POST EXPLOITATION:

Banner Grabbing, raw connections and webserver interaction

Service banners are often used by system administrators for inventory taking of systems and services on the network. The service banners identify the running service and often the version number too. Banner grabbing is a technique to retrieve this information about a particular service on an open port and can be used during a penetration test for performing a vulnerability assessment. When using Netcat for banner grabbing you actually make a raw connection to the specified host on the specified port. When a banner is available, it is printed to the console. Let's see how this works in practice.

Netcat banner grabbing

The following command is used the grab a service banner (make a raw connection to a service):

nc [ip address][port]

Let's try this on the FTP service on Metasploitable 2 which is running on port 21:

nc 192.168.100.100 21

nc [ip][port]is used to make a raw connection to the port which will return a service banner when it's available.

As we can see there is a vsFTPD service running on port 21. Have a look at the service enumeration tutorial if you want to learn more about this subject.

Netcat raw connection

To demonstrate how a raw connection works we will issue some FTP commands after we're connected to the target host on the FTP service. Let's see if anonymous access is allowed on this FTP server by issuing the USER and PASS command followed by anonymous.

```
root@kali:~# nc 192.168.100.108 21
220 (vsFTPd 2.3.4)
USER anonymous
331 Please specify the password.
PASS anonymous
230 Login successful.
pwd
257 "/"
help
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
```

Interaction with the FTP service over a raw connection.

This example demonstrates how to grab a banner and how to setup and use a raw data connection. In this example we've used an FTP service but this also works on other services such as SMTP and HTTP services.

Web server interaction

Netcat can also be used to interact with webservers by issuing HTTP requests. With the following command we can grab the banner of the web service running on Metasploitable 2:

nc 192.168.100.108 80

And then run this HTTP request:

HEAD / HTTP/1.0

```
root@kali:~# nc 192.168.100.108 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 29 Oct 2016 10:46:02 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```

Apache webserver banner.

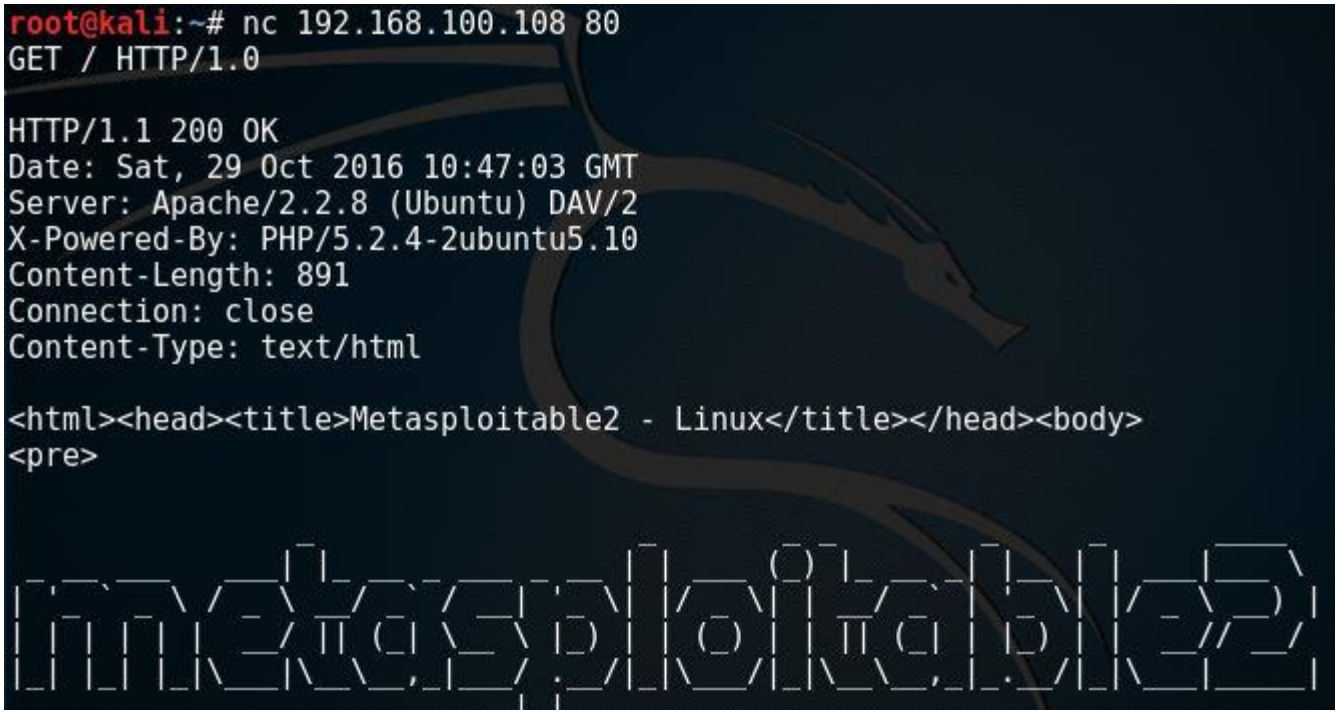
The webserver responds with the server banner: Apache/2.2.8 (Ubuntu) DAV/2 and the PHP version.

To retrieve the top level page on the webserver we can issue the following command:

nc 192.168.100.108 80

And then run this HTTP request:

GET / HTTP/1.0



Webserver page.

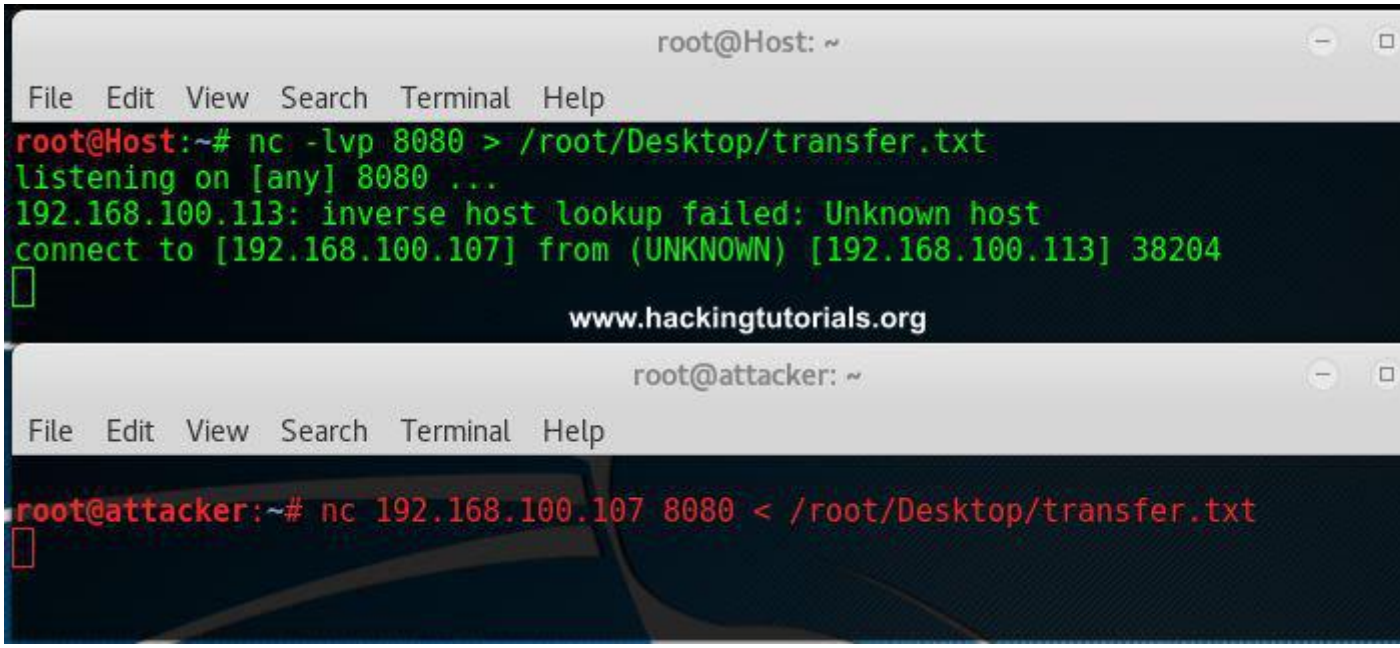
File transfers with Netcat

In this example we will be using a Netcat connection to transfer a text file. Let's assume we have remote command execution on the target host and we want to