Session 04 – Linux Privilege Escalation

Session 04 is designed to train you on the fundamentals of escalating privileges on Linux, meaning that you go from a regular user to a root user. This can often be done due to misconfigurations in servers that give users more trust than should be permitted.

Starting the Session

It should be noted that for the planned content for this session, you will require an account on TryHackMe (https://tryhackme.com/). I have specifically selected the free content on TryHackMe for this session.

If you have signed up for TryHackMe, you should be able to access the training content at https://tryhackme.com/r/room/linprivesc. You should be able to go through around half the content in the session. The TryHackMe content does give you plenty of opportunities to put the theory into practice on a number of target machines.

If you are unfamiliar with TryHackMe, I recommend looking at how to connect your computer to TryHackMe using Openvpn, instructions which can be found at https://tryhackme.com/r/access. A basic tutorial to make sure that your Openvpn software is working can be found at https://tryhackme.com/r/room/tutorial. Make sure to read the openvpn-specific information on both links.

Assorted Reading Materials

- https://book.hacktricks.xyz/
- https://gtfobins.github.io/
- https://github.com/peass-ng/PEASS-ng/blob/master/linPEAS/README.md