**BLUE TEAM**

* check apache version and update
* Apache harderning
* script to bring back server quickly
  + if down, if up (scheda di rete)
* hash della password, copia valore nella originale, cambiare in php
* cambiare codice di installazione
* disaster recovery
* snapshot del database:
  + operazione per operazione
  + ogni X tempo
  + monitor dei backup per trovare compromised info
    - se non ci sono caratteri strani
    - balance positive
    - confronto con backup precedente
* Iptables per evitare altre porte attive
* balancing anche al Gateway con iptables per droppare pacchetti con caratteristiche particolari?
* SYN COOKIE
* farsi pagine di errore per gestione
* Varnish/reverse proxy -> <https://serverfault.com/questions/32361/how-to-best-defend-against-a-slowloris-dos-attack-against-an-apache-web-server>   
    
   - To install varnish: sudo apt-get install varnish  
   - Set up configuration of varnish (still unknown how, important thing is to set port to 80 and to set destination server to 10.1.5.2 port 80)   
   can stop service and start it with command sudo /usr/sbin/varnishd -a :80 -b 10.1.5.2:80  
   - Add rule to iptables: sudo iptables -t nat -A PREROUTING -d 10.1.5.2 -p tcp --destination-port 80 -j DNAT --to-destination 10.1.1.3:80
* APACHE MODS: check also other mods
  + <https://sourceforge.net/projects/mod-antiloris/>
* QUESTION: how to assign points to blue and red team?
  + blue team: sia degli attaccanti che per il legitimate?
* SQL dedicated user for DB access

**RED TEAM**

* check ssh password -> if can login, just uninstall apache and delete routes to ssh interface
* check vulns of apache 2.4.18 (<https://www.cvedetails.com/cve/CVE-2019-0190/> ?)
* check other software installed for 0-days/other vulnerabilities that can be exploited
* QUESTION: can do attacks IRL?
* QUESTION: si può fare portforwarding? (oppure linxs?)
* QUESTION: confermiamo che non esiste un legitimate client? (ovvero che anche quello potrà eventualmente mandare crafted packets?)
* QUESTION: se possiamo cambiare le password degli utenti, chi può accedere agli account già esistenti (attaccanti possono usarlo?),
* QUESTION: is the legitimate client limited to have at least 1 request per second frequency?
* problemi su 1=1
* error handling mistakes
* drop la table
* without SQL injection → logic of the implementation
  + valori tipo stringhe su numeri
  + valori negativi
* QUESTION: E’ legito fare bruteforcing (dictionary) - con lo spoofing