all devices on your local network. What devices and services are found? 3. Use `nmap -sP 192.168.1.0/24` to perform a ping sweep, identifying all live hosts on the network.

Challenge: - Use `nmap -sV [IP address]` to detect the versions of services running on a target. Why is this useful for network security?

Reflection:

After completing the exercises, consider the following: - How do these networking commands help in troubleshooting network issues? - What additional tools or techniques might you explore to manage and secure a network?
