Como realizar varredura utilizando TCPing

É muito importante nos certificarmos de que nosso firewall está configurado corretamente e não temos nenhuma porta aberta exceto aquelas que queremos abrir especificamente para oferecer serviços externos como por exemplo SSH ou FTP.

TCPing é uma ferramenta que roda no console e funciona de forma muito semelhante ao 'ping', mas em vez de usar ICMP com echo-request e echo-reply, ele usa TCP e é capaz de nos mostrar se uma determinada porta de um computador está aberto ou fechado.

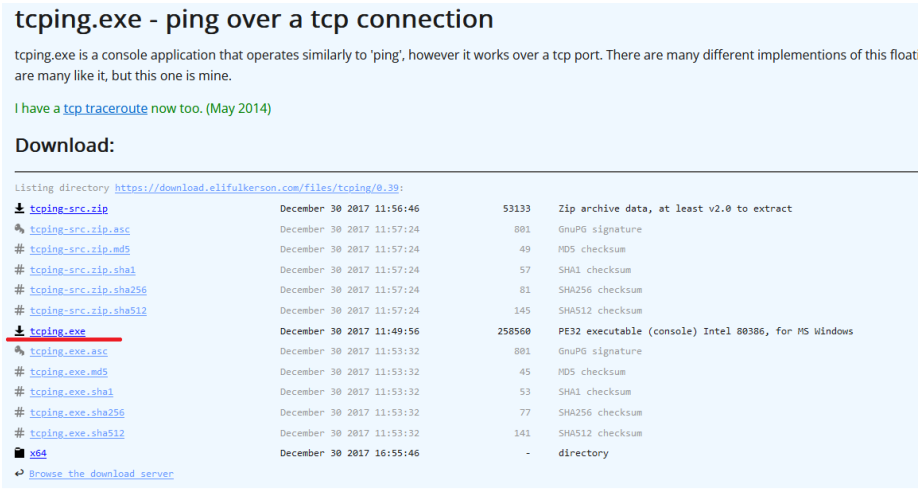
A ferramenta também pode usar a opção '-h', com está opção, conseguimos se conectara um host especifico usando o protocolo HTTP, além de nos informar se a porta 80 está aberta, poderá nos mostrar o status HTTP.

Neste artigo, iremos informar, como podemos realizar uma varredura, utilizando o TCPing.

1

Antes de tudo, iremos realizar o download da ferramenta, sendo possível através deste link: **https://www.elifulkerson.com/projects/tcping.php**

Ao acessar o link, devemos escolher a opção *tcping.exe:*



tcping.exe - ping over a tcp connection

tcping.exe is a console application that operates similarly to 'ping', however it works over a tcp port. There are many different implementions of this float are many like it, but this one is mine.

I have a tcp traceroute now too. (May 2014)

Download:

Listing directory https://download.elifulkerson.com/files/tcping/0.39:

tcping-src.zip	December 30 2017 11:56:46	53133	Zip archive data, at least v2.0 to extract
tcping-src.zip.asc	December 30 2017 11:57:24	801	GnuPG signature
tcping-src.zip.md5	December 30 2017 11:57:24	49	MD5 checksum
tcping-src.zip.sha1	December 30 2017 11:57:24	57	SHA1 checksum
tcping-src.zip.sha256	December 30 2017 11:57:24	81	SHA256 checksum
tcping-src.zip.sha512	December 30 2017 11:57:24	145	SHA512 checksum
tcping.exe	December 30 2017 11:49:56	258560	PE32 executable (console) Intel 80386, for MS Windows
tcping.exe.asc	December 30 2017 11:53:32	801	GnuPG signature
tcping.exe.md5	December 30 2017 11:53:32	45	MD5 checksum
tcping.exe.sha1	December 30 2017 11:53:32	53	SHA1 checksum
tcping.exe.sha256	December 30 2017 11:53:32	77	SHA256 checksum
tcping.exe.sha512	December 30 2017 11:53:32	141	SHA512 checksum
x64	December 30 2017 16:55:46	-	directory

