GPenT0ols

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

Abril 2021

Tutor:

-

Grau Superior - Administració de Sistemes Informàtics en Xarxa

especialitat en Ciberseguretat

Índice general

0.1. Descripció 2
0.2. Objectius 2
0.3. Justificació del projecte 2

0.1. Descripció

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. 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 convecer, 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 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

0.2. Objectius

0.3. Justificació del projecte

Per realitzar aquest projecte obviamente he necessitat tenir una base prèvia i també m'ajudarà a expandir els coneixements apresos en les següents unitats formatives:

La major part ho hem treballat a la uf2 de hacking ètic. El fet de crear una eina automatizada que fa un reconeixement inicial del serveis i vulnerabilitats actives a la xarxa, també et permetrà enumerar vulnerabilitats a nivell de web, linux i windows. Al final fare un recull d'eines funcionals i que aconsegueixin fer un report de forma automatizada. Aquest recull d'eines es trobaran en un contanidor dockeritzat. Aquest tema ho hem treballat sobretot en la UF d'en Jordi.

Finalment també m'agradaria tenir-ho a un web. Aquesta web estarà feta en un framework de python3. Estic aprenent flask, i es una webshell i em premet executar les comandes i falta mostra el output i sigui molt més visual. Apart també vull mostrar la checklist de la metodologia.