IDENTIFICATION: HOMEWORK1 ANSWERS/MC

Assignment 0 Overview of threats/attacks

No# / Type	Category	Impact	Likelihood
1 DDOS	Direct	High	High some companies
2 Trojans horses	Indirect / direct	High	High
3 Key loggers e.g. in WOW	Direct	High WOW:Low	High
4 Worms (spread virus)	Direct	High	High
5 Brute force, password cracking	Direct	High	Low
6 Adware	Indirect	Low	High
7 Spoofing	Direct	Low	Low
8 Rootkits	Direct	High	Low
9 Phising , e.g. Nemid	Indirect	Medium	Medium
10 Fake sites / drive by download	Indirect	Low	Medium
11 SQL Injections	Direct	High	High
12 Key locker	Direct	High	Low
13 Packet sniffing man-in-middle	Direct/Indirect	High	High
14 Spam mail	Direct	Low	High
15 Botnets (organizing virus/worms)	Direct/Indirect	High	High
16 Open ports	Direct	Medium	Low
17 Buffer overflow	Direct	High	Low
18 Stack overflow	Direct	High	Low
19 Iot rapberry usb program	Direct	Medium	Low
20 SW App. Layer attack	Direct	High	Medium

ref: https://www.hongkiat.com/blog/famous-malicious-computer-viruses/

ref: https://www.popsci.com/scitech/article/2009-04/top-10-computer-viruses#page-11

Definitions of terms

- **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.
- **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server…all the things you probably associate with the term *hacking*.
- **DoS attacks:** These are designed to prevent legitimate access to your system. And, as you will see in later chapters, this includes distributed denial of service (DDoS).
- **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session hijacking:** These attacks are rather advanced and involve an attacker attempting to take over a session.
- **Insider threats:** These are breaches based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

Assignment 1

Visit http://www.digitalattackmap.com/

Pick out 1-2 interesting periods of activity and describe the following:

- The date (period)
- A major botnet activity and list:
  Source and Destination

  How long the attack has been occurring

  How has the attack been pulled off?

On the 29th of January at 07:10
Someone in Denmark was DDOS'ed by a host of different countries, the DDOS attack lasted for at total of 24 min and maxed out at ~45.000 Mbps and was of the category of "Volumetric Attacks" which is an attempt to cause congestion by attempting to consume a lot of bandwidth.

Also the 29th of January at 10:56
China was DDOS'ed, the attack lasted 18 min and maxed out at ~151.000Mbps and was of the category 'TCP Connection Attacks' which is attempts to use up all the available connections to infrastructure like firewall and application servers.

Assignment 2

Find at least two major companies/organizations/NGO's that have been attacked lately.
Explain what happened and how the company handled the situation.

Useful links describing some real life attacks

The unknown case from 1982-84 KGB and FBI in Canada
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html

The fappening (*Emilio Herrera*).
[1] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

Operation Shady RAT
[2] http://www.telegraph.co.uk/technology/internet-security/9942462/Five-of-the-biggest-hacking-attacks.html

U.S. Office of Personnel Management
[3] https://www.yahoo.com/tech/the-biggest-computer-hack-attacks-of-the-last-5-125449860474.html

https://en.wikipedia.org/wiki

Drive by download Attack
https://www.comodo.com/resources/home/newsletters/nov-10/ask-geekbuddy.php

CSC-Tinglysning
http://www.version2.dk/artikel/kontroversiel-kopi-site-af-tingbogen-lukker-ned-570512

CSC- CPR-sagen
http://www.version2.dk/artikel/datatilsynet-kritiserer-flere-myndigheder-dele-mainframe-og-diske-hos-csc-542185

Twitch.Tv - Hacked unauthorized access - March 24, 2015.
https://www.usatoday.com/story/tech/gaming/2015/03/24/twitch-warning-breach/70366310/
Data breach of users. To protect its users, twitch is expiring passwords -- which means users must create a new one once they log in -- and disconnected accounts from Twitter and YouTube.

Taringa! - Hacked - unauthorized access – September 4, 2017.
https://thehackernews.com/2017/09/taringa-data-breach-hacking.html
"Latin American Reddit" massive data breach - 28 million users login details leaked. To protect its users, Taringa is currently sending a password reset link via an email to its users as soon as they access their account with an old password.

Krebsonsecurity-hit-with-record-ddos. 2016 September
https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos

Sony hacked cause of the movie "The Interview" (*Nordkorea*)
Sony PlayStation Network

CSC (*Gottfrid Warg*)

Biggest breaches and the costs of them: JP Morgan, YouTube + 14 more companies
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Mærsk Ransomware 2017 June
https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliardbeloeb
On 27.june 2017 was hit by the ransomware-attack called PetYa
The "Petya" malware attack came through a piece of software alot of companies use to file their tax returns in Ukraine. A security-expert called it an amateur-attack because the ransomware would encrypt the computer, but

they only demanded 300 dollars to open the computer again, if they had known that they would hit maersk they could have demanded a lot more, so they didn´t know who they were targeting.
After Mærsk got hit, they held a lot of crisis calls and meetings and they focused on the internal communication, constantly sending out updates on which ports were open or closed, and they quickly made a simple makeshift bookingsystem.
They had to use WhatsApp on their private phones.

