NETCAT NETWORK UTILITY

Software Guide

cloud academy
A QA COMPANY

NETCAT NETWORK UTILITY

This guide covers the basics of using Netcat, the Network Utility tool. It is often regarded as the "swiss army knife" of penetration testing.

Why use Netcat?

Netcat can be used to interact with a device that has a TCP or UDP port numbers open and can also be used for port scanning, as well as banner grabbing. It can be used to monitor and debug, as well as a backdoor into other networks.

Netcat Syntax

Netcat has a language syntax that needs to be followed in order for it to work.

The syntax follows a basic structure: [run netcat] [options] [host] [port].

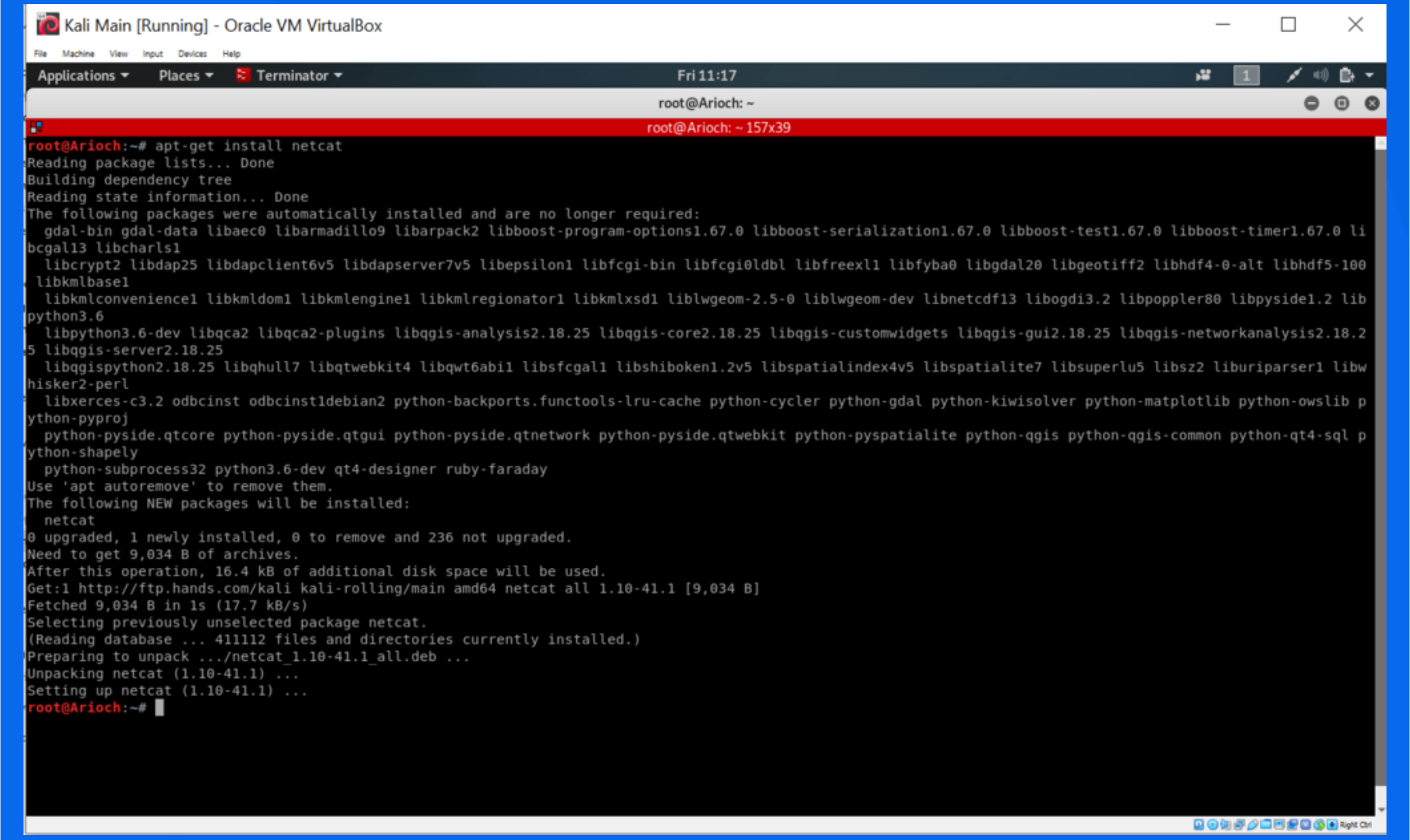
The example below would command Netcat to be set in listen mode, look at the IP address 10.1.1.102, and use port 8080.

```
netcat -l 10.1.1.102 8080
```

