

Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

Student:

Isaiah Mosley

Email:

isaiahmosley80@gmail.com

Time on Task:

130 hours, 33 minutes

Progress:

100%

Report Generated: Tuesday, December 2, 2025 at 1:24 PM

Hands-On Demonstration

Part 1: Review the SIEM configuration

8. Make a screen capture showing the list of log files monitored on web1.

The screenshot shows the Wazuh dashboard interface. At the top, there's a header with the title 'Investigating and Responding to Security Incidents (4e)', the date '2025-03-30 06:23:14', and the user 'Isaiah Mosley'. Below the header, there are tabs for 'Agents' (selected), 'web1', and 'Configuration'. The main content area is titled 'Log collection' and shows a list of log files under 'Logs files': '/var/ossec/logs/active-res...', '/var/log/auth.log', '/var/log/syslog', '/var/log/dpkg.log', and '/var/log/kern.log'. To the right of this list, there are input fields for 'Log format' (set to 'syslog'), 'Log location' ('/var/ossec/logs/active-responses.log'), and 'Redirect output to this socket' ('agent'). At the bottom right of the dashboard, there are 'SETTINGS JSON XML' links.



Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

13. Make a screen capture showing the real time monitoring setting for the blog folder.

The screenshot shows the Wazuh web interface with the URL [https://dashboard/app/wazuh#/agents?g=filter:\(refreshInterval:status:vWorkstation\(mn-3dh,to:now\)\)&_a=\(column:_source\).filters:@\(index:wazuh-alerts-*\).interval:@\(value:1m\).sort:@\(order:desc\).size:10](https://dashboard/app/wazuh#/agents?g=filter:(refreshInterval:status:vWorkstation(mn-3dh,to:now))&_a=(column:_source).filters:@(index:wazuh-alerts-*).interval:@(value:1m).sort:@(order:desc).size:10). The page title is "Investigating and Responding to Security Incidents (4e)". The top navigation bar includes "Wazuh", "Firewall", "Blog", "TheHive", "One or more installed add-ons cannot be verified and have been disabled.", "Learn More", "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!", "Refresh Firefox...", "Update available", "Download", and "Dismiss". The main menu on the left is "wazuh. ▾ Agents web1 Configuration". Under "Configuration", the "Selected item" is "/home/user/blog". The configuration table contains the following rows:

	Selected item	/home/user/blog
Enable realtime monitoring	yes	
Enable auditing (who-data)	no	
Report file changes	no	
Perform all checksums	no	
Check sums (MD5 & SHA1)	no	
Check MD5 sum	yes	
Check SHA1 sum	yes	
Check SHA256 sum	yes	
Check files size	yes	
Check files owner	yes	
Check files groups	yes	
Check files permissions	yes	
Check files modification time	yes	

16. Make a screen capture showing the default group configuration.

The screenshot shows the Wazuh web interface with the URL <https://dashboard/app/wazuh#/m/manager/?tab=groups>. The page title is "Investigating and Responding to Security Incidents (4e)". The top navigation bar includes "Wazuh", "Firewall", "Blog", "TheHive", "One or more installed add-ons cannot be verified and have been disabled.", "Learn More", "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!", "Refresh Firefox...", "Update available", "Download", and "Dismiss". The main menu on the left is "wazuh. ▾ Management Groups". The configuration editor shows the XML content of "agent.conf of default group":

