Toets Informatica

Modulenaam:	Forensic Scripting in Python	
Modulecode:	ifscp	
Studiejaar:	2014 – 2015	
Gelegenheid:	1e en 2e gelegenheid	
Toets opgesteld door:	Peter van der Wijden	
Toetsvorm:	Digitaal	
Aantal verwachte deelnemers:	35	

De duur van de toets bedraagt 20 minuten.

Hulpmiddelen:
Nvt

Opmerkingen:
De toetsing van ifscp vindt plaats aan de hand van gemaakte python-scripts. Deze scripts worden uiteindelijk samengevoegd in een script, zodanig dat de gebruiker de verschillende scripts kan aanroepen en eventueel de resultaten kan delen.

Bijzonderheden:
Aan deze toets is een tweede toets gerelateerd. Deze toets heeft betrekking op de documentatie met betrekking tot het onderhoud en het gebruik van de scripts.

Bijzonderheden:
Aan deze toets is een tweede toets gerelateerd. Deze toets heeft betrekking op de documentatie met betrekking tot het onderhoud en het gebruik van de scripts.

Puntentelling:

Toets Informatica

Opdracht 1

Installeer een aantal ontwikkelomgevingen gebruikmakend van virtuele machines, voor Linux en/of Windows installeer je een Python 2.7 als een Python 3.2 omgeving.
Zoek via internet of anderszins een voor jou plezierig leerboek/basiscursus Python. In de mindmap ifscp.mm vind je enige voorbeelden.
Tover zowel in Python 2.7 als 3.2 "Hello World!" op het scherm.
Maak hier en scriptje van, zodat je deze vanaf de prompt kunt runnen.

Opdracht 2

In deze opdracht ga je enige basisbeginselen van Python uitzoeken.:

- Wat doet het inspringen van de code?
- Syntax
- het import commando, welke modules kent Python zoal?
- input en en output
- datatypes, values, arrays
- for/while/if statements
- functies

Aan de hand van het door jou uitgekozen lesmateriaal maak je kleine programma's. Het lesmateriaal kan bestaan uit boeken, websites, MOOC.
Bewaar deze programma' s, het zijn de bouwstenen voor complexere scripts.

Opdracht 3

Schrijf een programma waarmee je een schijf kunt benaderen. Zorg dat je een directory kunt selecteren en laat vervolgens de namen van de bestanden zien. Sorteer deze namen op alfabet en/of extensie. Zorg dat je ook onderliggende directories aan kan. Zorg dat je de bestanden mbv een OS-commando kunt kopiëren naar een ander opgegeven directory.
Lees het volgende artikel:
http://simson.net/clips/academic/2009.SADFE.xml_forensics.pdf
Integreer deze techniek in een script.

Opdracht 4

Schrijf een programma die binnen een directory m.b.v. metadata kan herkennen welke bestanden hier aanwezig zijn. Laat de verschillende bestanden op soort kopieren naar een aparte directory per soort. Geef ook een lijstje met aantallen verschillende soorten bestanden.
Voor bestandsherkenning kun je de standaard Python mime-types gebruiken, echter deze schakelt op extensie. Een beter methode is gebruik te maken van de " Magic mime file". Hiervoor zijn aparte libraries beschikbaar, of je gebruikt natuurlijk een linux-commando.
Schrijf daarnaast kleine programma' s die van de volgende bestanden metadata uitlezen en presenteren:

- pdf
- office (.doc, .xls, etc)

Opdracht 5

Schrijf een programma die de gps informatie uitleest uit verschillende plaatjes en deze plot in Google maps. Geef daarnaast in een tijdlijn weer de verschillende creatiedatums en wijzigingsdatums van de (plaatjes) bestanden. Geef de diverse exif informatie zoals grootte, resolutie, etc. op grafische wijze weer.

Opdracht 6

Ga op zoek naar verschillende libraries voor het encrypten/decrypten van bestanden. Schrijf een programma waarin je deze libraries toepast. Doe ditzelfde voor steganografie.
Bestudeer de volgende site met tools gebouwd in Python:
https://www.volatilesystems.com/default/volatility

Toets Informatica

Opdracht 7

Zoek uit welke api' s er beschikbaar zijn voor social media als twitter , facebook en hyves.
Schrijf een programma dat deze api's gebruikt en daarmee de relaties van een persoon laat zien.
Schrijf daarnaast een programma waarmee je de headerinformatie van een email uitleest en analyseert.
Laat grafisch relaties , herkomst etc. zien

Eindopdracht / Opdracht 8

Integreer alle vorige opdrachten tot 1 gebruikersvriendelijke applicatie.
Maak een startmenu voor keuze functionaliteit.
Zorg voor helpfunctie en/of gebruikershandleiding.
Geef in de verslaglegging van welke testactiviteiten je hebt uitgevoerd. Beschrijf ook waarom je deze tests hebt uitgevoerd.
Deze laatste opdracht wordt uiteindelijk beoordeeld.