2020 juni examen - versie 2

Examen Juni 2020

Dit examen was tijdens de corona periode. Labo en theorie waren dus samen gevoegd.

Voor theorie: zie het bestande THEORIE.md

Dank aan: Pablopicasso en ISW

cn2_examen_juni2020.zip is gewoon een kopie van de Toledo website op dat moment,

Labo

Instructies

Het examen is gesloten boek, je mag enkel gebruik maken van onderstaande hulpmiddelen:

- pcre handleiding + Linux comand line cheat sheet. Zie dat je een lokale kopie hebt op je laptop (of op papier) voor aanvang van het examen, tijdens het examen is toegang tot de wiki verboden.
- ssh sessie naar server leia.uclllabs.be.

Antwoorden bestaan steeds uit een enkele ‘oneliner’, net zoals in de geziene labo’s en het voorbeeldexamen. Je mag commando’s aan elkaar lijmen met unnamed pipes (| symbool), maar &&, || en ; mogen enkel gebruikt worden wanneer dit echt noodzakelijk is (bijvoorbeeld voor de syntax van een for-loop).

Let op: Bij sommige opdrachten staat er vermeld welke commando's je (niet) mag gebruiken.

Veel succes!

Vraag 1 (voorbeeld): 0 punten

Dit is een voorbeeld vraag, inclusief het correcte antwoord. Bekijk ze goed, zodat je weet wat er exact verwacht wordt.

Maak een CLI oneliner die de directory permissies, eigenaar, groep,... (via ls -l) oplijst van de /etc directory zelf (niet van de inhoud) op server leia.

Daarna pipe je de output van je CLI oneliner in het commando md5sum. In het antwoordveld vul je beide in op deze manier:

```
ONELINER - md5 hash
```

Oplossing:

```
# Met deze onliner kan je de permissies,... opvragen van de /etc directory zelf:
ls -ld /etc
# En zo pipe je de output van deze oneliner in md5sum:
ls -ld /etc | md5sum


# En dit vul je in in het antwoordveld:
ls  -ld /etc - 69ede2180c67f4a59fea0206e031101f
```

Vraag 2: 10 punten

Het bestand Cnw2_ftp.pcap bevat een opgenomen FTP sessie. Je kan dit bestand vinden in /home/logs op server leia.

Maak een CLI oneliner met tshark die de gebruikersnaam toont van de gebruiker die succesvol inlogde. Enkel de gebruikersnaam mag getoond worden. Dus geen witregels, geen errors, geen andere tekst.
In je oneliner mag je enkel gebruik maken van het commando tshark. Geen enkel ander commando is toegestaan. Je mag wel gebruik maken van Wireshark als hulpmiddel om de juiste display filter ('s) te vinden.

Oplossing

```
tshark -r /home/logs/Cnw2_ftp.pcap -Y "ftp.request.command==USER && tcp.srcport==$(tshark -r
/home/logs/Cnw2_ftp.pcap -Y "ftp.response.code==230" -T fields -e tcp.dstport)" -T fields -e ftp.request.arg


# Deze kan ook maar is waarschijnlijk niet altijd juist
tshark -r /home/logs/Cnw2_ftp.pcap -Y 'ftp.request.command==USER' -T fields -e 'ftp.request.arg' | sort | head -1
```

Vraag 3: 10 punten

Maak een CLI oneliner met openssl die het certificaat van de server *wiki.uclllabs.be* als tekst laat zien. Enkel dit mag getoond worden. Sample output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:81:12:b8:1c:24:0c:f3:0d:46:af:cd:9a:9b:96:d2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = NL, ST = Noord-Holland, L = Amsterdam, O = TERENA, CN = TERENA SSL CA 3
        Validity
            Not Before: Jan 22 00:00:00 2020 GMT
            Not After : Jan 26 12:00:00 2022 GMT
        Subject: C = BE, L = Leuven, O = UC Leuven, CN = *.uclllabs.be
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:f5:46:f9:2c:94:f0:86:bd:6f:59:32:7c:4d:82:
                    06:da:d7:87:38:cb:74:98:6d:66:c0:4c:ca:f4:9e:
                    1f:5a:22:25:43:11:07:d4:86:1d:68:92:82:d3:eb:
                    4a:a5:bd:fb:4a:46:84:86:ed:40:be:92:7d:f1:f2:
                    56:3b:2b:9f:eb:84:33:59:0d:62:ef:8d:68:ac:4d:
                    d2:76:84:8c:69:93:47:cc:09:a2:2d:19:9d:ba:c6:
                    e7:e8:03:01:7d:df:44
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:67:FD:88:20:14:27:98:C7:09:D2:25:19:BB:E9:51:11:63:75:50:62

            X509v3 Subject Key Identifier:
                1B:19:0F:9E:AE:E4:39:61:82:08:79:0C:06:42:75:4A:EE:86:BF:6C
            X509v3 Subject Alternative Name:
                DNS:*.uclllabs.be, DNS:uclllabs.be
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl3.digicert.com/TERENASSLCA3.crl
```

```
    Full Name:
      URI:http://crl4.digicert.com/TERENASSLCA3.crl

X509v3 Certificate Policies:
    Policy: 2.16.840.1.114412.1.1
      CPS: https://www.digicert.com/CPS
    Policy: 2.23.140.1.2.2

