My solution to Activity Apply OS hardening techniques

Tags:

#Coursera/Google-Cyber-Security/Connect-and-Protect-Networks-and-Network-Security/Module-4/Lab

Date & Time: 2025-07-02 | 19:09

Google Cybersecurity Course-3 Module-4 Lab-1

Section 1:

Identify the network protocols involved in the incident
Based on the TCP/IP model, the process is started when the attacker target the admin panel using brute force attack, . But the security team using network analyzer tools in the phase of Investigate in the attack, The packet capture shows a DNS query (UDP) for `yummyrecipesforme.com`, followed by a DNS response containing its A-record, to access the website, and then when we get the response from the DNS server with the IPv4, we make another request to the web server to establish a connection using `HTTP Protocl`, to enter the target website. But after DNS resolution, the browser must establish a `TCP connection` to the web server before any HTTP traffic can flow(with its normal SYN/SYN-ACK/ACK handshake). After we successfully load the `yummyrecipesforme.com`, the browser will start loading(Downloading) the new files on the application layer using GET method, and `HTTP version 1.1`.

Section 2:

Document the incident

The incident occurred:
- **14:18:32:** DNS query for `yummyrecipesforme.com`

- **14:18:36:** TCP handshake begins

- **14:18:36.786589:** HTTP GET `/`, triggering download

- **+2 hrs:** Customer reports of slow PCs.

The incident discovered when the customer try to access the sites, but there's a new update, and that is a prompt website visitors to download an executable file(The malware). The owner to the malware is this host `192.0.2.17`. After the visitors run the file on there machine the malware start running on the background, after 2 hour, they noticed a slow performance, they report that to the security team. The site administrator attempted to log in to the admin panel but was denied access, indicating the password had been changed. So the website is compromised. Security team try to visit the website and they found the new update, so the response to the incident start now. They use a sandbox to run the malware on isolated environment, and use a `tcpdump`(Network analyzer tool) to see all the traffic, and also open the source code of the website to see the updates, and they found the JavaScript payload, and this will direct anyone will click the link to `192.0.2.17`. The incident happened because the Sys admin is still using the default password to open the admin panel to the website, and this make the website is a attack surface. The target website is a `E-Commerce`, so the attacker will impact the business continuity and reputation.

Document the incident

Section 3:

Recommend one remediation for brute force attacks

To prevent this attack for the future, we should implement a strong security controls:

