Experiment 1

For the first experiment we will not provide any information regarding the cyber range. You are allowed to use any information that you find on the GCP interface to answer the questions to the best of your ability. The first experiment is only related to one host. The time to gather information and answer the questions is **30 minutes. Since the time is limited, if you don't know the answer or you do not have the time to find it, please provide your best guess**.

All the following questions refer to the host named malval-instance55485 with IP 10.0.3.170 (since this is the only one available at this experiment, the rest of the cyber-range's hosts are hidden from you at this point)

The information you have available at this stage are:

- Nmap scan of the host
- Access on the GCP console

Time available: 30 minutes

Questions

1. Which one of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to service Tomcat
    b. Actively interact with and, if necessary, successfully authenticate to service SSH
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

2. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to service Tomcat
    b. Actively interact with and, if necessary, successfully authenticate to service FTP
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

3. Which of the following is easier
   a. Obtain a usable shell (of any privilege level)
   b. Perform an SQL injection exploit
   c. They are equally easy (0 on the scale)

   If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

   Scale 0-8:

4. Which of the following is easier
   a. Exploit any vulnerability
   b. Obtain from within the cyber range, by using any method, the credentials for the SSH service
   c. They are equally easy (0 on the scale)

   If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

   Scale 0-8:

5. Which of the following is easier
   a. Obtain from within the cyber range, by using any method, the credentials for the FTP service
   b. Obtain a usable shell (of root/administrator level)
   c. They are equally easy (0 on the scale)

   If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

   Scale 0-8:

Experiment 2

In this experiment you have an expanded view on the cyber-range so now you have to analyze 3 hosts of interest by providing us answers on the following questions.

The information you have available at this stage are:

- Access on the GCP console
- VPN access to the infrastructure
- Description of the network topology of the cyber-range
- Nmap scans of the hosts
- Vulnerability analysis reports from Nessus scanner (using a Basic Network Scan), also ran with SSH access to the hosts (where applicable)
- + Anything more you can find by yourself

Time available: 45 minutes

Questions

1. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to service SSH at host Malval-instance52480(10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

2. Which of the following is easier
    a. Get access and modify the DNS service at host Malval-instance36991 (10.0.2.218)
    b. Actively interact with and, if necessary, successfully authenticate to service Tomcat on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

3. Which of the following is easier
    a. Get access to the data stored in the SQL database on host Malval-instance52480 (10.0.3.141)
    b. Get access to the data stored on the operating system of host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

4. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to service Tomcat on host Malval-instance55485 (10.0.3.170)
    b. Actively interact with and, if necessary, successfully authenticate to service FTP on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

5. Which of the following is easier
    a. Obtain from within the cyber range, by using any method, the credentials for the FTP service on host Malval-instance55485 (10.0.3.170)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

6. Which of the following is easier
    a. Obtain a usable shell (of root/administrator level) on host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

7. Which of the following is easier
    a. Get access to the data stored on the operating system of host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

8. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    b. Get access and modify the DNS service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

9. Which of the following is easier
    a. Obtain from within the cyber range, by using any method, the credentials for the FTP service on host Malval-instance55485 (10.0.3.170)
    b. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

Experiment 3

In this experiment you have an expanded view on the cyber-range so now you have to analyze 3 hosts of interest by providing us answers on the following questions.

The information you have available at this stage are:

- Access to GCP console
- VPN access to the infrastructure
- SSH keys for the root user on the hosts (where applicable)
- Passwords/credential information and metadata
- Description of the network topology of the cyber-range
- Nmap scans of the hosts
- Vulnerability analysis reports from Nessus scanner (using a Basic Network Scan), also ran with SSH access to the hosts (where applicable)
- A supplementary list of the vulnerabilities and weaknesses found on each of the hosts
- + Anything more you can find by yourself

Time available: 45 minutes

Questions

1. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to service SSH at host Malval-instance52480(10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

2. Which of the following is easier
    a. Get access and modify the DNS service at host Malval-instance36991 (10.0.2.218)
    b. Actively interact with and, if necessary, successfully authenticate to service Tomcat on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

3. Which of the following is easier
    a. Get access to the data stored in the SQL database on host Malval-instance52480 (10.0.3.141)
    b. Get access to the data stored on the operating system of host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

4. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to service Tomcat on host Malval-instance55485 (10.0.3.170)
    b. Actively interact with and, if necessary, successfully authenticate to service FTP on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

5. Which of the following is easier
    a. Obtain from within the cyber range, by using any method, the credentials for the FTP service on host Malval-instance55485 (10.0.3.170)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

6. Which of the following is easier
    a. Obtain a usable shell (of root/administrator level) on host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)

c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

7. Which of the following is easier
    a. Get access to the data stored on the operating system of host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

8. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    b. Get access and modify the DNS service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

9. Which of the following is easier
    a. Obtain from within the cyber range, by using any method, the credentials for the FTP service on host Malval-instance55485 (10.0.3.170)
    b. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

Experiment 4

For the final experiment, we will provide you will all known information regarding the cyber range. You will also assess the entire cyber range and get 5 hours to answer the following questions.

