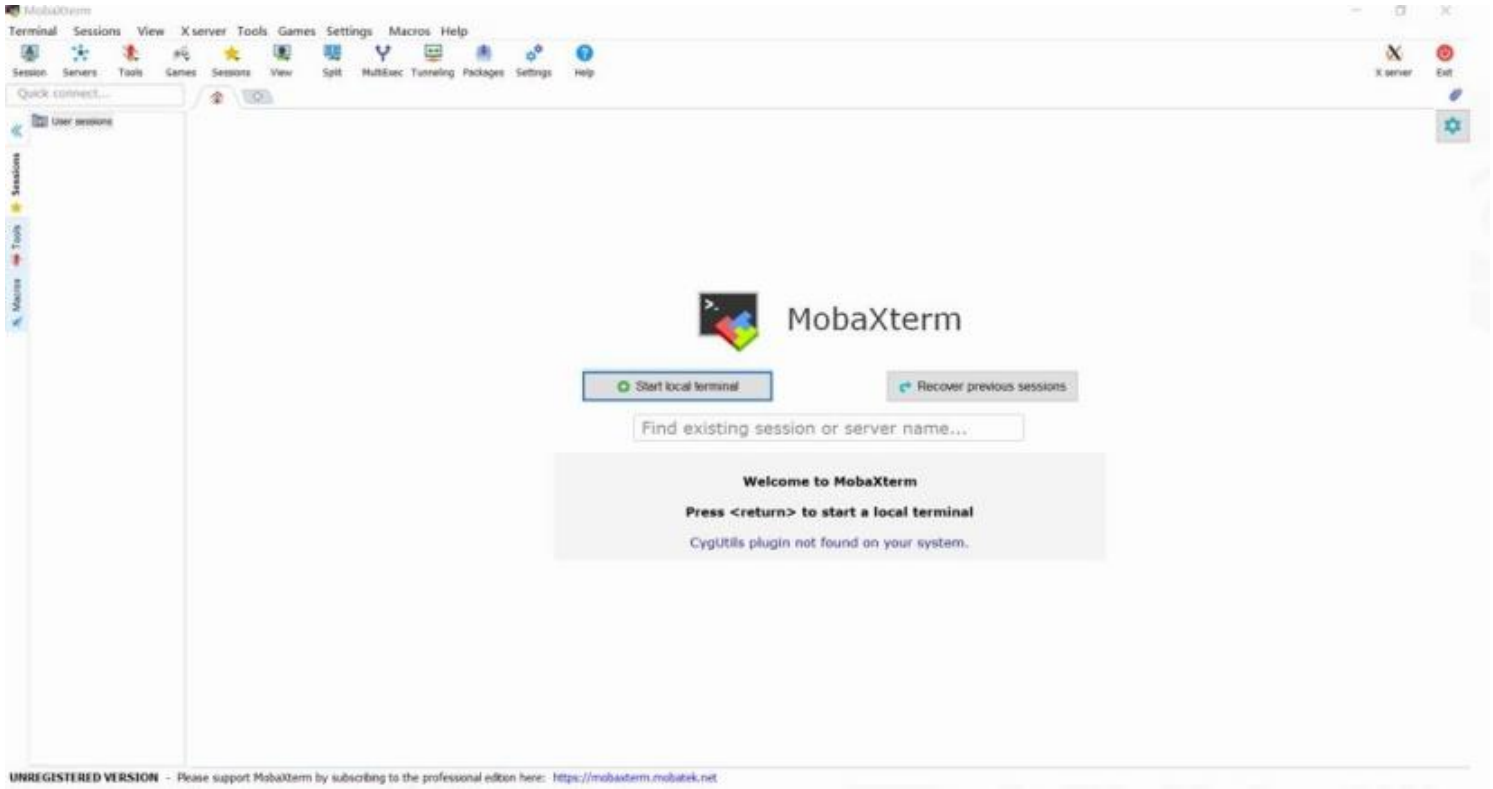
AWD（Attack With Defence）模式比赛技巧

第7课 AWD运维