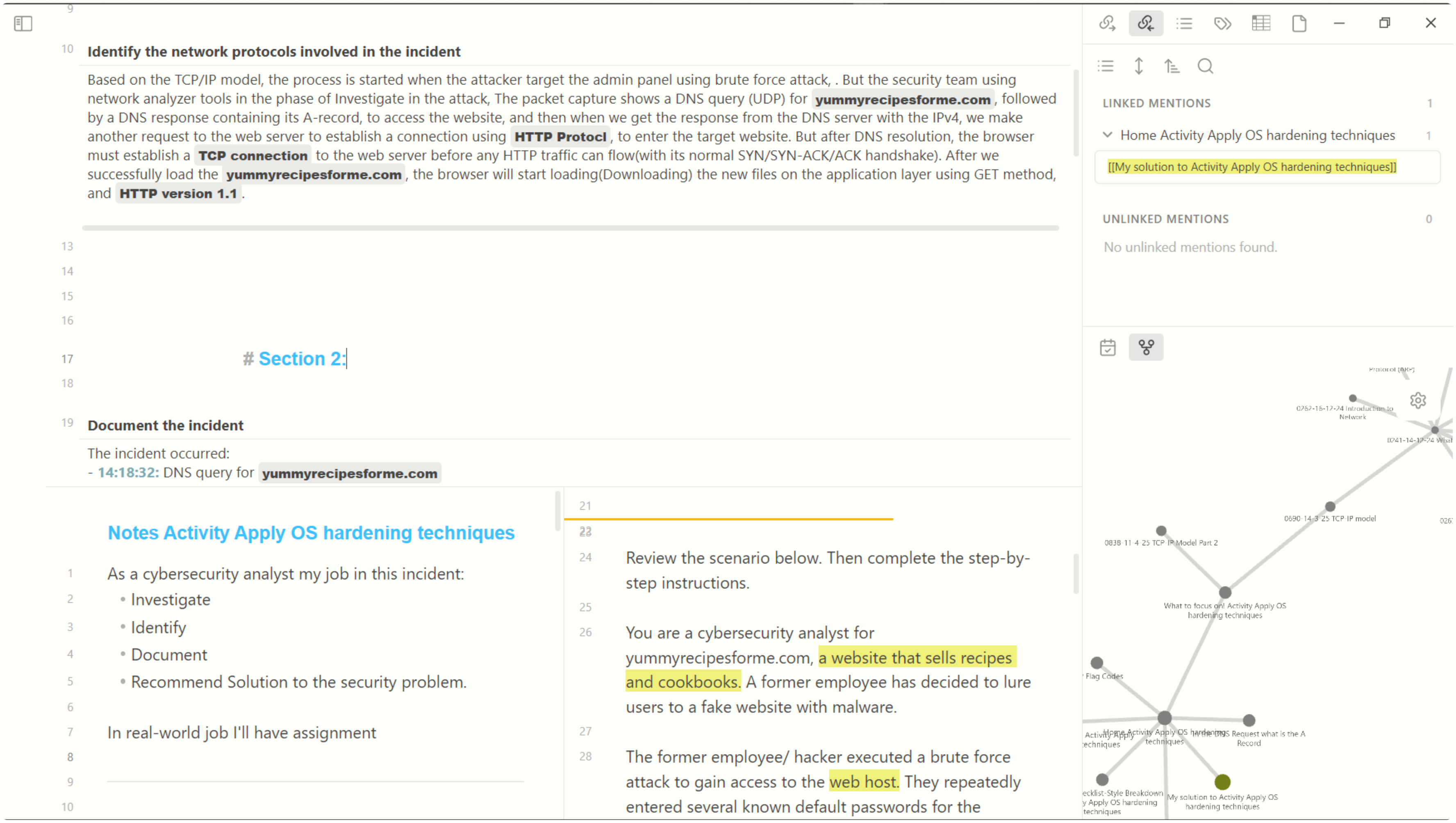
- Strong passwords
- 2FA
- Monitoring login attempts using SIEM tool
- Limiting the number of login attempts to prevent brute force attack.

Screenshot:

```
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>...
```

My workflow



Identify the network protocols involved in the incident

Based on the TCP/IP model, the process is started when the attacker target the admin panel using brute force attack, . But the security team using network analyzer tools in the phase of Investigate in the attack, The packet capture shows a DNS query (UDP) for `yummyrecipesforme.com`, followed by a DNS response containing its A-record, to access the website, and then when we get the response from the DNS server with the IPv4, we make another request to the web server to establish a connection using `HTTP Protocl`, to enter the target website. But after DNS resolution, the browser must establish a `TCP connection` to the web server before any HTTP traffic can flow(with its normal SYN/SYN-ACK/ACK handshake). After we successfully load the `yummyrecipesforme.com`, the browser will start loading(Downloading) the new files on the application layer using GET method, and `HTTP version 1.1`.

Section 2:

Document the incident

The incident occurred:
- **14:18:32:** DNS query for `yummyrecipesforme.com`

Notes Activity Apply OS hardening techniques

As a cybersecurity analyst my job in this incident:
- Investigate
- Identify
- Document
- Recommend Solution to the security problem.

In real-world job I'll have assignment

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A former employee has decided to lure users to a fake website with malware.

The former employee/ hacker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the

LINKED MENTIONS 1

Home Activity Apply OS hardening techniques 1

[[My solution to Activity Apply OS hardening techniques]]

UNLINKED MENTIONS 0

No unlinked mentions found.

Protocol (ARP)
0262-16-12-24 Introduction to Network
0241-14-12-24 What
0690-14-3-25 TCP-IP model
026
0838-11-4-25 TCP-IP Model Part 2
What to focus on! Activity Apply OS hardening techniques
Flag Codes
Activity Apply techniques
Home Activity Apply OS hardening techniques
In the DNS Request what is the A Record
ecklist-Style Breakdown y Apply OS hardening techniques
My solution to Activity Apply OS hardening techniques