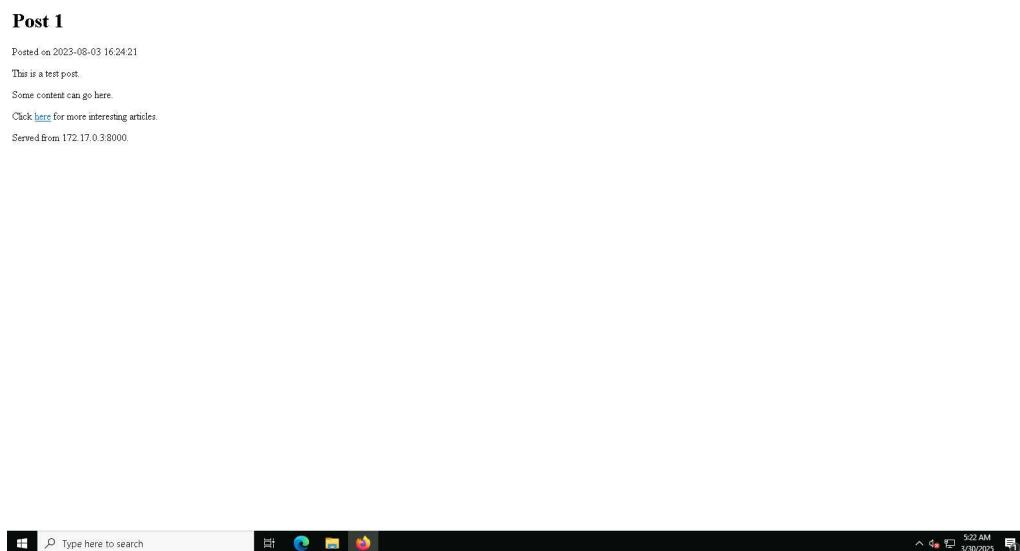
```
<!-- shared agent configuration here -->
<agent_config>
  <agent_config name="web1">
    <sychcheck>
      <directories realtime="yes">/home/user/blog</directories>
    </sychcheck>
  </agent_config>
<agent_config name="web2">
  <sychcheck>
    <directories realtime="yes">/home/user/blog</directories>
  </sychcheck>
</agent_config>
```

Part 2: Identify the scope of a reported issue

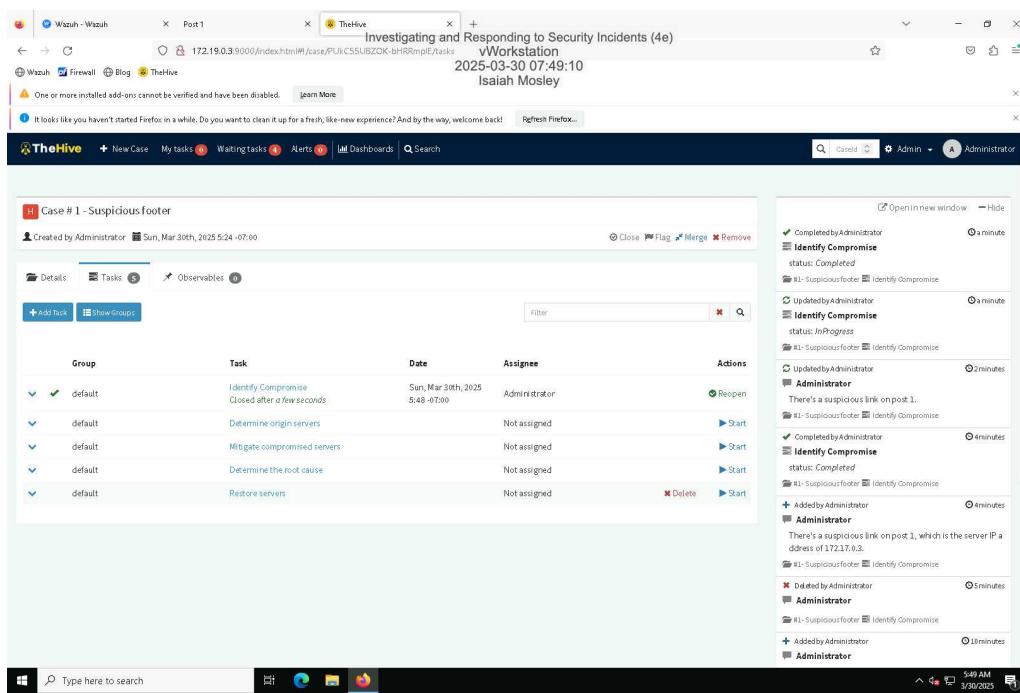
Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