Install NetCat

Netcat comes pre-installed on Kali Linux. If you need to install it however, open the terminal and use the following command:

```
sudo apt-install netcat
```



Kali Main [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminator ▾
Fri 11:17
root@Arioch: ~
root@Arioch: ~ 157x39

```
root@Arioch:~# apt-get install netcat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gdal-bin gdal-data libaec0 libarmadillo9 libarpack2 libboost-program-options1.67.0 libboost-serialization1.67.0 libboost-test1.67.0 libboost-timer1.67.0 li
bcgal13 libcharls1
  libcrypt2 libdap25 libdapclient6v5 libdapserver7v5 libepsilon1 libfcgi-bin libfcgi0ldbl libfreexl1 libfyba0 libgdal20 libgeotiff2 libhdf4-0-alt libhdf5-100
 libkmlbase1
  libkmlconvenience1 libkmldom1 libkmlengine1 libkmlregionator1 libkmlxsd1 liblwgeom-2.5-0 liblwgeom-dev libnetcdf13 libogdi3.2 libpoppler80 libpyside1.2 lib
python3.6
  libpython3.6-dev libqca2 libqca2-plugins libqgis-analysis2.18.25 libqgis-core2.18.25 libqgis-customwidgets libqgis-gui2.18.25 libqgis-networkanalysis2.18.2
5 libqgis-server2.18.25
  libqgispython2.18.25 libqhull7 libqtwebkit4 libqwt6abi1 libsfcgal1 libshiboken1.2v5 libspatialindex4v5 libspatialite7 libsuperlu5 libsz2 liburiparser1 libw
hisker2-perl
  libxerces-c3.2 odbcinst odbcinst1debian2 python-backports.functools-lru-cache python-cycler python-gdal python-kiwisolver python-matplotlib python-owslib p
ython-pyproj
  python-pyside.qtcore python-pyside.qtgui python-pyside.qtnetwork python-pyside.qtwebkit python-pyspatialite python-qgis python-qgis-common python-qt4-sql p
ython-shapely
  python-subprocess32 python3.6-dev qt4-designer ruby-faraday
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 236 not upgraded.
Need to get 9,034 B of archives.
After this operation, 16.4 kB of additional disk space will be used.
Get:1 http://ftp.hands.com/kali kali-rolling/main amd64 netcat all 1.10-41.1 [9,034 B]
Fetched 9,034 B in 1s (17.7 kB/s)
Selecting previously unselected package netcat.
(Reading database ... 411112 files and directories currently installed.)
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
root@Arioch:~# 
```

