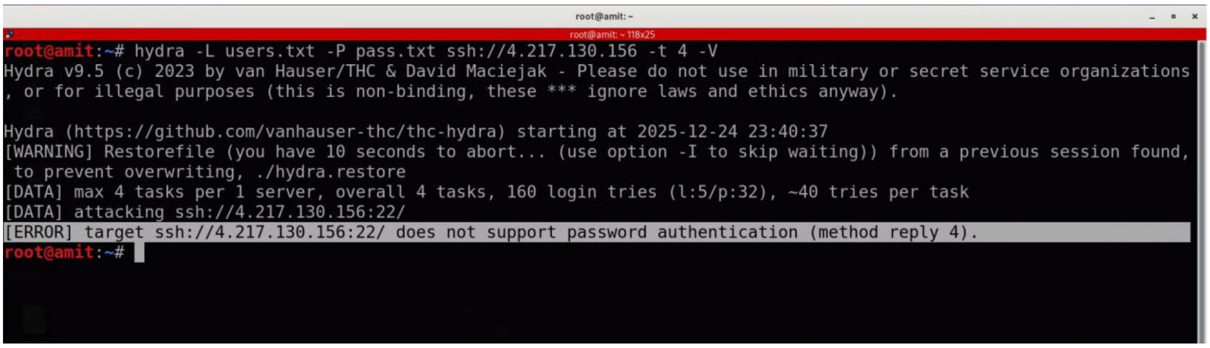
Project Title: Azure Cloud Security Lab - Hardening & Remediation
Role: Security Engineer
Date: December 25, 2025
Team Member Names Involved in System Hardening:

- **Shivam Kishor**
- **Parmeshwar Sao**

1. Objective To remediate identified vulnerabilities and reduce the attack surface of the cloud infrastructure based on the findings from the Red Team assessment.

2. Applied Hardening Measures

- **A. SSH Configuration (Access Control)**
  - **Vulnerability:** Password authentication allowed brute-force success.
  - **Fix:** Updated /etc/ssh/sshd_config to set PasswordAuthentication no and PermitRootLogin no.
  - **Verification:** Hydra attack now fails immediately with "Permission Denied."
  - **Evidence:**

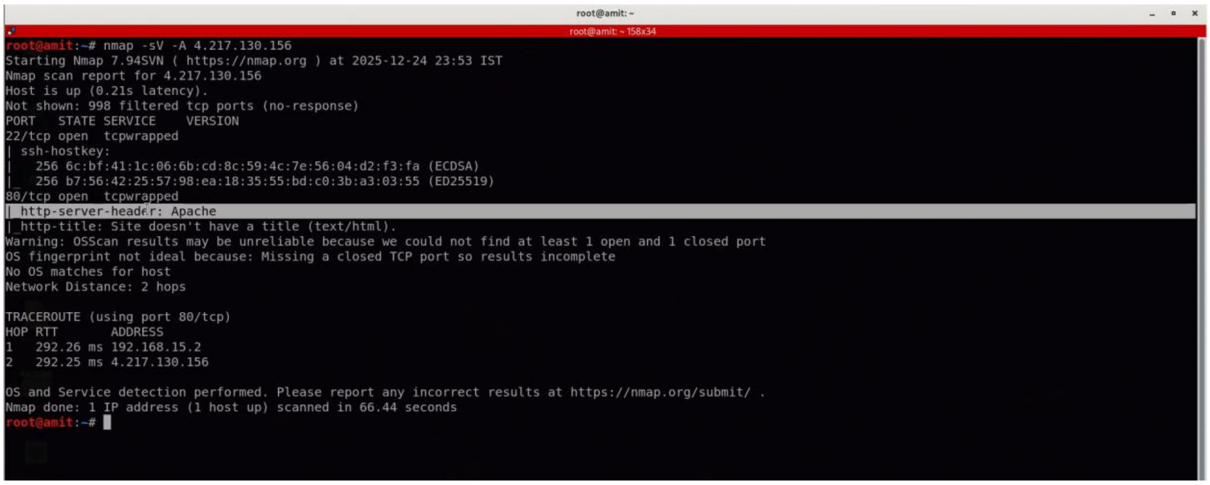


```
root@amit:~# hydra -L users.txt -P pass.txt ssh://4.217.130.156 -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-24 23:40:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 160 login tries (l:5/p:32), ~40 tries per task
[DATA] attacking ssh://4.217.130.156:22/
[ERROR] target ssh://4.217.130.156:22/ does not support password authentication (method reply 4).
root@amit:~# 
```

- **B. Apache Web Server (Information Hiding)**
  - **Vulnerability:** Server version banner leaking OS details.
  - **Fix:** Configured ServerTokens Prod and ServerSignature Off in Apache configuration.
  - **Verification:** Nmap scan now shows only "Apache" without version numbers.

  - **Evidence:**



```
root@amit:~# nmap -sV -A 4.217.130.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-24 23:53 IST
Nmap scan report for 4.217.130.156
Host is up (0.21s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
22/tcp open  tcpwrapped
| ssh-hostkey:
|   256 6c:bf:41:1c:06:6b:cd:8c:59:4c:7e:56:04:d2:f3:fa (ECDSA)
|_  256 b7:56:42:25:57:98:ea:18:35:55:bd:c0:3b:a3:03:55 (ED25519)
80/tcp open  tcpwrapped
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   292.26 ms 192.168.15.2
2   292.25 ms 4.217.130.156

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.44 seconds
root@amit:~#
```

- **C. Network Security (Segmentation)**
  - **Policy:** Enforced strict NSG (Network Security Group) rules.
  - **Implementation:** VM1 (Internal) rejects all traffic except from specific internal management IPs.

3. Final Security Posture The system is now resilient against dictionary attacks and automated reconnaissance. The attack surface has been significantly reduced.