6. Make a screen capture showing the blog post with the suspicious content.



17. Make a screen capture showing the log entry in the Identify compromise tab.



Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

27. Make a screen capture showing the Determine origin servers log entry.

The screenshot shows a Windows desktop with a Firefox browser window open to TheHive platform. The browser title bar reads "Wazuh - Wazuh" and "Port 2" and "TheHive". The main content area displays a case titled "Case # 1 - Suspicious footer". The log entry for "Determine origin servers" is highlighted. The log details are as follows:

Added by	Administrator	Open in new window	Time
Updated by	Administrator	Administrator	10 minutes ago
Task	Determine origin servers		
Status	InProgress		
Notes	There's a suspicious link on post 1.		
Comments	Administrator: There's a suspicious link on post 1.		
Logs	Servers from 172.17.0.3 on port 1 and 2 are delivering compromised content.		

Part 3: Contain and Investigate the event

16. Make a screen capture showing the log entry for the Mitigate compromised servers task.

The screenshot shows a Windows Command Prompt window titled "Administrator: cmd". The user has run several commands to check for updates, view the nginx configuration, and edit the sites-enabled file. The user then restarts the nginx service using systemctl. The terminal output is as follows:

```
To check for new updates run: sudo apt update
Last login: Fri Sep 1 19:57:46 2023 from 172.19.0.10
user@router:~$ cat -n /etc/nginx/nginx.conf
 1
 2 worker_processes auto;
 3 pid /run/nginx.pid;
 4 include /etc/nginx/modules-enabled/*.conf;
 5
 6 events {
 7     worker_connections 768;
 8 }
 9
10 http {
11     sendfile on;
12     tcp_nopush on;
13     tcp_nodelay on;
14     keepalive_timeout 65;
15     types_hash_max_size 2048;
16     server_tokens off;
17     gzip on;
18
19     include /etc/nginx/mime.types;
20     default_type application/octet-stream;
21
22     access_log /var/log/nginx/access.log;
23     error_log /var/log/nginx/error.log;
24
25     include /etc/nginx/conf.d/*.conf;
26     include /etc/nginx/sites-enabled/*;
27 }
28
29
user@router:~$ ls /etc/nginx/sites-enabled
default
user@router:~$ cat -n /etc/nginx/sites-enabled/default
 1
 2 upstream blog {
 3   server 172.17.0.2:8080;
 4   server 172.17.0.3:8080;
 5 }
 6
 7 server {
 8   listen 80;
 9
10   location / {
11     proxy_pass http://blog;
12   }
13 }
14
15
user@router:~$ sudo vim /etc/nginx/sites-enabled/default
[sudo] password for user:
user@router:~$ sudo systemctl restart nginx
sudo: systemctl: command not found
user@router:~$ sudo systemctl restart nginx
Job for nginx.service failed because the control process exited with error code.
see 'systemctl status nginx.service' and 'journalctl -xe' for details.
user@router:~$ exit
logout
Connection to 172.17.0.4 closed.
C:\Users\Administrator\Desktop>
```

Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

24. Make a screen capture showing at least the first three events in the list.

The screenshot shows the Wazuh Integrity monitoring interface. The main panel displays a table of events with the following columns: Time, syscheck.path, syscheck.event, rule.description, rule.level, and rule.id. The events listed are:

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Nov 11, 2024 @ 15:16:04.935	/home/user/blog/blog.e	modified	Integrity checksum change d.	7	568
Nov 11, 2024 @ 15:16:04.888	/home/user/blog/blog.n	deleted	File deleted..	7	563
Nov 11, 2024 @ 15:16:04.857	/home/user/blog/blog.e	modified	Integrity checksum change d.	7	568

