COMPUTER SUBJECT: BASIC NETWORK CONCEPTS

TYPE: GROUP WORK EXERCISE/DISCUSSION

IDENTIFICATION: HOMEWORK 1/MC

COPYRIGHT: *Michael Claudius*

LEVEL: EASY

DURATION: 1-3 hours

SIZE: 100 lines!!

OBJECTIVE: Introduction to network basic

REQUIREMENTS: **Computer Security**

COMMANDS:

CSF Chapter 1 Assignments

The following assignments must be solved in groups (3-5 persons) and followed up by a short presentation in the class later.

Assignment 0
Find 10 security threats/attacks and for each state:
- type(direct/indirect)
- likelihood (high, medium, low), how likely is this attack
- impact (high, medium, low), how severe is the damage of a successful attack

Assignment 0 Overview of attacks

No# / Type	Category	Impact	Likelihood
1 DDOS	Direct	High	High some companies

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

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's activity and list:

Source and Destination

How long the attack has been occurring

How has the attack been pulled off?

If you cannot access the attackmap skip this assignment !!

At home watch the video by Stephen Vries at

https://www.owasp.org

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.

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 botnet?
12. What is a zero day?
13. What is an n-day?
14. Is a bug the same as vulnerability?
15. What is a weakness?
16. Name 4 ways an attacker can act anonymously online

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

Goto menu projects and https://owasp.org/Top10/

You might prefer to look at https://owasp.org/www-project-top-ten/2017/Top_10