Hacking with Netcat part 1: The Basics

 6

BY **HACKING TUTORIALS** ON NOVEMBER 3, 2016**NETWORKING**

Netcat is a great network utility for reading and writing to network connections using the TCP and UPD protocol. Netcat is often referred to as the Swiss army knife in networking tools and we will be using it a lot throughout the different tutorials on Hacking Tutorials. Most common use for Netcat when it comes to hacking is setting up reverse and bind shells, piping and redirecting network traffic, port listening, debugging programs and scripts and banner grabbing. In this tutorial we will be learning how to use the basic features from Netcat such as:

- Banner grabbing
- Raw connections
- Webserver interaction
- File transfers

We will demonstrate these techniques using a couple virtual machines running Linux and through some visualization. The hacking with Netcat tutorials will be divided in the following 3 parts:

- Hacking with Netcat part 1: The Basics
- Hacking with Netcat part 2: Bind and Reverse shells
- Hacking with Netcat part 3: Advanced Netcat techniques

Let's start with the very basics and have a look at how we can make raw data connections to grab service banners.

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.
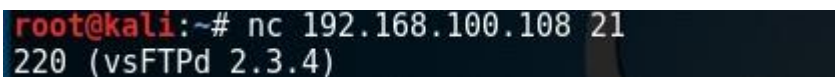
Netcat banner grabbing

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.

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:

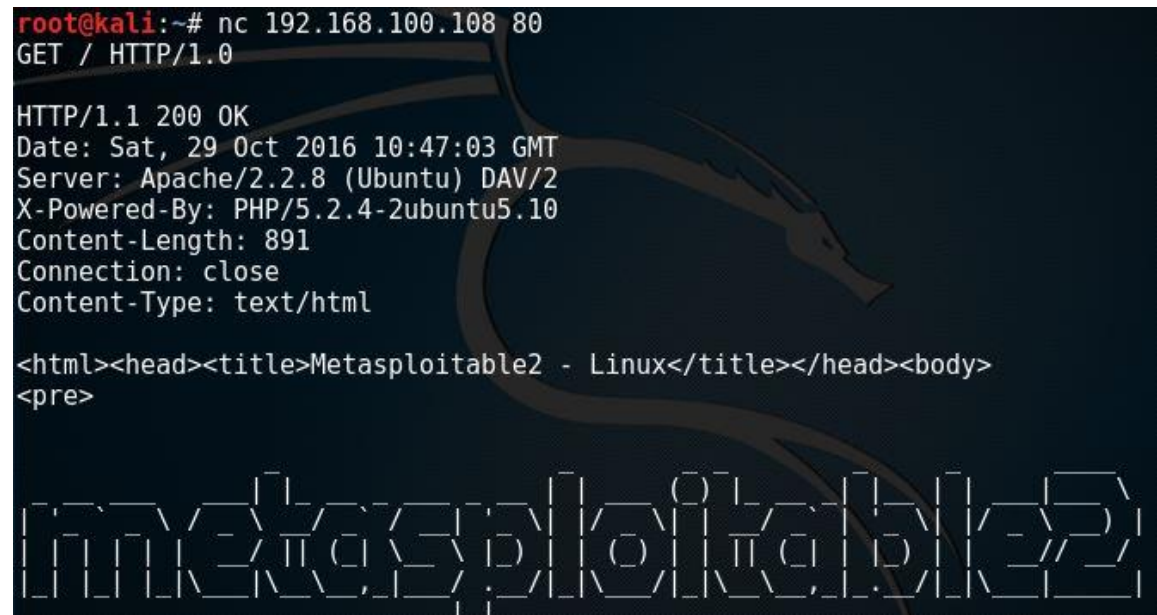HEAD / HTTP/1.0

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
```



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

HTTP/1.1 200 OK
Date: Sat, 29 Oct 2016 10:47:03 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```
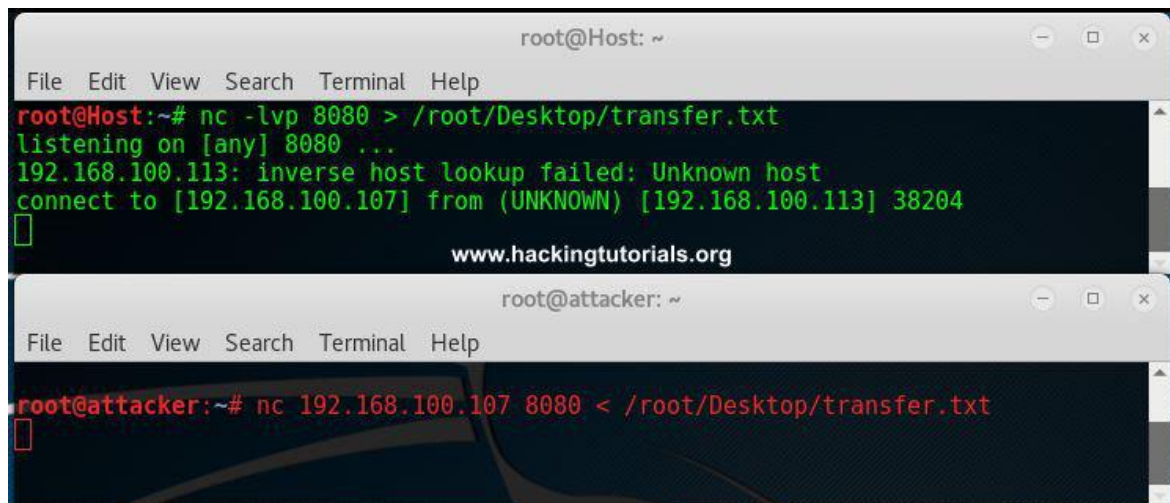
Webserver page.

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
```
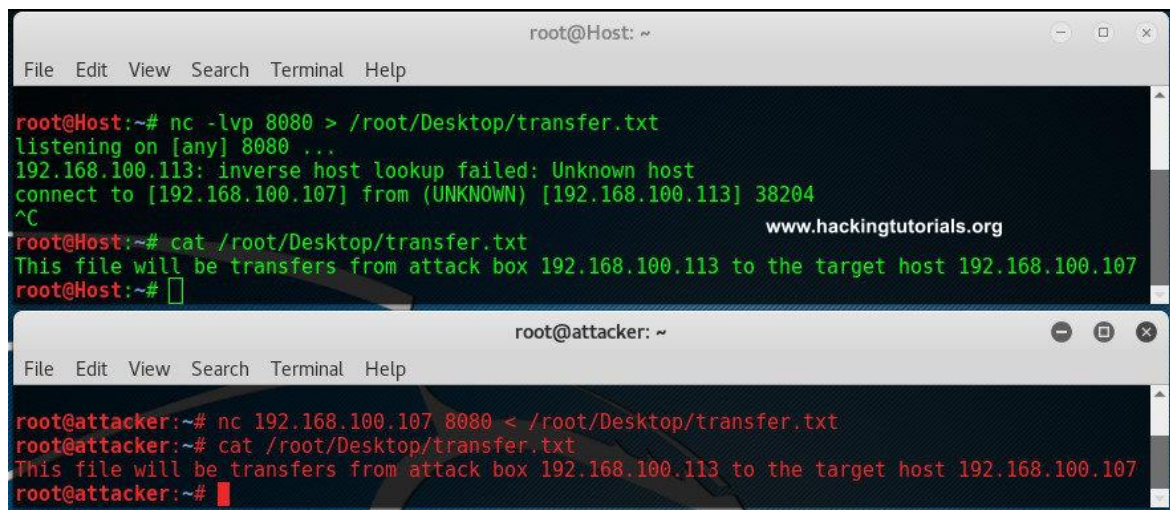
Netcat File transfer

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.

Lessons learned

In the first part of the Hacking with Netcat tutorials we have learned how to work with several basic features like raw connections, banner grabbing and file transfers. We have learned how to grab service banners which contain information about the service running on the specific port. We have also learned how to interact with services by using raw connections and Netcat. In the tutorial we have gained anonymous access to a FTP server using a raw data connection and issued some FTP commands. We have also learned how to use Netcat for interaction with a

webserver. We are able to retrieve webpages and send HTTP requests. Last but not least, we have learned how to transfer files from one box to another with Netcat.

In the following Hacking with Netcat tutorial we will be learning about how to use reverse shells and bind shells.