The information you have available at this stage are:

- Access to GCP console
- VPN access to the infrastructure
- SSH keys for the root user on the hosts (where applicable)
- Passwords/credential information and metadata
- Description of the network topology of the cyber-range
- Nmap scans of the hosts
- Vulnerability analysis reports from Nessus scanner (using a Basic Network Scan), also ran with SSH access to the hosts (where applicable)
- A supplementary list of the vulnerabilities and weaknesses found on each of the hosts
- + Anything more you can find by yourself

Time available: maximum 5 hours

Questions

1. Which of the following is easier
   a. Actively interact with any service via a TCP connection on host Malval-instance7115 (10.0.6.98)
   b. Actively interact with any service via a TCP connection on host Malval-instance52480 (10.0.3.141)
   c. They are equally easy (0 on the scale)

   If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

   Scale 0-8:

2. Which of the following is easier
   a. Actively interact with any service via a TCP connection on host Malval-instance30950 (10.0.7.104)
   b. Actively interact with any service via a TCP connection on host Malval-instance52480 (10.0.3.141)
   c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

3. Which of the following is easier
    a. Actively interact with any service via a TCP connection on host Malval-instance78296 (10.0.7.109)
    b. Obtain from within the cyber range, by using any method, the credentials for the SSH service at host Malval-instance7115 (10.0.6.98)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

4. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

5. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance36991 (10.0.2.218)
    b. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

6. Which of the following is easier
    a. Perform a CSRF attack on host Malval-instance52480 (10.0.3.141)
    b. Perform an SQL injection exploit on host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

7. Which of the following is easier
   a. Exploit a vulnerability on host Malval-instance52480 (10.0.3.141)
   b. Exploit a vulnerability on host Malval-instance53261 (10.0.3.60)
   c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

8. Which of the following is easier
   a. Get access and modify the DNS service at host Malval-instance36991 (10.0.2.218)
   b. Actively interact with and, if necessary, successfully authenticate to service Tomcat on host Malval-instance55485 (10.0.3.170)
   c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

9. Which of the following is easier
   a. Actively interact with and, if necessary, successfully authenticate to SSH service at host Malval-instance78296 (10.0.7.109)
   b. Actively interact with and, if necessary, successfully authenticate to SSH service at host Malval-instance23374 (10.0.7.71)
   c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

10. Which of the following is easier
   a. Obtain from within the cyber range, by using any method, the credentials for the SSH service at host Malval-instance23374 (10.0.7.71)
   b. Obtain from within the cyber range, by using any method, the credentials for the SSH service at host Malval-instance36991 (10.0.2.218)
   c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

11. Which of the following is easier
    a. Obtain a usable shell (of any privilege level) on host Malval-instance23374 (10.0.7.71)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

12. Which of the following is easier
    a. Obtain a usable shell (of any privilege level) on host Malval-instance23374 (10.0.7.71)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance71028 (10.0.6.130)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

13. Which of the following is easier
    a. Obtain a usable shell (of any privilege level) on host Malval-instance78296 (10.0.7.109)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance7115 (10.0.6.98)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

14. Which of the following is easier
    a. Obtain a usable shell (of any privilege level) on host Malval-instance7115 (10.0.6.98)
    b. Exploit the binary file that is located on host Malval-instance23374 (10.0.7.71)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

15. Which of the following is easier
    a. Get access to the data stored in the SQL database on host Malval-instance52480 (10.0.3.141)
    b. Get access to the data stored on the operating system of host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

16. Which of the following is easier
    a. Actively interact with and, if necessary, successfully authenticate to service Tomcat on host Malval-instance55485 (10.0.3.170)
    b. Actively interact with and, if necessary, successfully authenticate to service FTP on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

17. Which of the following is easier
    a. Obtain from within the cyber range, by using any method, the credentials for the FTP service on host Malval-instance55485 (10.0.3.170)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance55485 (10.0.3.170)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

18. Which of the following is easier
    a. Obtain from within the cyber range, by using any method, the credentials for the Tomcat service on host Malval-instance55485 (10.0.3.170)
    b. Connect to the Wi-Fi network hosted on host Malval-instance7115 (10.0.6.98)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

19. Which of the following is easier
    a. Obtain a usable shell (of root/administrator level) on host Malval-instance55485 (10.0.3.170)
    b. List the source code of a cloud function stored on GCP from Malval-instance78296 (10.0.7.109)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

20. Which of the following is easier
    a. Sniffing traffic originating from host Malval-instance23374 (10.0.7.71)
    b. Exploit the binary file that is located on host Malval-instance23374 (10.0.7.71)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

21. Which of the following is easier
    a. Obtain a usable shell (of root/administrator level) on host Malval-instance52480 (10.0.3.141)
    b. Actively interact with and, if necessary, successfully authenticate to the webserver at host Malval-instance52480 (10.0.3.141)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

22. Which of the following is easier
    a. List the source code of a cloud function stored on GCP from Malval-instance78296 (10.0.7.109)
    b. Actively interact with and, if necessary, successfully authenticate to Telnet service at host Malval-instance36991 (10.0.2.218)
    c. They are equally easy (0 on the scale)

If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

Scale 0-8:

23. Which of the following is easier
    a. List the source code of a cloud function stored on GCP from Malval-instance78296 (10.0.7.109)
    b. Obtain a usable shell (of any privilege level) on host Malval-instance7115 (10.0.6.98)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8:

24. Which of the following is easier
    a. Actively interact with any service via a TCP connection on host Malval-instance7115 (10.0.6.98)
    b. Sniffing traffic originating from host Malval-instance23374 (10.0.7.71)
    c. They are equally easy (0 on the scale)

    If you chose a or b, according to the Scale of Ease, how much easier is the option that you selected?

    Scale 0-8: