**Detect and Response Engineering (DARE) Technical Test 2021**

**Time limit:** 48 hours to complete Part 1 and Part 2  
 **Part 1 – An Online Store for Uncle Roger**

**Scenario:** Your uncle, Roger, has been running his fried rice store “Wok Way” for a couple of years. Recently, a pandemic struck, and dine-ins are banned. This caused a 40% reduction to his usual business. Uncle Roger recognizes that an online store is needed to draw other niece and nephews to make up for the losses suffered from during the pandemic. Having a few years of programming experience, you volunteered to help him set up the online store.

**Objectives:** To allow Uncle Roger to get a feel of what an online store front would look and feel like, you are required to develop an MVP with the following features:

|  |  |
| --- | --- |
| **Frontend Webpage** | **Backend API Server** |
| * A page to list all the items in the store * A form to add / update item in the store * Demonstrate calling API to perform CRUD | * CRUD   + CREATE an item in the store   + READ list of all items in the store   + UPDATE an item in the store   + DELETE an item in the store * JSON response * Item attributes:   + ID   + Name   + Price |
| **Note:** You are not required to integrate with payment gateways like Stripe. | |

Uncle Roger is also concerned about security. Specifically, he previously worked for an IT company and they typically fail their Penetration Testing audit due to poor input validation and poor logging practices. Uncle Roger does not know anything about “input validation” nor “logging” He hopes you can address them in your web application. Be sure you can explain the implemented security measures when you meet him.

**Optional Objectives:** The following are possible improvements to further impress Uncle Roger but are not necessary:

1. Extra points for good frontend design (frontend)
2. Extra points for usage of database wrapper – ORM (backend)
3. Usage of container technologies such as Dockers or Kubernetes
4. Deployment of security controls such as IDS, IPS, Firewall, etc.
5. Strong authentication with 2FA.
6. Usage of cloud technologies such as AWS, GCP or Azure

**Instructions:**

1. Create a public repository on any online git repository (such as Github or Gitlab)
2. Include a readme file within the repository which describes clearly:
   1. Steps required to run your developed application
   2. All objectives that you have attempted
3. Upon completion, email the link of the repository to: [andre\_ng@tech.gov.sg](mailto:andre_ng@tech.gov.sg), [kelvin\_kok@tech.gov.sg](mailto:kelvin_kok@tech.gov.sg), and [DARE@tech.gov.sg](mailto:DARE@tech.gov.sg) for assessment and interview for the next stage.

**Part 2 – Find the bad actor(s) on the network**

This is a simple packet analysis challenge that should not take more than 2 hours, including the time required to read up on the topic. This challenge requires you to use a packet analyser like Wireshark to analyse the .PCAP file.

The objective of this challenge is to identify malicious activities in the network, describe the situation in greater detail, communicate the impact and recommend countermeasures.

Inspect the packt\_analysis.pcap file using your favorite packet analyser. e.g. wireshark,

tcpdump, etc.

1. Identify the type of malicious activity found in the .pcap file and elaborate on what you found. Hint: Many found the “Follow Protocol Stream” of Wireshark useful.

For the network traffic between 192.168.26.103 to www4.l.google.com, there was status 403 forbidden returned due to multiple requests being sent (TCP Spurious Retransmission).

A picture containing calendar

Description automatically generated

For the network traffic between 26.54.25.36 and 192.168.26.25 – 192.168.26.138, it seems to be a phishing website or malicious website from what can be seen from below. Checksum is unverified for the packets as well.

Chart

Description automatically generated

There are also warnings on TCP Out Of Order packets as well as TCP Previous segment not captured which have risk of TCP out-of-order packet DoS attacks. An attacker can send a large number of 1-byte packets to an E Series router in which each packet is buffered, consuming an entire packet buffer and eventually consuming a large amount of resources

Background pattern

Description automatically generated

1. Describe potential impact of the identified malicious activity (if any)?

For TCP Out Of Order DoS attacks, TCP guarantees that applications receive data in order. This means that TCP buffers any out-of-order packets it receives until ordered delivery can occur. But if the receiver uses a fixed-size buffer, a packet that contains only one data byte might consume many data bytes of buffer space, but only one byte of TCP space.

1. Propose countermeasures to prevent this from happening.

To defend against this sort of attack, you can set defaults and limits on the number of outstanding buffers on reordering queues. You can configure these defaults and limits on a per-router, per-virtual router, or per-connection within the virtual router basis.

You can protect the router from TCP out-of-order packet DoS attacks with the following tasks:

* Limiting TCP Resequence Buffers per Router
* Limiting TCP Resequence Buffers per Virtual Router
* Limiting TCP Resequence Buffers per Connection