

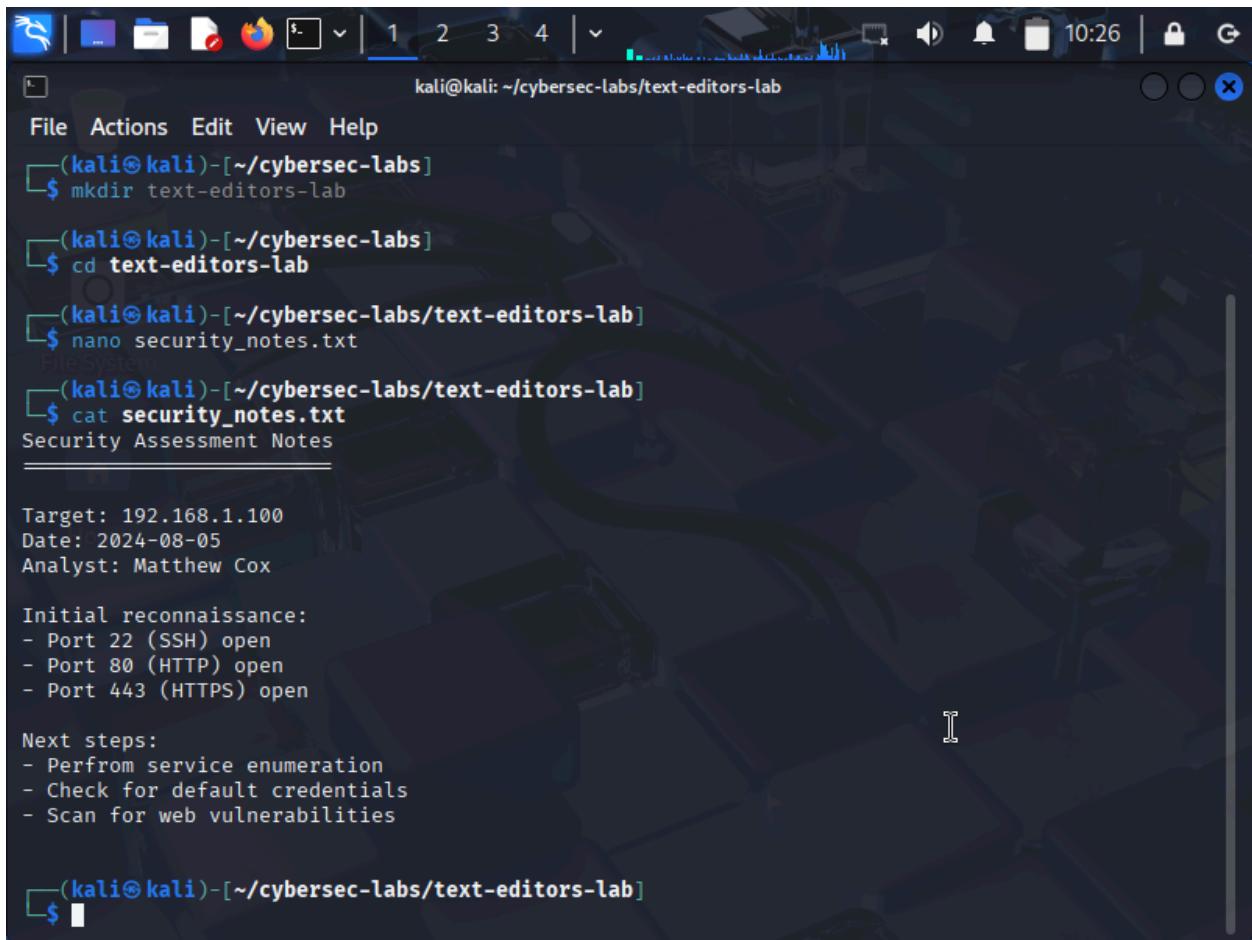
Matthew Cox

COMP 325

### Introduction:

In this lab, I will be showing my learning process using VIM and nano. I will be able to use text editing skills for common cybersecurity tasks. Whether modifying configuration files, creating custom scripts, analyzing log files, or editing exploit code, proficiency with command-line text editors is essential. This lab focuses on practical applications of nano and VIM in cybersecurity contexts, emphasizing real-world scenarios you'll encounter in penetration testing, incident response, and security administration.

