Oscar Velez Moncada 10123550 Tutorial 1

CPSC 329 W17 - Assignment 1

University of Calgary

Due Feb 8, 11:59 pm

Question 1 (6 pts)

Write one suggestion that you would like to see implemented in lectures/tutorials. A one-line answer is sufficient.

If the professor could use a microphone in class. Although the voice is heard, it's not sufficient enough for the people in the back.

Question 2 (24 pts)

For each of the following categories:

Hacktivism, Cyber Warfare , Cyber Crime , Cyber Espionage

1. The attackers were nine teenagers from Anonymous, with the victim being the Thai government. Because the Thai government started proposing a plan that would let all traffic internet go through one "tunnel" meant that the government would control Internet traffic. The hackers created a DDoS attack and used social media sites to get people to visit the government website and overload its internet traffic capacity. It's unsure how the attack was detected but several arrests were made. This fits the definition of Hacktivism as the people teenagers are activists and tried to stand up for what's right with the use of computers .The government was going to censor websites and spy in on private conversations, therefore this was the motivation of the attackers. https://www.bleepingcomputer.com/news/government/thai-police-arrests-nine-anonymous-hackers-for-role-in-opsinglegateway-attacks/. The author's name is at the bottom of the page, and date is recent, from December 2016
2. The attack came from a botnet with five major Russian banks being under attack. The botnets were automated from thousands of computers in several countries and attacked through DDoS. Several attacks from the botnet lasted for two days. They claim that the first attack was registered, and the bank's cybersecurity team located the attack. Motivation was most likely to obtain customer's bank information, and this attack was a big-scale attack that this kind of botnet attack can affect many other devices, and this was an ongoing attack from one state to another, which fits the definition of cyber warfare. https://www.rt.com/news/366172-russian-banks-ddos-attack/. Author's name in the article, and article is 2 months old.
3. It was unknown who the cyber criminals were but the attack was targeted towards Lloyds Banking Group. Using a denial of service attack, the criminals made fake accounts to bombard the website with more requests than it could handle. No bank accounts were taken from the attack. The article didn't go into detail how the attack was found but the IT team deployed what is called a "geo-block" which from my understanding blocked attacks from a specific geographical location, but that also meant it blocked customers from that location as well. Motivation of the attackers seem to be to obtain customer bank information, and a crime was committed though the use of a computer and network. https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack. Name of author is in the article, and date of article is from January 2017
4. Two Italian people (one a nuclear engineer and his sister) and the victims were two former prime ministers, Vatican cardinals and the president of the European Central Bank. The two siblings hacked into the emails of these people and were arrested for selling state secrets. The alleged hacking had been happening for years and attempted to hack into several thousand other emails. The attackers used a malware which allowed them to see the emails being interchanged between high ranking officials, and both siblings were

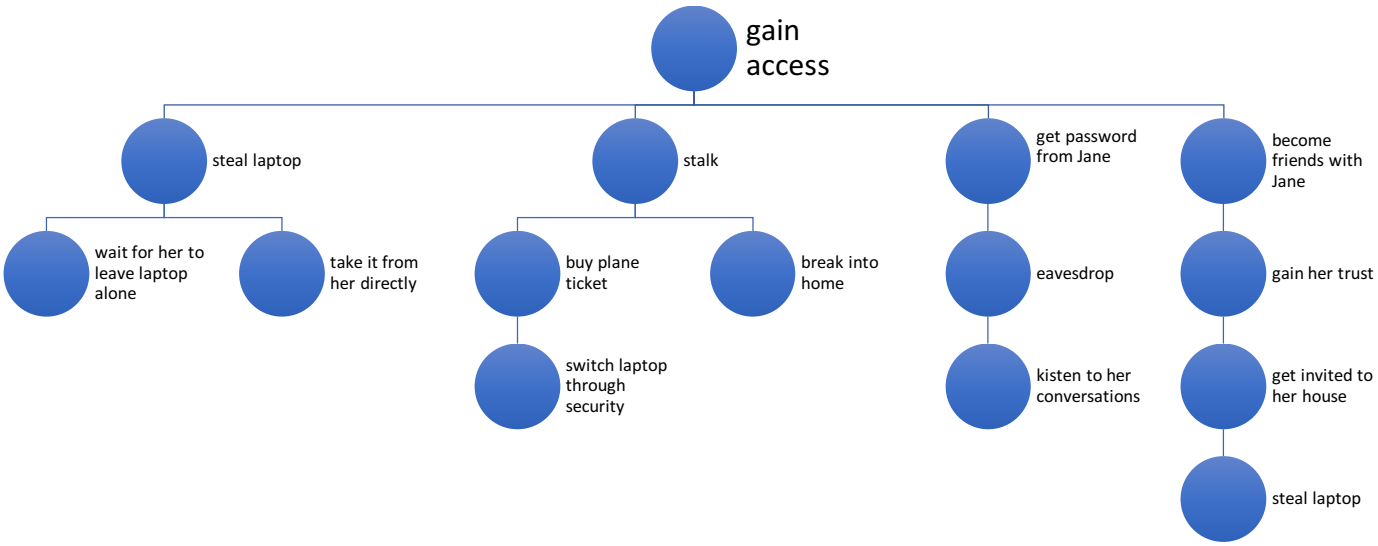
arrested. Money was the motivation to sell government secrets, and they used of computers to obtain secrets and information without permission. http://www.telegraph.co.uk/news/2017/01/10/italian-brother-sister-arrested-cyber-espionage-operation-tapped/. Author's name of the article is given, and the date is from January 2017

