

2019 extra oefeningen + oplossingen - Lars, Martijn, Jonas

Met dank aan de [Github van Martijn](#)

Opgave: cnw2.pdf

Met dank aan Lars Lemmens

Oplossingen

Met dank aan Jonas Berx

Monitoraat Netwerken - By JONAS BERX

```
# Neem niet zomaar de code over, zoek zelf een oplossing :) (man ...) of (... --help)
# Google is ook nog altijd je vriend
# Niet alle oefeningen zijn 100% juist
# Please geen haat als je uitkomst niet klopt
# Ik ben maar een arm studentje uit UCLL dat graag op Netwerken erdoor wilt zijn
# XXX JONAS XXX
#
```

```
1) wget -q -O - http://crl3.digicert.com/TERENASSLCA3.crl | openssl crl -inform DER -text -noout | grep
"Revocation Date" | wc -l
```

```
2) ssh -p 22345 rNummer@leia.ucll-labs.be
```

```
3) ping 127.0.0.1 -c $(ls | grep \.crl$ | wc -l)
```

```
4) tshark -r Cnw2_ftp_bruteforce.pcap -Y 'ftp.request.command==PASS' -T fields -e 'ftp.request.arg' 2>/dev/null
```

sort | uniq -c | sort -rn | head -3 | cut -d ' ' -f 7

5) gebruik de filter : 'http.request.command==POST'

6) nc -z -n -v 193.191.177.1 1-66535 |& grep succeeded ----- nmap -p- 193.191.177.1 --max-rate 50 (Max rate 50 is redelijk traag aangezien er +65000 poorten zijn)

7) who | awk '{print \$1,\$3}' | while read user time; do echo \$user \$(((\$((date +%s) - \$(date -d "\$time" +%s)))/60)) minutes; done | sort | uniq -c (Klopt niet 100% maar geeft je wel de tijd in minuten)

7A) who -H (Simpele oplossing beter te combineren met 7B)

7B) who | awk '{print \$3,\$4,\$1}' | sort | head -1

8) tar -cvf archive.tar /home/LDAP/r0748969 | openssl enc -aes-128-cbc -in archive.tar -out archive.tar.aes;
openssl enc -aes-128-cbc -in archive.tar.aes -out archive.tar.aes.aes (GOOGLE : Tar on the fly -> geen tussenbestanden)

9) ss -lnt4 | awk '/LISTEN/{print \$4}' | cut -d ':' -f 2 | grep -vP '(\.)*\1'

10) tshark -r Cnw2_ftp_bruteforce.pcap -Y 'ftp.response.code==230' (Juiste code wel : 230 maar niet juiste antwoord.. moet nog de login gegevens van de successfull login vinden)

11) #geen moeite in deze gestoken

12) grep -P '^([A-Za-z])([A-Za-z])\2\1\$' (achteraf nog een dict toevoegen om in te zoeken)

14) ls -ld (-d staat voor directory)

15) String = "TGludXggUIVMRVM=" echo TGludXggUIVMRVM= | openssl enc -d -a

16) nmap 193.191.177.1 -p- -r --open -sT

39) cat /usr/share/dict/dutch | grep -vP '(\.)*\1' | grep -P '^([a-zA-Z]{5})\$' (voorlaatste)

#rest zal deze week er wel bijkomen.. Ik doe m'n best

#Good luck all

#De antwoorden hieronder zijn van het examen dat in de les overlopen is

Voor examen : History en dan nummer geven -> handig om op het examen niet je code over te schrijven maar gewoon het nummer van het command te geven.

!!!!!!!!!!!!!!!!!!!!!!!!!!!! 2>/dev/null = vuilnisbak !!!!!!!!!!!!!!!!!!!!!!!!!!!!!

EXAMENVRAGEN

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

2) tshark -r Cnw2_ftp_bruteforce.pcap -Y 'ftp.request.command==USER' -T fields -e 'ftp.request.arg' | sort | uniq -c | sort -rn

3) date '+Time = %X (%X)' OF echo date : \$(date +%Y.%m.%d)

4) cat secret | base64 -d of cat secret | openssl enc -d -a

5) echo | openssl s_client -connect wiki.ucll labs.be:443 2>/dev/null | openssl x509 -noout -pubkey -serial -fingerprint -enddate

Revision #3

Created 17 June 2021 14:20:17 by Jasper G.

Updated 3 December 2021 22:13:08 by Jasper G.