Activity: Apply OS hardening techniques

Scenario

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A disgruntled baker has decided to publish the website's best-selling recipes for the public to access for free.

The baker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free.

Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.

In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event.

To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original site. However, the recipes your company sells are now posted for free on the new website.

The logs show the following process:

1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request for the webpage.

4. The browser initiates the download of the malware.
5. The browser requests another DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

DNS & HTTPS Traffic Logs:

```
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>...
```

Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the Hypertext transfer protocol (HTTP). As the issue was with accessing the web server for yummyrecipesforme.com, we can infer that the requests to web servers involve http traffic in the application layer of the TCP/IP model. This is substantiated by the corresponding tcpdump log file after running tcpdump , which showed the usage of the http protocol when contacting the DNS server. The malicious file is thus seen to be transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Initially, customers had contacted the website's helpdesk stating that when visiting the website, they were asked to download and run a file that contained access to new recipes. However, once the file has been downloaded, the speed and performance of their personal devices has taken a great toll. The owner of the website had also tried logging into the web server but found out that they had been locked out of their account. The cybersecurity analyst used a sandbox environment to open the website to ensure that that company network isn't impacted. The analyst then ran tcpdump to capture the network traffic packets produced by interacting with the website in the form of a log record. The analyst was prompted to download a file claiming it would provide access to free recipes, and thus accepted and ran the file. The browser then redirected the analyst to a fake website called greatrecipiesforme.com. When the tcpdump log record was available, the analyst inspected it and found that the browser initially requested the IP address for the yummyrecipesforme.com website. After the file had been downloaded, the logs showed a sudden change in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic had then been rerouted to the new IP address for the greatrecipesforme.com website.

The next step was to analyze the source code of both the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to add malicious code that prompted the users to download a malicious file disguised as a browser update. The attacker also used a brute force attack to access the account and change the admin password, causing the website owner to be locked out of their account.

Section 3: Recommend one or more remediations for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to ensure previously used passwords cannot be used again, since the vulnerability that led to this attack was the attacker's ability to use a default password to log in. Another remediation would be to introduce more frequent password updates, so that any unauthorized person who becomes aware of the password is less likely to be able to use that password if the password is updated. Finally, another helpful solution is to implement two-factor authentication (2FA). 2FA requires authentication via a password and a one-time passcode (OTP) sent to either their email or phone. A user will only gain access to the system once the user confirms their identity through their login credentials as well as the OTP. Any malicious actor that attempts a brute force attack will not likely gain access to the system due to the additional requirement.

- Sruthi Sathishkumar