Security incident report

Section 1: Identify the network protocol involved in the incident

As shown in the tcpdump logs, the source computer (your.machine.52444) using port 52444 sends a DNS resolution request to the DNS server (dns.google.domain) for the destination URL (yummyrecipesforme.com). Then the reply comes back from the DNS server to the source computer with the IP address of the destination URL (203.0.113.22). This is the TCP and IP protocols of the TCP/IP model which allows data packets to travel to the correct destination. It ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of a TCP/IP packet. Also The log entry with the code HTTP: GET / HTTP/1.1 shows the browser is requesting data from yummyrecipesforme.com with the HTTP: GET method using HTTP protocol version 1.1. This could be the download request for the malicious file.

Section 2: Document the incident

Incident was reported when multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. A former employee has decided to lure users to a fake website with malware. The baker executed a brute force attack to gain access to the web host. Sudden change in the logs indicate that The traffic is routed from the source computer to the DNS server again using port .52444 (**your.machine.52444 > dns.google.domain**) to make another DNS resolution request. This time, the DNS server routes the traffic to a new IP address (**192.0.2.172**) and its associated URL (**greatrecipesforme.com.http**).

```
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0
A 192.0.2.17 (40)
```

Section 3: Recommend one remediation for brute force attacks
Incident occured because the disgruntled baker was able to guess the password easily as the admin password was still set to the default password. Also there were no controls in place to prevent a brute force attack. One recommendation we can have in place to prevent brute force attacks is to set up Multiple Factor Authentication (MFA). Having password policies to standardized good password practice policies throughout the business can also prevent future brute force attacks.