Portfolio Project

Applying OS Hardening Techniques
Google Cybersecurity Professional Certificate

Prepared by :
Aleck Kitenge

1 Activity Overview

In this activity, you will take on the role of a cybersecurity analyst working for a company that hosts the cooking website, yummyrecipesforme.com. Visitors to the website experience a security issue when loading the main webpage. Your job is to investigate, identify, document, and recommend a solution to the security problem.

When investigating the security event, you will review a tcpdump log. You will need to identify the network protocols used to establish the connection between the user and the website. Network protocols are the communication rules and standards networked devices use to transmit data. Unfortunately, malicious actors can also use network protocols to invade and attack private networks. Knowing how to identify the protocols commonly used in attacks will help you protect your organization's network against these types of security events.

To complete the assignment, you will also need to document what occurred during the security incident. Then, you will recommend one security measure to implement to prevent similar security problems in the future.

2 Activity 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.

2 Activity Scenario cont. (1)

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.

2 Activity Scenario cont. (2)

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.

3 Activity 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

14:18:36.786589 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

14:20:32.192571 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 192.0.2.172 (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

3 Activity Q&A

Section 1: Identify the network protocol involved in the incident

The Hypertext Transfer Protocol (HTTP) was the protocol affected by this incident. To pinpoint the problem, capture protocol, and track traffic activity, we ran tcpdump and visited the yummyrecipesforme.com website. This produced a DNS & HTTP traffic log file that provided the necessary proof to support our conclusion. The malicious file is being transferred to users' computers using the HTTP protocol at the application layer, as we have observed.

3

Activity Q&A cont. (1)

Section 2: Document the incident

Multiple customers reported to the website owner that upon visiting the site, they were prompted to download and run a file claiming to update their browsers. Subsequently, their personal computers experienced performance issues. The website owner attempted to log into the web server but discovered they were locked out of their account.

To investigate without endangering the company network, a cybersecurity analyst employed a sandbox environment to test the website. The analyst then ran tcpdump to capture network traffic and protocol packets generated during interactions with the website. The analyst was prompted to download a file purported to update their browser, accepted the download, and executed it. The browser subsequently redirected the analyst to a fraudulent website (greatrecipesforme.com) that closely resembled the original site (yummyrecipesforme.com).

The cybersecurity analyst reviewed the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Upon establishing a connection with the website using the HTTP protocol, the analyst recalled downloading and running the file. The logs revealed a sudden shift in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then redirected to the new IP address for the greatrecipesforme.com website.

A senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to insert code prompting users to download a malicious file disguised as a browser update. Since the website owner indicated they had been locked out of their administrator account, the team surmised that the attacker had employed a brute force attack to gain access to the account and alter the admin password. The execution of the malicious file compromised the end users' computers.

3 Activity Q&A cont. (2)

Section 3: Recommend one remediation for brute force attacks

To enhance security and safeguard against brute force attacks, the team intends to implement two-factor authentication (2FA). This 2FA plan will mandate that users validate their identity by confirming a one-time password (OTP) sent to either their email address or phone number. Upon successfully verifying their identity through both their login credentials and the OTP, users will be granted access to the system. Any malicious actor attempting a brute force attack will face an additional layer of protection, making it highly unlikely that they will gain unauthorized access.