



GPenT0ols

Aquest projecte esta creat per en Marc Hortelano en el curs de Grau
Superior

Abril 2021

Tutor: Victor Marquina

Grau Superior - Administració de Sistemes Informàtics en Xarxa
especialitat en Ciberseguretat

Índice

1. Abstract	2
2. Introducció	2
3. Objectius	3
4. Anàlisi de la programació	3
5. Resultats	3
6. Conclusions	3
7. Referecies bibliografiques	3

1. Abstract

When you start a project you look for precision, but I think the most important thing for me is how you do it. It's how you do it. My main goal is to enjoy learning about this subject as much as possible. The topic I have chosen has been very complicated to define because it can be very broad and sometimes you can get saturated with so much information you find on the Internet. First of all I am going to write about my motivations. Why I have chosen this final project and not another one, since I have had in mind several alternatives and all of them very similar.

Then I would like to show how I have done the project, the steps I have followed and show the final result. Add that my goal of this project is that other people can use it as they want. Which I will show how I have planned it so that it has no security problems as well as how to use it.

As I said before I hope to enjoy and assimilate as much as I can doing this kind of work because I think it helps me a lot to get out of my comfort zone and this kind of challenges makes learning much more fun.

2. Introducció

Feia temps que volia crear-me una eina automatitzada per poder realitzar pentestings, a més a més treballar una mica el desenvolupament web i conèixer noves tecnologies també estava dins el meu pla. La idea del projecte es realitzar un entorn de pentesting de forma gràfic mitjançant una web. Aquest entorn és una infraestructura en Docker on recolliré totes les eines que son útils per a mi i poder realitzar una auditoria de pentesting i desplegar-la de forma còmode i ràpida.

Un pentest consisteix en realitzar un procés d'avaluació coordinat. La prova implica una varietat d'elements, però per a simplificar l'explicació, un individu o equip contractat accedeix al sistema, avaluaria tot el sistema cercant vulnerabilitats o febleses a través d'una metodologia predefinida, aquestes vulnerabilitats són explotades de manera controlada i permet identificar el risc per a l'organització.

La idea s'origina en la necessitat d'automatitzar i les ganes d'aprendre o millorar un llenguatge de programació, concretament Python. Com he comentat anteriorment aquest projecte no ha set la primera idea que he tingut, ja que abans han passat varies molt similars i molt interessants. Una d'aquestes i que m'ha ajudat molt a obtenir aquesta idea final, era crear un plugin del Framework caldera. Caldera és un framework que utilitza les tàctiques de MITRE AT&TCK, i s'utilitza tant per red team com per blue. Aquest inici em va permetre entendre una mica el funcionament de com estava programat. Però aquesta idea no m'acabava de convencer, ja que principalment volia crear una eina per realitzar pentesting i no de red team. Molta gent ho engloba tot i realment són metodologies diferents. Més endavant explicaré que signifiquen aquests conceptes, però detallar aquesta part ho he trobat important perquè ha set de gran ajuda per obtenir la idea final. Finalment vaig decidir crear la meva pròpia eina des de zero, anomenada GPenTools. Com he dit, ho escriure principalment amb Python tant l'entorn gràfic com la majoria de scripts. El que faré serà una web on hi hagui una shell interactiva i tindré totes les eines de pentesting que consideri. Aquesta web et permetrà modificar ràpidament el script i també crear tasques automatitzades. Tota la informació la compartiré en el meu repositori.

ri de Github, ja que ho vull fer de forma pública i que qualsevol persona la pugui utilitzar.

Enllaç del repositori: <https://github.com/Th3FirstAvenger/GPenT0ols>

3. Objectius

Per poder executar aquest projecte, ha set necessari complir uns requisits mínims. Aquest requisit seria comptar amb les bases de Linux i tenir uns coneixements de pen-testing. Els objectius que m'agradaria assolir serien aconseguir una primera experiència desenvolupant una eina automatitzada totalment pròpia amb el llenguatge de programació de python, poder aprofitar aquesta eina per implementar-la en les auditories i seguir treballant amb ella per aconseguir millors. Per complir els objectius ha set necessari una primera fase de planificació, aquesta part consider-ho que ha set la més important ja que soc una persona que li agrada realitzar inversions a llarg termini i tenir una bona preparació.

