

EXERCISE 9

Deployment of Honeypots and analysis of botnet activities

Aim: To deploy honeypots and analyze botnet activities in a controlled environment to understand attacker behaviors and automated exploitation techniques.

Introduction To Honeypots
A guided room covering the deployment of honeypots and analysis of botnet activities
Medium 60 min

Share your achievement Start AttackBox Help Save Room 334 Options

Room completed (100%)

- 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

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

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

Result: Successfully set up honeypots and captured real-world botnet traffic, analyzed patterns, and identified common attack signatures and behaviors.