HBV602M-2020
Miðmisserisverkefni

1 Um verkefnið

Verkefnið gildir 10% af lokaeinkunn. Það felst í að skrifa hugbúnað í python, helst python 3 en einnig er tekið við python 2 kóða. Nota má grindur sem fylgja verkefnislýsingu sem byrjun. Athugið að verkefnið verður prófað á Ubuntu 18.04 LTS sýndarvél.

Vinna má í hópum af stærð 1-3. Google skjali fyrir skráningar í hópa verður deilt.

1.1 Mat verkefnis

1.1.1 Framsetning kóða (20%)

- Kóðinn skal vera vel skipulagður og brotinn upp í stefjur (procedure) með rökréttum hætti. Hafa má í huga Google styleguide[1] fyrir python eftir því sem við á.
- Nöfn á stefjum og breytum skulu vera stutt og hnitmiðuð en lýsandi.
- Notið „documentation strings“ sbr. https://www.python.org/dev/peps/pep-0257/ til að lýsa stefjum og tilgangi þeirra stuttlega. Notið athugasemdir („inline comments“) þar sem við á til að skýra kóða. Meginregla í kóðaskrifum á þó að vera að kóðinn sjálfur sé nægileg skjölun, t.d. með að velja lýsandi nöfn á stefjur og breytur.
- Notið virtualenv og requirements.txt.
- Stuttar leiðbeiningar á textaformi – README – skulu fylgja öllum kóða. Í README skal lýsa forriti, virkni og tilgangi forritsins og allt sem kennari þarf til að setja upp keyrsluumhverfi og keyra forrit. Þar skal koma fram a.m.k.
    - Nöfn höfunda og tölvupóstur
    - Nafn hugbúnaðarins að eigin vali
    - Tilgangur í stuttu máli – hámark 20 línur
    - Leiðbeiningar um keyrslu – þ.e. skipanalína með mögulegum rofum og nokkur notkunartilvik. Einnig um uppsetningu á virtualenv (sjá kafla 3) s.s. hvort nota eigi python2 eða python3 við keyrslu.

1.1.2 Virkni forrits (50%)

Lítið á lýsinguna sem verkefni sem ykkur er falið af kaupanda og skal hugbúnaðurinn fylgja henni að öllu leiti. Aftur á móti hvetur verkkaupi ykkur til að vera skapandi og má bæta við verkefnið. Með sama hætti má útfæra með betri hætti en verkkaupa datt í hug, svo framarlega sem því er lýst í skjölun og skýrslu. Gefið er fullt fyrir forrit sem keyrir og framkvæmir þær aðgerðir sem beðið er um í verkefnislýsingu. Skilyrði er að kennari þurfi aðeins að setja upp virtualenv og keyra inn requirements.txt (sjá aftast) til að koma upp virku keyrsluumhverfi og kóði keyri villulaust fyrir þau notkunartilvik sem eru skilgreind í leiðbeiningum höfunda (README skrá – sjá 1.1.1).

[1] https://github.com/google/styleguide/blob/gh-pages/pyguide.md

1.1.3 Skýrsla (30%)

Skila skal skýrslu um verkefnið á pdf formi. Heiti skjalsins skal vera HBV602M-{númer hóps}.pdf. Skýrslu má skila með pakkaðri skrá eða sérstaklega. Skýrsla á að vera læsileg en hnitmiðuð – miðað er við sex síður að hámarki með forsíðu meðtalinni. Ekki setja kóða í skýrslu nema sé nauðsynlegt og þá eins lítið og hægt er að komast af með til að skilja texta í samhengi. Skýrsla skal vera vel fram sett með

