TATA CONSULTANCY SERVICES

Building on belief

TCS iON Remote Internship RIO- 125

Project - Secured Docker Based Lab: Enforcing end-to-end security

tcs iON

TCS iON RIO| Project Description

Project Objective and Brief

To create an infrastructure to develop highly secure docker based lab environment for running different applications in a secure way and protected manner that confirms security at different levels.

Project Guidelines

Context: It is required to create a cloud-based infrastructure to develop a secure docker based Lab environment for applications that seals vulnerabilities of all types.

Background: Developing cloud-based infrastructure for developing docker based secured lab environment for different application development is the need of the hour. This project would require nurturing the technical know-how of cloud-based securities and docker components along with security enforcements and testing at different levels.

Brief: Secured docker Lab project would involve technology scopes as: I) AWS Cloud instances II) Docker and its components III) Cybersecurity tools like Nmap, Metasploit framework, Hydra, John the Ripper, etc.

TCS iON RIO| Project Description (Continued)

Project Guidelines (Continued)

Action Item - 1: AWS Cloud infrastructure development

i. Create an AWS Cloud Account.

ii. Create an AWS EC2 instance within free-tier limit, having Ubuntu OS and storage of 8 GB.

iii. Install and configure the following within the EC2 instance created:
   a. Docker and docker-compose components.
   b. Cybersecurity Tools like Nmap, Metasploit Framework, Hydra, John the Ripper, traceroute, Nessus, etc.
   c. Pull and use docker container of Wireshark.

iv. Create an IAM user with admin privileges.

v. Configure AWS CLI using the IAM user configured.

vi. Test the tools using AWS console and AWS CLI.

TCS iON RIO| Project Description (Continued)

Project Guidelines (Continued)

Action Item - 2: Lab Environment Creation

i. Create a docker based Lab environment having the following features:
   a. Base OS would be Ubuntu
   b. Configure a private network with subnet.
   c. Configure Python and its components.
   d. Configure Java environment
   e. Configure a Web Server with static IP address.
   f. Open the required ports only for services to be exposed to the external environment.
   g. Configure MySQL. Configure static IP address and open ports as required.

ii. Build docker image and test the environment from EC2 cloud instance by running the individual applications using the static ip- addresses and the ports exposed.

TCS iON RIO| Project Description (Continued)

Project Guidelines (Continued)

Action Item - 3 : Check for Vulnerability Scanning and Penetration Testing

i. Use network troubleshoot utility traceroute to scan and identify any issues within the docker environment configured.

ii. Use Nmap tool for vulnerability scanning of the docker environment.

iii. Metasploit framework needs to be used to perform different ports scans and other vulnerability scanning of different applications configured within the docker environment.

iv. Use Nessus as vulnerability assessment tool and identify weaknesses (if any) in the network.

v. Use John/Hydra for password hacking of the MySQL and other applications configured within the docker environment.

vi. With the results of the different levels of security scanning and testing done above, modify the docker environment for enhanced security. If applicable, you may add encryptions as required.

TCS iON RIO| Project Description (Continued)

Project Guidelines (Continued)

Final Deliverables Required:

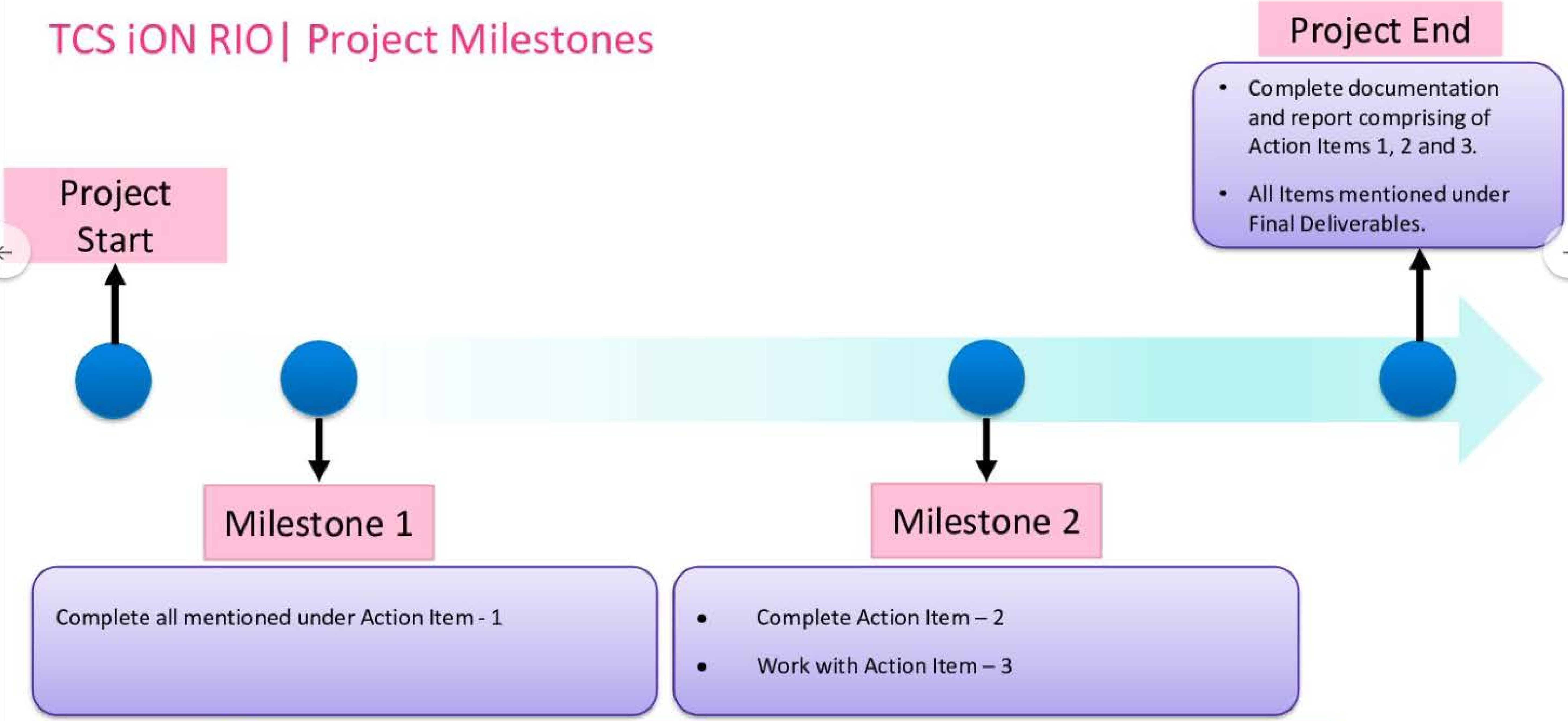
i. Scripts/Code/Screenshots for all action items explained.

ii. Project document covering topics like Approach, Logic Flow, Solutions and templates, enhancements suggested, etc.

iii. The entire set of documents along with code/scripts and outputs to be created as a zip file and uploaded to a public repository like GitHub. Share the public link of GitHub for final evaluation.

iv. Video of the product in execution. Run all the Action Items and all reports as mentioned. Capture screen and explain in the video all functionalities as explained. You can use Loom Video or any other free video recording software.

TCS iON RIO| Project Milestones



Project Start

Milestone 1

Complete all mentioned under Action Item - 1

Milestone 2

- Complete Action Item – 2
- Work with Action Item – 3

Project End

- Complete documentation and report comprising of Action Items 1, 2 and 3.
- All Items mentioned under Final Deliverables.

Project end: Complete all Action Items and documents with 5 min Video demo

TCS iON RIO| Expected Project Outcome

1 Develop conceptual understanding of Cloud Infrastructure and its applications.

2 Develop Docker based environment for different levels of applications.

3 Vulnerability scanning, penetration testing, password hacking and securing using Cybersecurity tools.

TCS iON RIO| Hands-on environment details

Project Hands-on Resources

Below are the hands-on environments or software required to implement the project –

- Working Internet Connection
- Operating Systems: Windows / Linux / MacOS with Google Chrome/Mozilla Firefox browsers
- AWS Cloud Account with root credentials
- ssh/putty to connect to AWS cloud
- Docker, docker-compose and its environment
- Java/JDK and JRE
- Python and its components
- Apache Tomcat Web Server
- MySQL database
- Cybersecurity Tools like traceroute, Nmap, Metasploit Framework, Hydra, Nessus, John the Ripper, Wireshark etc.
- Github account
- Any Free Video/Screen recording software for final demonstration of the execution of the project.

Note:

Copyright ownership of all learning and hands-on information mentioned in this RIO project rests with their respective owners. TCS does not have any business interest with these third-party copyright owners.

TCS iON RIO| Links and References

1. https://aws.amazon.com/getting-started/
2. https://docs.docker.com/get-started/
3. https://www.geeksforgeeks.org/docker-tutorial/
4. https://docs.metasploit.com/
5. https://hackertarget.com/nmap-tutorial/
6. https://nmap.org/bennieston-tutorial/
7. https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/traceroute
8. https://github.com/login