34. Make a screen capture showing the full_log field from the SSH event.

The screenshot shows the Wazuh Security events interface. The main panel displays a table of events with the following columns: _index, agent.id, agent.ip, agent.name, data.dsra_data, data.pvdf, data.script, data.airport, data.scrutinizer, data.dsra, data.dsra_id, decoderifcomment, decodername, decoderparent, full_log, id, inputtype, location, managername, predecoder.hostname, predecoder.program_name, predecoder.timestamp, rule_identities, and rule_id. One event is highlighted in yellow, showing the full_log field which contains the following log entry:

```
Nov 11 23:16:03 router sshd[3861]: Accepted publickey for user from 10.0.0.2 port 35658 ssh2: RSA SHA256:vcVexGxE2M0zn/BAq/HnPgbfWq78BTOT3YQubu8IA
```

Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

38. Make a screen capture showing the list of key fingerprints.

The screenshot shows a Windows desktop environment. In the foreground, a terminal window titled "Administrator: cmd" displays the following command-line session:

```
Administrator: cmd
 4 include /etc/nginx/modules-enabled/*.conf;
5 events {
6     worker_connections 768;
7 }
8
9 http {
10     sendfile on;
11     tcp_nopush on;
12     tcp_nodelay on;
13     keepalive_timeout 65;
14     types_hash_max_size 2048;
15     server_tokens off;
16     gzip on;
17
18     include /etc/nginx/mime.types;
19     default_type application/octet-stream;
20
21     access_log /var/log/nginx/access.log;
22     error_log /var/log/nginx/error.log;
23
24     include /etc/nginx/conf.d/*.conf;
25     include /etc/nginx/sites-enabled/*;
```

Below this, another terminal window titled "Administrator: ls /etc/nginx/sites-enabled" shows the contents of the directory:

```
Administrator: ls /etc/nginx/sites-enabled
default
user@user:~$ cat -n /etc/nginx/sites-enabled/default
 1
 2 upstream blog {
 3   server 172.17.0.2:8000;
 4   server 172.17.0.3:8000;
 5 }
 6
 7 server {
 8   listen 80;
 9
10   location / {
11     proxy_pass http://blog;
12   }
13 }
14
15 user@user:~$ sudo vim /etc/nginx/sites-enabled/default
[sudo] password for user:
user@user:~$ sudo systemctl restart nginx
sudo: systemctl: command not found
user@user:~$ sudo systemctl restart nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xe" for details.
user@user:~$ exit
logout
Connection to 172.17.0.4 closed.
```

Further down, a file explorer window shows a file named "authorized_keys" in the "authorized_keys" folder. The file contains the following content:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAw...  
-----END RSA PRIVATE KEY-----
```

At the bottom of the terminal window, there is a message: "user@user:~\$ 100% 622 40.5KB/s 00:00".

In the background, a browser window titled "TheHive" is open, showing a task list with several items. One item is expanded, showing its details. The task is titled "Determine the root cause" and has the following description: "On Nov 11, 2024 @ 15:16:04.935 was the suspected time a nd date of the compromise. The source IP is 10.0.0.2 autho rized_keys and user keys were affected. Someone logged i n from the source IP 10.0.0.2 as an enduser via a WebServer and utilized the SSHK ...".

47. Make a screen capture showing the log entry for the Determine the root cause task.

The screenshot shows a Windows desktop environment. A browser window titled "TheHive" is open, displaying a task list. One task, "Determine the root cause", is expanded, showing its details. The task was created by "Administrator" on "Sun, Mar 30th, 2025 5:24 -07:00". The description of the task is as follows:

On Nov 11, 2024 @ 15:16:04.935 was the suspected time a nd date of the compromise. The source IP is 10.0.0.2 autho rized_keys and user keys were affected. Someone logged i n from the source IP 10.0.0.2 as an enduser via a WebServer and utilized the SSHK ...

The task has several sub-tasks listed under it:

- Completed by Administrator: "Determine the root cause" (status: Completed)
- Added by Administrator: "Administrator" (status: InProgress)
- Completed by Administrator: "Mitigate compromised servers" (status: Completed)
- Added by Administrator: "Administrator" (status: InProgress)
- Completed by Administrator: "Mitigate compromised servers" (status: Completed)

Part 4: Recover from the incident

Investigating and Responding to Security Incidents (4e)

Ethical Hacking, Fourth Edition - Lab 09

13. Make a screen capture showing the log entry for the Restore Servers task.

The screenshot shows the TheHive interface with a log entry for the 'Restore Servers' task. The log entry details are as follows:

Task	Description	Status	Owner	Created	Last Updated
Restore servers	Use backups to restore the origin servers to proper functionality. Log all changes.	InProgress	Administrator	2025-03-30 09:31:53	Sun, Mar 30th, 2025 7:31:47:000
Determine the root cause	status: Completed owner: Administrator	Completed	Administrator	2025-03-30 09:31:53	Sun, Mar 30th, 2025 7:31:47:000
Mitigate compromised servers	status: Completed owner: Administrator	Completed	Administrator	2025-03-30 09:31:53	Sun, Mar 30th, 2025 7:31:47:000
Determine the root cause	status: InProgress owner: Administrator	InProgress	Administrator	2025-03-30 09:31:53	Sun, Mar 30th, 2025 7:31:47:000
Mitigate compromised servers	status: InProgress owner: Administrator	InProgress	Administrator	2025-03-30 09:31:53	Sun, Mar 30th, 2025 7:31:47:000

Applied Learning

Part 1: Investigate the root cause using log files

4. Make a screen capture showing the different file hashes

