RED TEAM ATTACK SIMULATION REPORT

(Heading 1)

- **Project Title : A Red team-Blue team Security Simulation on Microsoft (Major project)**
- **Your Name : Avinash Das ManikPuri**
- **ERP: 6604666**

1. Red Team Objective

The objective of the Red Team phase is to simulate realistic cyber-attacks against the cloud infrastructure in order to identify vulnerabilities, misconfigurations, and weak security controls while generating security logs for analysis.

---

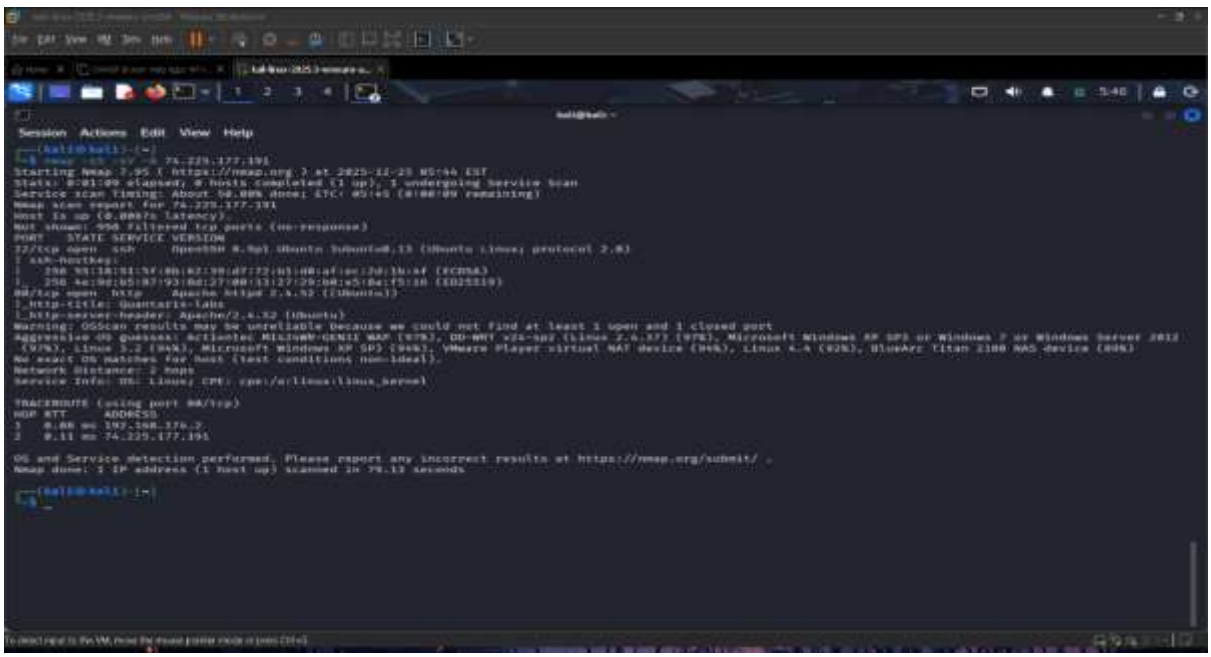
2. Attack Methodology

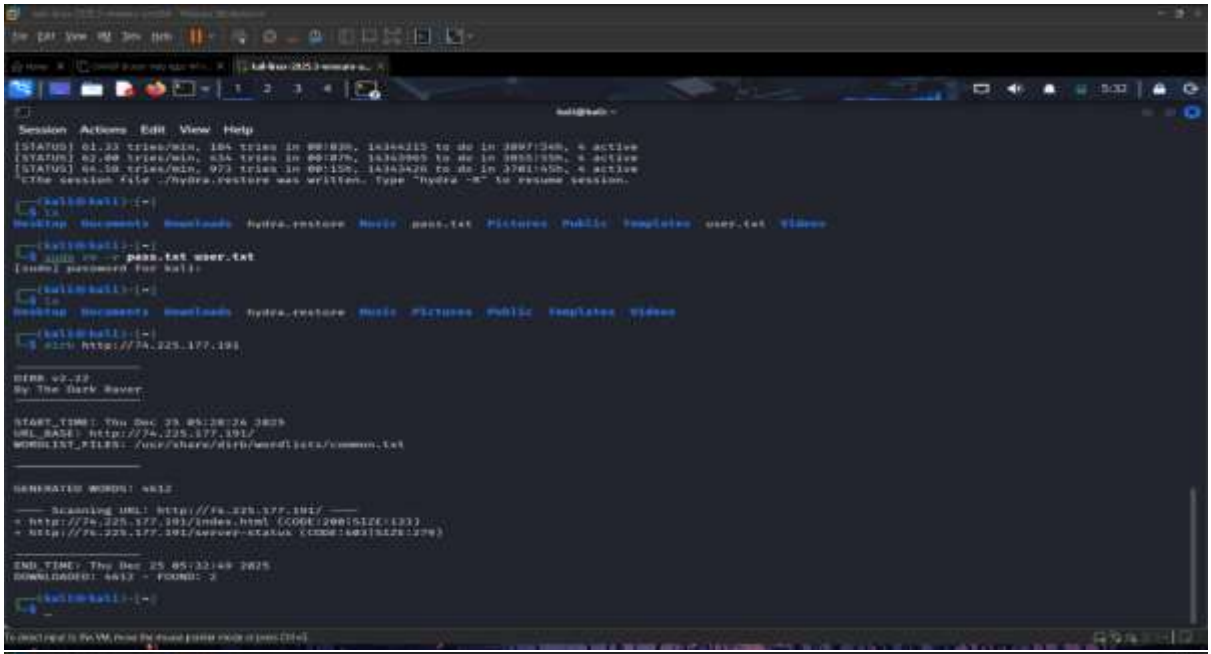
The attack methodology followed a structured penetration testing lifecycle:

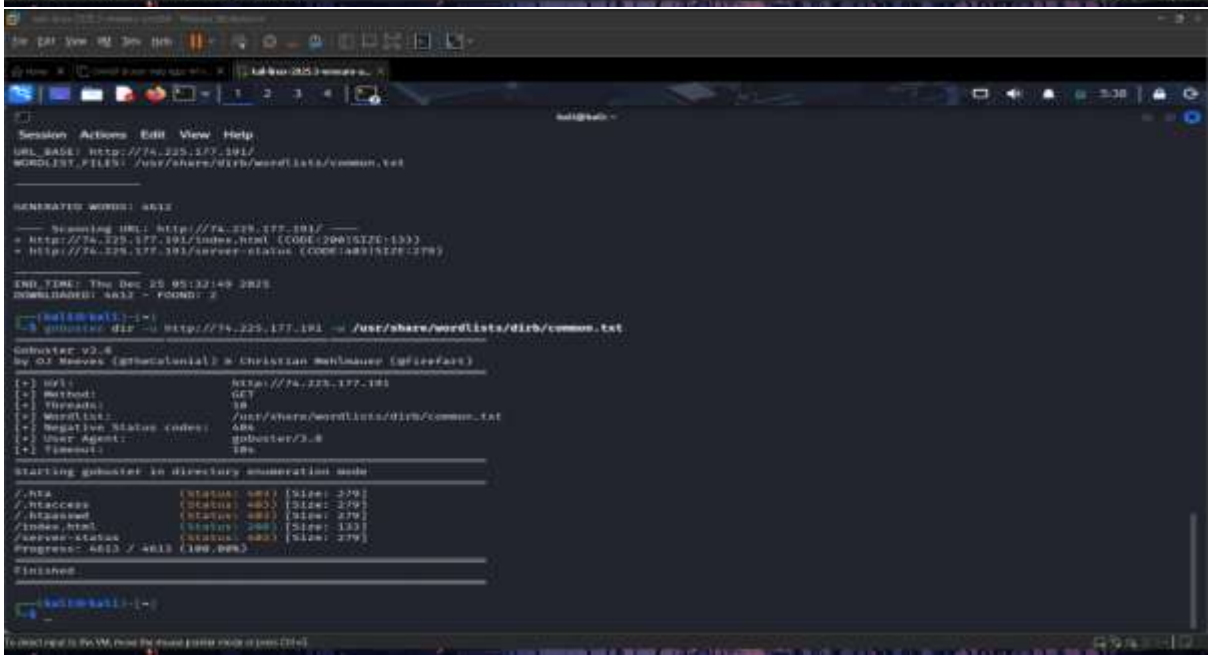
1. Reconnaissance and enumeration
2. Authentication attacks
3. Privilege escalation attempts
4. Web application exploitation
5. Identity and service enumeration

