Project Title: Azure Cloud Security Lab - Attack Phase

Role: Red Team (Attacker)
Date: December 25, 2025

Team Member Names Involved in Red Teaming

- **Tirath Chandravanshi**
- **Amit Kumar**

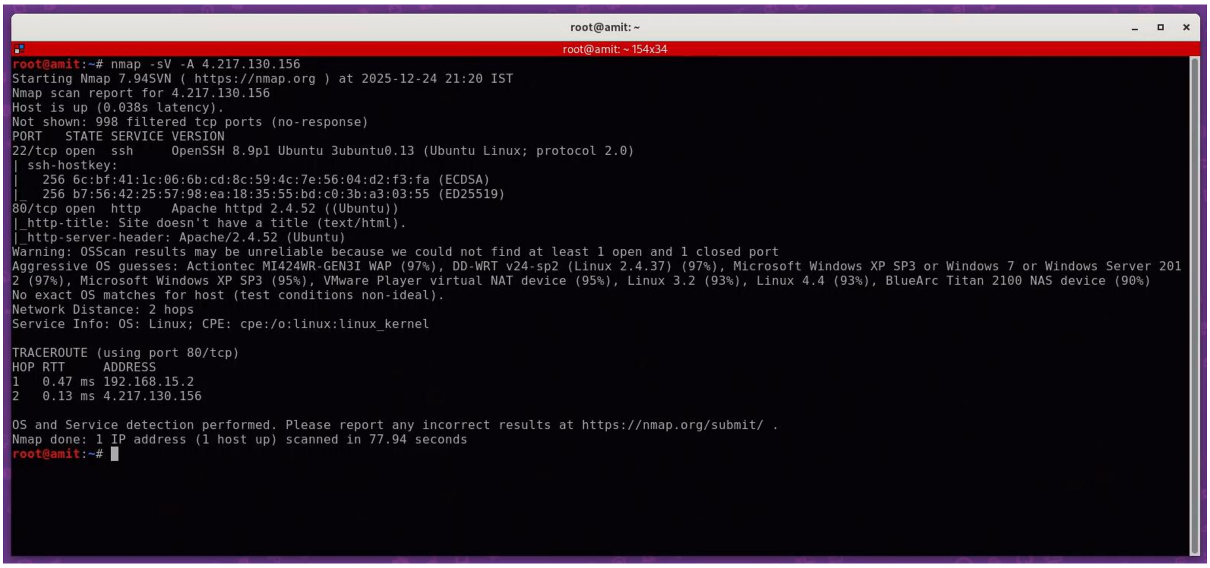
1. Objective To assess the security posture of the "Orbitalyn Solutions" cloud infrastructure by simulating real-world cyberattacks against external and internal assets.

2. Attack Methodology

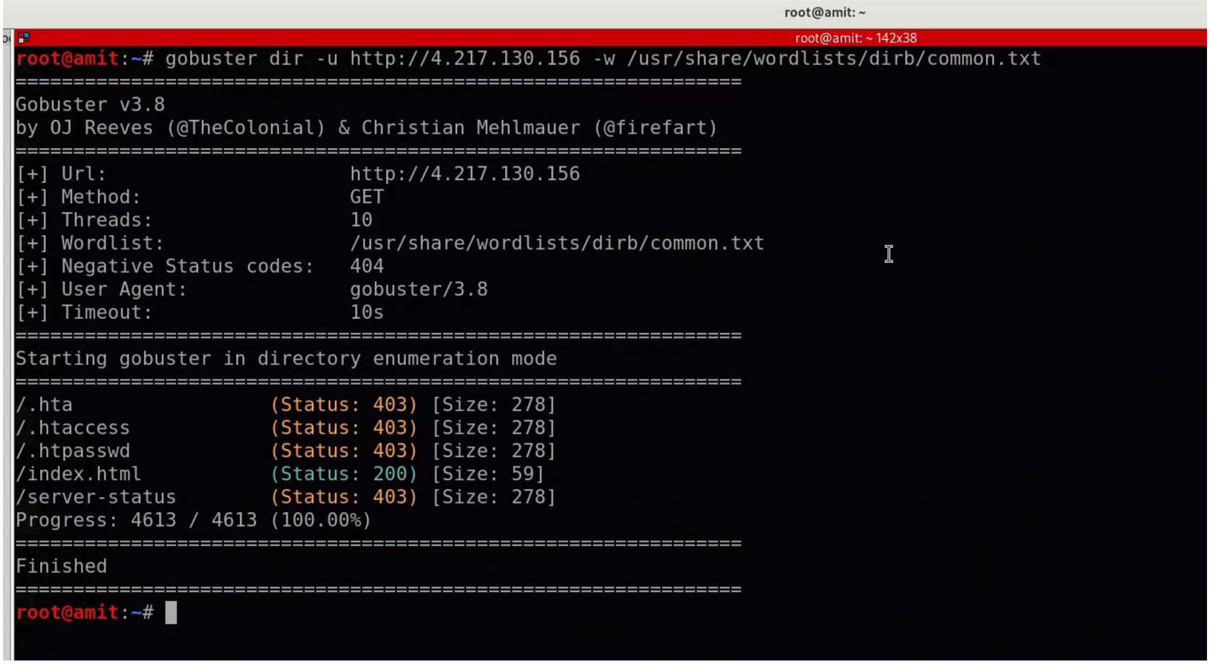
- **Target:** VM2 (Web Server - DMZ) and VM1 (Internal File Server).
- **Attacker Machine:** Kali Linux.
- **Tools Used:** Nmap (Reconnaissance), Hydra (Brute Force), Nikto (Vulnerability Scanning), Gobuster (Enumeration).

