Awesome — let’s combine **Stage 3 of Nmap** with learning how to use the **Nano text editor**, which is often used during hacking labs to edit configuration files, write scripts, or store scan results.

**✅ What is Nmap Stage 3?**

You’ve likely done:

* **Stage 1** → Basic scans (nmap IP)
* **Stage 2** → Port scans with flags (-sS, -sU, etc.)

**🧠 Stage 3 focuses on:**

* Advanced scan options
* Output formats
* Saving & documenting results
* Custom NSE (Nmap Scripting Engine) scripts

Now let’s bring **Nano** into the game to **save, edit, or write** these scan results/scripts.

**🧰 Nano Editor Basics – "Learning the Ropes"**

Nano is a simple **command-line text editor**.

**🔓 Launching Nano**

nano filename.txt

This opens (or creates) a file named filename.txt.

**✍️ Useful Nano Commands**

| **Shortcut** | **What It Does** |
| --- | --- |
| CTRL + O | Save (Write Out) |
| CTRL + X | Exit Nano |
| CTRL + K | Cut a line |
| CTRL + U | Paste |
| CTRL + W | Search inside the file |
| CTRL + G | Help menu |

**🛠 Example Use Case: Save Nmap Output**

1. Run an Nmap scan and **save results**:

nmap -sV -oN scanresult.txt 192.168.1.1

1. Open with Nano:

nano scanresult.txt

1. Add your notes:

# Vulnerable version of Apache detected.

# Consider further enumeration with nikto or gobuster.

1. Save and exit:

* Press CTRL + O → Enter (to save)
* Press CTRL + X (to exit)

**⚙️ Bonus: Writing a Simple Nmap Script Log**

Open a script file:

nano mynmaplog.sh

Write:

#!/bin/bash

echo "Running Nmap Scan..."

nmap -sC -sV -oN results.txt $1

Save and make it executable:

chmod +x mynmaplog.sh

./mynmaplog.sh 192.168.1.1

**🔒 Why Nano + Nmap Combo is Useful in Hacking**

* Quickly document findings on a target system
* Modify or write simple shell scripts during a pentest
* Store logs during red teaming or OSCP-like exercises
* Read or tweak Nmap NSE scripts if you dive deeper

Let me know if you want:

* Nano cheat sheet PDF
* Nano vs Vim for hackers
* Writing custom NSE scripts and editing in Nano

| **Switch** | **Example** | **Description** |
| --- | --- | --- |
|  | nmap 192.168.1.1 | Scan a single IP |
|  | nmap 192.168.1.1 192.168.2.1 | Scan specific IPs |
|  | nmap 192.168.1.1-254 | Scan a range |
|  | nmap scanme.nmap.org | Scan a domain |
|  | nmap 192.168.1.0/24 | Scan using CIDR notation |
| -iL | nmap -iL targets.txt | Scan targets from a file |
| -iR | nmap -iR 100 | Scan 100 random hosts |
| --exclude | nmap --exclude 192.168.1.1 | Exclude listed hosts |

| **Switch** | **Example** | **Description** |
| --- | --- | --- |
| -sS | nmap 192.168.1.1 -sS | TCP SYN port scan (Default) |
| -sT | nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU | nmap 192.168.1.1 -sU | UDP port scan |
| -sA | nmap 192.168.1.1 -sA | TCP ACK port scan |
| -sW | nmap 192.168.1.1 -sW | TCP Window port scan |
| -sM | nmap 192.168.1.1 -sM | TCP Maimon port scan |