

EX 9 : INTRODUCTION TO HONEYPOTS

AIM:

To learn about Honeypots and their working.

Problems:

room completed (4/10/19)

Task 2 ✓ Types of Honeypots

Task 3 ✓ Cowrie Demo

The Cowrie SSH Honeypot

The Cowrie honeypot can work both as an [SSH proxy](#) or as a simulated shell. The demo machine is running the simulated shell. You can log in using the following credentials:

1. IP - MACHINE_IP
2. User - root
3. Password - <ANY>

As you can see the emulated shell is pretty convincing and could catch an unprepared adversary off guard. Most of the commands work like how you'd expect, and the contents of the file system match what would be present on an empty Ubuntu 18.04 installation. However, there are ways to identify this type of Cowrie deployment. For example, it's not possible to execute bash scripts as this is a limitation of low and medium interaction honeypots. It's also possible to identify the default installation as it will mirror a Debian 5 Installation and features a user account named Phil. The default file system also references an outdated [CPU](#).

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

Room completed (100%)

Task 4 Cowrie Logs

Task 5 Attacks Against SSH

SSH and Brute-Force Attacks

By default, Cowrie will only expose SSH. This means adversaries will only be able to compromise the honeypot by attacking the SSH service. The attack surface presented by a typical SSH installation is limited so most attacks against the service will take the form of brute-force attacks. Defending against these attacks is relatively simple in most cases as they can be defeated by only allowing public-key authentication or by using strong passwords. These attacks should not be completely ignored, as there are simply so many of them that you are pretty much guaranteed to be attacked at some point.

A collection of the 200 most common credentials used against old Cowrie deployments has been left on the demo machine and can be used to answer the questions below. As you can see, most of the passwords are extremely weak. Notable entries include the default credentials used for some devices like Raspberry Pis and the Volumio Jukebox. Various combinations of '1234' and rows of keys are also commonplace.

Answer the questions below

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

Correct Answer

Hint

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

Correct Answer

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

Correct Answer

Room completed (100%)

- Perform some reconnaissance using the `uname` or `lsof` commands or by reading the contents of files like `/etc/issue` and `/proc/cpuinfo`. It's possible to change the contents of all these files so the honeypot can pretend to be a server or even an IoT toaster.
- Install malicious software by piping a remote shell script into bash. Often this is performed using `wget` or `curl` though, bots will occasionally use `FTP`. Cowrie will download each unique occurrence of a file but prevent the scripts from being executed. Most of the scripts tend to reference cryptocurrency mining in some way.
- A more limited number of bots will then perform some anti-forensics tasks by deleting various logs and disabling bash history. This doesn't affect Cowrie since all the actions are logged externally.

Bots are not limited to these actions in any way and there is still some variation in the methods and goals of bots. Run through the questions below to further understand how adversaries typically perform reconnaissance against Linux systems.

Answer the questions below

What CPU does the honeypot "use"?

Correct Answer

Hint

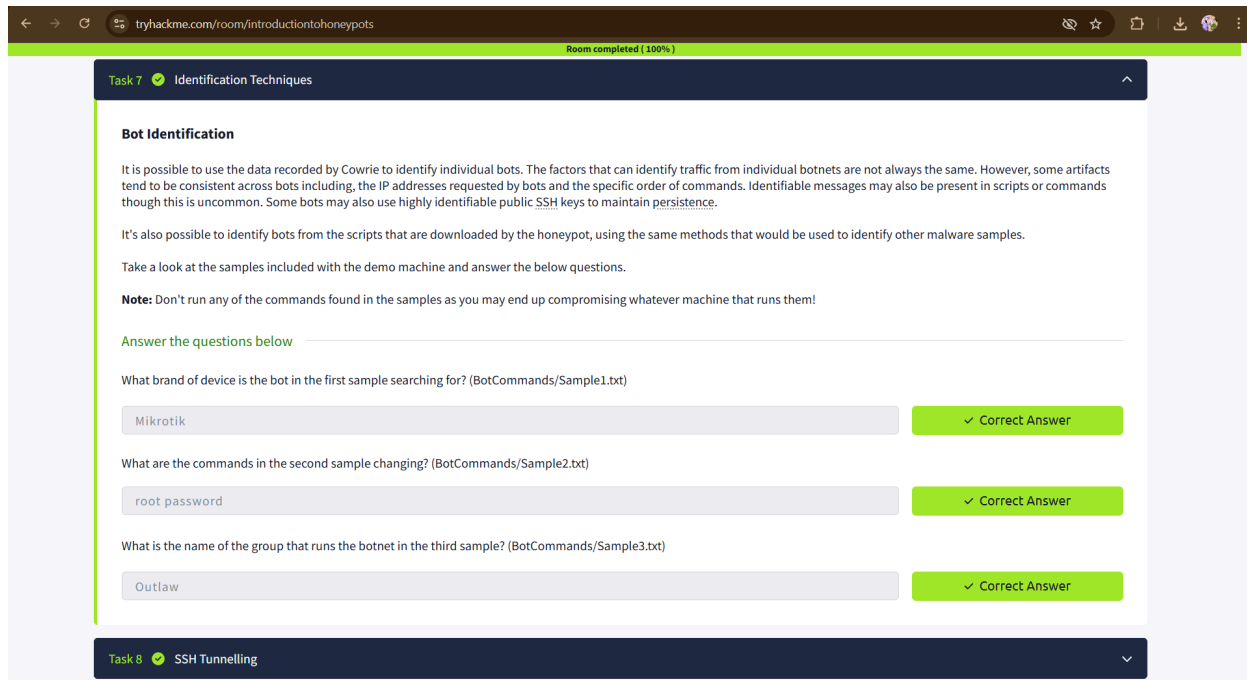
Does the honeypot return the correct values when `uname -a` is run? (Yay/Nay)

Correct Answer

Hint

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

Correct Answer



tryhackme.com/room/introductiontohoneypots

Room completed (100%)

Task 7 Identification Techniques

Bot Identification

It is possible to use the data recorded by Cowrie to identify individual bots. The factors that can identify traffic from individual botnets are not always the same. However, some artifacts tend to be consistent across bots including, the IP addresses requested by bots and the specific order of commands. Identifiable messages may also be present in scripts or commands though this is uncommon. Some bots may also use highly identifiable public SSH keys to maintain persistence.

It's also possible to identify bots from the scripts that are downloaded by the honeypot, using the same methods that would be used to identify other malware samples.

Take a look at the samples included with the demo machine and answer the below questions.

Note: Don't run any of the commands found in the samples as you may end up compromising whatever machine that runs them!

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

RESULT: Hence the experiments were done successfully.