Defensive System Training - 1

LAB: LINUX HOST INTERROGATION

SSgt Thomas Blauvelt
32 WPS/DOA | NELLIS AFB, NEVADA

Defensive System Training – 1: Linux Host Interrogation

CONTENTS

Lab: Threat Hunting with Linux Command Line 2

Overview 2

Procedures 3

Scenario Setup 3

Step 1. Initial Access 4

Step 2. File Permissions 4

Step 3. Process inspection 4

Step 4. Log Analysis 4

Step 5. Hidden Directory 4

Step 6. User History 4

Step 7. File Ownership 5

Step 8. Crontab Inspection 5

Step 9. The Lost Message 5

Step 10. Environment Variables 5

Step 11. The Port Listener 5

Step 12. Decipher The Message 5

Symbols Table

Symbol	Name	Meaning
✅	**Note**	Detailed information that is required to fully understanding the concept or to be able to execute a procedure but is not necessarily related to a key learning objective.
💡	**Learning Point**	Information related to key learning objectives.
⚠	**Warning**	Important information related to safety and security.
✋	**Raise Hand**	Raise your hand for instructor assistance. This is often used at critical points to validate your understanding of the material.

LAB: THREAT HUNTING WITH LINUX COMMAND LINE

OVERVIEW

Summary: The purpose of this lab is to acquire the necessary knowledge and skills to effectively navigate Linux command line. Throughout the course of this lab, you will be creating the flags that you'll be required to present during the assessment.

Outcomes: By the end of the lab, you will be able to perform the following:

- Perform:
  - Adding user accounts
  - Viewing and editing file permissions
  - Inspecting processes
  - Viewing and analyzing log files
  - Viewing hidden directories
  - Viewing command line history
  - Viewing and editing file ownership
  - Viewing and editing cron jobs
  - Viewing and editing environment variables
  - Using netcat, start a local listener
  - Viewing base64 encoded files and text

PROCEDURES

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.

Defensive System Training – 1: Linux Host Interrogation

STEP 1. INITIAL ACCESS

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

1. sudo adduser agent
    a. # 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:

1. touch /home/agent/.hiddenfile
2. echo "Flag{mamba_hidden}" > /home/agent/.hiddenfile
3. 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:

1. touch /home/agent/Flag{mamba_on_the_move}.txt
2. 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:

1. 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:

1. mkdir /home/agent/.hidden_directory
2. 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:

1. 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:

1. sudo touch /home/agent/root_file.txt
2. sudo chown root:root /home/agent/root_file.txt
3. echo "Flag{mamba_claimed_new_territory}" | sudo tee /home/agent/root_file.txt
4. 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:

1. 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:

1. echo "Flag{" > /tmp/message_part1.txt
2. echo "mamba_" > /etc/message_part2.txt
3. echo "message_retrieved}" > /var/message_part3.txt

STEP 10. ENVIRONMENT VARIABLES

Add a clue to the environment variables:

1. 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:

1. echo "Flag{mamba_calls_for_help}" | nc -lk 8888 &

STEP 12. DECIPHER THE MESSAGE

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

1. echo "Flag{mamba_location_decoded}" | base64 > /home/agent/encoded_message.txt