HBO 2017 August Ransomware
https://www.ft.com/content/7156e7b2-7639-11e7-90c0-90a9d1bc9691
The company kicked off August 2017 with an apparently massive breach of its servers, in which hackers pilfered everything from full episodes of unreleased shows to sensitive internal documents. Not long after, in separate and distinct incidents, two episodes of Game of Thrones leaked out early. And Thursday, hacker group OurMine hijacked HBO's main Twitter account, along with those of several HBO shows. It's been a hell of a couple of weeks.
Hacker that identified as Mr. Smith dropped four unreleased episodes of HBO shows, as well as the script to an unreleased episode of Game of Thrones. They suggested they had 1.5 terabytes of HBO data in total, ranging from more shows to financial statements and other sensitive documents. A week later, the same person or group followed up with a ransom note demanding millions of dollars in exchange for the leaks to stop.
Industry analysts say HBO has done a good job in responding quickly with public and internal messaging. One of the mistakes companies that have been hit by a data-security breach often make is that they release partial or inaccurate information that only extends the story. Furthermore, HBO decided to offer a $250,000 payoff to the hacker.

2017 Power grid attack in Ukraine
https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack
Power plants stopped working for 1-6 hours affecting 0.2% of the electric power supply.

Assignment 3

Look at the following keywords and state a short answer:

1. What is confidentiality?
2. What is integrity?
3. What is authentication?
4. What is authorization?
5. What is availability?
6. What is a Denial of Service (DoS) attack?
7. What is DDos?
8. What is a virus?
9. What is a Trojan horse?
10. What is a worm?
11. What is a bot?
12. What is a botnet?
13. What is a zero day?
14. What is an n-day?
15. Is a bug the same as vulnerability?
16. What is a weakness?

Name 4 ways an attacker can act anonymously online Look at the following keywords and state a short answer:

1. What is confidentiality? Prevents unauthorized observation of data.

2. What is integrity? Prevents unauthorized modification of data.

3.What is authentication? Assures that communicating entities are the ones they claim to be.

4. What is availability? System information/resources that are available authorized users whenever they need them.

5. What is a Denial of Service (DoS) attack? An attempt to make a machine or network unavailable to its users, by disrupting the internet access on the machine or network. This is done by overloading the machine or network with requests, to prevent the machine or network to fulfill all the request. These attacks are easy to stop as the user can just block the IP the attack is coming from.

6. What is DDos? Similar to a Denial of Service attack, though the requests are coming from a lot of different sources and are therefore much harder to track and block.

7. What is a virus? A virus is a malicious software program, that once executed, replicates itself by changing other programs code and replacing its own code with it.

8. What is a Trojan horse? A trojan horse is malware that appears harmless but is not, and its main goal is to mislead users of its original purpose.

9. What is a worm? A computer worm is a standalone malware computer program that replicates itself to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

10. What is a bot. bot is short for robot and also called an internet bot-- is a a software program that performs automated tasks over the internet . It can act as an agent for a user or other program or to simulate a human activity. Bots are normally used to automate certain tasks, meaning they can run without specific instructions

11. What is a botnet? A botnet is a group of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack.

12. What is a zero day? Also known as a computer zero day, is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw.

13. What is an n-day? This is where 1-day or n-day exploits kick in: now that vendors have admitted to a fault and started repairing it publicly, attackers can write exploits that target those systems that were not yet updated since the time of disclosure. The term 1-day or n-day indicates that a delay of 1 or more day / n days has occurred between the time of disclosure and the time a system is attacked.

14. Is a bug the same as vulnerability? Not to a full extend, but some people can make use of it and exploit it.

15. What is a weakness? Exploitable part of system, which can be easily manipulated by malicious entities

16. Name 4 ways an attacker can act anonymously online?
Create a false email-address, false profile on facebook tiktok, dating sites. Steal identity information.

Assignment 4

Look at your list from assignment 0.

Then choose 1-2 of these attacks and detail the description, i.e. state the:

- exploitability, how easy is it to do (and possibility of doing it)
- prevalence(likelihood), how often does it occur (how common is it)
- detectability, how easy is it to detect the vulnerability
- impact, how severe is the damage of a successful attack

all using the scale: high, medium, low

Tip: Take a good look at www.owasp.org …..find top ten security risks

https://owasp.org/www-project-top-ten/2017/Top_10

Look at the OWASP pdf file in it-security/solutions