```
Administrator cmd
1624 SHA256:cVx0o3R2Qn/B4q/HMP26fWqJ3BTOT3Y2qubv8JA developer (RSA) [Investigating and Responding to Security Incidents (46)]
C:\Users\Administrator\Desktop>scp web2:/home/user/blog/blog.elf . [VMWorkstation]
2025-03-30 09:35:27
C:\Users\Administrator\Desktop>scp backup/web2/blog.elf web2:/home/user/blog/blog.new
blog.elf
Isaiah Mosley
100% 8276kB 24.0MB/s 00:00

C:\Users\Administrator\Desktop>ssh web2 /home/user/blog/update.sh

C:\Users\Administrator\Desktop>ssh web2
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-155-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System Information as of Sun 30 Mar 2025 02:22:42 PM UTC

 System Load: 0.57 Processes: 149
 Usage of /: 37.98% of 14.66GB Users logged in: 0
 Memory usage: 57% IP# address for ens192: 172.17.0.4
 Swap usage: 0% IP# address for ens224: 102.168.253.162

155 updates can be installed immediately,
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New releases "22.04.5 LTS" available.
Run "do-release-upgrade" to upgrade to it.

less: log: sun Mar 28 13:07:56 2025 From [172.17.0.10
user@outer:~$ sudo vim /etc/nginx/sites-enabled/default
[sudo] password for user:
user@outer:~$ sudo systemctl restart nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xe" for details.
user@outer:~$ exit
logout
connection to 172.17.0.4 closed.

C:\Users\Administrator\Desktop>powershell -c "Get-FileHash blog.elf"

Algorithm Hash Path
---- ----
SHA256 6620fF85CC53300B802B401508FA3A11FE12712598006E56737C8F1F106E555FC C:\Users\Administrator\Desktop\blog.elf

C:\Users\Administrator\Desktop>powershell -c "Get-FileHash backup\web2\blog.elf"

Algorithm Hash Path
---- ----
SHA256 E1449803B412BE0B1ED49C0FC8A3E174AC08208CD4AE6F70EA896C896DE14E59EE C:\Users\Administrator\Desktop\backup\web2\blog.elf

