Introduction To Honeypots

EX-NO-09

AIM:

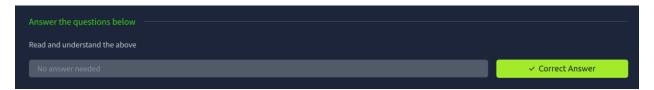A guided room covering the deployment of honeypots and analysis of botnet activities.

PROCEDURE:

- Task 1 Introduction
- Task 2 Types of Honeypots
- Task 3 Cowrie Demo
- Task 4 Cowrie Logs
- Task 5 Attacks Against SSH
- Task 6 Typical Bot Activity
- Task 7 Identification Techniques
- Task 8 SSH Tunnelling
- Task 9 Recap and Extra Resources

Task 1 Introduction :

Answer the questions below

Deploy the demo machine

No answer needed	✓ Correct Answer

Task 2 Types of Honeypots :

Answer the questions below

Read and understand the above

No answer needed	✓ Correct Answer

Task 3 Cowrie Demo :

Answer the questions below

Try running some commands in the honeypot

No answer needed	✓ Correct Answer

Create a file and then log back in is the file still there? (Yay/Nay)

Nay	✓ Correct Answer

Task 4 Cowrie Logs :

Answer the questions below

Have a look through the logs and see how the activity from the last task has been recorded by the system.

| No answer needed | ✓ Correct Answer |

Task 5 Attacks Against SSH :

Answer the questions below

How many passwords include the word "password" or some other variation of it e.g "p@ssw0rd"

| 15 | ✓ Correct Answer | ♀ Hint |

What is arguably the most common tool for brute-forcing SSH?

| hydra | ✓ Correct Answer |

What intrusion prevention software framework is commonly used to mitigate SSH brute-force attacks?

| Fail2Ban | ✓ Correct Answer |

Task 6 Typical Bot Activity :

Answer the questions below

What CPU does the honeypot "use"?

| Intel(R) Core(TM) i9-11900KB CPU @ 3.30GHz | ✓ Correct Answer | ♀ Hint |

Does the honeypot return the correct values when `uname -a` is run? (Yay/Nay)

| Nay | ✓ Correct Answer | ♀ Hint |

What flag must be set to pipe `wget` output into bash?

| -O | ✓ Correct Answer |

How would you disable bash history using `unset` ?

| unset HISTFILE | ✓ Correct Answer |

Task 7 Identification Techniques :

Answer the questions below

What brand of device is the bot in the first sample searching for? (BotCommands/Sample1.txt)

| Mikrotik | ✓ Correct Answer |

What are the commands in the second sample changing? (BotCommands/Sample2.txt)

| root password | ✓ Correct Answer |

What is the name of the group that runs the botnet in the third sample? (BotCommands/Sample3.txt)

| Outlaw | ✓ Correct Answer |

Task 8 SSH Tunnelling :

Answer the questions below

What application is being targetted in the first sample? (Tunnelling/Sample1.txt)

WordPress   ✓ Correct Answer

Is the URL in the second sample malicious? (Tunnelling/Sample2.txt) (Yay/Nay)

Nay   ✓ Correct Answer

Task 9 Recap and Extra Resources :

Answer the questions below

Read and understand the above

No answer needed   ✓ Correct Answer

RESULT:

Thus the Introduction To Honeypots is completed using tryhackme platform.