Question 3 (25 pts)

Attack trees provide a graphical method of analyzing attacks. Consider a scenario where Jane, the CEO of a company, has stored the company's highly confidential investment plan on her laptop. Jane has a busy travel schedule, passing through airports and staying at hotels in different cities. In addition to doing work, she uses her laptop for email as well as browsing internet for per personal purposes. Draw an attack tree assuming the goal of the attacker is to gain access to the investment plan document. The tree should have at least 3 levels (including root).

Further reading on attack trees: B. Schneier, Attack Trees, Dr. Dobb's Journal, December 1999

https://www.schneier.com/academic/archives/1999/12/attack_trees.html



Question 4 (8 pts)

Estimate the entropy of passwords of length 10 for the following scenarios:

- passwords consist of lowercase characters only, e.g. **`helloworld`**;

~47 bits

- passwords consist of lowercase and uppercase characters, e.g. **`HelloWorld`**;

~57 bits

- passwords consist of lowercase and uppercase characters, and also digits, e.g. **`He110W0r1d`**

~60 bits

- password consists of lowercase and uppercase characters, digits, and also 11 symbols e.g.

`He!!0W0r1d`

- `~62 bits`

Only the following 11 symbols are used: `? ! @ # $ % * ( ) - +` .

Question 5 (14 pts)

Estimate the entropy of 4 passwords (from previous question) by doing your own calculations, and also by using two tools, such as:

https://apps.cygnius.net/passtest/

http://rumkin.com/tools/password/passchk.php

Record your results in a table (4 pts):

Password	My estimate	Tool 1 estimate	Tool 2 estimate
`helloworld`	47	14.8	36.4
`HelloWorld`	57	16.874	44.2
`He110W0r1d`	60	27.5	46.5
`He!!0W0r1d`	62	31.2	43.8

Briefly describe your conclusions from this study and in particular comment on

a) the effect of password set size of on the entropy of passwords, (5pts)
From my conclusion passwords that have a set size can only have a maximum entropy, and you're limited to what you can input, although the more choices you're given for a password the bigger the entropy result is.

b) the effectiveness of tools for password estimation (5 pts).
It is effective to the point where it tells you if your password is strong or not, and forces you to think of a harder password, but both websites gave different results in entropy numbers even for the same password which doesn't seem to be consistent.

Question 6 (23 pts)

Consider a password system that uses password hashing for password verification. Each password consists of a string of 4 digits: ($\square_3\square_2\square_1\square_0$), that is each $\square_\square$ can be a digit {0,1,2,...,9}. So $\square_0$ represents the rightmost digit, while $\square_3$ is the leftmost digit in the password. The hash function is defined as:

$$h(\square_3\square_2\square_1\square_0) = (\square_3^4 + \square_2^3 + \square_1^2 + \square_0) \ mod\ 100$$

where "*mod 100*" is the remainder of integer division by 100.

1. How many different passwords are possible in this system? (1 pt)

   $10^4 + 10^3 + 10^2 + 10 = 11\ 110$

2. Calculate *h(7819)*. (2 pt)

   23

3. Find a password *x* such that *h(x) = h(7819)* but $x \neq 7819$. (5 pts)

X = 5776

4. How many different passwords will have hash value equal to h(7819)? You may find it useful to write a program to get a precise answer. (5 pts)

   Infinitely many passwords as long as the number equals 23 + (n*100) where n >1.

5. Suppose an attacker wants to access John's account using an online attack. What is the probability the attacker will guess John's password if no hashing is involved, and when hashing is involved? (5 pts)

   If no hashing is involved it will take the attacker $\log_2(10^4)$.

6. Suppose the password system is used with a 2 digit salt($\square_1\square_0$).The salt will be simply added to the hash value (integer addition) and (mod 100) operation will be used to make it into a 2 digit number. In other words, the hash function is now:

$$\square(\square_1\square_0, \square_3\square_2\square_1\square_0) = (10\square_1 + \square_0 + \square_3^4 + \square_2^3 + \square_1^2 + \square_0) \square\square\square\ 100$$

   For example, the hash for password 2745 given salt 39 is:

   h(39,2745) = (39 + 2^4 + 7^3 + 4^2 + 5) mod 100 = 19.

   Explain how adding salt affects success chance of an attacker who tries to guess the password. Explain your answer using the password 7819. (5 pts)

   Even after using the password 7819 you end up with a hash value of 62, which means there are other integer congruent to 62 mod 100 will give you the same result