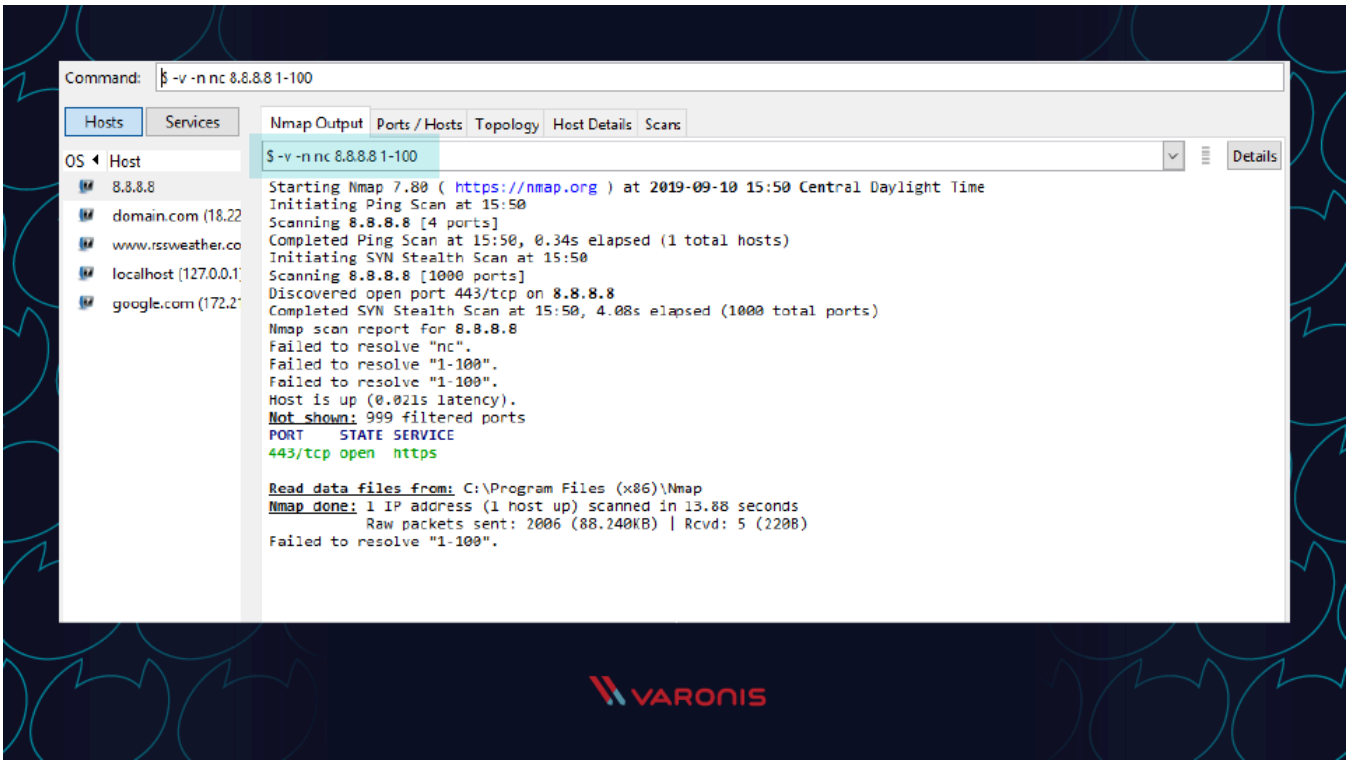
blocking mechanism is in place.

A basic port scan command for an IP ncat address looks like this:

nc -v -n 8.8.8.8 1-1000



Note that the numbers at the end of the command tell Netcat to only scan for ports between numbers 1 and 1000.