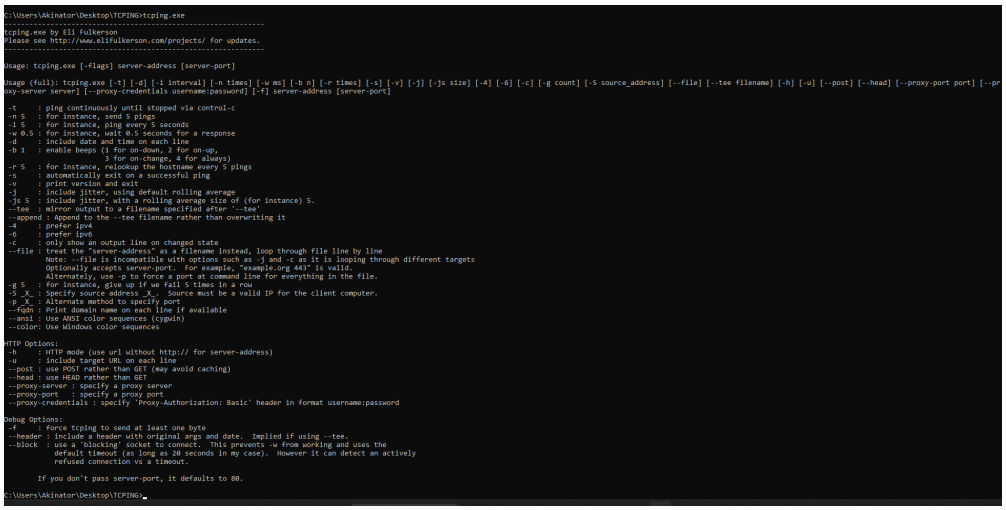
Browse the download server

2

Ao fazer o download, abrimos o prompt de comando (cmd.exe), devemos ir ao caminho onde salvamos a ferramenta e colocamos diretamente o nome del para executá-la.

Por não introduzir nenhum parâmetro, por padrão obteremos ajuda direta do TCPing, conforme o caminho do exemplo: C:\Users\Akinator\Desktop\TCPING>

Executando o TCPing com: C:\Users\Akinator\Desktop\TCPING>tcping.exe , após utilizar o comando na pasta do arquivo baixando "tcping.exe" é aberto um help com inúmeras opções de testes, conforme abaixo:



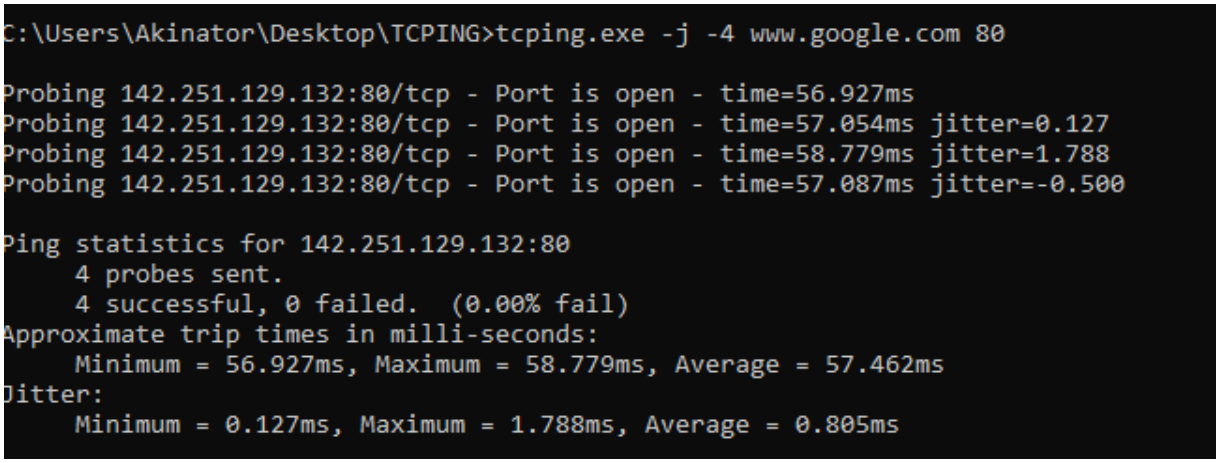
```
C:\Users\Akinator\Desktop\TCPING>tcping.exe
------------------------------------------------------------
tcping.exe by Eli Fulkerson
Please see http://www.elifulkerson.com/projects/ for updates.
------------------------------------------------------------

Usage: tcping.exe [-flags] server-address [server-port]

Usage (full): tcping.exe [-t] [-d] [-i interval] [-n times] [-w ms] [-b n] [-r times] [-s] [-v] [-j] [-js size] [-4] [-6] [-c] [-g count] [-S source_address] [--file] [--tee filename] [-h] [-u] [--post] [--head] [--proxy-port port] [--pr
oxy-server server] [--proxy-credentials username:password] [-f] server-address [server-port]

 -t    : ping continuously until stopped via control-c
 -n 5  : for instance, send 5 pings
 -i 5  : for instance, ping every 5 seconds
 -w 0.5 : for instance, wait 0.5 seconds for a response
 -d    : include date and time on each line
 -b 1  : enable beeps (1 for on-down, 2 for on-up,
                       3 for on-change, 4 for always)
 -r 5  : for instance, relookup the hostname every 5 pings
 -s    : automatically exit on a successful ping
 -v    : print version and exit
 -j    : include jitter, using default rolling average
 -js 5 : include jitter, with a rolling average size of (for instance) 5.
 --tee  : mirror output to a filename specified after "--tee"
 --append : Append to the --tee filename rather than overwriting it
 -4    : prefer ipv4
 -6    : prefer ipv6
 -c    : only show an output line on changed state
 --file : treat the "server-address" as a filename instead, loop through file line by line
          Note: --file is incompatible with options such as -j and -c as it is looping through different targets
          Optionally accepts server-port.  For example, "example.org 443" is valid.
          Alternately, use -p to force a port at command line for everything in the file.
 -g 5  : For instance, give up if we fail 5 times in a row
 -S _X_ : Specify source address _X_.  Source must be a valid IP for the client computer.
 -p _X_ : Alternate method to specify port
 --fqdn : Print domain name on each line if available
 --ansi : Use ANSI color sequences (cygwin)
 --color: Use Windows color sequences

HTTP Options:
 -h    : HTTP mode (use url without http:// for server-address)
 -u    : include target URL on each line
 --post : use POST rather than GET (may avoid caching)
 --head : use HEAD rather than GET
 --proxy-server : specify a proxy server
 --proxy-port   : specify a proxy port
 --proxy-credentials : specify "Proxy-Authorization: Basic" header in format username:password

Debug Options:
 -f    : force tcping to send at least one byte
 --header : include a header with original args and date.  Implied if using --tee.
 --block  : use a 'blocking' socket to connect.  This prevents -w from working and uses the
            default timeout (as long as 20 seconds in my case).  However it can detect an actively
            refused connection vs a timeout.

      If you don't pass server-port, it defaults to 80.

C:\Users\Akinator\Desktop\TCPING>
```

Abaixo, alguns parâmetros mais usados:

- -4: Utiliza o protocolo IPv4 para conexão
- -6: Usa o protocolo IPv6 para conexão
- -t: O TCPing, continua até que cancelemos com 'ctrl+c'
- -n NUM: executa um número especificado (NUM) de pings para um host
- -S: Permite selecionar o endereço IP original dos pacotes, devemos ter este IP no próprio sistema
- -j: Nos informa o jitter da conexão
- destino: IP ou domínio do host a ser verificado
- porta: a porta de 1 a 65535 que queremos verificar, onde se nada for especificado, a 80 será utilizada.

3

Aqui podemos ver um exemplo de teste utilizando a opção IPv4(-4) mais Jitter (-j) para o Google na porta 80:



Verificar se todas as portas estão fechadas em um host é essencial, deve-se lembrar que quando uma porta está aberta e com um serviço escutando por trás dela, ela pode trazer um criminoso cibernético e 'explorar' uma vulnerabilidade no serviço. Caso possua alguma dúvida ou dificuldade em um destes processos, entre em contato com um de nossos analistas a partir dos meios de comunicação oficial.

Este artigo te ajudou?

Your Rating:

Results:

1 rates

Ainda precisa de ajuda?

ABRIR UM CHAMADO