Security incident report

Network protocol involved in the incident

The **DNS** (Domain Name System) protocol is used to resolve domain names into IP addresses. This is evident in the logs where the source machine (your.machine) queries the DNS server (dns.google.domain) to resolve domain names like yummyrecipesforme.com and receives corresponding IP addresses.

Once the IP address is obtained, the **TCP** (Transmission Control Protocol) is used to establish a reliable connection between the source and the destination server. The logs show the source machine initiating the connection with a SYN flag (`Flags [S]`), while the destination acknowledges it with a SYN-ACK flag (`Flags [S.]`).

Following the connection, **HTTP** (Hypertext Transfer Protocol) is used to transfer data, such as requesting a web page or a file. For example, the HTTP GET request (`GET / HTTP/1.1`) indicates a data retrieval attempt from the server, potentially downloading a malicious file.

Throughout this process, the **IP** (Internet Protocol) ensures packets are routed between the source and destination. By analyzing the DNS queries, TCP connection attempts, and HTTP requests, patterns of unusual or repeated activity can be identified, which may point to potential brute force attacks or malicious activities.

Incident Documentation

This incident involves analyzing a tcpdump traffic log to identify a potential brute force attack. The logs show the source computer (your.machine) first resolving domain names via DNS requests to dns.google.domain, receiving IP addresses for domains like yummyrecipesforme.com and greatrecipesforme.com. Following the DNS resolution, the source computer initiates TCP connections with these destinations using SYN flags, and the destinations acknowledged with SYN-ACK responses. HTTP GET requests are observed, likely used to request or download malicious files. A notable change occurs when the DNS server routes traffic to a different IP address associated with a spoofed domain (greatrecipesforme.com), and the source computer establishes a new connection to this spoofed site with a different port number. The repeated DNS queries, new IP redirection, and connection attempts suggest potential malicious activity requiring further investigation.

Remediation for brute force attacks
Some of the common security methods used to prevent brute force attacks include: ● Requiring strong passwords ● Enforcing two-factor authentication ● Monitoring login attempts ● Requiring more frequent password changes ● Disallowing previous passwords from being used ● Limiting the number of login attempts