2018 juni examen

Theorie

- 8 multiple choice vragen
- DNS
- Waarom wordt er bij SSL/TCL zowel symmetrische als asymmetrische encryptie gebruikt? Leg uit met een schema van SSL en zeg waar welke gebruikt wordt.

Praktijk

Praktijkexamen 23/05/2018

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

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

- 2. Ontcijfer de volgende boodschap: RGUgcHVudGVuIG9wIGRlemUgdnJhYWcgemlqbiBhbCBiaW5uZW4uCg== (deze boodschap staat in het bestand /home/logs/secret | base64 -d

```
cat /home/logs/secret | base64 -d
```

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

```
cat /etc/debconf.conf | grep -Ev "^#"
```

- 4. Use Netcat to download an image from "http://darthvader.uclllabs.be/nw2/images/". You can use a browser to choose an image. 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.

```
echo -ne "GET /nw2/images/image1.jpg HTTP/1.0\r\n\r\n" | nc darthvader.uclllabs.be 80 > image1.jpg; cat image1.jpg | tail -n +13 > imagetester.jpg
```

- 5. Perform a zone transfer of the cnw2.uclllabs.be zone to see which hostnames you need to use. Use "dig axfr cnw2.uclllabs.be @ns2.uclllabs.be". Sort the output and format it as follows:

    *.1.cnw2.uclllabs.be. 3600 IN A 193.191.176.1
    *.2.cnw2.uclllabs.be. 3600 IN A 193.191.176.2
    *.3.cnw2.uclllabs.be. 3600 IN A 193.191.176.3
    *.4.cnw2.uclllabs.be. 3600 IN A 193.191.176.4
    *.5.cnw2.uclllabs.be. 3600 IN A 193.191.176.5
    *.6.cnw2.uclllabs.be. 3600 IN A 193.191.176.6
    *.7.cnw2.uclllabs.be. 3600 IN A 193.191.176.7
    *.8.cnw2.uclllabs.be. 3600 IN A 193.191.176.8
    *.9.cnw2.uclllabs.be. 3600 IN A 193.191.176.9
    *.10.cnw2.uclllabs.be. 3600 IN A 193.191.176.10

```
dig axfr cnw2.uclllabs.be @ns2.uclllabs.be | awk '{print $1,$2,$3,$4,$5}' | grep "IN A" | sort -V
```

Praktijkexamen 22/05/2018

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

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

- Give a list of words with 5 letters that are also palindromes.

```
grep -P '^(.)(.).\2\1$' dutch
```

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

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

- Give a list of the usernames tried in ftp_bruteforce.pcap. You can only use tshark and sort (Step by step solution: https://wiki.uclllabs.be/index.php/TShark_Tutorial#Exercises)

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

- Write a oneliner to display the fingerprint, serial and public key of wiki.uclllabs.be

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

Revision #1
Created 17 June 2021 12:06:05 by Jasper G.
Updated 3 December 2021 22:13:08 by Jasper G.