MEETUP 0x07 INTRODUCTION TO CTF NEPSE

SYDNEY

Capture the Flag (CTF)

- Hacker's Game
- Exploits/Enumerate to get the flag and capture the points.
- Basic step to get into the world of hacking.
- Helps one understand different tools used.
- Helps initiate the hacker mindset in you.

PICO CTF?

- Basic CTF Challenges.
- Aimed for beginners to all level of hackers.
- Introduces different tools on linux used for hacking.
- Introduces basic command line usage.

https://2018game.picoctf.com

Tools/Techniques for CTF

- strings → Used to extract all the text (strings) from whatever you are using this with.
- grep → Used to search specific pattern/text in a file or command usage.
- Netcat (nc) → TCP/IP swiss army knife;) (thats what the manual says and is:p). Used to open/receive and print/write different data from one connecting node to another in a network.

Contd...

- file → Used to determine the filetype;). Don't always rely on extensions. Verify it.
- hash-identifier → Used to identify what type of hash/encoding is the given data is.
- binwalk → Find whether the binary file has anything embedded
- Steganography → A technique to hide data in files like audio,images.
- Ciphers → Used to encode data to not let attacker understand the real data in it.

Ciphers

- Some classical ciphers normally used in CTFs are :
- Caesar ciphers → Data is encrypted by shifting the characters by number you assign.
- Example: Hi there (shift 1) → Ij uifsf (shifted characters one times ahead).
- Vignere Cipher → Data is encrypted by using a series of interwoven caesar ciphers.

https://www.dcode.fr/

PentesterLab

A online hacking lab created to help one get into the field of hacking.

Has lots of video and text based tutorials for the exercises.

Teaches from the basics of Unix Command Line to new exploits.

Let the game Begin

Winner will receive subscription of Pentesterlab Pro for 2months' access.