### Body:



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "kali@kali: ~/cybersec-labs/text-editors-lab". The terminal content is as follows:

```
(kali㉿kali)-[~/cybersec-labs]
$ mkdir text-editors-lab

(kali㉿kali)-[~/cybersec-labs]
$ cd text-editors-lab

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]
$ nano security_notes.txt
File System
(kali㉿kali)-[~/cybersec-labs/text-editors-lab]
$ cat security_notes.txt
Security Assessment Notes
_____
Target: 192.168.1.100
Date: 2024-08-05
Analyst: Matthew Cox

Initial reconnaissance:
- Port 22 (SSH) open
- Port 80 (HTTP) open
- Port 443 (HTTPS) open

Next steps:
- Perform service enumeration
- Check for default credentials
- Scan for web vulnerabilities

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]
$
```

This is the first file that I have created with nano.

kali@kali: ~/cybersec-labs/text-editors-lab

File Actions Edit View Help

VIM Essential Commands for Cybersecurity

---

File Operations:

- :w - Save file
- :q - Quit
- :wq - Save and quit
- :q! - Quit without saving
- :e filename - Open file

---

Editing Commands (Normal Mode):

- i - Insert before cursor
- a - Insert after cursor
- o - Open new line below
- O - Open new line above
- x - Delete character
- dd - Delete line
- yy - Copy line
- p - Paste
- u - Undo
- Ctrl+r - Redo

---

Search and Replace:

- /pattern - Search forward
- ?pattern - Search backward
- n - Next search result
- N - Previous search result
- :s/old/new/g - Replace all on current line
- :%s/old/new/g - Replace all in file

---

E35: No previous regular expression

29,0-1 All

Here, I am just getting very comfortable with VIM commands. I also just completed using some VIM navigation tools.

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]

File Actions Edit View Help

Basic Navigation (Normal Mode):  
h,j,k,l : Left, Down, Up, Right  
w : Next word  
b : Previous word  
0 : Beginning of line  
\$ : End of line  
gg : Go to first line  
G : Go to last line

File System

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]  
\$ vim exploit\_template.py

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]  
\$ vim vim\_commands.txt

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]  
\$ cat > security\_log.txt << EOF

```
heredoc> 2024-08-05 10:15:23 INFO: User admin logged in from 192.168.1.100
heredoc> 2024-08-05 10:16:45 WARNING: Failed login attempt for user root from 203.0.113.50
heredoc> 2024-08-05 10:17:12 ERROR: Multiple failed login attempts detected
heredoc> 2024-08-05 10:18:33 INFO: User admin logged out
heredoc> 2024-08-05 10:19:44 WARNING: Failed login attempt for user test from 203.0.113.50
heredoc> 2024-08-05 10:20:15 CRITICAL: Potential brute force attack from 203.0.113.50
heredoc> 2024-08-05 10:21:30 INFO: IP address 203.0.113.50 blocked by firewall
heredoc> 2024-08-05 10:22:10 INFO: Security scan completed
heredoc> 2024-08-05 10:23:25 WARNING: Suspicious file detected: /tmp/backdoor.sh
heredoc> 2024-08-05 10:24:40 ERROR: Malware signature match in file scan
heredoc> EOF
```

(kali㉿kali)-[~/cybersec-labs/text-editors-lab]  
\$

This shows that I created a VIM for log analysis. I'm proceeding with using a few other VIM navigation tools. Then I will proceed with a few more advanced features.