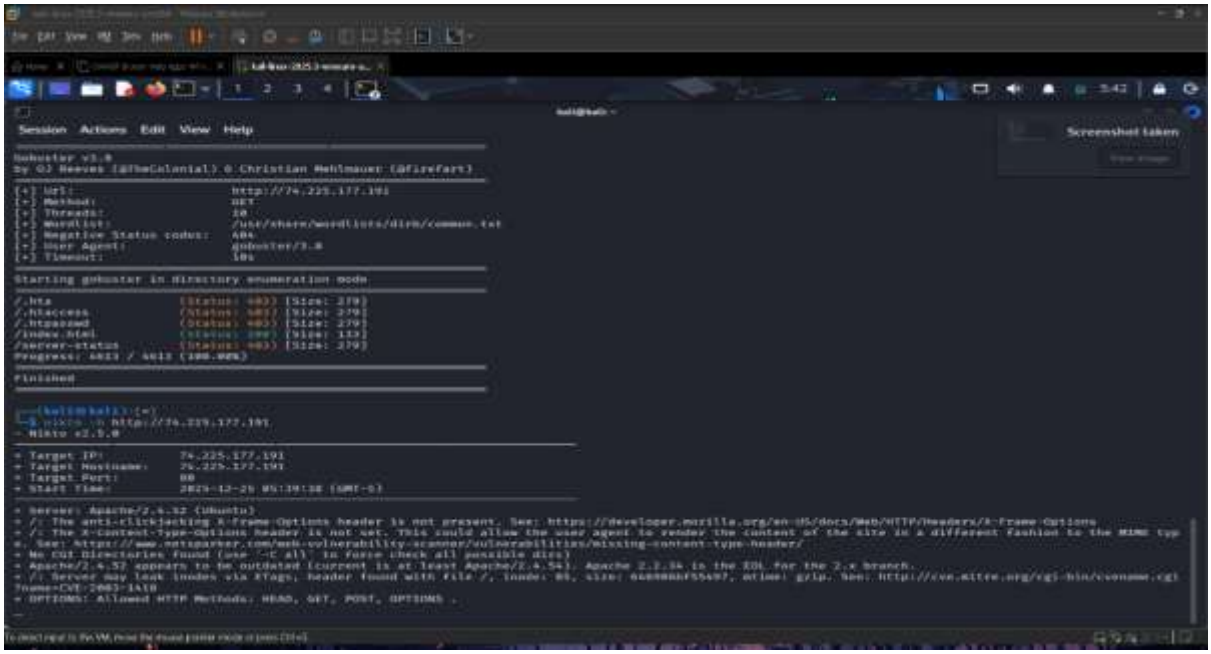
---

3. Reconnaissance and Enumeration




Session Actions Edit View Help
[STATUS] 61.33 tries/min, 184 tries in 00:03h, 14344415 to do in 3897:34h, 4 active
[STATUS] 62.00 tries/min, 434 tries in 00:07h, 14343965 to do in 3855:55h, 4 active
[STATUS] 64.50 tries/min, 973 tries in 00:15h, 14343426 to do in 3781:45h, 4 active
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
Desktop Documents Downloads hydra.restore Music pass.txt Pictures Public Templates user.txt Videos
sudo rm -r pass.txt user.txt
[sudo] password for kali:
Desktop Documents Downloads hydra.restore Music Pictures Public Templates Videos
dirb http://74.225.177.191
DIRB v2.22
By The Dark Raver
START_TIME: Thu Dec 25 05:28:24 2025
URL_BASE: http://74.225.177.191/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://74.225.177.191/ ----
+ http://74.225.177.191/index.html (CODE:200|SIZE:133)
+ http://74.225.177.191/server-status (CODE:403|SIZE:279)
END_TIME: Thu Dec 25 05:32:49 2025
DOWNLOADED: 4612 - FOUND: 2

