Linux Tools for Networking and Firewall Management

HyperionDev

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Explored the Berkeley Socket API in Python

Objectives

- Explore Linux tools related to Networking
- Recap on Networking components
- Recap on Firewalls
- Explore Firewall management tools
- How the above ties into Security

Why is it important?

- Protection against unauthorized access, malicious attacks, and data breaches requires effective networking and firewall management.

- Reduced attack surfaces and blocked unauthorized network connections are two ways that properly configured networks and firewalls help reduce risks.

- Managing networks and firewalls effectively can boost systems' responsiveness and efficacy.

- Networking and firewall management procedures assist organizations in fulfilling these demands by ensuring they follow laws and standards to network safety and data security.

- By keeping secure and trustworthy network connections, organizations can avoid network outages, safeguard vital systems and data, and lessen the effects of potential security incidents.

Fundamental components (Networking)

- Network Interfaces: An interface to a network is a piece of hardware or software that enables a device to join a network. It could be a virtual interface produced by software or a physical network interface card (NIC).

- IP addresses: Each device connected to a network is given a specific numerical identifier known as an IP address. In order for devices to find and communicate with one another, it acts as the address.

- Subnet Masks: An IP addresses network and host parts are determined by a subnet mask, which is a numerical value. Subnet masks help devices determine if a destination IP address is within the same local network or requires routing through a gateway.

- Default Gateways: An IP address for a device that acts as a router or entry point to connect one network to another is referred to as a default gateway. Default gateways enable devices to connect to remote networks by routing data between networks

Linux CLI Tools(Networking)

Ifconfig: On Linux systems, network interfaces are configured and managed using ifconfig (interface configuration).

ip: A more sophisticated and flexible tool for network configuration is the ip command. For managing network interfaces, routes, IP addresses, tunnels, and other things, it offers a wide range of functionality.

netstat: Network connection details, routing tables, and network statistics are all displayed by the tool known as netstat (network statistics). You can view open network connections, listening ports, running network services, information about routing, and statistics about network interfaces.

Network administrators and system administrators can efficiently manage network interfaces, assign IP addresses, monitor network connections, troubleshoot networking problems, and collect network-related data by using these tools.

Linux CLI Tools(Networking)

tcpdump: A command-line packet analyzer called tcpdump records network traffic in real-time. It enables you to apply filters to capture particular kinds of traffic, capture packets on a specific network interface, and save the captured packets for later analysis.

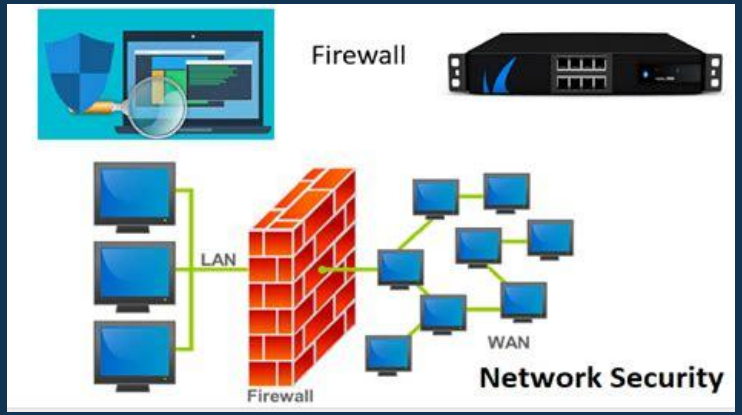
Wireshark: Popular graphical packet analyzer Wireshark offers a thorough interface for capturing, examining, and inspecting network packets. You can analyze network protocols at different layers and it provides extensive protocol support.

Iftop: Iftop is a command-line tool that shows a network interface real-time bandwidth usage. It displays a real-time breakdown of network traffic by protocols, ports, and source and destination IP addresses.

These resources are necessary for diagnosing network issues, enhancing network performance, and ensuring the effectiveness and security of network communications.

Firewalls Recap

By serving as a barrier between trusted internal networks and outside, untrusted networks, like the internet, firewalls play a crucial part in network security. They keep an eye on and manage incoming and outgoing network traffic in accordance with pre-established security rules.



https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fsophisticnetworks.com%2Fwp-content%2Fuploads%2F2020%2F04%2Fwhat-is-Firewall-and-its-types.png&f=1&nofb=1&ipt=5e96445cc6b4e412a35290982a12465953a74e9837b810ee322f539fcec384f1&ipo=images

Firewalls Recap

Host-Based: Directly installed on individual devices, host-based firewalls manage traffic to and from that particular host. They offer detailed management of network connections on a particular device.

Network-Based: On the other hand, network firewalls control the flow of traffic between internal and external networks and are placed at the network perimeter. To secure the entire network, they frequently use stateful inspection, access control lists (ACLs), and other methods.

https://www.webtoolsoffers.com/wp-content/uploads/2020/10/How-firewall-works-Firewall-Technology-2048x1024.jpg

Linux Firewall Management:

Through the use of programs like iptables and firewalld, Linux offers strong firewall management capabilities.

iptables: A command-line tool that enables complex packet filtering and manipulation rules. Administrators can define rules for different network protocols, ports, and IP addresses because it operates at the network packet level.

firewalld: On the other hand, firewalld is a more advanced tool that offers a flexible and user-friendly interface for managing firewall rules. By using zone-based rules, it simplifies firewall configuration and supports simple management of network services and ports.

https://www.hugeserver.com/blog/wp-content/uploads/2016/12/firewalld_vs_iptables.png

Security is P0

- Security is important, and firewall and networking configuration management are key to keeping an environment secure. Firewalls and network services that are properly configured aid in preventing unauthorized access, data breaches, and other cyber threats.

- Follow best practices for securing network services if you want to prevent security breaches. This includes actions like turning off unnecessary services, regularly installing patches and updates, creating strong, one-of-a-kind passwords, and using encryption protocols when necessary.

- One of the core components of network security is access control and strict firewall rule implementation. In order to accomplish this, firewalls must be configured to permit only necessary traffic and to block potentially dangerous or unauthorized connections.

- Network security is an ongoing process, and it's crucial to regularly update and monitor firewall configurations. This includes staying up to date with security patches, firmware updates, and vendor recommendations.

Homework: Play around with *ping*, *ifconfig* and *traceroute*

Wrapping Up.

- Linux networking and firewall management tools are essential for keeping systems secure and effective.
- In network configurations, factors such as network interfaces, IP addresses, subnet masks, and default gateways are crucial.
- For managing and troubleshooting networks, tools like ifconfig, ip, netstat, tcpdump, wireshark, and iftop offer powerful capabilities.
- Network security depends on firewalls, and Linux provides powerful firewall management tools like iptables and firewalld.
- When managing networking and firewall configurations, security should be given top priority. Best practices include securing network services, limiting access, and putting in place strong firewall rules.

Next up

- Linux Tools for Encryption and Hashing

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"