Security incident report

Section 1: Network Protocol Identification in the Incident

The initial portion of the DNS and HTTP traffic log file reveals that the source computer (your.machine.52444) initiates a DNS resolution request to the DNS server (dns.google.domain) using port 52444, querying for the destination URL (yummyrecipesforme.com). The server then responds with the IP address of the destination URL (203.0.113.22), which is sent back to the source computer.

In the TCP/IP model, both DNS and HTTP operate at the application layer, the highest layer of the model. This layer provides services to applications, enabling communication between them through various protocols, such as HTTP and DNS.

Elaboration:

- **Application Layer:** The topmost layer of the TCP/IP model, responsible for providing network services to applications.
- **DNS (Domain Name System):** A protocol that translates human-readable domain names (e.g., www.google.com) into machine-readable IP addresses (e.g., 172.217.160.142).
- **HTTP (Hypertext Transfer Protocol):** A protocol used for web communication, facilitating the request and retrieval of information between web browsers (and other clients) and servers.
- **Other protocols in the application layer:** Common protocols like FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol) also operate at this level.

Section 2: Incident Documentation

The logs reveal the following sequence of events:

1. **The browser initiates a DNS request:**
   The browser requests the IP address for the URL *yummyrecipesforme.com* from the DNS server.

   ```
   14:18:32.192571 IP your.machine.52444 > dns.google.domain:
   35084+ A? yummyrecipesforme.com. (24)

   14:18:32.204388 IP dns.google.domain > your.machine.52444:
   35084 1/0/0 A 203.0.113.22 (40)
   ```

   The DNS server responds with the correct IP address for the destination website.

2. **The browser initiates a TCP connection (SYN request):**
   The browser sends a SYN request to the web server at *yummyrecipesforme.com* on port 80 (HTTP), attempting to establish a connection.

   ```
   14:18:36.786501 IP your.machine.36086 >
   yummyrecipesforme.com.http: Flags [S], seq 2873951608, win
   65495, options [mss 65495,sackOK,TS val 3302576859 ecr
   0,nop,wscale 7], length 0

   14:18:36.786517 IP yummyrecipesforme.com.http >
   your.machine.36086: Flags [S.], seq 3984334959, ack
   2873951609, win 65483, options [mss 65495,sackOK,TS val
   3302576859 ecr 3302576859,nop,wscale 7], length 0
   ```

3. **The browser initiates an HTTP request:**
   Following the established TCP connection, the browser sends an HTTP GET request to retrieve the website's content using the IP address obtained from the DNS response.

   ```
   14:18:36.786589 IP your.machine.36086 >
   yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1,
   ```

```
win 512, options [nop,nop,TS val 3302576859 ecr
3302576859], length 73: HTTP: GET / HTTP/1.1
```

The log entry with the HTTP GET request indicates that the browser is attempting to retrieve data from *yummyrecipesforme.com* using the HTTP GET method (version 1.1). This could represent the download request for a potentially malicious file.

4. **The browser initiates a DNS request for a different domain:**
   A DNS request is made for the URL recetasriquitasforme.com.

5. **The DNS server responds:**
   The DNS server responds with the IP address for greatrecipesforme.com.

```
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 192.0.2.172 (40)
```

6. **The browser initiates an HTTP request to the new IP address:**
   The browser establishes a TCP connection and sends an HTTP request to the newly resolved IP address of greatrecipesforme.com.

```
14:25:29.576493 IP your.machine.56378 >
greatrecipesforme.com.http: Flags [S], seq 1020702883, win
65495, options [mss 65495,sackOK,TS val 3302989649 ecr
0,nop,wscale 7], length 0

14:25:29.576510 IP greatrecipesforme.com.http >
your.machine.56378: Flags [S.], seq 1993648018, ack
1020702884, win 65483, options [mss 65495,sackOK,TS val
3302989649 ecr 3302989649,nop,wscale 7], length 0
```

Section 3: Recommendation for Remediating Brute Force Attacks

The attacker was able to easily guess the password because the administrator account still had the default password, and there were no mechanisms in place to defend against a brute force attack.

A brute force attack is a cyberattack method in which an attacker attempts to crack passwords, encryption keys, or other access credentials by systematically testing all possible combinations, much like trying every possible combination on a combination lock. This attack is known for its simplicity and its guaranteed success, provided the attacker has enough time and computing power.

To mitigate the risk of brute force attacks, the following recommendations should be implemented:

1. **Require strong passwords:** Ensure that passwords meet complexity requirements, such as a minimum length and a mix of characters (uppercase, lowercase, numbers, and special characters).

2. **Enforce two-factor authentication (2FA):** Implementing 2FA adds an additional layer of security, requiring users to verify their identity with something they know (password) and something they have (e.g., a code sent to their phone).

3. **Monitor login attempts:** Keep track of failed login attempts to identify suspicious behavior, such as multiple incorrect login attempts within a short period of time.

4. **Require frequent password changes:** Periodically require users to change their passwords, reducing the risk of unauthorized access due to stale or compromised credentials.

5. **Prevent the use of old passwords:** Implement a policy that prevents users from reusing old passwords, ensuring that new passwords are unique and secure.

6. **Limit the number of login attempts:** Implement account lockouts or delays after a certain number of failed login attempts to slow down brute force attempts.