Security Incident Report: OS hardening techniques

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). By running tcpdump and accessing the yummyrecipesforme.com website, we were able to capture the DNS and HTTP traffic activity and generate a log file. This log file provided the necessary evidence to determine the protocol's impact. It was observed that the malicious file was delivered to users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Multiple customers contacted the website owner to report their experience of being prompted to download and run a file for browser update when visiting the website. They noticed a significant slowdown in their personal computers since then. Additionally, the website owner encountered difficulties logging into the web server, as they found themselves locked out of their account. To investigate the incident, the cybersecurity analyst set up a sandbox environment, ensuring the company network remained unaffected. By running tcpdump, the analyst captured network and protocol traffic packets generated during interactions with the website. During this process, the analyst encountered a prompt to download a file that claimed to update the user's browser. Accepting the download and executing the file led to the browser redirecting the analyst to a counterfeit website (greatrecipesforme.com) that closely resembled the original site (yummyrecipesforme.com). Analyzing the tcpdump log, the cybersecurity analyst observed that the browser initially requested the IP address of the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. Subsequently, a noticeable change in network traffic occurred as the browser sought a new IP resolution for the greatrecipesforme.com URL. Consequently,

the network traffic was rerouted to the new IP address associated with the greatrecipesforme.com website.

Upon reviewing the source code for both websites and the downloaded file, the senior cybersecurity professional identified malicious alterations. The analysis revealed that an attacker had manipulated the website by inserting code that prompted users to download a malicious file disguised as a browser update. Considering the website owner's account lockout situation, the team concluded that the attacker likely employed a brute force attack to gain access to the account and change the administrator's password. The execution of the malicious file resulted in the compromise of end users' computers.

Section 3: Recommend one remediation for brute force attacks

To fortify the defense against brute force attacks, the team intends to implement a robust security measure, namely, two-factor authentication (2FA). The proposed 2FA plan will incorporate an extra layer of user verification, requiring individuals to authenticate their identity by confirming a unique one-time password (OTP) sent to either their email or phone. By combining the conventional login credentials with the OTP validation, users will gain access to the system. The introduction of this additional authorization significantly mitigates the likelihood of any malicious actor successfully executing a brute force attack and compromising 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>...
```