### **Security Incident Report**

#### **identifying the network protocol involved in the incident**

**The network protocols involved in this incident are:**

1. **DNS (Domain Name System) – Used to resolve the domain names (yummyrecipesforme.com and greatrecipesforme.com) to their respective IP addresses.**
2. **HTTP (Hypertext Transfer Protocol) – Used to facilitate web page requests and downloads.**
3. **TCP (Transmission Control Protocol) – Used to establish and maintain connections between the client and the web server.**
4. **TLS/SSL (if HTTPS was involved, though logs show HTTP) – If encryption was used, this would also be involved.**

#### **Document the incident**

1. **Incident Summary:**
   1. **A brute force attack was executed by a former employee who guessed the default administrative password for the website yummyrecipesforme.com.**
   2. **After gaining access, the attacker modified the website's source code by inserting malicious JavaScript that prompted visitors to download and execute a malicious file.**
   3. **Once executed, the malware redirected users from yummyrecipesforme.com to greatrecipesforme.com, which contained further malware.**
2. **Timeline of Events (from tcpdump logs):**
   1. **14:18:32 – A DNS query was made for yummyrecipesforme.com, which returned an IP address 203.0.113.22.**
   2. **14:18:36 – A TCP handshake was successfully completed between the client and the compromised yummyrecipesforme.com server.**
   3. **14:18:36 – The client sent an HTTP GET request to access the website.**
   4. **Malicious JavaScript executed → The client was prompted to download an executable file.**
   5. **14:20:32 – The browser sent a new DNS query for greatrecipesforme.com, receiving IP 192.0.2.17.**
   6. **14:25:29 – A new TCP connection was initiated to greatrecipesforme.com, where the client was unknowingly served additional malware.**
3. **Impact of the Incident:**
   1. **Customers were redirected to a malicious website, which likely infected their devices.**
   2. **The website owner was locked out as the attacker changed the admin password.**
   3. **Company reputation was damaged due to the security breach.**
   4. **Potential legal consequences if customer data was compromised.**

#### **Recommend remediation for brute force attacks**

**A key remediation step to prevent future brute force attacks is:**

**Implement Multi-Factor Authentication (MFA)**

* **Require an additional authentication factor (e.g., a one-time password via email or authenticator app) alongside the admin password.**
* **Even if the attacker guesses the password, they would still need access to the second authentication factor, preventing unauthorized logins.**

**Other best practices:**

* **Disable default credentials – Force users to create strong passwords upon setup.**
* **Implement account lockout policies – Lock the account after multiple failed login attempts.**
* **Monitor login activity – Use Intrusion Detection Systems (IDS) to detect unusual login behavior.**