TEST PROJECT CYBER SECURITY

RegionalsSkills2021_TP54

Infrastructure Hardening & Incident Response

Submitted by: TP54_Jury

MODULE

INTRODUCTION

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please **carefully read** the following instructions!

When the competition time ends, please leave your station in a running state. The assessment will be done in the state as it is. *No reboot will be initiated as well as powered off machines will not be powered on!*

The provided tasks can be completed in any order. Just ensure that all goals are achieved

CHALLENGE SERVER (INDIVIDUAL FOR EACH TEAM)

The webserver is an Ubuntu 20.04 machine running on 2 vCPU and 4GB RAM

All traffic to the servers would be logged

Root credentials to the server would be provided on site

FILE SERVER (COMMON FOR EACH TEAM)

All teams will have access to a common file server to download files relevant to the challenge(Private key, etc..) as well as other files which deemed relevant for the competition to not provide unfair advantage to any team

TIE-BREAKER

Teams are encouraged to improve the security of the provided servers by whatever means they deem fit without compromising the accessibility of the website. Mention these steps in the excel sheet. If the additional steps are security relevant steps, these steps would be considered for tie-breaker.

TASKS

Part 1: Infrastructure Hardening

In Part 1 you will be responsible for hardening the infrastructure provided to you

1. **Server SSH Policies**
    a. Setup SSH Policy on the server to only allow access through the provided private key
    b. Setup SSH MOTD Banner “Unauthorized Access is prohibited!”
2. **Snort**
    a. Write a Snort rule to alert and log for any ICMP traffic hitting on your sever
3. **Certificate**
    a. Setup a self-signed certificate for the provided IP and configure the website running on the server for HTTPS using nginx.
4. **Misconfiguration**
    a. In your report mention all the misconfigurations you found in the server and how you fixed it. Ensure the website is functioning.

Part 2: Incident Response

In Part 2 you will be responsible for forensic analysis of the compromised webserver and cleaning the system to prevent reinfection.

1. **Code Review**
    a. Review the website running on your webserver to identify vulnerable code
    b. Make a report which includes:
        i. Screenshot of the vulnerable line(s) of code
        ii. The attack against the vulnerable code
        iii. The payload/tool command for the attack
        iv. How can one make the code secure?
        v. Screenshot of the fixed version
2. **Incident Response**
    a. Identify how the website and server was compromised
    b. Find and report all the backdoors, for each backdoor
        i. Find the attacker’s IP
        ii. Find its location
        iii. What was its purpose
    c. Create a storyline which explains how the compromise happened, deployed malwares etc.
3. **Clean-up**
    a. Remove all the backdoors to prevent further re-compromise into the system
    b. Mention the location of these backdoors