- Titli, dagsetningu, nafni hóps og nafni allra höfunda á forsíðu
- Stuttum inngangi sem tekur saman tilgang, virkni og af hverju höfundar völdu þetta tiltekna verkefni. Einnig almennt um tól af þessu tagi og stutt umfjöllun um eitt til tvö sem eru til á markaði eða sem opinn hugbúnaður.
- Kaflanum „Virkni og notknun“ sem lýsir í stórum dráttum því sama og README skrá en má vera ítarlegra og gjarnan með notkunardæmum.
- Kaflanum „Hönnun“ sem lýsir hvernig höfundar tókust á við verkefnislýsinguna og þær hönnunarákvörðunum sem teknar voru
- Einum eða fleiri köflum sem svara þeim spurningum sem fylgja verkefninu
- „Lokaorð“ sem fjalla um verkefnið, helstu áskoranir og hvernig höfundar myndu fylgja vinnunni eftir ef þeir hefðu meiri tíma.
- Heimilda sem eru notaðar skal getið. Nægilegt að að heimildir af netinu séu URL í fótnótu (footnote).

1.1.4 Bónus (+5%)

Þeim hópum sem eiga hraðvirkustu útfærslurnar verða veittir 5 bónuspunktar (og hugsanlega einhver smá verðlaun að auki). Skilyrði fyrir bónuspunktum er að öll skilyrði verkefnislýsingar séu uppfyllt, þ.m.t. að skilað sé á réttum tíma. Tímataka á keyrsluhraða verður gerð með eftirfarandi:

```
sudo chrt -f 99 /usr/bin/time --verbose sleep 1
```

hér sýnt með sleep 1 skipuninni. Kennari mælir. Ef vafi leikur á hraða framlaga mun meðaltími yfir nokkrun fjölda tilrauna gilda.

1.2 Tímarammi

Gert er ráð fyrir að skrif hugbúnaðar, prufukeyrslur og skýrsla taki alls 10-14 vinnustundir í samræmi við vægi verkefnisins (10%). Takist höfundum ekki að ljúka við alla þætti verkefnis innan skynsamlegs tímaramma (alls ekki yfir 20 vinnustundir) skal fjalla um árangur sem náðist í skýrslu og ræða það sem út af stendur í lokaorðum.

1.3 Skil

Skilað skal í Uglu – skýrslu á pdf formi og pakkaðri skrá (zip, tar eða tar.gz) með kóða. Passið að pökkuðu skránni séu eingöngu þær skrár sem eru nauðsynlegar, s.s. README, .py og requrements.txt. Ekki pakka virtualenv með og hreinsið út allar .pyc skrár.

1.3.1 Sein skil

Tekið verður við verkefnum allt að einni viku eftir að frestur rennur út en dregið er 10% af heildareinkunn fyrir hvern dag. Það gildir bæði um kóða og skýrslu.

2 Verkefnin

Veljið **eitt eftirtalinna verkefna** (skráið með verkefnahópi ykkar). Þið megið skipta um skoðun hvenær sem er en vinsamlegast passið uppá að skráning sé rétt fyrir skil.

2.1 Portscanner

Skrifið skanna („portscanner“) sem getur fundið TCP port. Þið fáið í hendur python grind að skanna sem virkar til að skanna eina IP tölu með „connection scan“, þ.e. fullt 3-way handshake.

Inntak:

Inntak skannans er

- Ein eða fleiri IP tölur. Nota má CIDR framsetningu eða netrange. Einnig þarf skanninn að geta lesið IP tölur úr textaskrá sem er sniðin með eina IP tölu í línu. Leyft skal vera að setja inn hostnafn (dæmi scanme.nmap.org) fyrir skönn á stökum vélum.
- Port sem á að skanna. Sjálfgefið svið á að vera „well-known ports“, þ.e. TCP port eins og lýst er í https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. Einnig þarf að vera hægt að skilgreina port sem svið, þ.e. {lægsta port}-{hæsta port}. Valkvætt: Sé hægt að skilgrena port til að skanna í textaskrá sem er sniðin með eitt portnúmer í línu.
- Tegund skanns sem á að beita s.s. FULL, SYN, ACK, XMAS
- Hvort gera skuli „host discovery“ fyrst til að greina lifandi IP tölur eða fara beint í skann (sjá nmap -Pn).

