Security incident report

Section 1: Identify the network protocol involved in the incident

The security incident involves the use of DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol) protocols. The DNS protocol was used for resolving domain names to IP addresses, and the HTTP protocol was used for communication between the user's machine and the compromised website.

DNS Protocol:

1) DNS request initiated by the user's machine (your.machine.52444) to resolve yummyrecipesforme.com: ‘**your.machine.52444 > dns.google.domain: 35084+ A? Yummyrecipesforme.com.’**
2) DNS reply from the DNS server (dns.google.domain) with the IP address of yummyrecipesforme.com: **‘dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22.’**
3) Another DNS request initiated for greatrecipesforme.com: ‘**your.machine.52444 > dns.google.domain: 21899+ A? Greatrecipesforme.com.’**
4) DNS reply for greatrecipesforme.com: ‘**dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.172.’**

HTTP Protocol:

1) Connection initiated by the user's machine to yummyrecipesforme.com: **‘your.machine.36086 > yummyrecipesforme.com.http: Flags [S] …’m**
2) HTTP GET request for the yummyrecipesforme.com webpage: **‘your.machine.36086 > yummyrecipesforme.com.http: Flags [P.] … HTTP: GET / HTTP/1.1’**
3) Similar HTTP communication occurs after redirection to greatrecipesforme.com.

Section 2: Document the incident

A security incident was identified at yummyrecipesforme.com involving a disgruntled former employee who executed a brute force attack. The attacker gained unauthorized access to the web host by repeatedly trying known default passwords for the administrative account until they got it correct. Then the attacker accessed the admin panel and modified the website's source code. The modification included embedding a JavaScript function that prompted visitors to download and run a file when entering the website. This file redirected users to a fake website (greatrecipesforme.com) which contains malware.

Many customer complaints were received hours after the attack, reporting that the website prompted them to download a file to access the free recipes. When running the file, the website's address changed, and their personal computers started to run slower.

An analysis using tcpdump revealed the following events:

1) DNS resolution requests for yummyrecipesforme.com and greatrecipesforme.com.
2) HTTP connections were initiated for both websites.
3) Malicious download and redirection to greatrecipesforme.com.

The web server was affected by a successful brute force attack because of weak security practices. The administrative password was still set to the default, and no controls were in place to prevent brute force attempts.

Section 3: Recommend one remediation for brute force attacks

To mitigate the risk of future brute-force attacks, I recommended implementing the following measures:

Password Policy Improvements:

1) Enforce a strong password policy, making sure that all administrative accounts use complex and unique passwords.
2) Regularly update and change default passwords, especially for high-privileged accounts.
3) Implement account lockout mechanisms to temporarily disable accounts after a certain number of unsuccessful login attempts.

By enhancing password security practices, the organization can significantly reduce the likelihood of successful brute-force attacks. Conducting regular security audits and implementing intrusion detection systems can also improve overall security posture.