Linux Fundamentals CTF - Operation Mamba

Scenario Setup:

The international spy agency has lost one of its valuable assets, codenamed "MAMBA". Your mission, should you choose to accept it, is to track down MAMBA. You have gained access to a server suspected of having information related to MAMBA's whereabouts. Use your skills to complete this mission and save MAMBA.

\*\*Step 1: Initial Access\*\*

Create a new user named "agent" with password "mission":

sudo adduser agent

# Enter the password as 'mission' and fill in the user info as needed

\*\*Step 2: File Permissions\*\*

Create a hidden file with no read permissions, it contains the first clue to MAMBA's whereabouts:

touch /home/agent/.hiddenfile

echo "Flag{mamba\_hidden}" > /home/agent/.hiddenfile

chmod 000 /home/agent/.hiddenfile

\*\*Step 3: Process Inspection\*\*

Start a process (tail on a text file) running in the background, it contains the second clue to MAMBA's whereabouts:

touch /home/agent/Flag{mamba\_on\_the\_move}.txt

nohup tail -f /home/agent/Flag{mamba\_on\_the\_move}.txt &

\*\*Step 4: Log Analysis\*\*

Add an unusual entry to the system logs, it contains the third clue to MAMBA's whereabouts:

echo "Flag{mamba\_spotted}" | sudo tee -a /var/log/syslog

\*\*Step 5: Hidden Directory\*\*

Create a hidden directory and add the fourth clue to MAMBA's whereabouts:

mkdir /home/agent/.hidden\_directory

echo "Flag{mamba\_hideout\_found}" > /home/agent/.hidden\_directory/flag.txt

\*\*Step 6: User History\*\*

Add an unusual command to the user history. The command contains the fifth clue to MAMBA's whereabouts:

echo "Flag{mamba\_moves\_tracked}" >> /home/agent/.bash\_history

\*\*Step 7: File Ownership\*\*

Create a file owned by 'root' in the home directory. The file contains the sixth clue to MAMBA's whereabouts:

sudo touch /home/agent/root\_file.txt

sudo chown root:root /home/agent/root\_file.txt

echo "Flag{mamba\_claimed\_new\_territory}" | sudo tee /home/agent/root\_file.txt

sudo chmod 000 /home/agent/root\_file.txt

\*\*Step 8: Crontab Inspection\*\*

Add a suspicious cron job. The job contains the seventh clue to MAMBA's whereabouts:

echo '\* \* \* \* \* echo "Flag{mamba\_scheduled\_to\_move}" >> /home/agent/cron\_script.sh' | crontab

\*\*Step 9: The Lost Message\*\*

Scatter the parts of a message (eighth clue) in different directories:

echo "Flag{" > /tmp/message\_part1.txt

echo "mamba\_" > /etc/message\_part2.txt

echo "message\_retrieved}" > /var/message\_part3.txt

\*\*Step 10: Environment Variables\*\*

Add a clue to the environment variables:

echo 'export FLAG="Flag{mamba\_breathes\_in\_the\_wild}"' >> /home/agent/.bashrc

\*\*Step 11: The Port Listener\*\*

Open a port listener that sends a clue:

echo "Flag{mamba\_calls\_for\_help}" | nc -lk 8888 &

\*\*Step 12: Decipher The Message\*\*

Create a file with a base64 encoded message (final clue):

echo "Flag{mamba\_location\_decoded}" | base64 > /home/agent/encoded\_message.txt