Technical Security Analyst – Interview Assignment

Assignment Instructions

1. Please send a PDF containing all the answers to the questions below.
2. The assignment itself is meant to be solved in a single day.

Question 1: AWS (Amazon Web Services) EC2 Instance

The Amazon Web Service cloud platform exposes a computing service named EC2, which allows users to instantiate virtual machines within their cloud environments. One of Wiz's top customers, Beyond-Air, has requested Wiz to trigger an alert whenever an EC2 instance that Wiz has discovered is using IMDSv1, since it is a vulnerable service that can expose sensitive data.

1. Research the AWS API and provide an example JSON payload of a **specific** EC2 instance.
    i. You are encouraged to set up an AWS account to help you with this question.
    ii. What information within the JSON in (1) can determine if this specific instance is using IMDSv1?
2. Write an OPA (Open Policy Agent) Rego code whose input is a **single** AWS EC2 JSON and whose output must contain a "match" Boolean key:
    i. If the input Json corresponds to an EC2 instance that is using IMDSv1 – "match" shall be set to true.
    ii. Else, match shall be set to "false".

- You are encouraged to use The Rego Playground to test your code.
- The input in (i) should be based on the answer of (a).
- Please add clear and concise comments in the code.

3. We should also instruct the user how to solve the configuration issues that we have detected.
    i. What are the AWS CLI command for editing an existing EC2 instance to stop using IMDSv1 and use instead IMDSv2?
4. Please connect to the EC2 instance - what files exist in the user directory by default?
5. Please write a short report (1 page at most) covering the following topics - Review a notable cloud incident that exploited IMDSv1. What is the potential risk of using IMDSv1? What were the attack stages? Why IMDSv2 is needed? What mitigations and controls can prevent this attack?

Question 2: Insecure Security Group Ports Used

AWS Security Groups (SG) are a firewall service that allows users to determine what ports and protocols are allowed to be used for network related resources. A high priority customer has provided the following use case, and expects to see it supported within a few days:

“”

*Security Group **inbound** rules should not allow the use of insecure ports.*
Insecure ports are:
Any port lower than 1024 that not using ICMP protocol; or
any port lower than 1024 except TCP protocol for these specific ports: 22, 53, 135, 443, 445, 563, 993.
“”

1. Research the AWS API, and provide an example JSON payload for each of the above security groups:
    i. An SG with one **inbound** rule that allows ingress traffic for specific IPv4 IP for SMB protocol, and one **outbound** rule that allows All traffic for any IPv4 IP.
    ii. An SG with two **inbound** rules that allow ingress traffic for Any IPv4 in LDAP protocol and any IPv6 IP for IMAPS protocol (No **outbound** rules should be set).
    iii. An SG with two **outbound** rules that allow all traffic in any port and IP; no **inbound** rules should be set.
2. Write an OPA (Open Policy Agent) Rego code whose input is all the examples above (a), that validates the customer’s use case. Output must contain a “match” Boolean key:
    i. If the input Json corresponds to an SG that allows the customer *insecure ports, “*match” shall be set to true.
    ii. Else, match shall be set to “false”.
    iii. For example,
        i. A match should be true if port 21 is allowed by the SG rules.
        ii. A match should be false if port 7001 is allowed by the SG rules.
3. You are encouraged to use The Rego Playground to test your code.
4. The input in (2) should be based on the answer of (a).
5. Please add clear and concise comments in the code.