3. Attack Scenarios & Evidence

- **Scenario A: External Reconnaissance**
  - **Action:** Performed Nmap scan on VM2 Public IP.
  - **Finding:** Port 22 (SSH) and Port 80 (HTTP) were found open. Apache version 2.4.52 was visible.
  - **Evidence:**

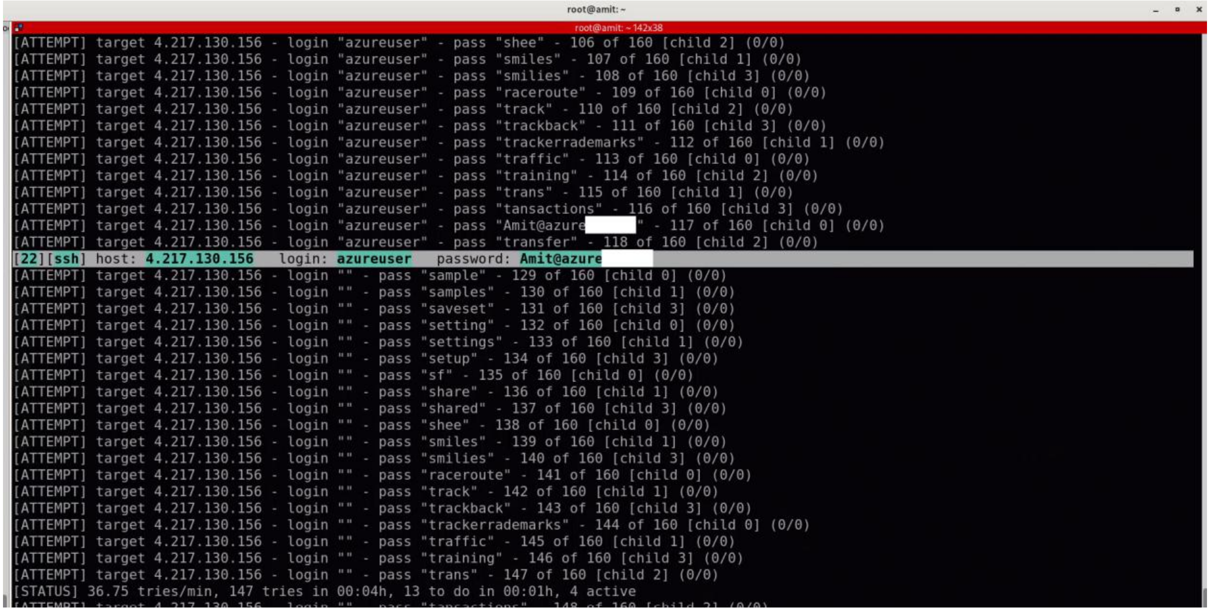


```
root@amit:~# nmap -sV -A 4.217.130.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-24 21:20 IST
Nmap scan report for 4.217.130.156
Host is up (0.038s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| 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  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.52 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (97%), DD-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 201
2 (97%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT device (95%), Linux 3.2 (93%), Linux 4.4 (93%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.47 ms 192.168.15.2
2   0.13 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 77.94 seconds
root@amit:~# 
```



