TD: Is ethical hacking even ethical?

Part 1: Identify the key ideas and logical sequences of the article.
What type of document is it? What is the underlying idea and goal?

Write a summary of the article by rephrasing the main points.

Introduction: briefly mention the source and main theme of the text.

Conclusion: what is interesting in this article from the perspective of a company?

Part 2: You're responsible for the IT stock of a British company that has just suffered a cyberattack, in spite of all the security measures you've taken. John Berry, the director of the company, asks you to write a report on cybersecurity within the company.

10 minutes preparation in pairs (only English allowed)

Write the report in English. You're expected to give a brief description of the precise nature of the attack and to review all the measures to be taken by the employees. Also mention one or two new techniques likely to test the reliability of the computer system to avoid any further intrusion/break-in.

Writing a report

A report is a systematic, well-organised document which defines and analyses a subject or problem, and which may include:

- the record of a sequence of events
- interpretation of the significance of these events or facts
- evaluation of the facts or results of research presented
- discussion of the outcomes of a decision or course of action
- conclusions
- recommendations

Reports must always be:

- accurate
- concise
- clear
- well-structured

Mindmaps

Have a look at the link below to find out how to draw a mindmap. Listen to the video by Tony Buzan.
http://library.bcu.ac.uk/learner/Study%20Skills%20Guides/11%20Mind%20Maps.htm

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.