2019 oplossingen labo tussentest - Lars Lemmens

Met dank aan de Github van Martijn en natuurlijk Lars Lemmens

LABO TEST

Exercise 1:

Copy the content of your it-enabled grandmothers id_rsa.pub file in your ~/.ssh/authorized_keys file"

```
'user@:~$' • ssh user@leia.uclllabs.be -p 22345 -i "/path/to/your grandmothers identity_file"
```

- The ssh command is a remote login program
- The -p argument is used for a port to connect to on the remote host.
- The -i argument selects a file from which the identity (private key) for public key authentication is read.

```
'user@:~$' • ssh user@leia.uclllabs.be -p 22345
```

- The ssh command is a remote login program
- The -p argument is used for a port to connect to on the remote host.

Exercise 2:

Try to find out which TCP ports are open on leia without using tools like netstat or ss. Execute on leia for increased speed.

```
'user@:~$' • nc -zv -w 1 leia.uclllabs.be 1-65535 2>&1 | grep succeeded | awk '{print $4}'

'user@:~$' • for foo in {1..65535}; do nc -N -w1 leia.uclllabs.be $foo </dev/  null >/dev/null && echo $foo;done

'user@:~$' • nmap -p 1-65535 leia.uclllabs.be | grep -P '\d+/tcp.*open' |cut -d'/' -f1

'user@:~$' • nmap --reason -p 1-65535 leia.uclllabs.be | grep -oP '\d+(?=/tcp.*open)'
```

- The nc command is a TCP/IP swiss army knife
- The -z argument is used for scanning
- The -v argument is used for verbose
- The -w (# in seconds) arguments is timeout for connects and final net reads
- The grep command prints lines matching a pattern
- The awk command is used for pattern scanning and processing language
- \d matches a digit (equivalent to [0-9])
- '+' matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
- . matches any character (except for line terminators)
- '*' matches the previous token between zero and unlimited times, as many times as possible, giving back as needed (greedy) open matches the characters open literally (case sensitive)
- The cut command removes sections from each line of files
- The -d argument use DELIM instead of TAB for field delimiter
- The command nmap is a network exploration tool and security / port scanner
- The --reason argument shows the reason each port is set to a specific state and the reason each host is up or down
- The -p argument specifies which ports you want to scan and overrides the default.
- The -o argument print only the matched (non-empty) parts of a matching line, with each such part on a separate output line.
- The -o argument prints only the matched (non-empty) parts of a matching line, with each such part on a separate output line.
- The -p argument Interpret I as Perl-compatible regular expressions (PCREs).

Exercise 3:

Create a oneliner which lists all palindromes with exactly 6 letters in a dictionary.

```
'user@:~$' • cat dutch | grep -P '^(.)(.)(.)\3\2\1$'
```

- ^ asserts position at start of a line
- . matches any character (except for line terminators)
- in ^(.)(.)(.) ==> the first (.) is the first capturing group, the second (.) is the second capturing group, the third (.) is the third capturing group,
- \3 matches the same text as most recently matched by the 3rd capturing group, \2 matches the same text as most recently matched by the 2nd capturing group and \1 matches the same text as most recently matched by the 1st capturing group

Exercise 4:

As a web server administrator you have been asked to give your manager a Linux CLI oneliner to extract the 5 IP addresses that contacted the web server the most

The apache log is located in /home/logs. Create a correct oneliner. The output should look something like this: (count IPs)

```
'user@:~$' • cat apache_google.log | cut -d ' ' -f1 | sort | uniq -c | sort -rn | head -5
```

- The cut command removes sections from each line of files
- The -d argument uses DELIM instead of TAB for field delimiter
- The -f argument selects only these fields
- 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 occurrences
- The -r reverses the result of comparisons
- The head command shows output the first part of files

Exercise 5:

What Linux ssh command do you use to bind your local port 3000 to a web server on port 4444 on the network of the ssh server

```
'user@:~$' • ssh -p 22345 username@leia.uclllabs.be -L 3000:IP_web_server:4444
```

- The -p argument shows which port to connect to on the remote host
- The -L argument specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side.