Authority Information Access:
    OCSP - URI:http://ocsp.digicert.com
    CA Issuers - URI:http://cacerts.digicert.com/TERENASSLCA3.crt

X509v3 Basic Constraints: critical
    CA:FALSE
CT Precertificate SCTs:
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
                    3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
        Timestamp : Jan 22 11:03:02.541 2020 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:44:02:20:5B:C2:BD:AA:16:4F:D8:18:42:10:D7:48:
                    9D:37:37:0B:4D:D6:65:65:F1:BF:08:A4:8D:B4:81:31:
                    02:BF:15:06:02:20:0D:DB:02:07:86:E1:2B:C0:24:04:
                    BE:42:FC:13:5E:77:D5:BF:E9:4B:53:0D:F1:6D:5E:78:
                    51:0A:3F:E4:26:31
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : 87:75:BF:E7:59:7C:F8:8C:43:99:5F:BD:F3:6E:FF:56:
                    8D:47:56:36:FF:4A:B5:60:C1:B4:EA:FF:5E:A0:83:0F
        Timestamp : Jan 22 11:03:02.760 2020 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:46:02:21:00:FF:25:60:84:19:69:76:91:D6:8E:C5:
                    54:ED:7C:D4:40:9F:9B:14:99:2F:22:89:F0:0A:3F:9E:
                    3F:15:98:A3:66:02:21:00:92:05:A1:8D:F3:06:A8:DD:
                    92:E2:86:83:54:C1:BC:F9:5F:03:2E:62:F9:DA:5A:17:
                    2D:F8:D1:E6:5B:A2:78:6A
```

```
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : EE:4B:BD:B7:75:CE:60:BA:E1:42:69:1F:AB:E1:9E:66:
                            A3:0F:7E:5F:B0:72:D8:83:00:C4:7B:89:7A:A8:FD:CB
                Timestamp : Jan 22 11:03:02.616 2020 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:44:02:20:7E:42:D6:3A:55:8B:7B:5A:1E:E0:05:48:
                            09:80:89:E5:A5:7A:FD:8C:5F:EE:AB:2E:7E:D1:07:A0:
                            C2:B4:63:EA:02:20:3A:12:1E:14:28:50:F7:8D:C3:73:
                            EA:9E:6C:AB:5D:B4:A8:AE:27:4C:D1:40:18:23:80:1E:
                            F3:87:B8:A8:98:71
    Signature Algorithm: sha256WithRSAEncryption
        7b:8b:b1:71:c4:73:c9:1f:30:d9:74:ea:b0:e9:a3:a7:a0:7b:
        23:a3:24:cf:e4:c4:f3:8f:82:47:15:4a:e7:4a:05:da:57:0a:
        89:db:90:50:62:0f:a8:95:47:5a:22:eb:5b:2f:a3:fd:31:d0:
        b5:b1:86:02:a1:91:87:65:42:70:ea:fc:49:79:ea:2c:13:fb:
        b0:4e:a5:15:ab:80:82:9d:c9:82:e9:da:9e:bb:81:8a:f0:65:
        eb:ef:73:1c:e4:e2:69:ce:06:fc:38:92:fc:7a:06:72:ae:c7:
        7e:37:37:21:b9:71:52:93:ed:18:b4:5d:91:9c:95:48:62:d6:
        ed:ab:3a:db:1d:22:ed:01:de:7d:56:58:f3:0a:7a:49:4c:cb:
        8b:73:b9:5f:83:f8:c4:b3:1a:ec:54:52:b9:83:ae:db:f7:0b:
        b2:cb:76:d0:99:19:e9:26:f9:c2:12:5d:ec:ea:0b:e3:f4:28:
        8a:da:c2:f5:b3:76:a4:03:c7:02:da:d0:44:a8:7a:6b:19:a0:
        99:99:f4:e8:e9:6b:ab:2e:ce:c8:5f:31:bb:e9:bb:52:35:61:
        ed:5a:22:fa:1c:ed:d0:4c:fe:83:8d:78:8a:43:79:fa:a3:38:
        5b:c2:f0:6e:b5:13:8e:28:fc:c7:f4:2c:a1:fe:79:b4:5a:68:
        fa:41:d5:a3
```

Oplossing

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

Vraag 4: 10 punten

Met welke CLI oneliner kan je volgende string decoderen?

```
RGUgcHVudGVuIG9wIGRlemUgdnJhYWcgemlqbiBhbCBiaW5uZW4uCg==
```

Je kan deze string ook terugvinden in het bestand /home/logs/secret op server leia. Je mag enkel gebruik maken van het commando openssl. Geen andere commando's zijn toegestaan.

Oplossing

```
openssl base64 -d -in /home/logs/secret
# Of een andere oplossing:
cat /home/logs/secret | openssl base64 -d
# Of een andere oplossing:
echo "RGUgcHVudGVuIG9wIGRlemUgdnJhYWcgemlqbiBhbCBiaW5uZW4uCg==" | openssl base64 -d
```

Dit is ook mogelijk maar is volgende de vraag fout, je **moet** *openssl* gebruiken.

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

Examenbestanden:

Revision #4
Created 17 June 2021 13:21:49 by Jasper G.
Updated 23 December 2021 15:49:03 by Baki