Security incident report

Section 1: Identify the network protocol involved in the incident

Protocol: DNS, TCP, HTTP

Section 2: Document the Incident

Date: 10/8/2024

Incident: Brute force attack and DNS hijacking

Impact: Website visitors were redirected to a fake website and downloaded malware

Source IP: My machine.52444

Destination IP: 203.0.113.22 and 192.0.2.172

Description: A brute force attack was conducted on the website's admin panel, allowing the attacker to gain access and embed malware. The malware redirects visitors to a fake website, which downloads additional malware onto their devices.

Tool(s) used: Tcpdump

When: 14:18:32.192571

Who: Formal employee

Where: Company's website

What: Bruce force attack that leads to dns hijacking

Why: To gain unauthorized access to admin panel and distribute malware

Section 3: Recommend one remediation for brute force attacks

Implement account lockout policies after a specified number of failed login attempts like 5-10 times. This will prevent attackers from guessing passwords repeatedly, reducing the risk of successful brute force attacks.