

BUUCTF在线评测之Linux Labs 1

原创

轻落青雨 于 2022-03-02 16:21:45 发布 3575 收藏 2

分类专栏: [BUUCTF在线评测](#) 文章标签: [linux](#) [ssh](#) [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_49182737/article/details/123232476

版权



[BUUCTF在线评测](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

这个测试没什么技术要求, 只要了解ssh以及linux系统即可

Linux Labs

1

2020年10月24日 更新: 目前所有靶机均能直接访问互联网。

点击启动靶机可以启动一台安装好了 LAMP 的机器。

并且这台机器位于靶机内网, 所有动态靶机均可直接通过主机名访问这台机器。

但由于目前一个账户只能同时启动一台靶机, 您如果有需要建议浏览器开一个隐私窗口, 注册一个新账号来启动这个靶机。

ssh 用户名: root 密码: 123456 地址和端口为动态分配的。

靶机信息

剩余时间: 10781s

node4.buuoj.cn:29788

<http://906f11f7-b9af-4341-9063-66232a70ce9e.node4.buuoj.cn:81>

[销毁靶机](#) [靶机续期](#) [已解锁](#)

Flag

提交

CSDN @轻落青雨

点击启动靶机, 出现的页面

点击所给的http链接, 得到如下界面 Index of

Index of /

[Name](#) [Last modified](#) [Size](#) [Description](#)

Apache/2.4.18 (Ubuntu) Server at 906f11f7-b9af-4341-9063-66232a70ce9e.node4.buuoj.cn Port 81

CSDN @轻落青雨

这个页面啥也没有，没啥用
返回第一个界面，给出了ssh

ssh 用户名：root 密码：123456 地址和端口为动态分配的。

以及映射地址和端口（这个地址+端口是随机的）

node4.buuoj.cn:29788

所以直接启动ssh链接即可
however!!! 这里要 banter 一下BUUCTF网站的这个Linux Labs 1测试中的这句话

并且这台机器位于靶机内网，所有动态靶机均可直接通过主机
名访问这台机器。

这句话，不仅是说主机可以访问，且只有主机可以访问!!!

As we all know，我们最常用的Windows OS没有自带的ssh连接插件!!! 所以如果要用Windows做这个，需要另行安装一个ssh程序。而kali linux里自带ssh，但我相信大部分kali linux是存在于虚拟机中的，而用虚拟机中的kali linux中的浏览器上做这个实验简直就是煎熬...

所以我用了Windows来做这个实验

下了一个ssh程序。。。

[ssh下载链接](#)

然后安装。。。

装好之后，然后开始

CMD 输入ssh 指令格式：ssh -p 端口 用户名@地址

然后输入密码

```
ssh -p 29788 root@node4.buuoj.cn
```

```
123456
```

```
Microsoft Windows [版本 10.0.18363.1556]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\86157>ssh -p 29788 root@node4.buuoj.cn
The authenticity of host '[node4.buuoj.cn]:29788 ([117.21.200.166]:29788)' can't be established.
ECDSA key fingerprint is SHA256:X9Br7UuSD7eoX2tSxw10RVfhpK3iiUW5dELgEVd5oro.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[node4.buuoj.cn]:29788, [117.21.200.166]:29788' (ECDSA) to the list of known hosts.
root@node4.buuoj.cn's password:
root@out:~#
```

CSDN @轻落青雨

连上了

然后查找

```
Flag
```

输入ls

```
root@out:~# ls
root@out:~#
```

啥也没有，证明刚连上就进入的文件夹是个空文件夹

返回上级目录看看

```
cd ...
```

再ls

```
root@out:~# cd ..
root@out:/# ls
bd_build  boot  etc      get-pip.py  lib  media  opt  root  sbin  sys  usr
bin       dev  flag.txt  home        lib64  mnt    proc  run   srv   tmp  var
root@out:/#
```

有个flag.txt

打开康康

```
cat flag.txt
```

```
flag{4c176048-1cb7-41fe-b0a5-28dbc43e79d2}
```

得到flag然后交差。