Com bé deia Abraham Lincoln "Give me six hours to chop down a tree and I will spend the first four sharpening the ax." Dona'm sis hores per tallar un arbre i em passaré les quatre primeres afilant la destral.

Al tenir poca experiència en desenvolupar un projecte de programació a llarg termini, com es normal he comès alguns errors i imprevistos. Sent veritat, que gràcies a l'haver planificat una idea inicial i ben estructurada he rectificar a temps sense que hagi complicat molt el projecta. Quan dic que no tinc experiència vull fer referència que jo en l'àmbit de programació he realitzat sigui scripts automatitzats o creació d' algun exploit web.

4. Anàlisi de la programació

5. Resultats

Listing 1: Python example

6. Conclusions

7. Referències bibliografiques

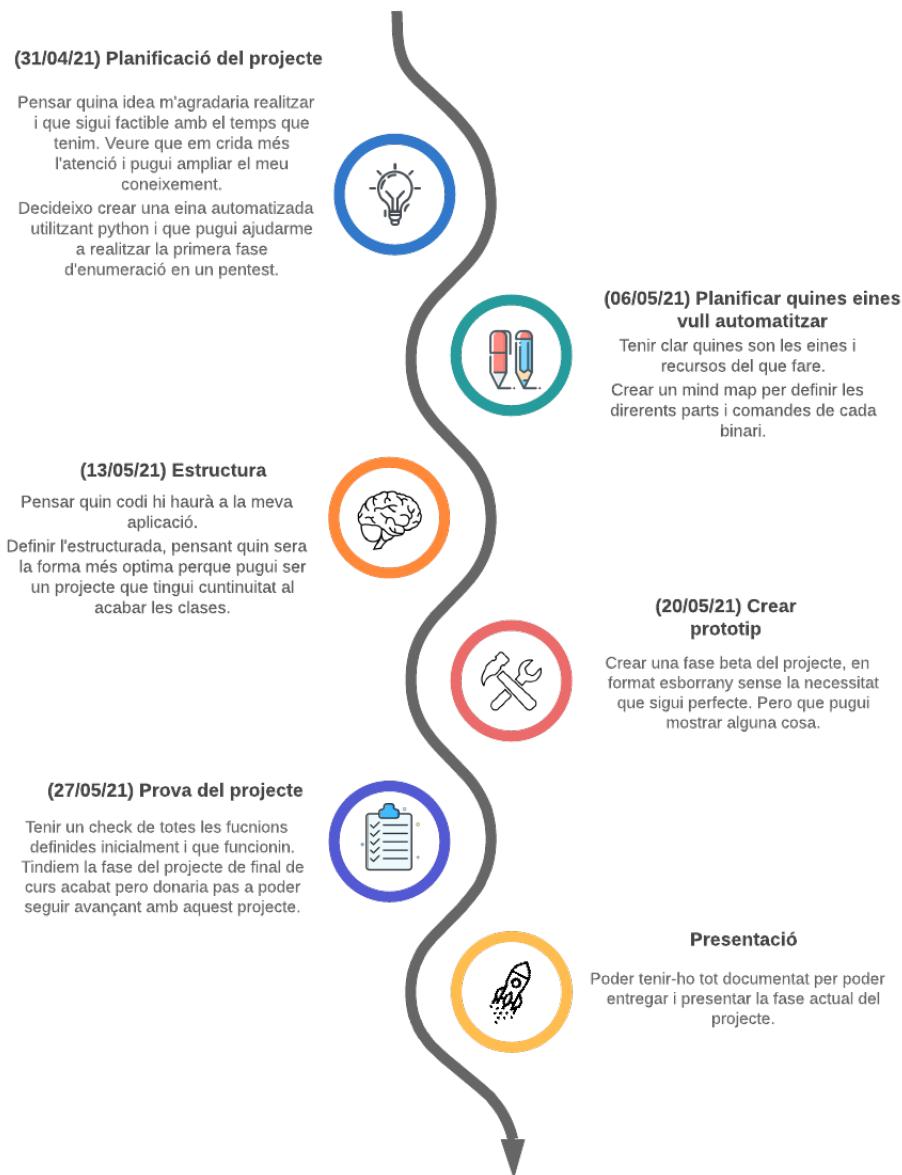


Figura 1: Cronograma del projecte