2019 oplossingen labo 2 - Lars Lemmens

Met dank aan de Github van Martijn en natuurlijk Lars Lemmens

LABO 2

What is the IP address of your computer?

What is the status code returned from the server to your browser?

When was the HTML file that you are retrieving last modified on the server?

```
'user:~$' • echo -ne '
HEAD /HTTP-Wireshark-file1.html HTTP/1.1\r\nHost:  virtualhostname.x.cnw2.uclllabs.be\r\n\r\n' | nc localhost 80 |
 grep 'Last-Modified:'

'user:~$' • tshark -r http.pcapng -Y http -T fields -e http.last_modified
```

- The -n argument does not output the trailing newline
- The -e argument enables interpretation of backslash escapes
- The nc command is a TCP/IP swiss army knife
- The -r argument reads the packet date from infile
- The -Y command captures the link type
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected

How many bytes of content are being returned to your browser?

What software and version is the web server running?

```
'user:~$' • tshark -r http.pcapng -Y http.server -T fields -e ip.src -e http.server | sort -u
```

- The -r argument reads the packet date from infile
- The -Y argument captures the link type
- The -T argument sets the format of the output when viewing decoded packet data.
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The -u argument output only the first of an equal run

Explain in detail the above tshark command.

What TCP ports are in use at the client and the server during your browsing session?

```
'user:~$' • tshark -r http.pcapng -Y http -T fields -e tcp.port | sort -u
```

- The -r argument reads the packet date from infile
- The -Y argument captures the link type
- The -T argument sets the format of the output when viewing decoded packet data.
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The -u argument output only the first of an equal run

Exercise 1:

Which HTTP method was used the most during the entire browsing session?

```
'user:~$' • tshark -r http.pcapng -Y http.request.method -T fields -e http.request.method | sort | uniq -c | head -1 |
 awk '{print $2}'
'user:~$' • tshark -r http.pcapng -Y http.request.method -T fields -e http.request.method | sort | uniq -c | awk '
NR=1{print $2}'
```

- The tshark command dumps and analyzes network traffic
- The -r argument reads the packet date from infile
- The -T argument sets the format of the output when viewing decoded packet data.
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The uniq command reports or omits repeated lines
- The -c argument prefixes lines by the number of occurences
- The head command shows output for only the first part of files
- The awk command is used for pattern scanning and processing language

In case you would like to automate this: With tshark and a Bash loop"

```
'user:~$' • tshark -r http.pcapng -Y 'http.request.method==GET' -T fields -e tcp.srcport | sort -u | while read PORT
;do tshark -r http.pcapng -Y "tcp.dstport==$PORT && http.server contains Apache" -T fields -e ip.src;done |
 sort -u
```

- The tshark command dumps and analyzes network traffic
- The -r argument reads the packet date from infile
- The -T argument sets the format of the output when viewing decoded packet data.
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The -u argument output only the first of an equal run
- The -Y command captures the link type

Exercise 2:

How many HTTP GET request messages did your browser send?

```
'user:~$' • tshark -r http.pcapng -Y http.request.method==GET | wc -l
```

- The tshark command dumps and analyzes network traffic
- The -r argument reads the packet date from infile
- The wc command prints a newline, word, and byte counts for each file
- The -l argument prints the newline counts

To which Internet addresses were these GET requests sent?

```
'user:~$' • tshark -r http.pcapng -Y http.request.method==GET -T fields -e ip.dst | sort -u
```

- The tshark command dumps and analyzes network traffic
- The -r argument reads the packet date from infile
- The -Y command captures the link type
- The -T argument sets the format of the output when viewing decoded packet data.
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The -u argument output only the first of an equal run

Exercise 5:

Use Netcat to download these images. check the echo -ne options or use printf. If needed, slow down netcat with option -i.

The image part in the HTTP stream starts after a blank line.

```
'user:~$' • echo -ne "GET /nw2/images/image1.jpg HTTP/1.1\r\nHost: darthvader.uclllabs.be\r\n\r\n" |\
nc darthvader.uclllabs.be 80 | sed '1,/^\r/d' > image1.jpg

'user:~$' • echo -ne "GET /nw2/images/image1.jpg HTTP/1.1\r\nHost: darthvader.uclllabs.be\r\n\r\n" |\
nc darthvader.uclllabs.be 80 | grep -A9999999999999999 -B0 -Pa 'JFIF' > image1.jpg
```

- The -n argument does not output the trailing newline
- The -e argument enables interpretation of backslash escapes
- The sed command is a stream editor for filtering and transforming text
- The nc command is a TCP/IP swiss army knife
- The -A argument prints NUM lines of trailing context after matching lines.
- The -B argument interprets PATTERN as a Perl regular expression (PCRE, see below).
- The -a argument processes a binary file as if it were text; this is equivalent to the --binary-files=text option.

