

Testy Penetracyjne

szczepionka przeciwko cyberwłamywaczom

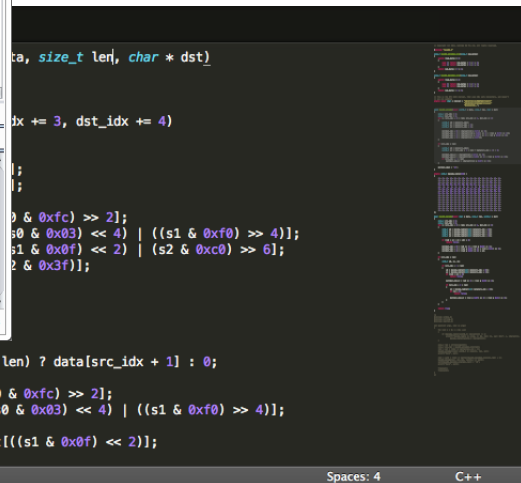
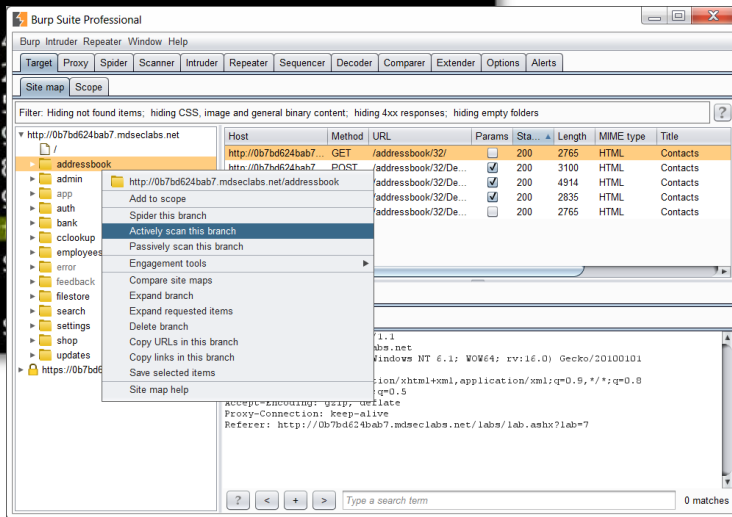


Jak wygląda typowe
„hakowanie”?

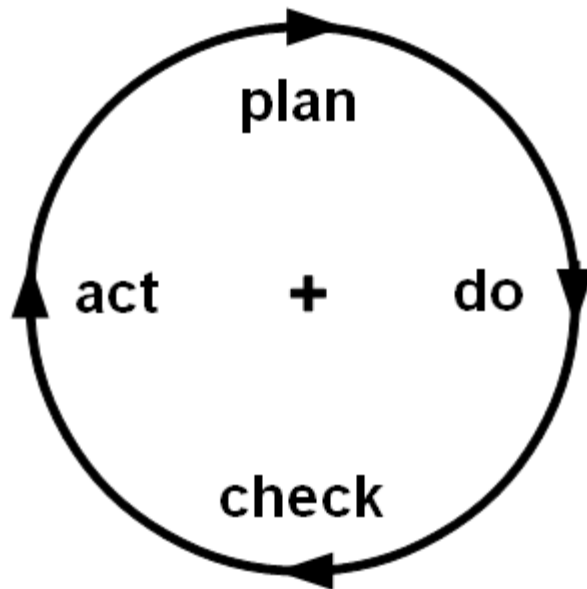
Czy konieczne elementy to picie wina, tańczenie na krześle obrotowym i wizualizacje 3D na ekranie?

Jak wygląda typowe „hakowanie”?

```
vivek@wks01:~/scripts$ pwd
/home/vivek/scripts
vivek@wks01:~/scripts$ ls -l
total 32
-rwxr-xr-x 1 vivek vivek 54
-rw-r--r-- 1 vivek vivek 17
-rwxr-xr-x 1 vivek vivek
drwxr-xr-x 2 vivek vivek 409
-rwxr-xr-x 1 vivek vivek 1028
drwxr-xr-x 2 vivek vivek 409
vivek@wks01:~/scripts$ cd py
vivek@wks01:~/scripts/python
/home/vivek/scripts/python
vivek@wks01:~/scripts/python
```



Typowy schemat działania



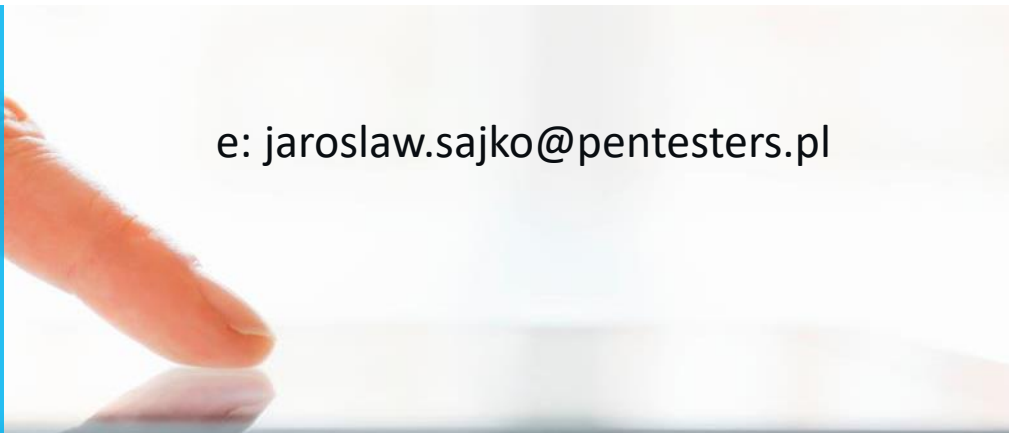
Czego nauczyliśmy się
podczas realizacji 1000
testów penetracyjnych?

Kluczowe wnioski

- 1 Hakerów nie obchodzą Wasze firewalles i antywirusy, etc.
- 2 Regularne testy to przede wszystkim transfer wiedzy, który podnosi kwalifikacje personelu IT, uczy dobrych nawyków obronnych i przystosowuje do mobilizacji w przypadku rzeczywistego zagrożenia. Poza tym pozwala wyeliminować największe widoczne gołym okiem problemy.
- 3 Do prawdziwych cyberwłamania dochodzi na skutek wykorzystania z reguły dobrze znanego, z reguły łatwego w identyfikacji, z reguły prostego w zabezpieczeniu zagrożenia

Czy Testy Penetracyjne to rzeczywiście szczepionka przeciwko cyberwłamywaczom?

Testy Penetracyjne od prawdziwego ataku różnią się tym, że są zaplanowane, przebiegają w sposób kontrolowany i ograniczają się do identyfikacji wzorca ataku i obrony (nie wyrządzają prawdziwej szkody).



e: jaroslaw.sajko@pentesters.pl