Security incident report

Section 1: Identify the network protocol involved in the incident

Based on the tcpdump traffic log analysis, the following network protocols were identified during the security incident:
DNS (Domain Name System):

- Used at timestamps 14:18:32 for resolving yummyrecipesforme.com to IP 203.0.113.22
- Used at timestamp 14:20:32 for resolving greatrecipesforme.com to IP 192.0.2.17
- DNS operates at the Application Layer of the TCP/IP model

HTTP (HyperText Transfer Protocol):

- Used at timestamp 14:18:36 for establishing connection with yummyrecipesforme.com on port 80
- Used at timestamp 14:25:29 for establishing connection with greatrecipesforme.com on port 80
- HTTP operates at the Application Layer of the TCP/IP model

Section 2: Document the incident

Incident Summary: On the reported date, the company website yummyrecipesforme.com was compromised through a successful brute force attack targeting the administrative account.

Attack Timeline and Methodology:

1. A former employee initiated a brute force attack against the website's administrative panel
2. The attacker systematically attempted multiple default passwords until successfully guessing the correct administrative credentials
3. Upon gaining unauthorized access, the attacker modified the website's source code
4. Malicious JavaScript code was embedded that prompted visitors to download an executable file

5. The attacker changed the administrative account password to prevent legitimate access

Technical Evidence from tcpdump Log:

- Initial DNS query resolved yummyrecipesforme.com to IP address 203.0.113.22
- HTTP connection established to the legitimate website
- Malware download was triggered upon page load
- Secondary DNS query resolved the malicious domain greatrecipesforme.com to IP address 192.0.2.17
- Browser was redirected to the malicious website via HTTP

Impact Assessment:

- Multiple customers reported being prompted to download files for "free recipes"
- Customer systems experienced performance degradation after executing the downloaded file
- Website administrator lost access to the admin panel
- Customer trust and website reputation were compromised

Root Cause Analysis: According to the cybersecurity team investigation:

- Administrative account was still using default password
- No brute force protection mechanisms were in place
- Lack of proper access controls and monitoring systems

Source of Information:

- Customer complaints to helpdesk
- tcpdump network traffic logs from sandbox environment
- Source code analysis by senior analyst
- Cybersecurity team forensic investigation

Section 3: Recommend one remediation for brute force attacks

Recommended Security Measure:
Implementation of Account Lockout Policy with Progressive Delays

Recommendation Details: Implement an account lockout mechanism that temporarily disables login attempts after a specified number of failed authentication attempts (recommended: 5 failed attempts triggers a 15-minute lockout, with progressive increases for repeated violations).