

2019 oplossingen

Testexamen - Lars Lemmens

Met dank aan de [Github van Martijn](#) en natuurlijk Lars Lemmens

Exercise 1

Create a CLI oneliner to match all words with 14, 15 or 16 unique letters. The output should look like:

Words with 14 letters: EHBO-diploma's bruiloftsdagen katrolschijven verontschuldigd ...

Words with 15 letters: dampkringslucht sandwichformule ...

Words with 16 letters: ...

```
'user@:~$' • for foo in 14 15 16; do echo "Words with $foo letters:" $(grep -vP '(.)*\1' /usr/share/dict/dutch | grep -P "^.{$foo}$");done
```

- `for name [[in [word ...]] ;] do list ; done` The list of words following `in` is expanded, generating a list of items. The variable `name` is set to each element of this list in turn, and `list` is executed each time. If the `in word` is omitted, the `for` command executes `list` once for each positional parameter that is set (see **PARAMETERS** below). The return status is the exit status of the last command that executes. If the expansion of the items following `in` results in an empty list, no commands are executed, and the return status is 0.
- `echo` displays a line of text

Exercise 2

Create a linux CLI oneliner to extract an overview of the different FTP usernames in the file ftp_bruteforce.pcap. Only the commands tshark and sort are allowed.

```
'user@:~$' • tshark -r ftp_bruteforce.pcap -Y 'ftp.request.command == USER' -T fields -e ftp.request.arg |sort -u
```

- The -r command opens the recording
- The -Y command is used for displaying the filter
- The -T fields -e is used to specify the fields you want to show
- The sort command is used to sort lines of text files
- The -u command is used to show the output of only the first of an equal run

Exercise 3

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@:~$' • date '+Time = %X (%x)'
```

- The date command prints or sets the system date and time
- The +Time is used to set time
- The %X command is used to set the systems time
- The %x command is used to set the date -> with () is used to put () around the date

Exercise 4

Create a linux CLI oneliner to decode the following string

'RGUgcHVudGVuIG9wIGRlemUgdnJhYWcg
emlqbiBhbCBiaW5uZW4uCg=='.
(/home/logs/secret)

```
'user@:~$' • cat /home/logs/secret | openssl enc -a -d
```

- The cat command is used to concatenate files and print on the standard output
- The enc command is used to encrypt or decrypt a file
- The -a command is used if encryption is taking place the data is base64 encoded after encryption. If decryption is set then the input data is base64 decoded before being decrypted
- The -d command is used to decrypt

Exercise 5

Create a CLI oneliner using openssl to retrieve the certificate of the server wiki.uclllabs.be and to display only it's fingerprint, serial and public key. Sample output:

SHA1

Fingerprint=8C:CB:D9:A1:F3:3C:78:C2:2E:F6:EB:1C:CD:4B:F3:39:1B:9A:EE:4Eserial=0966DB4115B74092EE07D6
DA585547D8-----BEGIN PUBLIC KEY-----

MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE2NHdNb3iWbb7mx9UFYzbv05YvUe+uBD8lunSnpj4SSol+5RG5EKZh
FAcXwH9FCUxXE7ZZP3FDLNG0qG8cLSHjg==-----END PUBLIC KEY-----

```
'user@:~$' • echo | openssl s_client -connect wiki.ucllabs.be:443 2>/dev/null |  
openssl x509 -noout -fingerprint -serial -pubkey
```

- The `s_client` command implements a generic SSL/TLS server which accepts connections from remote clients speaking SSL/TLS
- The `x509` command outputs a self signed certificate instead of a certificate request.
- The `-noout` command is used to prevent output of the encoded version of the request
- The `-fingerprint` command is used to show the fingerprint
- The `-serial` command outputs the certificate serial number.
- The `-pubkey` command outputs the the certificate's `SubjectPublicKeyInfo` block in PEM format.

Revision #1

Created 17 June 2021 14:16:30 by Jasper G.

Updated 3 December 2021 22:13:09 by Jasper G.