

# 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.

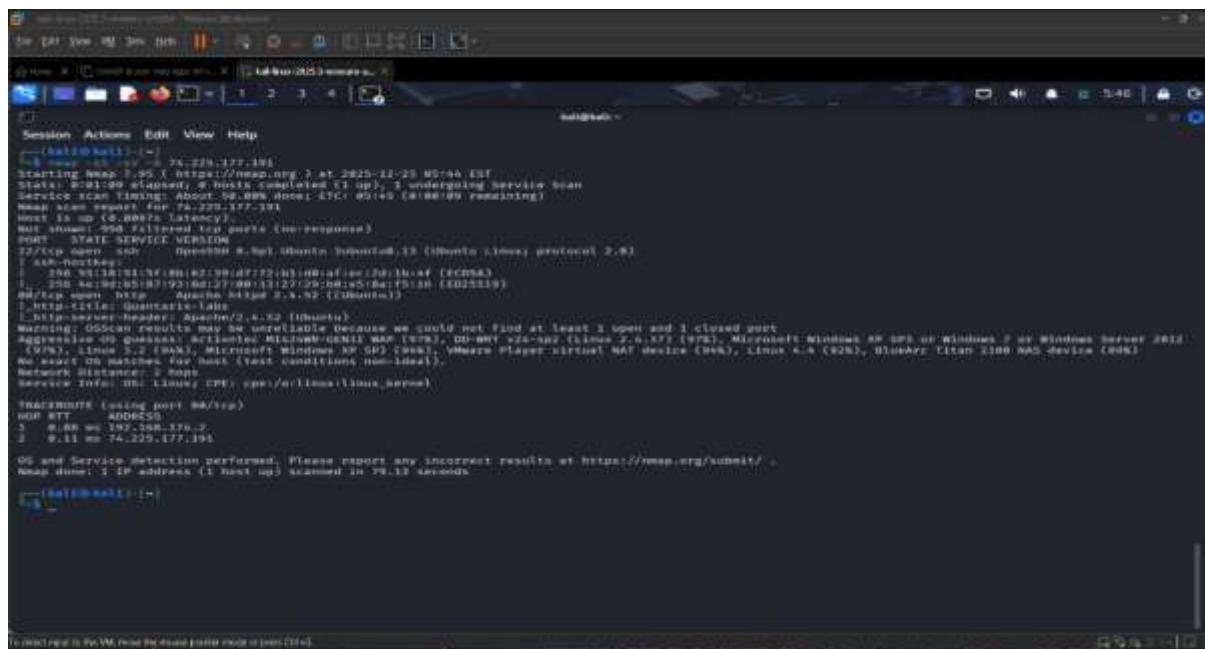
---

## 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



The screenshot shows a terminal window with the following output:

```
Starting Nmap 7.90 ( https://nmap.org ) at 2023-11-23 05:45 EST
Nmap scan report for 74.229.177.191
Host is up (0.000s latency).
Nmap scan timing: About 0.000s done; ETC: 05:45 (0:00:00 remaining)
Nmap scan request for 74.229.177.191
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 8.0p1 Ubuntu Subversion-13 (Ubuntu Linux; protocol 2.0)
|_RSA-HMAC
|_ SSH-2.0-OpenSSH_8.0p1_Ubuntu_Subversion-13_Ubuntu
|_ 22/ssh             open  ssh  OpenSSH_8.0p1_Ubuntu_Subversion-13_Ubuntu
|_ 80/tcp             open  http  Apache/2.4.42-(Ubuntu)
|_ HTTP-Title: Quantitative-Labs
|_ HTTP-Server-Header: Apache/2.4.42 (Ubuntu)
Warning: OSScan results are not 100% accurate because we could not find at least 1 open and 1 closed port
Reason: OS fingerprinting failed. This may be caused by missing or disabled OS modules in Nmap's database.
Nmap scan timing: 0.00s done; ETC: 05:45 (0:00:00 remaining)
Network Distance: 2 hops
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

```

The terminal also displays a message about connecting to the VM and a status bar indicating 79% completion.



The screenshot shows the NetworkMiner interface with a single captured session. The session details are as follows:

- Session ID: 02 Reeves (TheColonial) 0-Christian Heilmann (GFireFart)
- URL: http://74.225.177.191
- Method: GET
- Threads: 20
- Workers: /usr/share/wfuzz/fuzz/common.txt
- Request Status codes: All
- HTTP Agent: mitmproxy/3.8
- Timeout: 10s

The analysis section shows the following results:

- Starting gobuster in DIRECTORY ENUMERATION mode.
- Targets: 1 (Status: 403) (Size: 279)
- Success: 0 (Status: 403) (Size: 279)
- Blocked: 0 (Status: 403) (Size: 279)
- Slow Read: 0 (Status: 403) (Size: 279)
- Unknown Status: 0 (Status: 403) (Size: 279)
- Progress: 0/0 (0%)

Printed:

```
([Autodetect])  
-> mitmproxy -> http://74.225.177.191  
-> mitmproxy v2.0.0  
  
+ Target IP: 74.225.177.191  
+ Target Hostname: 74.225.177.191  
+ Target Port: 80  
+ Start Time: 2023-12-25 05:19:18 (GMT-8)  
  
+ Server: Apache/2.4.32 (Ubuntu)  
+/- The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+/- The Content-Security-Policy header is not set. This could allow the user agent to render the content of the site in a different fashion to the WMM type.  
+/- The Content-Security-Policy-Report-Only header is not set. This could allow the user agent to report violations without blocking.  
+/- No Content-Security-Policy header found (was <all>). In fact, check all possible sites.  
+/- Apache/2.4.32 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is in the EOL for the 2.x branch.  
+/- Server may leak inodes via X-File-Header found with file ./, inode: 86, size: 6400000055407, offset: 0x10. See: http://www.citrix.org/cgi-bin/cvechecker.cgi  
Name-CVE-2003-1410  
OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
```

To connect to this VM, press the mouse pointer inside or outside the title bar.

