VulnUniversity

* Deploy The Machine
  + No answer needed
* Reconnaissance
  + Scan the box, how many ports are open?
    - Nmap -sV 10.10.121.69
    - 6

Text

Description automatically generated

* + What version of the squid proxy is running on the machine?
    - 3.5.12
  + How many ports will nmap scan if the flag -p-400 was used?
    - 400
  + Using the nmap flag -n what will it not resolve?
    - DNS
  + What is the most likely operating system this machine is running?
    - Ubuntu
  + What port is the web server running on?
    - 3333
* Location directories using GoBuster
  + Run GoBuster

Text

Description automatically generated

* + What is the directory that has an upload form page?
    - /internal/
* Compromise the Webserver
  + Run this attack what extension is allowed?
    - .phtml
  + Upload a reverse php shell
    - Download from <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>
    - Edit the ip to be attackbox ip
    - Rename .phtml
    - Open listener on attackbox (nc -lvnp 8899)
    - Upload reverse shell and navigate to location of shell
      * http://10.10.133.204:3333/internal/uploads/shell\_name.phtml
    - check connection

Text

Description automatically generated

* + What is the name of the user who manages the webserver?
    - bill
  + What is the user flag?
    - 8bd7992fbe8a6ad22a63361004cfcedb

Graphical user interface

Description automatically generated

* Privilege Escalation
  + One the system, search for all SUID files. What file stands out?
    - /bin/systemctl

A screenshot of a computer

Description automatically generated with medium confidence

* + Become root and get the last flag (/root/root.txt)
    - GTFObins and search for systemctl
    - Graphical user interface, application

      Description automatically generated
    - a58ff8579f0a9270368d33a9966c7fd5