Security incident report

Section 1: Identify the network protocol involved in the incident
Based on the provided network log, here is a list of network protocols involved in the incident: DNS (Domain Name System): • Appears at 14:18:32.192571 and 14:20:32.192571. • Used for domain name resolution. • Example: "your.machine.52444 > dns.google.domain," and the response from DNS. HTTP (Hypertext Transfer Protocol): • Appears in the HTTP traffic. • Example: "your.machine.36086 > yummyrecipesforme.com.http" and "your.machine.56378 > greatrecipesforme.com.http." • Used for communication between the client (your.machine) and the web servers (yummyrecipesforme.com and greatrecipesforme.com). • Example HTTP request: "GET / HTTP/1.1." TCP (Transmission Control Protocol): • Appears in the flags of TCP packets. • Example: Flags like [S], [S.], [P.], [.], etc. • Used for reliable, connection-oriented communication. IP (Internet Protocol): • Appears in the source and destination IP addresses. • Example: "your.machine.52444 > dns.google.domain." • Used for addressing and routing packets in the network. These protocols are essential for the communication between your machine and the DNS server, as well as between your machine and the web servers hosting the recipes websites.

Section 2: Document the incident

- **DNS Query for "yummyrecipesforme.com":**
  Log Entry: 14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)
  Explanation: The user's machine initiates a DNS query to resolve the IP address of "yummyrecipesforme.com" using the DNS server at "dns.google."

- **DNS Response for "yummyrecipesforme.com":**
  Log Entry: 14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)
  Explanation: The DNS server responds with the IP address (203.0.113.22) associated with "yummyrecipesforme.com."

- **HTTP Connection to "yummyrecipesforme.com":**
  Log Entries: 14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495... (Followed by subsequent HTTP traffic)
  Explanation: The user's machine initiates an HTTP connection to "yummyrecipesforme.com" over port 80, indicating a standard unsecured connection.

- **DNS Query for "greatrecipesforme.com":**
  Log Entry: 14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)
  Explanation: Another DNS query is made to resolve the IP address of "greatrecipesforme.com" using the DNS server at "dns.google."

- **DNS Response for "greatrecipesforme.com":**
  Log Entry: 14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)
  Explanation: The DNS server responds with the IP address (192.0.2.17) associated with "greatrecipesforme.com."

- **HTTP Connection to "greatrecipesforme.com":**
  Log Entries: 14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495... (Followed by subsequent HTTP traffic)
  Explanation: The user's machine initiates an HTTP connection to "greatrecipesforme.com" over port 80, again indicating a standard unsecured connection.

Security Analysis:

- *Sudden Change in Port:* While the DNS queries use a non-standard port (52444), the subsequent HTTP connections for both domains utilize the standard unsecured port 80.

- *Website IP Change:* The IP addresses associated with the websites "yummyrecipesforme.com" and "greatrecipesforme.com" are different (203.0.113.22 and 192.0.2.17, respectively).

- *Non-Secure Connection:* The use of port 80 for HTTP traffic indicates a lack of encryption, making the data exchange between the user's machine and the websites susceptible to interception. Security measures such as HTTPS should be considered for secure communication.

Section 3: Recommend one remediation for brute force attacks
One effective remediation for brute force attacks is to implement account lockout policies. Account lockout policies help mitigate the impact of brute force attacks by locking out user accounts after a certain number of failed login attempts. This prevents attackers from repeatedly attempting to guess passwords, as the account becomes temporarily or permanently disabled after a predefined number of unsuccessful login attempts.