Exercise 6:

Create an apache vhost (netcat.X.cnw2.uclllabs.be) which displays a single web page (index.html). How can you update/alter this website (index.html) via a Netcat connection from your laptop."

```
'root@myserver' 1)  mkdir /var/www/html/netcat
'root@myserver' 2)  nano netcat.conf
```

```
<VirtualHost *:80>
    ServerAdmin root@netcat.X.cnw2.uclllabs.be
    ServerName netcat.X.cnw2.uclllabs.be
    DocumentRoot /var/www/html/netcat

    LogLevel info
    ErrorLog ${APACHE_LOG_DIR}/netcat-error.log
    CustomLog ${APACHE_LOG_DIR}/netcat-access.log combined
</VirtualHost>
```

```
'# root@myserver' 1)  a2ensite netcat
'# root@myserver' 2)  systemctl reload apache2
'# root@myserver' 3)  nc -l -p 10000 >> /var/www/html/netcat/index.html
'user@laptop:~$'  4)  echo test | nc netcat.X.cnw2.uclllabs.be 10000
```

Exercise 7:

On server Leia, use the list of logged in users to print only the username that has been logged in to the server for the longest time

```
'user@:~$' • who | awk '{print $3$4 " " $1}' | sort -n | awk '{print $2}' | head -1
```

- The command who shows who is logged in
- The command sort sorts lines of text files
- The -n argument compares acoording to string numerical value
- The head command outputs the first part of files

Exercise 8:

Some subdirectory of /tmp contains a bunch of movies. However, their extension is wrong.

The extension should be .avi instead of .jpg. Copy these files to your homedirectory and correct their extensions in one line. "

```
'user@:~$' • ls -1 *.jpg | while read foo; do echo cp $foo ~/$(basename $foo .jpg).avi;done
'user@:~$' • ls -1 *.jpg | while read foo; do echo cp $foo ~/${foo%.jpg}.avi;done
```

- The -1 argument lists one file per line
- cp $foo ~/$(basename $foo .jpg).avi ==> Echo the STRING(s) to standard output.

Exercise 9:

Create a Linux CLI oneliner to decode the following string 'SWYgeW91IGNhbiByZWFkIHRoaXMsIHlvdSBmb3VuZCB0aGUgY29ycmVjdCBhbnN3ZXIK'

```
'user@:~$' • echo 'SWYgeW91IGNhbiByZWFkIHRoaXMsIHlvdSBmb3VuZCB0aGUgY29ycmVjdCBhbnN3ZXIK' |
 openssl enc -a -d

'user@:~$' • echo 'SWYgeW91IGNhbiByZWFkIHRoaXMsIHlvdSBmb3VuZCB0aGUgY29ycmVjdCBhbnN3ZXIK' |
 base64 -d
```

- The -a argument ==> Base64 process the data
- The -d argument ==> decrypts the input data
- The -base64 argument = The -a argument

Exercise 10:

Create a regular expression to match all words in a dictionary with 5 unique letters. "

```
'user@:~$' • cat /usr/share/dict/dutch | grep -P '^[a-zA-Z]{5}$'| grep -vP '(.).*\1'
```

- ^ asserts position at start of a line
- A-Z matches a single character in the range between A and Z (case sensitive)
- a-z matches a single character in the range between a and z (case sensitive)
- {5} matches the previous token exactly 5 times
- . matches any character (except for line terminators
- '*' matches the previous token between zero and unlimited times, as many times as possible, giving back as needed (greedy)
- -v stands for inverted match.
- -P stands for perl expression

Exercise 11:

Create a oneliner to show ‘Time = 15:44:25 (11/10/1901)' or 'Time = 15:44:25 (11-10-1901)’ each time with the current time and date.

```
'user@:~$' • echo "Time = $(date '+%X (%x)')"
'user@:~$' • date '+Time = %X (%x)'
'user@:~$' • date '+Time = %X (%Y/%d/%m)'
```

- date matches the characters date literally (case sensitive)
- '+' matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
- The %X argument sets locale's time representation
- the %x argument sets locale's date representation
- The %Y arguments = year
- The %d arguments = day
- The %m arguments = month

Exercise 12:

Create a oneliner which lists the top 3 most used passwords in the ftp brute force attack captured in "ftp_bruteforce.pcap". Use a suitable sniffer filter which only displays whats really needed.

```
'user@:~$' • tshark -r ftp_bruteforce.pcap -Y 'ftp.request.command==PASS' -T fields -e 'ftp.request.arg' 2> /dev/null| sort | uniq -c | sort -rn | head -3
```

- 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 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
- The head command shows output for only the first part of files

---

Revision #1
Created 17 June 2021 14:15:56 by Jasper G.
Updated 3 December 2021 22:13:09 by Jasper G.