Is Ethical Hacking even Ethical?

We have been seeing cyber crime all over the news recently. President Obama and President Xi of China recently came together for a summit in California to discuss their future relationship, particularly in regards to their cyber warfare; the American NSA leaked information about the PRISM Program, and the list goes on. Many fear for the safety of their country and governments, but how about your businesses?

Data breaches are one of the most detrimental problems a business of any size could experience. Having a service like Digital Locksmiths perform a penetration test could save companies from serious financial losses of up to $42.7 billon.

The biggest question that arises after suggesting such a service is common: is Ethical Hacking even ethical? I mean, you are allowing someone to break into your system. This could involve some sneaky tactics like social engineering where we trick a user by doing something like clicking on a link they shouldn't open, or by having them give us their password over the phone. It might seem drastic, however, we believe that this is the best method in testing the security of your establishment.

The first thing to know about the hacking community is that it has three subsections: the Black Hats, Grey Hats, and White Hats.

Black hats: these are the guys you need to watch out for. They hack for the purpose of destruction with little care of the final result. They are usually interested in defacing, stealing, or exposing your information and/or property.

Grey Hats: while they're problematic and have the potential to be dangerous, Grey Hats aren't necessarily trying to wreak havoc. They are more likely trying to hack for the purpose of proving they can. However, they still might accidentally damage your content on their way in or out.

White Hats: That's us, the good guys! We're the ones you hire to check and make sure everything is secure in your networks. We have all of the nasty skills of a Black Hat, but we only use these skills with your permission and with your best interests at heart. To properly test your systems, we need to do everything that a black hat would do. The difference is that you know that we're doing it. We are employing a type of esoteric morality that entrusts us to use our skills to achieve the greatest good, and we have been properly trained and educated to act in such a way. To put yourself in the mindset of a Black Hat hacker is the only way to adequately test the security quality.

It is important to outline with your Penetration Testers the processes that they will go through to test your networks, and have it approved by the most senior executive to ensure the safety of the company. You also need to understand that they may find access to areas with sensitive information. However, trusting a Penetration Tester is like trusting your doctor; we will have you sign thorough contracts trusting us to keep your information confidential.

Chris Kirsch, a product marketing manager at Rapid7, compares Penetration Tests to doing a crash safety test on a car: "You might have really smart engineers. They are putting the car together. They are focusing on safety, but you don't really know how safe the car is until you actually do a crash test. A crash test is seemingly quite scary, but it actually is the only way to find out how safe the car is, how secure the car is."

Preemptively hiring a Penetration Testing services firm is an assurance that all of your company's information and property is completely safe and inaccessible. After all, you don't want to wait until it is too late. [...]

Terry Cutler, *www.terrycutler.com*, June 21, 2013
Terry Cutler is an ethical hacker and co-founder of Digital Locksmiths, on IT security and data defense firm.

CONSIGNES

PREMIÈRE PARTIE (10 POINTS)

Vous rédigerez **en français** un compte rendu du texte.

Votre compte rendu devra comprendre une brève introduction qui indiquera la source et le thème du document. Vous synthétiserez et reformulerez les idées essentielles du texte.
Une brève conclusion personnelle qui dégage l'intérêt du document dans une perspective professionnelle sera valorisée.

(200 mots +/- 10%) *Vous indiquerez impérativement le nombre de mots de votre compte rendu.*

DEUXIÈME PARTIE (10 POINTS)

Vous êtes responsable du parc informatique d'une entreprise britannique qui, malgré toutes vos précautions, vient de subir une cyber-attaque. John Berry, votre directeur, vous demande de lui rédiger un rapport sur la sécurité informatique au sein de l'entreprise.

Rédigez ce rapport **en anglais**. Vous décrirez la nature précise de l'attaque et vous referez le point sur toutes les mesures à prendre par l'ensemble du personnel. Vous évoquerez également une ou plusieurs des nouvelles techniques capables de vérifier la fiabilité du système informatique pour éviter une nouvelle intrusion.

(200 mots +/- 10%) *Vous indiquerez impérativement le nombre de mots de votre rapport.*

PREMIÈRE PARTIE (10 POINTS)

Suggestion de barème :

14 points pour le compte rendu selon le barème ci-dessous
4 points pour la correction et la qualité de la langue française
2 points pour la synthèse et la reformulation des idées
Possibilité d'attribuer jusqu'à 2 points de bonus pour une conclusion personnelle qui dégage l'intérêt du document dans une perspective professionnelle

Diviser le total par 2 pour obtenir une note sur 10

Respect du nombre de mots : ne pas prendre en compte ce qui est écrit au-delà du nombre de mots précisé dans la consigne

Source, (date) : www.terrycutler.com (21 juin 2013) Nature précise de la source Thème : l'éthique dans le domaine de la cybercriminalité	/1
Le thème de la cybercriminalité est récurrent selon des informations récentes	/ 1
Les présidents américain et chinois se sont réunis pour en discuter	/ 1
Les failles de la sécurité des données sont un des problèmes majeurs des entreprises	/ 1
quelle que soit leur taille	/ ½
La question est : dans quelle mesure les techniques de piratage peuvent servir à protéger les systèmes informatiques des entreprises ?	/ 1
Il existe trois sortes de pirates informatiques	/ 1
Les chapeaux noirs commettent des actes de malveillance	/ 1
Les chapeaux gris n'ont pas forcément l'intention de détruire le système piraté	/ 1
Les chapeaux blancs tentent d'assurer la protection des données informatiques	/ 1
Les responsables de la sécurité informatique doivent pouvoir faire confiance aux chapeaux blancs	/ 1.5
Ce test est indispensable à la sécurité informatique au même niveau que le crash test de voiture	/ 2

Ce test est à faire avant qu'il ne soit trop tard	/1
Compte rendu	**/ 14**
Qualité de l'expression en français	/ 4
Capacité à reformuler et à synthétiser de manière personnelle les idées du texte	/ 2
Bonus *: conclusion personnelle dégageant l'intérêt du document dans une perspective professionnelle*	/ 2
Total	**/ 20**
Note de la première partie	**/ 10**

DEUXIÈME PARTIE (10 POINTS)

Suggestion de barème :

Respect du format demandé (rapport) → 1 point

Adéquation de la réponse avec la situation → 4 points

Correction grammaticale et richesse lexicale → 4 points

Capacité à rendre son discours technique accessible à un destinataire non spécialisé → 1 point