PenTest Lab Exercise Ex0f0 – `Linux is Broken`

Goal

Exploit a linux machine using a relatively recent vulnerability

Tasks

1. Check out an Ex0f0 exercise pod.
2. Use previous information to gain ssh access to `devbox.artstailor.com`. You will be disappointed to find that the method you used previously to get root access on devbox can no longer be employed–the configuration on that machine has changed since you exploited it. Sadly, that happens in penetration testing, a computer network is not a static thing.
3. Check the linux kernel version, services, and various files on devbox to determine whether you can identify any linux vulnerabilities of which you may be aware. Understand that just because a machine appears to be vulnerable to an exploit, that does not mean that the exploit will necessarily work correctly. There is at least one vulnerability on devbox that, though it can be exploited, is different enough from what you have seen to require you to be creative.
4. Make sure to look around the file system to see if you can find any useful information that may help you now or in the future. You may be disappointed if you are looking for a key file like the ones you have seen before, but those who persist will be rewarded.
5. If you have several possible vulnerabilities you are pursuing, don't get fixated on just one. Spend some time on each vulnerability you have not totally eliminated.
6. Write a partial penetration test report.