transfer a file from the attack box to the host. First we would need to set up a listener on the target host and connect to it from the attack box. We will be using port 8080 for this purpose and we safe the file to the desktop:

nc -lvp 8080 > /root/Desktop/transfer.txt

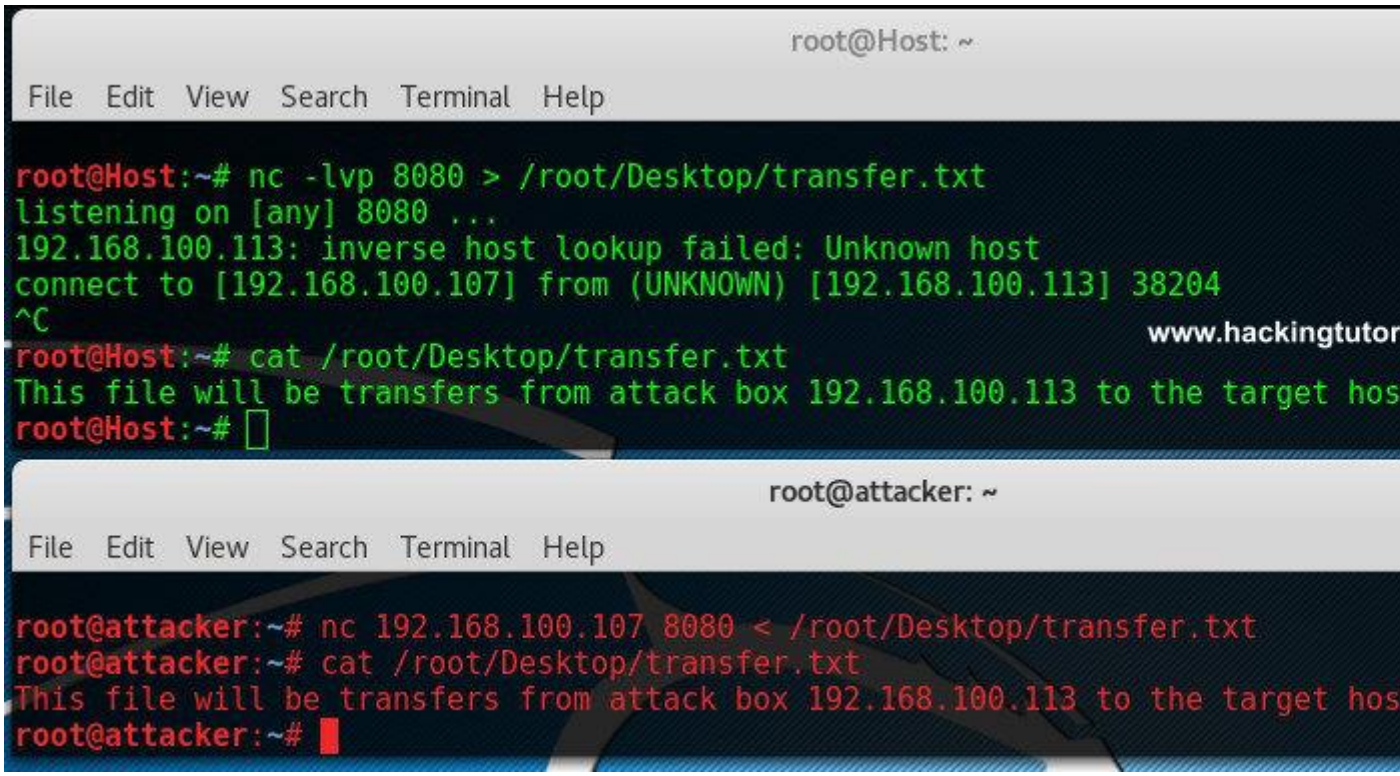
On the attack box we connect to port 8080 and send a file name transfer.txt:

nc 192.168.100.107 8080 < /root/Desktop/transfer.txt



Netcat File transfer

Than we hit control + c and cat the contents of the file on both the attack box and target host.



File was transferred from the host to the target.

As we can see here the contents of the files are equal which means it has been transferred from the attack box to the target host.