WE HEK YOU

UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

Getting you, yes you, ready to win Big Hak

What to expect next week

- **Free pizza**
- On each table we will have a list of the people on that team, find your name and join the team
  - In case some people don’t come we may re-organise teams slightly on the day
- When the CTF starts you will be told how to access the challenges
  - Challenges will require you have your own laptop, and some will require a Kali Virtual-Machine (see our setup guide)

Challenge categories

`web`	Exploit services that would normally be found on the web
`rev`	Reverse engineer and exploit binary programs
`prog`	Write custom software to overcome challenges
`embedded`	Hack a hardware device
`revenge`	Get back into an already exploited system

How to score points

- When you solve a challenge you will get a flag in the format “cybersoc{s0me_t3xt_h3r3}”, submit this flag to get points
- If you get stuck on challenges don’t give up, always remember to ask your team for help
  - Don’t be afraid to ask questions, while we might not be able to directly help a team we might be able to guide you in the right direction

ඇ Topics

- See our slides on: cybersoc.cf/resources
  - WEP
  - Reverse engineering
  - SQLi + XSS
  - LFI + SSTI + SSRF + Prototype pollution
  - Linux essentials + PrivEsc
- Any questions feel free to ask today, or in discord at any time

WEP (What is it)?

- Wired Equivalent Privacy
- Old (no-longer recommended to be used) Wireless authentication protocol
- Tools:
  - aircrack-ng

Reverse engineering

- Taking a binary and attempting to understand what it is doing without the original source code
  - May also involve patching binaries to change what they do
- Tools:
  - Cutter
  - Ghidra
  - IDA

Web attacks

- SQLi (SQL Injection)
  - Injecting SQL commands into the database
- XSS (Cross-Site Scripting)
  - Injecting javascript code into some website
- LFI (Local File Inclusion)
  - Accessing some file on a server you're not supposed to
- SSTI (Server-Side Template Injection)
  - Exploiting templating engines to run code
- SSRF (Server-Side Request Forgery)
  - Exploiting a server to send network requests within it's internal networks
- XXE (XML External Entity Injection)
  - Importing custom objects via magic XML
- Prototype Pollution
  - Overwriting properties on the global object in javascript

Linux PrivEsc

- The basics
  - Weird cronjobs (`cat /etc/crontab`)
  - Sudo privs (`sudo -l`)
  - Setuid bins (`find / -type f -perm /6000 2>/dev/null`)
- Check for exploits you can use on gtfobins
- Automated scanners:
  - Linpeas.sh
  - meterpreter

Okay wow, that’s quite a lot of stuff

- CTFs cover a broad range of topics and require you to use a range of skill-sets
  - This doesn’t mean you have to know everything going in, often the best way to learn stuff is by doing it (google is your best friend)
  - Don’t worry if you don’t know some or any of this stuff, the main goal is to have fun and maybe learn some things along the way
- As mentioned before there are lots of resources to help
  - Our slides
  - Hack tricks (CTF cheat-sheet)

Want a hoodie?

Fill out the form here

UNIVERSITY OF LIVERPOOL
CYBER SECURITY SOCIETY

cybersoc.cf

See you there (or else)

Book ticket here

- Get some practice
  - Internal ctf ctf.cybersoc.cf
  - CTF Walk-trough's & Challenges tryhackme.com
  - Hard CTF Challenges hackthebox.com
  - Upcoming public CTFs ctftime.org