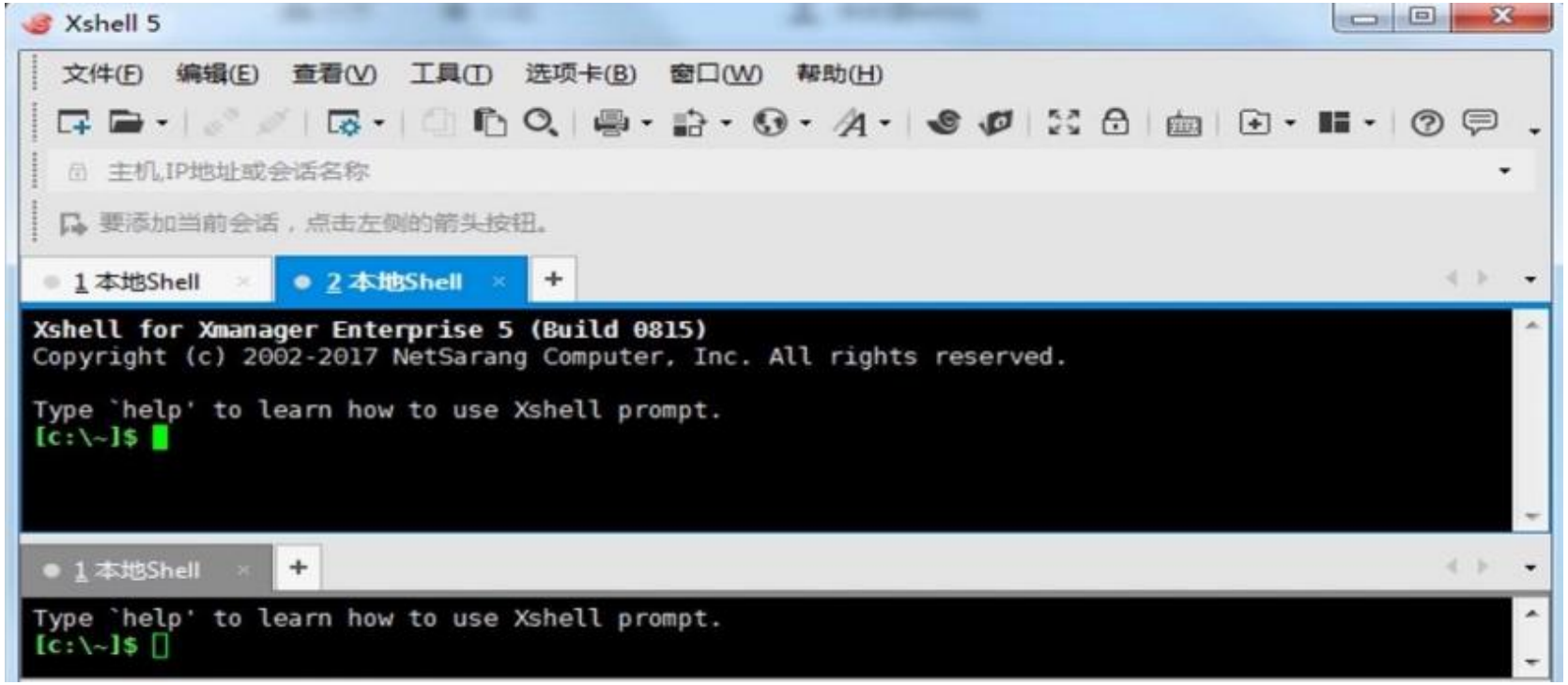
mobaxterm

(https://mobaxterm.mobatek.net/)