NETCAT NETWORK UTILITY

Sanity Checking

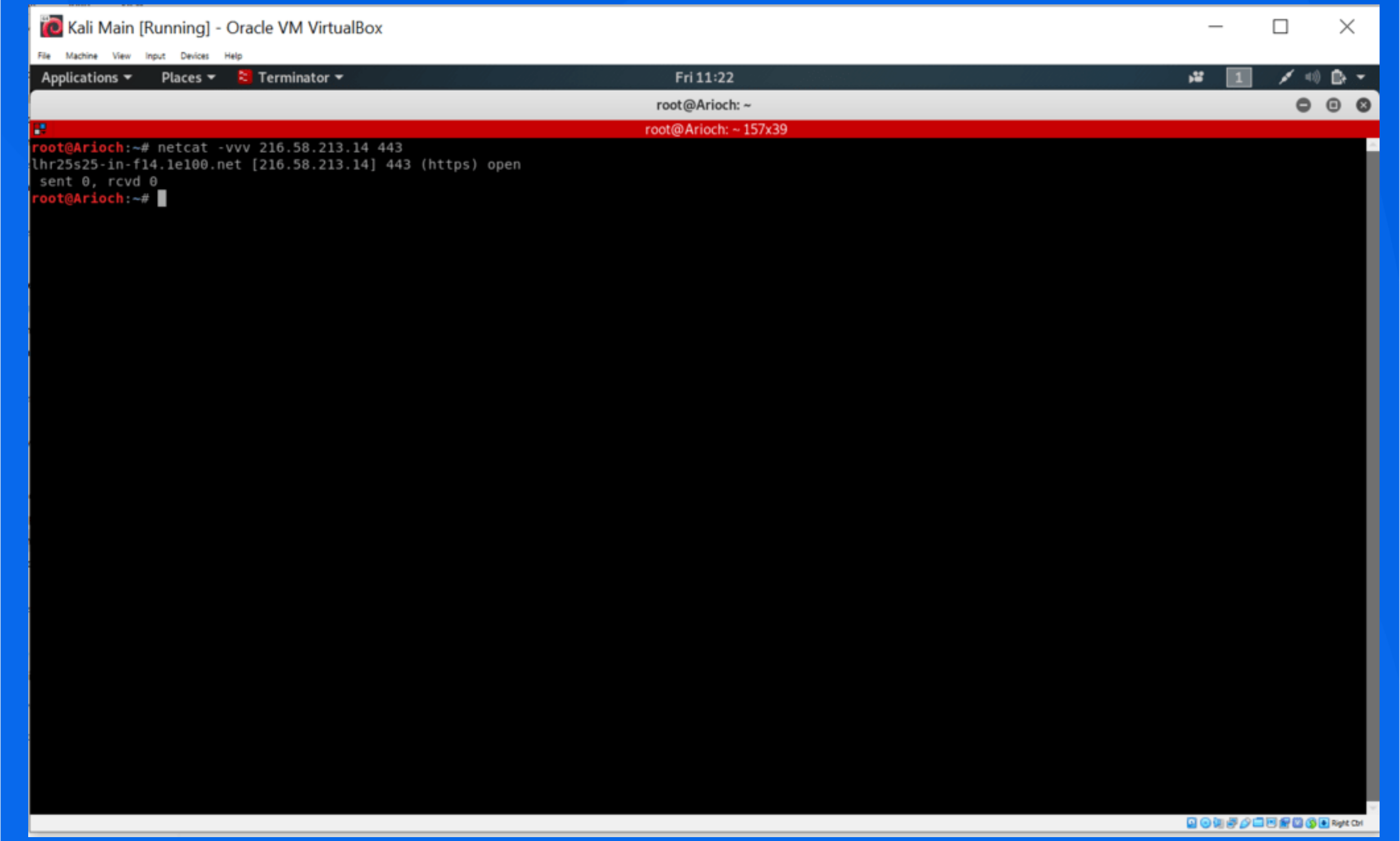
If you've already scanned a website, it's a good idea to make sure that everything that has been scanned is correct; this is known as sanity checking.

The example to the right has sanity checked what was found in a Nmap scan.

In the code example below, following the Netcat syntax, has Netcat turned on by typing *netcat. -vvv* means that it has extreme verbosity switched on, which will show everything that NetCat is finding.

It then has the IP address, which points it to the address it is looking at. Finally, the scan has looked at the HTTP port, port 80.

```
netcat -vvv 101.10.10.102 80
```



```
root@Arioch:~# netcat -vvv 216.58.213.14 443
lhr25s25-in-f14.1e100.net [216.58.213.14] 443 (https) open
 sent 0, rcvd 0
root@Arioch:~# 
```