Exercise 7:

Use httpie, a cURL-like tool for humans to inspect the various HTTP headers in request and responses. Connect to various websites and explain the use of the HTTP headers.

```
'user:~$' • http -v -a Rey:StarWars http://darthvader.uclllabs.be/nw2/private/
```

- The -v argument is for verbose

Exercise 8:

A simulated phone is running at http://darthvader.uclllabs.be/nw2/phone/. Create a oneliner to bruteforce the pincode. Tip: pincode range: 1200-1300

```
'user:~$' • for foo in {1200..1300}; do if wget -q --http-user='admin' --http-password=$foo
 http://darthvader.uclllabs.be/nw2/phone; then echo $foo;break;fi;done
```

- The wget command is the non-interactive network downloader
- The -q argument turns of the wget's output
- The --http-user AND --http-password specifies the username and the password on a http server

Exercise 9:

"Put the following text.txt on your web server. This text contains the string Goed bezig :-)

Write an HTTP request by using the Range header so your web server will only return this exact string 'Goed bezig :-)'. Try to do this by only using netcat

```
'user:~$' • curl http://your.server.name/output.txt -i -H "Range: bytes=1-"
'user:~$' • echo -ne "GET /output.txt HTTP/1.1\r\nHost: your.server.name\r\nRange: bytes=1-\r\n\r\n" |
 nc your.server.name 80
```

- The curl command is used to transfer a URL
- The -i argument includes the HTTP-header in the output
- The -H argument is used as a extra header to use when getting a web page
- The nc command is a TCP/IP swiss army knife
- The -n argument does not output the trailing newline
- The -e argument enables interpretation of backslash escapes

Exercise 10:

This can be accomplished by sending the output of tshark or tcpdump to STDOUT instead of a regular file. Direct this STDOUT stream to Wireshark running on your local computer.

```
'root #' • ssh myserver.X.cnw2.uclllabs.be tcpdump -nli eth0 not tcp port 22345 -s0 -w - | wireshark -nki -

'root #' • ssh myserver.X.cnw2.uclllabs.be 'tshark -nli eth0 -f "not tcp port 22345" -s0 -w -' | wireshark -nki -
```

- The ssh command is a remote login program
- The -n argument redirects stdin from /dev/null (actually, prevents reading from stdin).
- The -l argument specifies the user to log in as on the remote machine.
- The -i argument selects a file from which the identity (private key) for public key authentication is read.
- The -s argument may be used to request invocation of a subsystem on the remote system
- The -w argument Requests tunnel device forwarding with the specified tun(4) devices between the client (local_tun) and the server (remote_tun).
- The -n argument disables network object name resolution (such as hostname, TCP and UDP port names), the -N flag might override this one.
- The -k argument starts the capture session immediately.
- The -i argument sets the name of the network interface or pipe to use for live packet capture.
- The -f argument (in tshark command) sets the capture filter expression

Exercise 11:

Capture some HTTP traffic while browsing several websites and save it to the file http.pcapng.

You can also use the test capture in /home/logs on leia. create a CLI oneliner which parses the captured file http.pcapng and displays all HTTP server strings which do not contain Apache.

Only the commands tshark and sort are allowed.

```
'user:~$' • tshark -r http.pcapng -Y 'http.server && !(http.server contains Apache)' -T fields -e http.server | sort -u
```

- The -r argument reads the packet date from infile
- The -Y command captures the link type
- The -T argument sets the format of the output when viewing decoded packet data.
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The -u argument output only the first of an equal run

Exercise 12:

This exercise is a small variation of the previous one. Count and sort all HTTP server strings which do not contain Apache in HTTP responses on your GET requests.

```
'user:~$' • tshark -r http.pcapng -Y '!(http.request.method==GET)' -T fields -e tcp.srcport | sort -u | while read
 PORT;do tshark -r http.pcapng -Y "tcp.dstport==$PORT && http.server && !(http.server contains Apache)"
 -T fields -e http.server;done | sort | uniq -c | sort -rn
```

- The tshark command dumps and analyzes network traffic
- The -r argument reads the packet date from infile
- The -Y command captures the link type
- The -e argument (in tshark command) adds a field to the list of fields to display if -T fields is selected
- The sort command sorts lines of text files
- The -u argument output only the first of an equal run
- The -T argument sets the format of the output when viewing decoded packet data.
- The uniq command reports or omits repeated lines
- The -c command prefixes lines by the number of occurrences
- The -r argument (in sort command) reverses the results of comparisons
- The -n compare according to string numerical value

Revision #1
Created 17 June 2021 14:13:05 by Jasper G.
Updated 3 December 2021 22:13:09 by Jasper G.