Virkni:

- Inntak IP talna eða URL eins og skilgreint að ofan. Hægt skal vera að skanna heilt subnet í einu.
- Inntak porta eins og skilgreint að ofan. Sjálfgefið er „well-known ports“.
- Skanninn skal geta framkvæmt „host discovery“ að lágmarki með ICMP ping. Jafnframt á að vera hægt að slökkva á þeirri virkni.
- Skanninn skal geta greint milli opinna, lokaðra og blokkaðra („filtered“) porta.
- Grunnvirkni er fullt „TCP handshake“ fyrir hvert port og má nota SimpleScanner klasann í grindinni sem gefin er sem byrjun, sem er byggð á dæmi af Python for beginners[2]. Einnig skal í það minnsta útfæra SYN skann og má hafa til hliðsjónar dæmi um stealth scanner sem notar scapy[3].
    - Eftir það má útfæra fleiri skann tegundir s.s. ACK skann, X-mas scann eða RST skann.
- Skanninn skal keyra eins hratt skann og mögulegt er þ.e. fyrir hverja IP tölu prófa öll valin port í röð. Eftir það skal útfæra minnst tvær eftirfarandi tegundir af skannaðferðum fyrir allar skanntegundir sem þið útfærið (hægt að velja á skipanalínu):
    - nota handahófsröð á völdum portum (öll séu þó prófuð)
    - nota handahófsröð á völdum IP tölum (allar séu þó prófaðar)
    - útfæra „low and slow“ skann – þ.e. fyrir hvern skannpakka:
        1) velja IP tölu af handahófi
        2) velja port af handahófi
        3) senda pakka af valinni gerð og skrá niðurstöðu
        4) bíða í mátulega langan tíma þar til ferli er endurtekið

[2] https://www.pythonforbeginners.com/code-snippets-source-code/port-scanner-in-python/
[3] https://pastebin.com/YCR3vp9B

Tilgangur „low and slow“ er að reyna að komast hjá að sá sem fyrir skanninu verður taki eftir því. Mátulega langur tími er því skilgreiningaratriði en þumalputtaregla fyrir þetta verkefni er að hver IP tala ætti ekki að sjá skann atburð í sínum loggum oftar en á 1 mínútu fresti.

Úttak:

Skanninn skal skila notendavænu úttaki sem tilgreinir í það minnsta:

- Netsvið sem var skannað og tegund skanns
- Heildarfjölda porta sem voru skönnuð og niðurbrot í open, closed, filtered
- Öll open port. Ef um er að ræða „well known port“[4] skal einnig skila nafni líklegrar þjónustu.
- Notandi geti einnig skilgreint að sjá lokuð og filtered port (rofi á skipanalínu).
- Valkvætt: Skila „banner“ eða annarri vísbendingu um þjónustu sem hlustar á viðkomandi porti.

Skýrsla:

Í skýrslu skal svara eftirfarandi:

- Skýra útfærsu og hönnunarforsendur.
- Lýsa þeim tegundum skanna sem voru útfærðar. Hvaða pakkar eru sendir og hvaða pökkum getum við búist við til baka? Hvernig geta tiltekin skönn hjálpað okkur sem árásaraðila til að komast framhjá vörnum s.s. blokkun í eldveggjum?
- Gerið prófun á scanme.nmap.org og a.m.k. einu öðru skotmarki - *passið að nota eingöngu kerfi sem þið eigið/hafið yfirráð yfir eða fáið leyfi fyrir prófuninni*. Gerið grein fyrir árangri ykkar skanna í samanburði við nmap. Er ykkar hægvirkari eða greinir minna? Ef svo, hvernig væri hægt að bæta úr? Voru einhverjar skanntegundir sem reyndust betur en aðrar og af hverju?
- Hvað mynduð þið gera til að bæta skannan ef þið hefðuð tíma.