If you don't know the IP address of a server or website, then you can look it up via a ping terminal command or just insert the domain into the Netcat command:

nc -v -n google.com 1-1000

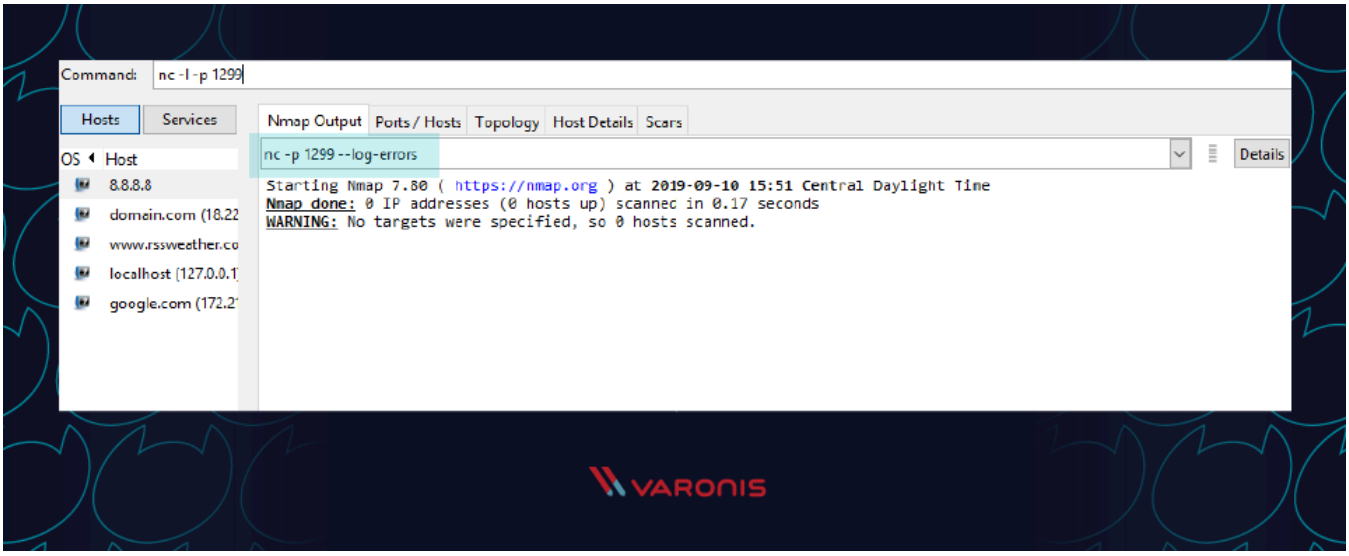
You should always perform port scans when connected to your local enterprise network. If not, you can configure your router with a VPN service to create a secure tunnel into the network.

Create a Chat or Web Server

tools available to enterprise organizations. The reality is that some IT experts and system administrators would prefer a simple text-only solution. Windows Netcat can actually fill that need and allow for the transmission of messages across a local network.

To get started, you first need Netcat to start listening on a port number. Make sure not to choose a port that is already in use by another application or service.

nc -l -p 1299



Then all you need to do is launch the chat session with a new TCP connection:

nc localhost 1299

This process can also be used to spin up a basic web server from your local machine. Netcat will function as the web host and allow you to store HTML content which can then be viewed through a web browser.

First, create a new text document on your local system and make sure to use valid HTML tags. Then save the file as “index.html” and store it in the root of your Netcat directory. Now switch back to the Netcat tool and run this command:

printf ‘HTTP/1.1 200 OK\n\n%s’ “$(cat index.html)” | netcat -l 8999

To see the HTML in action, simply open any web browser and navigate to your local IP address with: 8999 at the end to specify the port of the host.

was successful or not. For troubleshooting and debugging purposes, you'll want to gather as much information and logs as possible while also investing in solutions like Varonis Datalert to detect threats and respond quickly. Netcat can help thanks to the verbose parameter which can be added to any basic Netcat command. Simply include "-v" to your command and run it again.

Even with this setting turned on, Netcat will not reveal any of your credentials or authentication data.

HTTP Requests with Netcat Commands

We've covered how you can use Netcat to host HTML pages on your local system. But the utility program can also be used to make web requests to outside servers. In this way, Netcat will essentially function as a web browser by obtaining raw HTML code.

