TransferRoom

TransferRoom – Lead InfoSec Tech Assignment

Version 1.0

Goal

1. Verify the candidate's ability to take high-level requirements and deliver a working solution
2. Verify the candidate's ability to create a working POC
3. Verify the candidate's ability to investigate common InfoSec scenarios
4. Verify the candidate's ability to manage cloud resources
5. Verify the candidate's ability to think creatively

Deliverables

1. Candidates should deliver the solution to **2 of the 4 tasks in the assignment**
    a. Provide any code and supporting documentation involved in scripting and/or automating the assignments in the form of a GitHub repository.
    b. Recorded video walking the viewer through the tasks that they have completed in as much detail as possible.
    c. Server with RDP login details and credentials.

Notes

1. Provide as much detail as you feel necessary, including documentation and diagrams, as you will be asked to present this back to us as part of the final stage of the process
    a. The assignment is open-book.
2. Please complete the assignment within 72 hours of receipt.

Assignment

Objective

The objective of this exercise is to demonstrate the candidate's ability to deliver common InfoSec tasks and functions.

The candidate should **attempt 2** of the 4 following assignment tasks.

Nominate any online server of your choice.

Assignment Tasks

TASK 1: Recon & Vulnerability Assessment

- Provision a small test server on Microsoft Azure.
- Scan the server and identify open ports and running services.
- Run a vulnerability scan.
- Provide a prioritised list of findings and assess their severity.

TASK 2: Security Configuration Review

- Provision a small test server on Microsoft Azure.
- Review SSH settings, firewall rules, user permissions, and audit logs.
- Highlight any misconfigurations and optimisations that you would recommend.

TASK 3: Exploit Demonstration

- Provision a small test server on Microsoft Azure.
- Choose one vulnerability and demonstrate a non-destructive exploit (e.g., SQL injection, exposed admin panel, weak SSH keys).
- Document and discuss in detail the impact and risk.

TASK 4: Remediation & Hardening

- Provision a small test server on Microsoft Azure.
- Demonstrate and implement remediations:
    - Firewall hardening
    - SSH key-based login
    - Least privilege configuration

Helpful Resources

- https://azure.microsoft.com/en-gb/Free

TransferRoom

Questions and Tasks:

1. Explain, with as much detail, how each of your solutions meets the requirements outlined above.
2. Please explain any technical challenges or considerations you encountered during the delivery of the task.