2019 juni examen

Theorie

- 30 multiple choice vragen (waarvan 6-7 vragen letterlijk uit het voorbeeldexamen kwamen), hierbij zijn ook enkele vragen over de theorie in de labo's

DE VOLGENDE 3 VRAGEN WAREN EXACT HETZELFDE OP HET HEREXAMEN!

- Als er door ftp 6 files gedownload moeten worden hoeveel connecties dan op laag 4? (antwoord: 1 sessie)
- Hoe wordt er bij SSL/TCL ervoor gezorgd dat er geen truncation attack of lagere level encoding aanval kan gebeuren?
- Modulo rekenen (a*b)modn a=17023 b=90004, n = 1000? Zeg ook welke eigenschap van modulo rekenen je gebruikt? (oplossing: 23 * 4 = 92)

Praktijk

Praktijkexamen 1

- Companies like Google and Microsoft make heavily use of the X.509 subjectAltName extension. UCLL also uses this extension to add an alternative name *.ucll.be to the common name (ucll.be) of the certificate. Create a oneliner which calculates the amount of DNS Subject Alternate Names used in the SSL certificate of facebook.com.

```
echo | openssl s_client -connect facebook.com:443 | openssl x509 -text -noout | grep -o 'DNS'
| wc -l
```

- Create a regular expression to match all words in a dictionary with 11 unique letters.

```
cat /usr/share/dict/dutch | grep -P '^[a-zA-Z]{11}$' | grep -vP '(.).*\1'
```

- Show the file /etc/debconf.conf on screen without comment lines (i.e. lines starting with a #).

```
cat /etc/debconf.conf | grep -vP '^#'
```

- Create a linux CLI oneliner to extract an overview of the different FTP usernames in the file ftp_bruteforce.pcap. You can only use the commands tshark and sort.

```
tshark -r ftp_bruteforce.pcap -Y 'ftp.request.command == USER' -T fields -e ‘ftp.request.arg’
| sort -u
```

- Create a CLI oneliner to find a match between different rsa private key files and their companion crt files. The output should look something like:

alfa.key matches to beta.crt gamma.key matches to delta.crt

```
for key in $(ls -1 *.key); do for crt in $(ls -1 *.crt); do if [ [ $(openssl rsa -in $key -
noout -modulus | md5sum) == $(openssl x509 -in $crt -noout
 -modulus | md5sum) ]]; then echo $key matches $crt; fi; done; done
```

--> er is een bestand '/home/logs' op leia waar je dit mee kan testen

Praktijkexamen 2

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

Words with 14 letters: bedrijfsomvang ... Words with 15 letters: ...

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

- Bob needs to send a text file through an encrypted tunnel to Alice. Both already agreed on a shared

secret 'mysecret' using the Diffie Hellman algorithm. Alice wants to display the contents of the file directly on her screen in stead of storing it locally and then opening it. Use a suitable encryption algorithm. The data is sent over a medium which only allows ASCII text. Alice is logged in on debbie and Bob on the virtual machine.

- As a web server administrator you have been asked to give your manager a linux CLI oneliner to extract

the 5 IP adresses that contacted the web server the most. The apache log is located in /home/log. Create a correct oneliner. The output should look something like this: (count IPs) 8000 10.10.10.10 ... 82 81.30.45.89

```
cat /home/logs/apache_google.log | awk '{print $1}' | sort | uniq -c | sort -rn | head -5
```

- Log into leia with a RSA key pair instead of logging in with your password.
- ?????

Praktijkexamen 3

- Use tshark to create an overview of the different HTTP servers in the file http.pcapng(you can find this file in /home/logs). Filter out all of the Apache servers. You can only use the commands tshark and sort.
- Create a oneliner which lists all palindromes with exactly 5 letters in a dictionary.

```
grep -P '^([a-zA-Z])([a-zA-Z])[a-zA-Z]\2\1$' /usr/share/dict/dutch
```

- Create a CLI oneliner using openssl to retrieve the certificate of the server facebook.com and to display only it's fingerprint, serial and public key.

```
echo | openssl s_client -connect wiki.uclllabs.be:443 2>/dev/null | openssl x509 -fingerprint -serial -pubkey -noout
```

- Bob needs to send a text file through an encrypted tunnel to Alice. Both already agreed on a shared secret 'mysecret' using the Diffie Hellman algorithm. Alice wants to display the contents of the file directly on her screen in stead of storing it locally and then opening it. Use a suitable encryption algorithm. The data is sent over a medium which only allows ASCII text. Alice is logged in on debbie and Bob on the virtual machine.
- Make the following directories with a oneliner ~/temp/dir1/dir2/dir3. The solution must be generic: It should work from any location.

```
mkdir -p ~/temp/dir1/dir2/dir3
```

Revision #1
Created 17 June 2021 12:05:34 by Jasper G.
Updated 3 December 2021 22:13:08 by Jasper G.