Pentest : Les audits d'intrusion pour mieux agir.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 27/6/2019 13:00:00

Maillon-clÃ© de lâ□□audit dans le domaine de la cybersÃ©curitÃ©, le Pentest (ou test dâ□□intrusion) permet aux entreprises et collectivitÃ©s de mieux connaitre les vulnÃ©rabilitÃ©s de leur SI et de prendre des mesures leur permettant de cartographier et de monitorer leur degrÃ© dâ□□exposition au risque.

Entre fantasme de geek et expertise rÃ©elle : quels sont les contours de cette mÃ©thode ? ConcrÃ¨tement, le test dâ□□intrusion permet dâ□□analyser une cible du point de vue dâ□□un hacker.

Il sâ□□agit donc dâ□□une rÃ©elle mise en situation qui permettra de tirer de prÃ©cieux enseignements sur la permÃ©abilitÃ© dâ□□un SI Ã des attaques variÃ©es en ciblage (IP, applicatives, rÃ©seaux,â□¦) ou en approche (force brute, white, grey ou black box, â□¦)

Ã□ quoi servent les tests dâ□□intrusion ?

Globalement, le Pentest permet dâ□□identifier les vulnÃ©rabilitÃ©s, puis dâ□□Ã©valuer les risques et (finalement) de conseiller sur le type de correctifs Ã mettre en place.

Ainsi, cette approche permettra dâ□□adopter une dÃ©marche de sensibilisation et dâ□□Ã©valuation concrÃ¨te de la menace potentielle qui servira de base pour proposer des actions correctives adaptÃ©es (Ã ce stade, il sera possible de planifier des interventions, en fonction du niveau de criticitÃ© des risques identifiÃ©s).

En approfondissant, on remarque que la technique du pentest se fonde sur plusieurs angles dâ□□attaques possibles, se distinguanten trois grandes catÃ©gories. Nous parlons ici des approches dites de White Box, Grey Box et Black Box.

Dans cette segmentation, qui impose une complÃ©mentaritÃ© des trois approches, lâ□□angle dâ□□attaque des pentesteurs dÃ©pend de leur rÃ´le simulÃ© au sein de la structure testÃ©e. Super-admin (avec les pleins droits), salariÃ© Â« standard Â» ou encore en situation Â« rÃ©elle Â» de piratage : telles sont les trois options majeures entre lesquelles un vÃ©ritable Ã©ventail de possibilitÃ©s existent .

Un autre point tient au moment oÃ¹ sont rÃ©alisÃ©s les tests dâ□□intrusion sur lâ□□infrastructure Ã lâ□□Ã©preuve. Depuis la conception dâ□□un systÃ¨me jusquâ□□Ã lâ□□analyse postÃ©rieure Ã une intrusion ; le timing propre Ã lâ□□intervention du pentesteur dÃ©finira aussi son approche.

Que recherche un pentesteur ?

De nombreuses rÃ©ponses existent parmi lesquelles nous pouvons citer : un accÃ¨s Ã des informations, une cartographie des vulnÃ©rabilitÃ©s (SI, applications, infrastructures), des tests dâ□□efficacitÃ© des systÃ¨mes de dÃ©tection dâ□□intrusion ,le type de rÃ©ponse apportÃ©e par les Ã©quipes cyber des entreprises, etc. Les cas dâ□□usages sont multiples et dÃ©pendent de facteurs complÃ©mentaires : organisationnels, techniques, etc.

Suivant le rÃ´le endossÃ© par le White Hat Ã lâ□□origine du test dâ□□intrusion, les rÃ©sultats attendus diffÃ¨rent. Le pentesteur pourra ainsi mettre Ã jour une faille dans lâ□□authentification des collaborateurs dâ□□une entreprise â□¦ comme une problÃ©matique de sÃ©curitÃ© du code

inhÃ©rent aux serveurs dâ□□une application. Tout dÃ©pend du pÃ©rimÃ¨tre de sa mission et de son analyse.

Le pentest occupe donc une place importante dans le processus dâ□□audit de sÃ©curitÃ© IT. En se concentrant sur une approche trÃ¨s opÃ©rationnelle, il Ã©value concrÃ¨tement les risques cyber en se positionnant du point de vue dâ□□un hackeur Ã un moment donnÃ©.

Â

- Les mÃ©tiers de la cybersÃ©curitÃ© â□□ Interview de Maxence Bobin, Directeur RÃ©gional Squad Paris :Â