A screenshot of a terminal window titled "kali@kali: ~/cybersec-labs/text-editors-lab". The window shows a Vim editor with the following content:

```
File Actions Edit View Help
Network Configuration Analysis
-----
Interface: eth0
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
DNS Server: 8.8.8.8
[InterSystem]
Interface: eth1
IP Address: 10.0.0.100
Subnet Mask: 255.255.255.0
Gateway: 10.0.0.1
DNS Server: 8.8.4.4

Security Settings:
Firewall: Enabled
SSH: Port 22
HTTP: Port 80
HTTPS: Port 443
Interface: eth0
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
DNS Server: 8.8.8.8
~
~
~
~
5 more lines
```

The status bar at the bottom right indicates "21,1" and "All".

This is an example of text manipulation using the VIM commands. I was able to yank five lines, copy and paste them at the bottom.

The screenshot shows a terminal window titled "kali@kali: ~/cybersec-labs/text-editors-lab". The window displays a security audit report. It includes sections for User ID, Network Configuration (IP address 172.17.0.1), Open Ports, Running Processes (listing tasks like splash, kthreadd, pool\_workqueue\_release, kworker/R-kvfree\_rcu\_reclai, kworker/R-rcu\_gp, kworker/R-sync\_wq, kworker/R-slub\_flushwq, kworker/R-netns, and kblockd), File Permissions Audit (noting world-writable files in /tmp), and Recent Log Entries (mentioning recent authentication attempts and no auth log accessible). The audit completed at 10:51:19 AM EDT on Wednesday, September 24, 2025.

```
User ID: uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),107(bluetooth),115(scanner),127(lpadmin),135(wireshark),137(kaboxer),138(vboxsf),987(docker)

==== Network Configuration ====
IP addresses:
172.17.0.1

==== Open Ports ====

==== Running Processes ====
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.7 23088 14380 ?
root           2  0.0  0.0     0     0 ?
root           3  0.0  0.0     0     0 ?
root           4  0.0  0.0     0     0 ?
root           5  0.0  0.0     0     0 ?
root           6  0.0  0.0     0     0 ?
root           7  0.0  0.0     0     0 ?
root           8  0.0  0.0     0     0 ?
root          11  0.0  0.0     0     0 ?

==== File Permissions Audit ====
World-writable files in /tmp:

==== Recent Log Entries ====
Recent authentication attempts:
No auth log accessible

Audit completed at Wed Sep 24 10:51:19 AM EDT 2025
```

I created a security audit script in VIM. Then I made it executable. I then tested it, and everything seems to go accordingly.

Following this process, I didn't take screenshots of the following exercises. But everything went smoothly without any troubles. A list of things I completed without documenting includes creating incident response notes, creating an IOC tracking file with VIM, updating IOC's with VIM, creating a SSH hardening configuration, and creating firewall rule configurations.

Knowledge Assessment:

**Question 1:** True or False: In VIM, you must be in Insert mode to save a file using ":w".  
**False**

**Question 2:** Which nano shortcut saves the current file?  
**Ctrl+O**

**Question 3:** True or False: VIM has three main modes: Normal, Insert, and Command mode.  
**False**

**Question 4:** In VIM, which command would replace all occurrences of "password" with "credential" in the entire file?

**b) :%s/password/credential/g**

**Question 5:** Which editor would be better for a quick configuration file edit on a remote server with limited terminal capabilities?

**b) Nano, because it's more user-friendly and shows shortcuts on screen**

#### **Conclusion:**

With the completion of this lab, I have gained a good understanding of using nano and VIM. As well as learning tools such as text editing and creating, and modifying scripts. This lab had a concentration on some real job executions, such as Configuration Management: Editing security tool configurations, firewall rules, and system settings. Incident Response: Quickly documenting incidents, tracking IOCs, and creating response playbooks. Log Analysis: Searching through large log files, extracting relevant information, and correlating events.