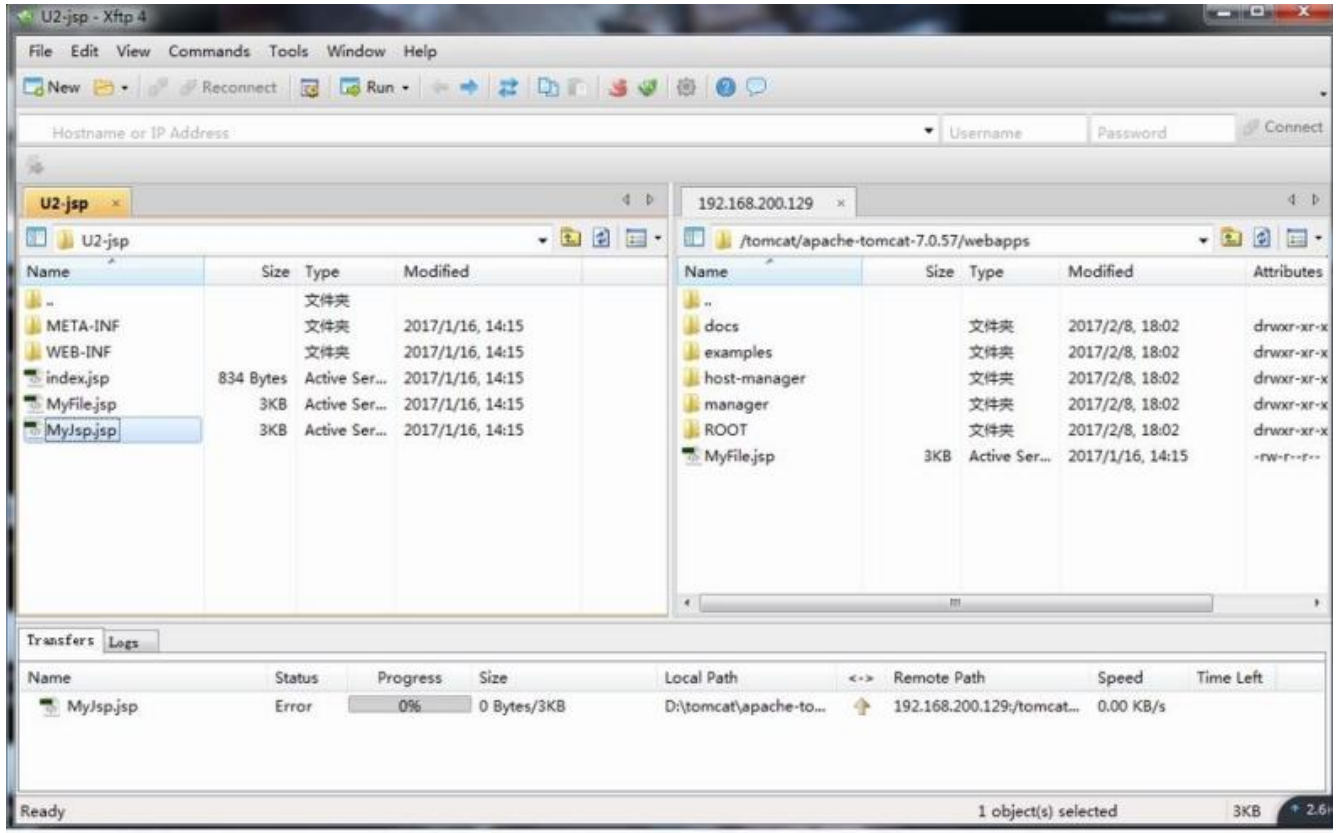
xshell

(https://xshell.en.softonic.com/)



