Lab - Introduction to Netcat

In this lab, students will become introduced to the network utility tool called Netcat. Netcat is often referred to as the Swiss army knife in networking tools. Most common use for Netcat is setting up reverse and bind shells, piping and redirecting network traffic, port listening, debugging programs, scripts, and banner grabbing. In this tutorial, students will use Netcat for the following purposes:

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

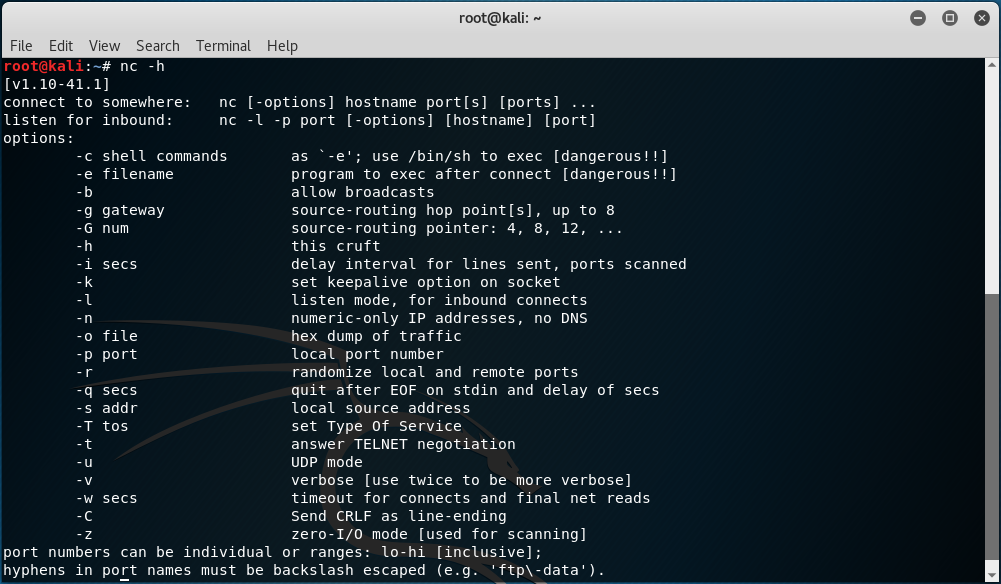
Hardware Requirements

* One virtual install of Kali Linux
* One virtual install of Metasploitable2 (My IP Address: 192.168.145.128)

Begin the lab

Open Netcat

At your Kali prompt type: nc -h



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 service on an open port and can be used during a penetration test for performing a vulnerability assessment.

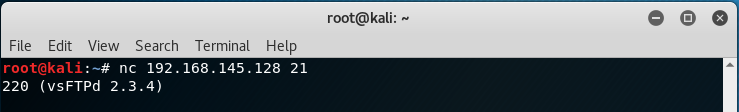
When using Netcat for banner grabbing you make a raw connection to the specified host on the specified port. When a banner is available, it is printed to the console. Let’s see how this works in practice.

Netcat banner grabbing

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

This on the FTP service on Metasploitable 2 which is running on port 21:

nc 192.168.145.128 21 (This is my Metesploitable2 address, not your!)

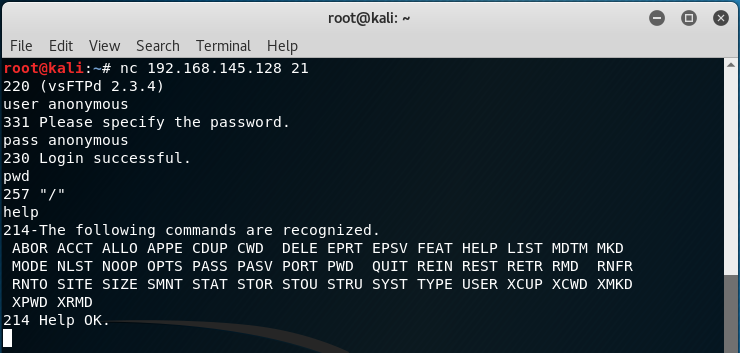


Netcat makes a raw connection to the port which will return a service banner when it’s available.

As we can see there is a vsFTPD service running on port 21.

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.



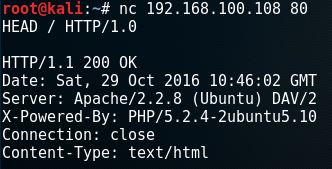
You can see that by using Netcat to see what server was running on port 21, we able to identify that the vsFTPd server version 2.3.4 was running. We were then able to interact with the FTP server using some very basic FTP commands.

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:



Apache webserver banner.

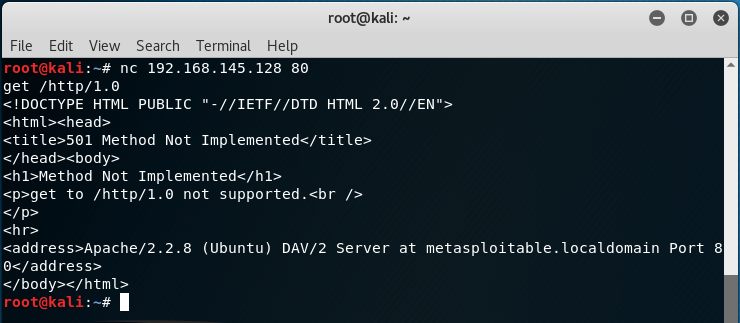
The webserver responds with the server banner: Apache/2.2.8 (Ubuntu) DAV/2 and the PHP version.

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

nc 192.168.145.128 80 (This is my Metesploitable2 address, not your!)

At the cursor, the following command:

GET / HTTP/1.0



Summary

In the first part of the Hacking with Netcat tutorials we have learned how to work with several basic features like raw connections and banner grabbing. 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.

End of the lab!