ComSec - Let's Think CUEHack

By Jack Orcherton

Introduction

- This presentation is more to get you thinking of ideas of what to do for the upcoming How to Build a CTF hackathon, rather than the technicalities.
- Uncreative? Same, hopefully there will be someone in you team who is (teams will be shared soon) – if not this PowerPoint should hopefully give you some inspiration.

Why Make CTF's

- Great experience for blue teaming (on what not to do).
- Reverse Psychology – understanding how things are made vulnerable can help with red teaming as well.

Starting Point

- For the event we will be releasing a blank docker file, which will have certain services available for you to make vulnerable.
- One of these will be a nginx web server on port 80.
- If this is your first CTF, ComSec recommends creating a vulnerable web server.

~~Awkward~~ People

- For those of you who are awkward, I mean like a challenge, you can do whatever you like as long as it meets the following criteria:
  - It's a hacking related CTF
  - Your team is in agreement
  - You won't blame us looking at you with blank expressions when you ask for help

I've got a web server what now?

- I'd say you need to pick a good theme/story for your challenge as it can make more interested to hack it & closer to real life. For example, which sounds better?
- Option 1 - Due to Covid-19, GCHQ has adopted a new work from home policy. Therefore they have had to make an encrypted messaging platform to send state secrets, can you decode the messages?
- Option 2 - Decode this:
- Which is better? - Straw Poll

The Exploit

- Now you have a back story, you can begin to make your machine vulnerable. To begin think of the following
  - Build your own
  - Find a good real world exploit.
  - Change the configuration of something to make it vulnerable.

Build your Own

- Most websites have similar vulnerabilities that are grouped together
- For this approach, you create your own website and deliberately introduce flaws
- For inspiration look at OWASP Top 10

- First Years – think of your php service that you created this semester… Was there anything that you did to make your platform secure? Why not try to recreate that bug? NB: don't use the exact same one you created for your CW though

Real World Exploit

- People are always finding bugs in content management systems, like Wordpress, Drupal, Moodle, Evolution...
- So hop onto the CVE website and try and replicate – maybe install an old version of the CMS

Bad Security Configurations

- A lot of vulnerabilities are due to human error (especially when they start messing around with configurations) – so grab a web server and configure it badly!
  - An example could be allowing an intern to set a very important password to solarwinds123 and including it on a public GitHub account…
  - Forgetting to turn off telnet
  - Improper session management