C:\Users\Administrator\Desktop>
```

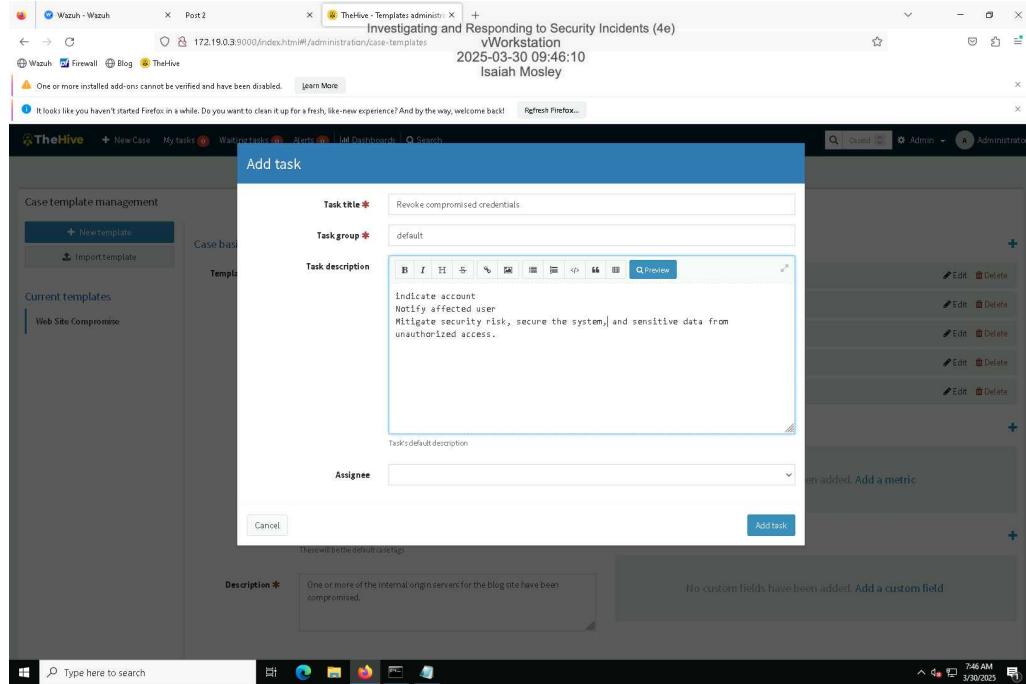
8. Make a screen capture showing all the events found using the previous two commands.

Investigating and Responding to Security Incidents (4e)

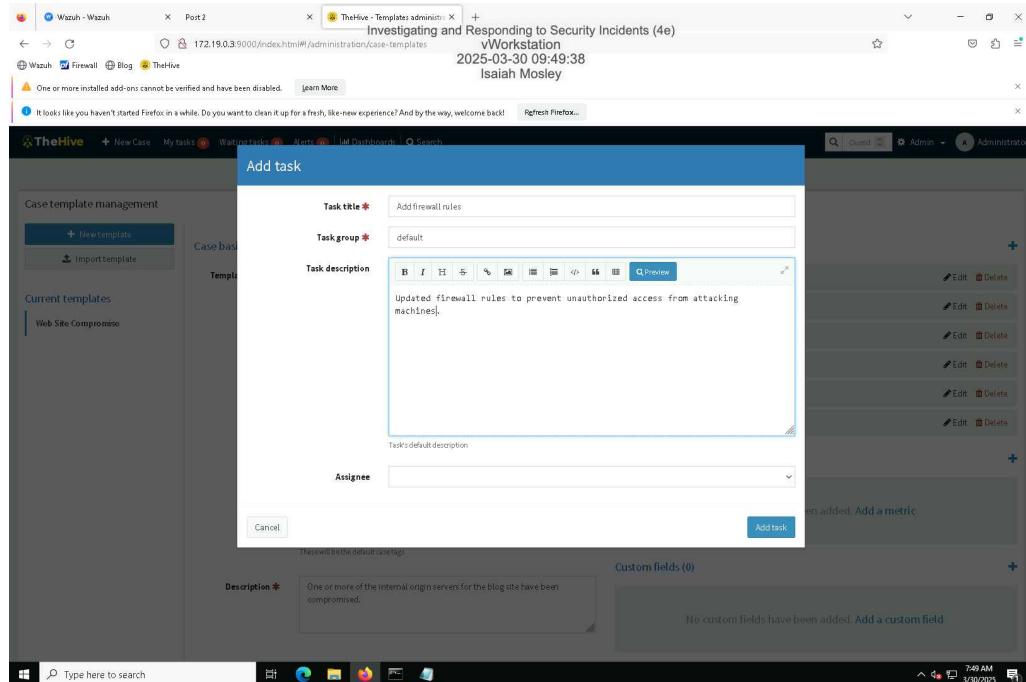
Ethical Hacking, Fourth Edition - Lab 09

Part 2: Add remediation tasks

6. Make a screen capture showing your task description.



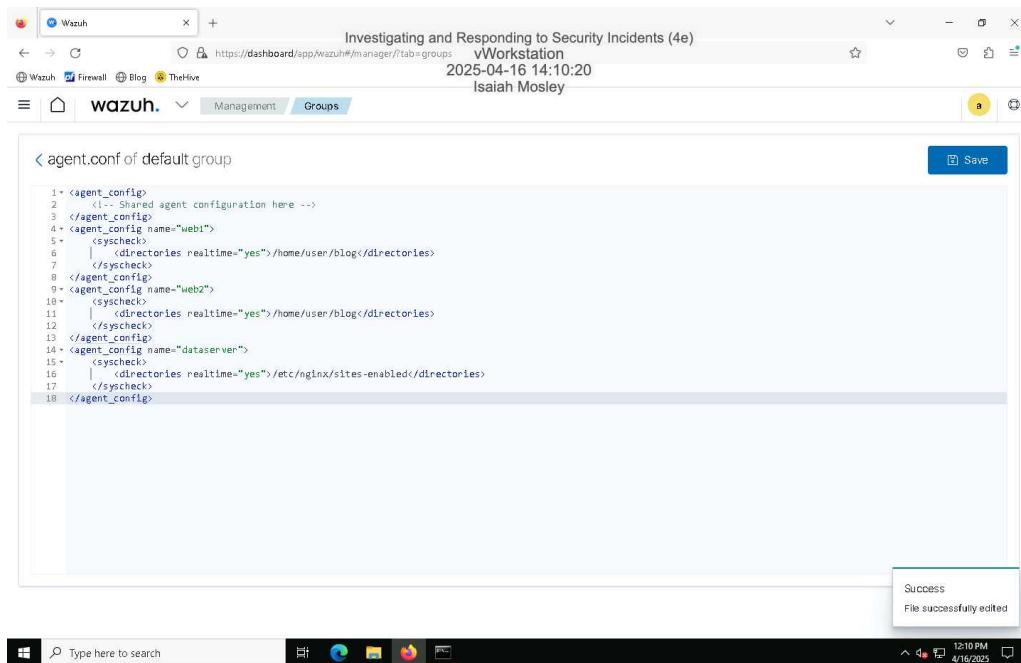
9. Make a screen capture showing your task description.



Challenge and Analysis

Part 1: Add real time monitoring for nginx load balancer configuration

1. Make a screen capture showing the updated group configuration.



```
< agent.conf of default group >
1< agent_config>
2  |<!-- Shared agent configuration here -->
3 </agent_config>
4< agent_config name="web1">
5  |<syscheck>
6  |  |<directories realtime="yes">/home/user/blog</directories>
7  |</syscheck>
8 </agent_config>
9< agent_config name="web2">
10 |<syscheck>
11 |  |<directories realtime="yes">/home/user/blog</directories>
12 |</syscheck>
13 </agent_config>
14< agent_config name="dataserver">
15 |<syscheck>
16 |  |<directories realtime="yes">/etc/nginx/sites-enabled</directories>
17 |</syscheck>
18 </agent_config>
```

Part 2: Disable the compromised key

1. Document all changes made to the SSH configurations and any other steps required.

The compromised credentials was deleted from WebServer01, WebServer02, and the DataServer. I logged into each server using the the following commands : ssh user@webserver01, ssh user@webserver02, ssh @172.17.0.4. Next i entered the command nano ~/.ssh/authorized_keys to edit each servers "authorized_keys" file and removed the compromise keys. Afterwards, i press Ctrl +X to exit editing, pressed Y to confirm save, and enter to confirm the filename.These steps removed the compromised keys and prevents unauthorized access. No additional changes to the system was needed.