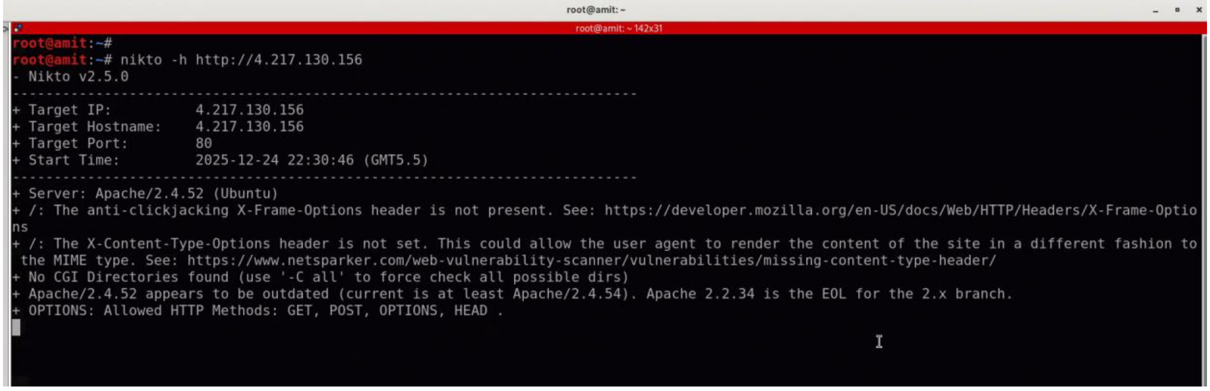
```
root@amit:~# gobuster dir -u http://4.217.130.156 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://4.217.130.156
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 59]
/server-status        (Status: 403) [Size: 278]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
root@amit:~# 
```

- **Scenario B: SSH Brute Force**
  - **Action:** Used Hydra to attempt a dictionary attack against the azureuser account on VM2.
  - **Finding:** Successfully cracked the password. Password Authentication was enabled.
  - **Evidence:**



```
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "shee" - 106 of 160 [child 2] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "smiles" - 107 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "smilies" - 108 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "raceroute" - 109 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "track" - 110 of 160 [child 2] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "trackback" - 111 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "trackerrademarks" - 112 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "traffic" - 113 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "training" - 114 of 160 [child 2] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "trans" - 115 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "tansactions" - 116 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "Amit@azure[redacted]" - 117 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "azureuser" - pass "transfer" - 118 of 160 [child 2] (0/0)
[22][ssh] host: 4.217.130.156   login: azureuser   password: Amit@azure[redacted]
[ATTEMPT] target 4.217.130.156 - login "" - pass "sample" - 129 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "samples" - 130 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "saveset" - 131 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "setting" - 132 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "settings" - 133 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "setup" - 134 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "sf" - 135 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "share" - 136 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "shared" - 137 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "shee" - 138 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "smiles" - 139 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "smilies" - 140 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "raceroute" - 141 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "track" - 142 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "trackback" - 143 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "trackerrademarks" - 144 of 160 [child 0] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "traffic" - 145 of 160 [child 1] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "training" - 146 of 160 [child 3] (0/0)
[ATTEMPT] target 4.217.130.156 - login "" - pass "trans" - 147 of 160 [child 2] (0/0)
[STATUS] 36.75 tries/min, 147 tries in 00:04h, 13 to do in 00:01h, 4 active
[ATTEMPT] target 4.217.130.156 - login "" - pass "tansactions" - 148 of 160 [child 2] (0/0)
```

- **Scenario C: Web Vulnerability Scanning**
  - **Action:** Deployed Nikto to scan for web server misconfigurations.
  - **Finding:** Detected outdated software and missing security headers (X-Frame-Options).
  - **Evidence:**



```
root@amit:~#
root@amit:~# nikto -h http://4.217.130.156
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          4.217.130.156
+ Target Hostname:    4.217.130.156
+ Target Port:        80
+ Start Time:         2025-12-24 22:30:46 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Optio
ns
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
 the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
```

- **Scenario D: Lateral Movement (Pivoting)**
  - **Action:** Used the compromised VM2 as a "Jump Box" to scan the private internal network.
  - **Finding:** Discovered VM1 (Internal Server) on the private subnet and successfully brute-forced it.