Along with a tool like Varonis Edge, Netcat can be helpful for IT professionals who are looking into internet traffic issues or proxies. Here's an example of how to obtain the HTML content from Google's homepage:

printf "GET / HTTP/1.0\r\n\r\n" | nc google.com 80

Note that the port number 80 is required for this type of command since the world wide web uses it as a default for TCP over IP connections.

TCP Server and TCP Client Commands

Although the TCP protocol is primarily used for transferring web traffic around the world, it can actually be implemented at a local level for file transfers. To accomplish this, you need to run Netcat from two locations: one that will act as a server to send the file and one that will act as the client to receive it.

Run this Netcat command on the server instance to send the file over port 1499:

nc -l 1499 > filename.out

Then run this command on the client to accept, receive, and close the connection:

server.

ITEM with Netcat Commands

Newer versions of Netcat allow you to use ITEM format for transferring data instead of the standard TCP or UDP protocols. To accomplish this, you must follow this syntax:

file_path (pipe) device_path (pipe) network host

Prevent DNS Lookup with Netcat Commands

Netcat commands run fastest when they are operating purely on IP addresses. This because no time is wasted talking to domain name servers (DNS) to translate server names into IP addresses. If you find that your Netcat commands are still running slow, make sure to add the “-n” operator so that the utility knows that DNS lookups are not required.

Shell Scripting with Netcat

As mentioned earlier, one of the benefits of using Netcat is that it can be included as part of a larger script that performs an automated function. As part of your security procedures, you might want to run a full port scan on all of your servers to detect new malicious applications that are listening for a connection.

You could write a script that:

1. Imports a text file of server names or IP addresses
2. Calls Netcat to run a port scan on each server
3. Writes the output to a new text file for analysis

Multiple Netcat commands can be grouped together in a single script and be run through either a Linux or Windows shell. In some cases, it may be worthwhile to have the scripts on a regular timetable.

Launching Reverse (Backdoor) Shells

nc -n -v -l -p 5555 -e /bin/bash

Then from any other system on the network, you can test how to run commands on host after successful Netcat connection in bash.

nc -nv 127.0.0.1 5555

A reverse shell is a remote access approach where you run administrative commands from one terminal while connecting to another server on the network. To get started, you need to enable the shell tool over a Netcat command by using Netcat reverse shell:

nc -n -v -l -p 5555 -e /bin/bash

Then from any other system on the network, you can test how to run commands on the selected host after successful Netcat connection in bash:

nc -nv 127.0.0.1 5555

Netcat Cheat Sheet

Until you start using Netcat on a regular basis, you might get confused about the command syntax or forget what some of the parameters do. Don't worry! We've included a cheat sheet below to help you find what you need quickly to run a working Netcat command.

Netcat Fundamentals

nc [options] [host] [port] – by default this will execute a port scan

nc -l [host] [port] – initiates a listener on the given port

Netcat Command Flags

nc -4 – use IPv4 only

nc -6 – use IPv6

nc -u – use UDP instead of TCP

nc -v – provide verbose output

Netcat Relays on Windows

nc [host] [port] > relay.bat – open a relay connection

nc -l -p [port] -e relay.bat – connect to relay

Netcat Relays on Linux

nc -l -p [port] 0 (less than) backpipe (pipe) nc [client IP] [port] (pipe) tee backpipe

Netcat File Transfer

nc [host] [port] (greater than) file_name.out– send a file

nc [host] [port] (less than) file_name.in – receive a file

Netcat Port Scanner

nc -zv site.com 80 – scan a single port

nc -zv hostname.com 80 84 – scan a set of individual ports

nc -zv site.com 80-84 – scan a range of ports

Netcat Banners

echo “” | nc -zv -wl [host] [port range] – obtain the TCP banners for a range of ports

Netcat Backdoor Shells

nc -l -p [port] -e /bin/bash – run a shell on Linux

nc -l -p [port] -e cmd.exe – run a shell on Netcat for Windows