**Integrating Bash and Nmap for Efficient Network Scanning**

* **Nmap**

Nmap (Network Mapper) is a powerful open-source network scanning tool used to Discover hosts and services on a computer network. Perform security audits. Detect open ports, running services, and OS versions.

* **Common Uses**

Port scanning.

Vulnerability detection.

Network inventory and monitoring.

* **Why We Use Nmap**

We use Nmap to check system exposure on a network, find misconfigured or vulnerable services, detect unauthorized devices, and automate reconnaissance during penetration testing.

* **Bash**

Bash (Bourne Again shell) is a command-line shell and scripting language commonly used in Unix/Linux systems

* **Why we use Bash**

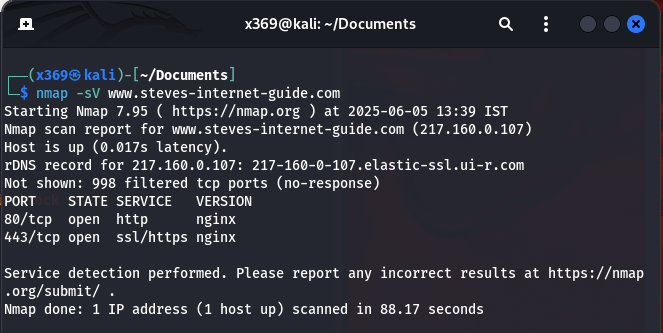
Bash is used to automate repetitive tasks, combine multiple Linux tools, manage files, run scans, process output efficiently, and schedule jobs using corn

* **Practical: Combine Nmap with Bash**
* **Power of Combining Nmap and Bash**

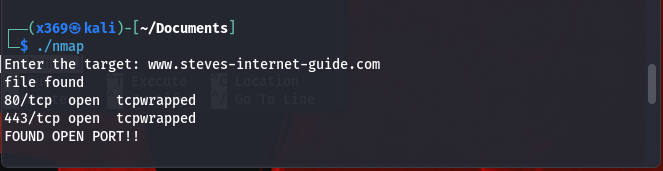
Integrating Nmap with Bash scripting enables automated, efficient network scanning. It streamlines tasks like scanning multiple targets, filtering results, and generating reports — ideal for penetration testing and routine security audits.

Practical

* Before combining bash script with Nmap

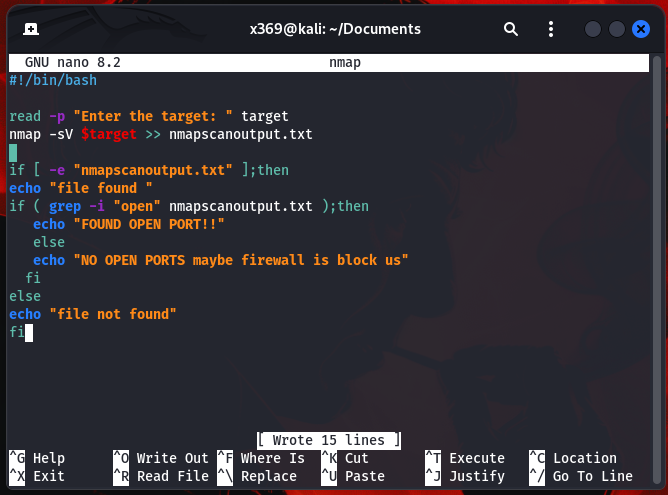


* After combining the bash with Nmap



Manual Nmap provides detailed scan results with service detection, while Bash with Nmap automates the scan process and adds custom logic like alerts or file output for open ports

Bash Script to Perform Nmap Scan and Detect Open Ports Automatically



This Bash script scans a specified target for open ports. If any open ports are detected, it displays a summary of the results, providing a clear and concise overview of the scan findings. This helps in efficiently identifying exposed services on the target system.