Brute Force Attack: Security incident report

Section 1: Identify the network protocol involved in the incident

This is an application layer attack focusing on abusing HTTP and DNS requests

Section 2: Document the incident

A disgruntled user executed an attack to gain unauthorized access to the web server hosting yummyrecipesforme.com. The attacker used a brute force technique to crack the admin account password. After gaining admin access, the attacker added malicious JavaScript code to the website source files. The code prompted visitors to download and run an executable file, which then redirected them to a phishing site spoofing the domain greatrecipesforme.com. On this fake site, the attacker uploaded all of the original site's premium recipes for free. Visitors also reported performance issues on their machines after running the downloaded file, indicating it had malware payloads. Analysis in a sandbox environment revealed the attack flow: The browser requests and gets a valid DNS response for yummyrecipesforme.com The browser loads the compromised site and is prompted to download malware The malware redirects the browser to greatrecipesforme.com A DNS request resolves to the attacker's fake IP address The browser loads the phishing site impersonating the victim domain By cracking the admin password, the attacker planted malware on the site to steal data and traffic. Technical analysis confirmed unwanted redirections, DNS spoofing, stolen data uploads, and malware execution resulting from this attack.

Section 3: Recommend one remediation for brute force attacks

The root cause of this breach was the admin account having an easily guessed default password. To prevent future brute force credential attacks, stronger password policies and access controls should be implemented for administrator accounts across the organization. Specific safeguards include: Rate-limiting failed login attempts to block brute force password guessing. Automatically block IPs after a reasonable number of failures. Enforce stronger password complexity rules requiring minimum length and a mix of uppercase, lowercase, numbers and symbols. Require regular password changes every 60-90 days. Add multi-factor authentication (MFA) using a secondary credential check like a code sent to a mobile device. A key priority is implementing account lockout policies throttling repeated failed logins, which is the attack vector exploited to crack the weak admin password. Without these safeguards, attackers can unlimitedly submit password guesses through brute force tools. Securing admin access with layered security controls like complex passwords, lockout mechanisms, expiration cycles and MFA will drastically reduce exposure to password cracking attempts in the future.