Bónus:

Tímataka kennara verður framkvæmd með SYN skanni á ákveðið sett skotmarka og port lista. Tekinn verður tími yfir nokkurn fjölda skanna á allan skotmarkalistann. Sá skanni sem á besta meðaltímann vinnur. nmap SYN skann verður notað til að finna opin port og árangur ykkar skanna metinn út frá því.

[4] https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

2.2 Hash cracker

Skrifið forrit til að brjóta lykilorðasafn. Þið fáið i hendur grind af forriti sem virkar fyrir einfalt notkunartilvik með regnboatöflu og eftirfarandi skrár:

- Safn lykilorða sem eru hökkuð án salts með MD5, SHA1 og SHA256
- Safn lykilorða sem eru hökkuð með salti og MD5, SHA1 og SHA256

Einnig verður afhentur kóði fyrir hakkafallið sem beitt er og hjálparskrár til að kóða ykkar eigin prófunarskrár og smíða regnbogatöflu. Lykilorðin eru af eftirfarandi gerðum:

- Einföld og þekkt lykilorð sem eru fengin úr lista Daniel Miessler[5]
- Örlítið sterkari lykilorð byggð á sama lista en með táknum og tölustöfum bætt aftan við
- Lykilorð byggð á sama lista en beita „leet-speak“ (þ.e. 0=o, 1=l, 3=e, 4=a, 5=s) umbreytingu
- Slembilykilorð sem nota stafrófið:
  `0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1#$%&*?`
  Flest eru stutt þ.e. 4-6 stafir en nokkur eru lengri.

Söltuð lykilorð nota 4 bæta salt og er stafasett það sama og notað er fyrir base64 kóðun.

Inntak:

Nota má grind sem ykkur er afhent til skilgreiningar á inntaki. Bæta má við virkni að vild.

Virkni:

Cracker skal geta brotið söltuð og ósöltuð lykilorð. Beita má aðferð að eigin vali en mælt er með að byrja á að útfæra rainbow tables.

Úttak:

Skila skal lista af notendanöfnum og samsvarandi „plaintext“ lykilorðum, ásamt heildarfjölda í skrá og hlutfalli sem tókst að brjóta, bæði sem tölu of hlutfalli af heild.

Skýrsla:

- Fjallið um ykkar útfærslu og hönnunarforsendur.
- Hvað tókst ykkur að endurheimta af hverju safni fyrir sig og hvaða tíma tók það?
- Hvaða áhrif hafði algrímur (MD5, SHA1 eða SHA256) og salt á erfiðleikastig þess að brjóta lykilorðasafnið?
- Hvaða aðferðir mynduð þið velja ef þið hefðuð tíma til að endurbæta s.s. að nýta „hash collisions“?

Bónus:

Tímataka kennara verður framkvæmd á söltuðu SHA256 safni með lykilorðasafni sem smíðað verður sérstaklega fyrir það. Sá cracker sem finnur fyrst 80% af lykilorðum sigrar. Meðaltal yfir nokkurn fjölda keyrslna verður notað.

[5] https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10k-most-common.txt

3 Virtualenv

Þessar leiðbeiningar eiga við um þróun á Ubuntu 18.04 LTS sbr. sýndarvélarnar sem við höfum notað í vinnustofum.

Setjið inn virtualenv[6] pakkann:

```
sudo apt-get install virtualenv
```

Búið til vinnumöppu t.d. cracker og setjið upp virtualenv:

```
mkdir cracker
cd cracker
virtualenv -p python3 VENV
```

Ræsið ykkar VENV

```
source VENV/bin/activate
```

Hlaðið inn „dependencies“, þ.e. pip pökkum sem forritið ykkar þarfnast:

```
pip install -r requirements.txt
```

Eftir þetta er umhverfið tilbúið til keyrslu og þróunar. Til að fara úr VENV:

```
deactivate
```

requirements.txt þarf að innihalda nöfn þeirra pip pakka sem þarf að setja upp til að forritið keyri. Nota má skipunina

```
pip freeze
```

til að búa til listann. Passið að hann sé örugglega uppfærður fyrir skil.

[6] https://virtualenv.pypa.io/en/latest/