Application of OS Hardening Techniques

Security Incident Report

Network Protocol Involved in the Incident:
Based on the DNS and HTTP traffic log below, the following network protocols were identified during the investigation:

- DNS (Domain Name System): This protocol translates domain names to IP addresses. This was observed in the logs when the browser requested the DNS resolution of both **'yummyrecipesforme.com'** and **'greatrecipesforme.com'**.
- HTTP (Hypertext Transfer Protocol): This protocol facilitates the transfer of hypertext documents on the internet. It was observed when the browser initiated an HTTP request to fetch the webpage for both domains.

Reference: TCP/IP Model Layers

- Application Layer: HTTP, DNS
- Transport Layer: TCP
- Internet Layer: IP
- Network Access Layer: Not identified in this log.

Summary of the Incident:
An unauthorized individual executed a brute force attack to gain access to the web host of **'yummyrecipesforme.com'**. After obtaining administrative access, the attacker modified the source code, adding a JavaScript function. This malicious code prompted visitors to download an executable file which, when run, redirected them to a counterfeit version of the original website **'greatrecipesforme.com'**. On this fraudulent site, the company's premium recipes were being offered for free. Several customers reported suspicious activities and a change in the website's behavior, they also reported their personal computers have been operating slowly, and the website owner tried logging into the web server but noticed they were locked out of their account prompting this investigation.

Details of the Incident:

- Location: The incident occurred on the website **'yummyrecipesforme.com'**.
- Discovery: Customers reported being prompted to download an executable file upon visiting **'yummyrecipesforme.com'**. After downloading and executing this file, they were redirected to **'greatrecipesforme.com'** where recipes were available for free.
- Evidence: Using a sandbox environment to test the website without impacting the company network, I ran tcpdump. Logs showed multiple HTTP requests to and from **'yummyrecipesforme.com'** and **'greatrecipesforme.com'**, along with DNS resolutions for both domains. A JavaScript code prompting the download of an executable file was also discovered in the source code.
- Sources of Information: The information was obtained from tcpdump logs, direct examination of the website's source code, and customer reports.

Recommendations for Remediation:
To prevent brute force attacks, I recommend implementing a system that limits the number of unsuccessful login attempts a user can make within a certain time frame. After reaching this limit, the user's IP should be temporarily blocked for a predetermined period. By limiting the number of login attempts, attackers will find it challenging to use brute force methods as they will be locked out after a few unsuccessful tries. This mechanism not only hinders brute force attacks but also serves as a deterrent for potential attackers, as it increases the time and effort required to infiltrate the system.

DNS and HTTP Traffic Log

14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)

14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
...<a lot of traffic on the port 80>...

14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1

14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0
...<a lot of traffic on the port 80>...