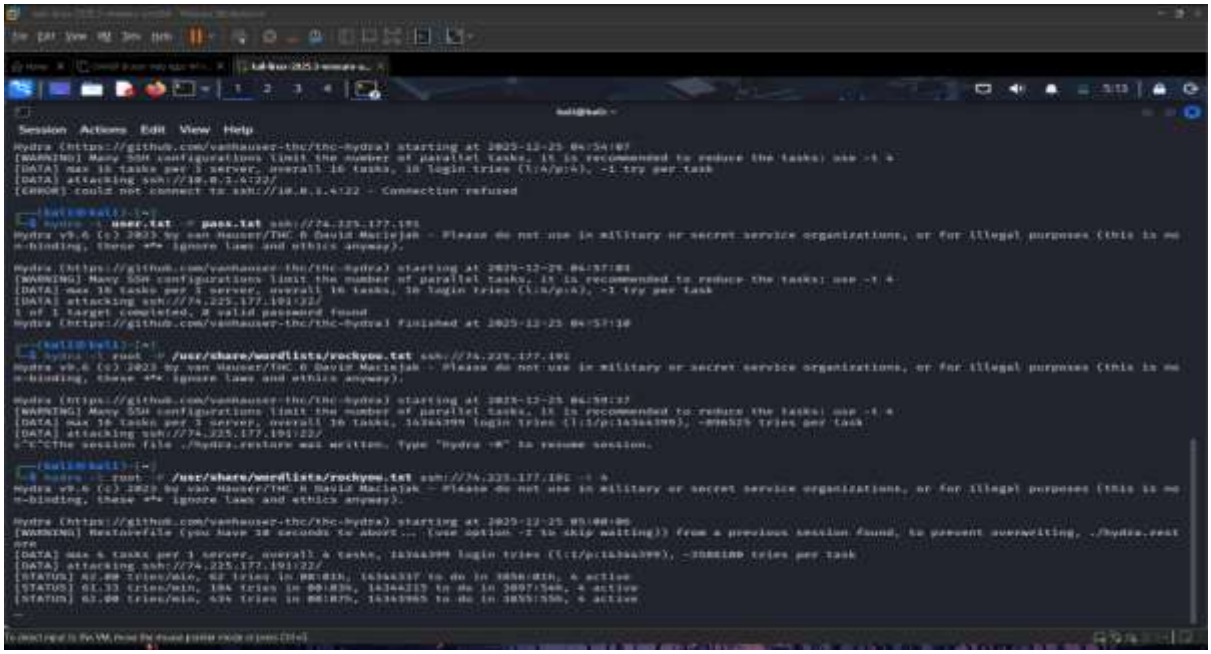

Session Actions Edit View Help
URL_BASE: http://74.225.177.191/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://74.225.177.191/ ----
+ http://74.225.177.191/index.html (CODE:200|SIZE:133)
+ http://74.225.177.191/server-status (CODE:403|SIZE:279)
END_TIME: Thu Dec 25 05:32:49 2025
DOWNLOADED: 4612 - FOUND: 2
gobuster dir -u http://74.225.177.191 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://74.225.177.191
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.hta (Status: 403) [Size: 279]
/.htaccess (Status: 403) [Size: 279]
/.htpasswd (Status: 403) [Size: 279]
/index.html (Status: 200) [Size: 133]
/server-status (Status: 403) [Size: 279]
Progress: 4613 / 4613 (100.00%)
Finished



Network scanning and service enumeration were performed to identify open ports, exposed services, and operating system details.

