Projet PTF Challenge

Objectifs

- Le projet se décompose d'une partie de prise de connaissance sur des sujets CYBER (apprentissage).
- Puis de développement de pages WEB de restitution sous forme de tutoriels, présentations ou challenges.
- Pour les tutoriels il sera recommandé d'utiliser docker

- Ce projet s'inscrit dans la suite des projets des années précédentes.

ASPECT TECHNIQUE

- Technologie de développement :
  - PHP
  - mysql
  - js +
  - bootstrap.

- Plateforme opensource licence MIT :
  - GitHub - secyourdev/SecChallenge
- Intégration des meilleurs sujets sur la plateforme :
  - https://syd-academy.secyourdev.com

Les sujets ou logiciels à explorer

- Anonymizer
- Billcypher
- burps suite (https://portswigger.net/burp)
- Cewl
- Coffre fort mot de passe firefox
- Colasoft Packet Builder
- crunch
- Cutter
- dnsExfiltrator
- Dns twister
- DnsRecon
- Empire
- ExeJoiner
- Exegol
- Firewalk
- Firewall
- FOCA
- Forensic
- Gofish
- harverest
- http.server (SimpleHTTPServer)
- httrack
- ida pro
- impacket
- InfoGa
- Kerberoast
- knockd
- Metagoofil
- mimikatz
- NetScanTools
- Network Topology Mapper
- nmap
- NSE
- OSfooler-ng
- OSINT Framework
- Openvas
- ophcrack
- OSRFramework
- packer
- Recon-ng
- Réputation des sites
- Reverse
- Searchslpoit
- Shellter
- sherlock.py
- Shodan
- Shred
- SmartWhois
- Smishing
- Snmp
- Snmpwalk
- Socks
- spiderfoot (https://www.spiderfoot.net/)
- Spearfishing
- tcpdump
- theHarvester
- timestomp
- Traceroute
- Typosquatting
- UHR
- Visualroot
- VPN
- WAF
- winrtgen
- Vishing
- wget
- XEE
- XSS
- Zenmap
- ssh
- sslyze
- sslstrip
- Stegseek
- Sublist3r
- peCloakCapstone
- portentry
- port knock
- powersploit
- proxy
- proxy switcher
- rainbow tables
- Rat
- Heartbleed
- hping2
- hping3

Contact

- carlos.pinto2@esiee.fr