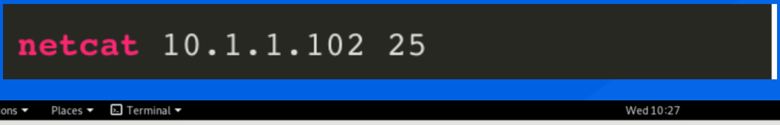
NETCAT NETWORK UTILITY

Banner Grabbing

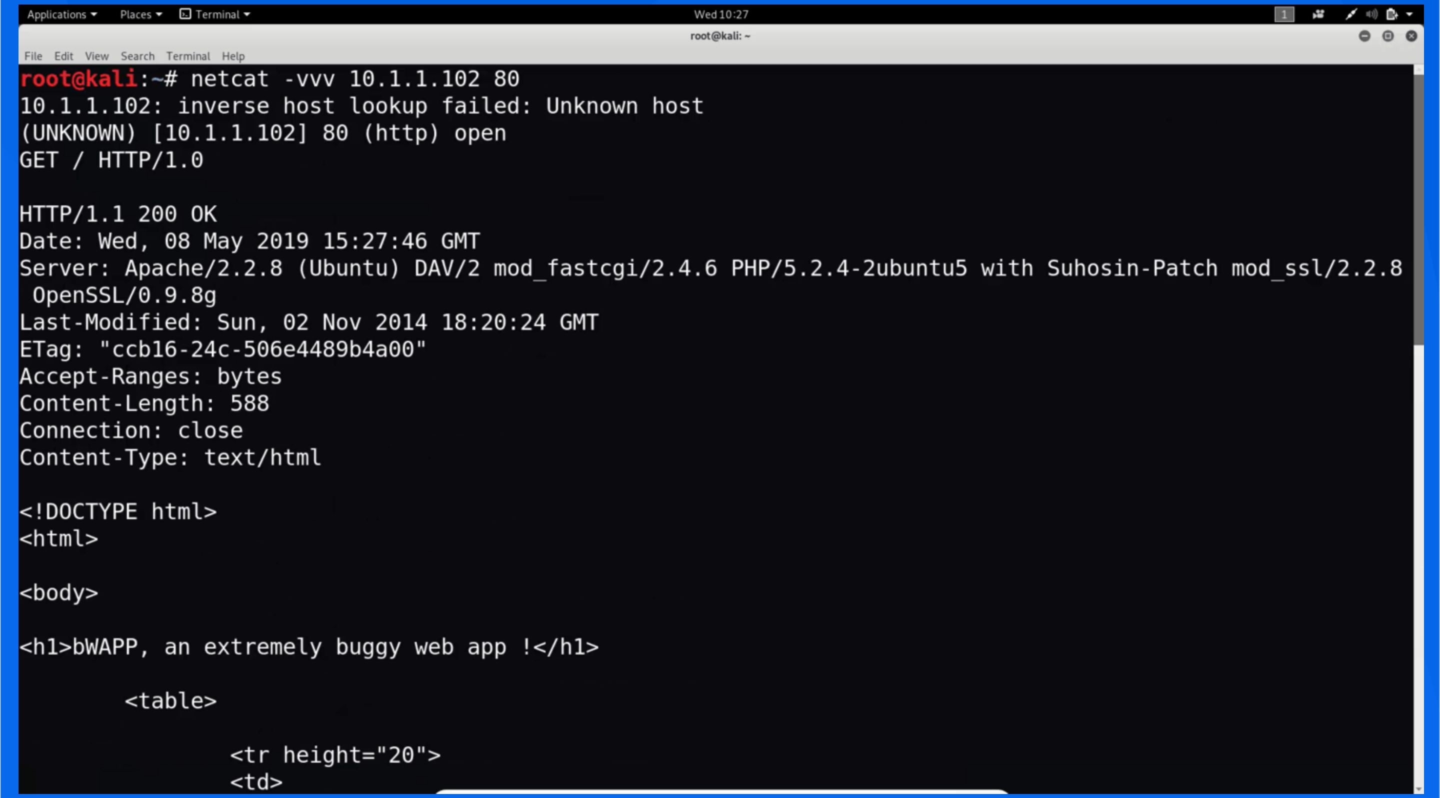
Banner Grabbing is the process of gaining information about a network and the services running on its open ports. The information that can be gained with banner grabbing can allow us to find out if the network is running any applications or operating systems that have known exploits on them. The information gained in Netcat can be used in another application, like MetaSploit, to upload an executable payload, and gain entry to the network.

Service ports are commonly used, such as ports 80 (HTTP), 21 (FTP) and 25 (SMTP).

If you have found an open port, the way to banner grab would be [host] [port], such as below:



```
netcat 10.1.1.102 25
```



```
root@kali:~# netcat -vvv 10.1.1.102 80
10.1.1.102: inverse host lookup failed: Unknown host
(UNKNOWN) [10.1.1.102] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 08 May 2019 15:27:46 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
 OpenSSL/0.9.8g
Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
ETag: "ccb16-24c-506e4489b4a00"
Accept-Ranges: bytes
Content-Length: 588
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>

<body>

<h1>bWAPP, an extremely buggy web app !</h1>

        <table>

                <tr height="20">
                <td>
```

NETCAT NETWORK UTILITY

Useful Netcat Options

```
Use IPv4 addressing only: nc -4

Use IPv6 addressing only: nc -6

Use UDP instead of TCP:   nc -u

Listen for an incoming connection: nc -l

Continue listening after client has disconnected: nc -k -l

No DNS lookups: nc -n

Use specific source port: nc -p

Use source IP: nc -s

Apply number of seconds timeout: nc -wN  [change N for the number of seconds until session timeout]

Verbose output: nc -v

Very verbose output: -vv

Extremely verbose output: -vvv
```

cloud academy
A QA COMPANY