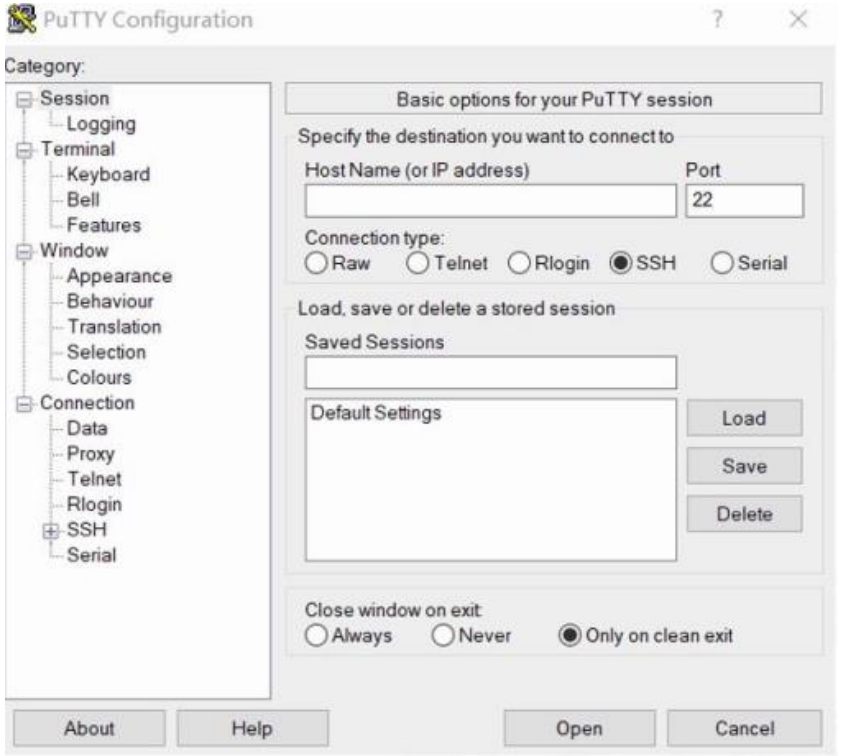
工具

xftp


U2-jsp - Xftp 4
File Edit View Commands Tools Window Help
New Reconnect Run
Hostname or IP Address
Username
Password
Connect
U2-jsp
192.168.200.129
/tomcat/apache-tomcat-7.0.57/webapps
Name Size Type Modified
META-INF 文件夹 2017/1/16, 14:15
WEB-INF 文件夹 2017/1/16, 14:15
index.jsp 834 Bytes Active Ser... 2017/1/16, 14:15
MyFile.jsp 3KB Active Ser... 2017/1/16, 14:15
MyJsp.jsp 3KB Active Ser... 2017/1/16, 14:15
Name Size Type Modified Attributes
docs 文件夹 2017/2/8, 18:02 drwxr-xr-x
examples 文件夹 2017/2/8, 18:02 drwxr-xr-x
host-manager 文件夹 2017/2/8, 18:02 drwxr-xr-x
manager 文件夹 2017/2/8, 18:02 drwxr-xr-x
ROOT 文件夹 2017/2/8, 18:02 drwxr-xr-x
MyFile.jsp 3KB Active Ser... 2017/1/16, 14:15 -rw-r--r--
Transfers Logs
Name Status Progress Size Local Path <-> Remote Path Speed Time Left
MyJsp.jsp Error 0% 0 Bytes/3KB D:\tomcat\apache-to... 192.168.200.129:/tomcat... 0.00 KB/s
Ready
1 object(s) selected
3KB

putty

(https://www.chiark.greenend.org.uk/~sgtatham/putty/)



filezilla

- **https://www.wikiwand.com/zh-sg/FileZilla**

python一把梭

ssh是一个协议，OpenSSH是其中一个开源实现，paramiko是Python的一个库，实现了SSHv2协议(底层使用cryptography)。

我们可以使用Paramiko在Python代码中直接使用SSH协议对远程服务器执行操作，而不是通过ssh命令对远程服务器进行操作。

Paramiko

- **https://github.com/paramiko/paramiko**
- **Python SSHv2 协议实现**
- **安装**
- **pip install paramiko**
- **使用**

非工具

```
import paramiko

##1.创建一个ssh对象client =paramiko.SSHClient()

#2.解决问题：如果之前没有，连接过的ip,会出现选择yes或者no的操作，##自动选择yes

client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

#3.连接服务器

client.connect(hostname='172.17.68.1',port=22,username='root',password='123456')

#4.执行操作

stdin,stdout,stderr =client.exec_command('hostname')

#5.获取命令执行的结果result=stdout.read().decode('utf-8')print(result)

#6.关闭连接

client.close()
```

工具

```
def sshConnect(CTFname, i):
    WebWorkPath = CTFname + '/' + str(i) + '/'
    ConfigFilePath = WebWorkPath + '/' + 'Config' + '/' + 'ssh.txt'
    my_ssh = open(ConfigFilePath, 'r').read().split(',')
    IP, port, username, password, pkeyfile, RemoteFilePath = my_ssh[0], int(my_ssh[1]), my_ssh[2], my_ssh[3], my_ssh[4], \
                                                             my_ssh[5]
    MysqlUsername = ''
    MysqlPassword = ''
    a = Back.AWD(IP=IP, port=port, username=username, password=password, pkeyfile=pkeyfile, WebWorkPath=WebWorkPath,
                 RemoteFilePath=RemoteFilePath, MysqlUsername=MysqlUsername, MysqlPassword=MysqlPassword)
    a.startup()
    return a
```

基本的运维linux指令

passwd username修改用户ssh密码

mysql -uawd -p123465

set password for username@localhost =password(xxx')修改数据库密码

打包备份web源码，细小文件传输太耗费时间

备份数据库

要将主服务的目录及文件权限最小化(满足自己的运维需要即可)

目录监控

Inotify操作系统提供的一组API,用于监控文件系统产生的事件

例如:

文件访问　文件创建　文件写入并关闭　文件移动.....

使用pyinotify

监控创建的新文件

偷梁换柱

明明已经getshell了，cat/flag提交为什么不对?

利用命令别名(alias)

alias get_flag='python -c "import hashlib;import time;print \"flag{%s}\"%(hashlib.md5(str(time.time())).hexdigest())""

alias curl='python -c"_import_(\"sys\").stdout.write(\"flag{9%s}\\n\"%(_import_(\"hashlib\").md5(\"\"join([_import_(\"random\").choice(import__(\"string\").letters)for i in range(0x10)])).hexdigest()))""

WAF

谢谢观赏