---

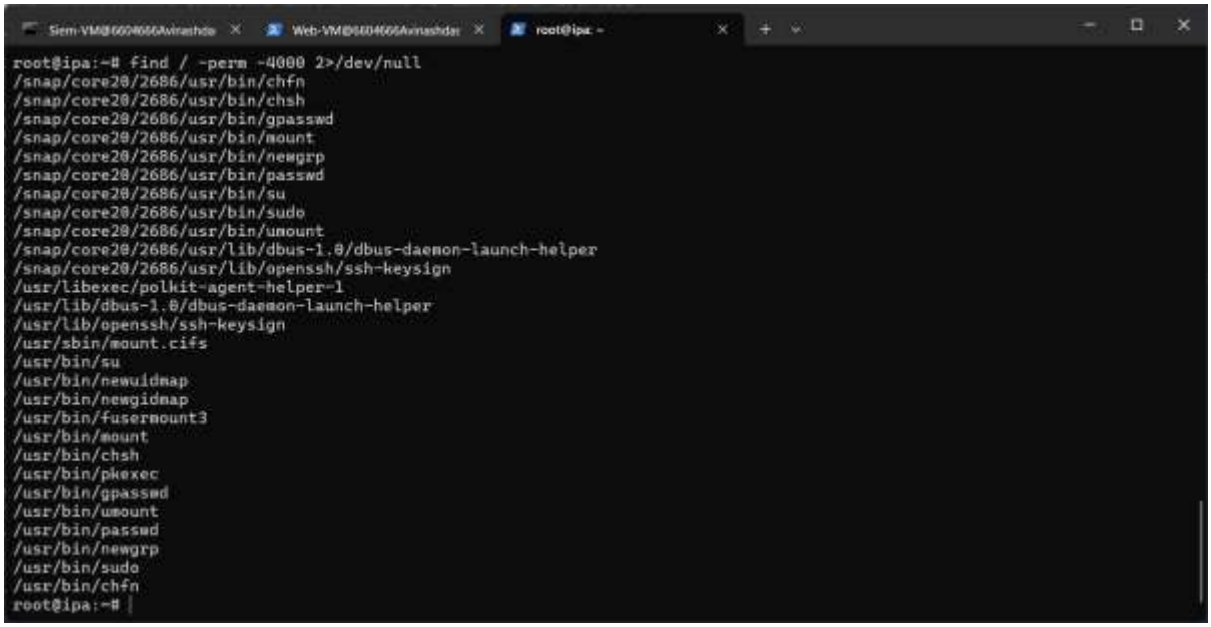
4. SSH Brute-Force Attacks



Password-based SSH brute-force attacks were conducted to simulate credential-stuffing and weak authentication exploitation.

---

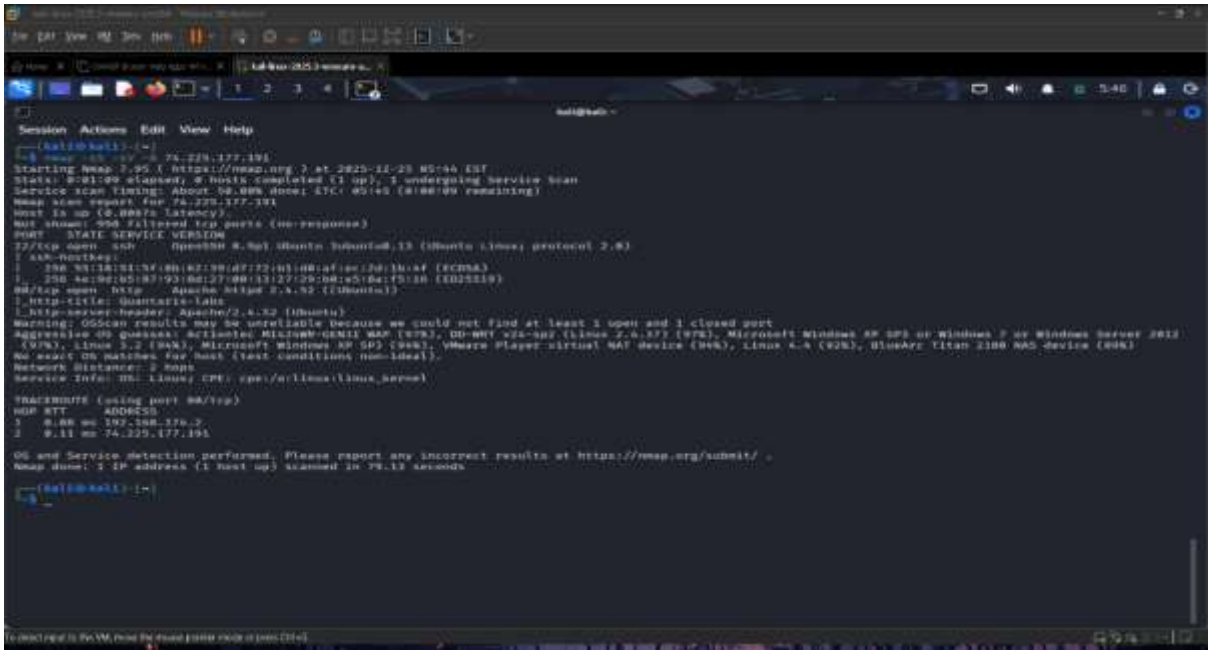
6. Privilege Escalation Attempts



Post-authentication enumeration was performed to identify misconfigured sudo permissions and SUID binaries.

---

7. **Web Application Attacks**



The following attacks were executed against the web server:

- Directory traversal attempts
- SQL injection testing

- File and directory enumeration
- Web vulnerability scanning

---

8. Outcome of Red Team Phase

The Red Team successfully identified multiple attack vectors and generated extensive security events across the infrastructure.

Screenshot Evidence Table – Red Team Attacks

Screenshot No.	Attack Type	Target VM	Evidence
1	Nmap Scan	VM-Internal	Open ports
2	SSH Brute Force	VM-Internal	auth.log
3	Web Enumeration	VM-Web	access.log