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

#### 4. SSH Brute-Force Attacks

The screenshot shows the Hydra tool running multiple attacks simultaneously. The tasks are as follows:

- Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-25 04:54:07 [WARNING] Many SSH configurations limit the number of parallel tasks. It is recommended to reduce the tasks: use -t 4 [DATA] max 16 tasks per 5 servers, overall 16 tasks, in 1 login tries (lin/pas), -1 try per task [DATA] attacking ssh://18.8.0.4:4222/ [ERROR] could not connect to ssh://18.8.0.4:4222 -- Connection refused
- Hydra (https://github.com/vanhauser-thc/thc-hydra) -> pass.txt ssh://74.225.177.191 [WARNING] Many SSH configurations limit the number of parallel tasks. It is recommended to reduce the tasks: use -t 4 [DATA] max 16 tasks per 5 servers, overall 16 tasks, in 1 login tries (lin/pas), -1 try per task [DATA] attacking ssh://74.225.177.191:22/ [INFO] progress completed, a valid password found [HYDRA] https://github.com/vanhauser-thc/thc-hydra finished at 2023-12-25 04:57:14
- Hydra (https://github.com/vanhauser-thc/thc-hydra) -> pass.txt ssh://74.225.177.191 [WARNING] Many SSH configurations limit the number of parallel tasks. It is recommended to reduce the tasks: use -t 4 [DATA] max 16 tasks per 5 servers, overall 16 tasks, in 1 login tries (lin/pas), -1 try per task [DATA] attacking ssh://74.225.177.191:22/ [INFO] progress completed, a valid password found [HYDRA] https://github.com/vanhauser-thc/thc-hydra finished at 2023-12-25 04:57:14
- Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-25 04:58:07 [WARNING] Many SSH configurations limit the number of parallel tasks. It is recommended to reduce the tasks: use -t 4 [DATA] max 16 tasks per 5 servers, overall 16 tasks, in 1 login tries (lin/pas), -1 try per task [DATA] attacking ssh://74.225.177.191:22/ [INFO] progress completed, a valid password found [HYDRA] https://github.com/vanhauser-thc/thc-hydra finished at 2023-12-25 04:58:07
- Hydra (https://github.com/vanhauser-thc/thc-hydra) -> rockyou.txt ssh://74.225.177.191 -- [HYDRA] 2023-12-25 04:58:07 by van Hauser/THC 0.9.0! Maciejah -- Please do not use in military or secret service organizations, or for illegal purposes (this is no m-binding, these \*# ignore laws and ethics anyway).
- Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-25 04:58:09 [WARNING] Many SSH configurations limit the number of parallel tasks. It is recommended to reduce the tasks: use -t 4 [DATA] max 16 tasks per 5 servers, overall 16 tasks, in 1 login tries (lin/pas), -1 try per task [DATA] attacking ssh://74.225.177.191:22/ [INFO] progress completed, a valid password found [HYDRA] https://github.com/vanhauser-thc/thc-hydra finished at 2023-12-25 04:58:09
- Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-25 04:58:10 [WARNING] Restorable file (you have 30 seconds to abort ... use option -z to skip waiting) from a previous session found, to prevent overwriting, -z/hydra-rest now [DATA] max 8 tasks per 1 server, overall 8 tasks, 13344399 login tries (1111/11111111), -3000000 tries per task [DATA] attacking ssh://74.225.177.191:22/ [STATS] 0.13 login/min, 13K tries in 00:00:30, 13344399 to do in 3855:558, 8 active [STATS] 61.00 tries/min, 13K tries in 00:00:30, 13344399 to do in 3857:558, 8 active [STATS] 61.00 tries/min, 43K tries in 00:00:30, 13344399 to do in 3855:558, 8 active

To connect to this VM, press the mouse pointer inside or outside the title bar.

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

#### 6. Privilege Escalation Attempts

```
root@ipa:~# find / -perm -4000 2>/dev/null
/snap/core28/2686/usr/bin/chfn
/snap/core28/2686/usr/bin/chsh
/snap/core28/2686/usr/bin/gpasswd
/snap/core28/2686/usr/bin/mount
/snap/core28/2686/usr/bin/newgrp
/snap/core28/2686/usr/bin/passwd
/snap/core28/2686/usr/bin/su
/snap/core28/2686/usr/bin/sudo
/snap/core28/2686/usr/bin/umount
/snap/core28/2686/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core28/2686/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/mount.cifs
/usr/bin/su
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/fusermount3
/usr/bin/mount
/usr/bin/chsh
/usr/bin/pexec
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chfn
root@ipa:~# |
```

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

---

---