Solutions: Sheet 5

1. Malware

(a) Explain the following terms: "Malware", "Virus", "Trojan", "Worm", "Spyware", "Adware", "Ransomware", "Zombie", "Backdoor", "Root Kit".

- **Malware:** The word malware is a combination of the words *malicious software*. It describes software that affects or changes the functionality of a computer in a malicious way.
- **Virus:** A virus describes malware which spreads uncontrollably on a system by infecting (e.g files, programs).
- **Worm:**
- **Trojan:** A Trojan describes malware that looks like a normal, non-malicious software, but contains hidden features that negatively affect the system from the user's point of view.
- **Spyware:** Software that is installed with other programs. Used to analyzes the behavior of users.
- **Adware:** Software that is installed with other programs. Used to displays unwanted advertisements.
- **Ransomware:** Program that blocks access to the users's data unless a ransom is paid.
- **Zombie:** An infected system with Internet connection that can be used for all kinds of malicious activities.
- **Backdoor:** A backdoor can be used by a hacker to gain control over a system. It manipualtes various parts of an operating system to ensure it's not discovered and to monitor the system.
- **Root Kit:** A rootkit is a set of tools that you run on a target computer when you have somehow gained access to it with root privileges. The purpose of the rootkit is to turn this temporary access into an always-open door.

(b) What are the two essential aspects to classify malware?

Malware can either be classified based on . . .

- . . . means and mechanism of distribution. So how the malware distributes, e.g via email or self-replicaitng.
- . . . the malicious behavior of the malware.

(c) Give four possibilities of what damage malware may cause and what purpose the attacker could pursue with it.

1. The attacker could encrypt the data and blackmail the affected person, e.g. either the person pays or the data is destroyed.
2. The attacker could gain access to the computer to include it in a bot-network. The computer is then used for attacks like DDos, spam mails or other things without the owner's knowledge. The malware thus also harms third parties and not only the infected computer.

3. The attacker might not have malicious intentions, instead it could be a pentester trying to discover security vulnerabilities in a system or of a software.
4. The attacker could use the malware to obtain information. The purpose could depend on the party, e.g., a central authority, a hacktivist, or a blackhat.

(d) List three different types of viruses and briefly describe how they work in your own words. Research an implementation example type for each virus type and describe it briefly. (Don't forget to include the source in your solution.)

- **Boot Viruses:** A boot virus infects the boot sector of a system. A boot sector is a physical sector on a hard disk that contains information about booting an operating system. Hard disks and other storage devices have boot sectors. When the computer boots, the BIOS looks in the first sector of a storage device for the information needed to boot the operating system. The first sector/boot sector is often either the Master Boot Record (MBR) or the Volume Boot Record (VBR). The boot sector is a potential attack point for malware. The advantage is that the boot sector always starts automatically and sometimes without any protection (modern hardware usually has protection mechanisms). So when the infected boot sector code runs, the malicious code is executed. [1]
- **Michelangelo:** The boot virus *michelangelo* was first detected in 1991. The virus infected the MBR and always format 1 hard drive sector on the 6th march of every year. It overwrites hard disk data with random characters - including the root directory and FAT (File allocation table). This combination makes the hard disk unusable and makes recovery of data and MBR practically impossible. [2]

Source:
[1] https://www.lifewire.com/what-is-a-boot-sector-2625815
[2] https://compscistation.com/boot-sector-virus-examples/#4_Michelangelo_-_Detected_1991

- **File Viruses:** A file virus insert code into executable files. When the file is opened or used may overwrite the file and cause damgae to the content of the file. [3]
- **Sunday:** The file virus *sunday* was detected in 1989. It infect `.exe`, `.com` and `.ovl` files and demage them. Symptoms of the virus were increased file size and infected files contained the string "Today is SunDay! Why do you work so hard? All work and no play make you a dull boy! Come on! Let's go out and have some fun!" [4]

Source:
[3] https://www.techopedia.com/definition/55/file-infecting-virus
[4] https://en.wikipedia.org/wiki/Sunday_(computer_virus)

- **Macro Viruses:** Macro viruses are written in a macro langauge. (programming language which is embedded inside a software application). When the macro is executed, e.g when opening a program, the malicous code is executed. [5]
- **Nuclear:** The macro virus sprads through Word Documents. The creator first attached the virus on a word document, with a discription of the virus implentation and furthermore the virus was attached to this document. The virus consists of a series of Word macros and infects the document when it is

opened. The virus manipulates the default Word template NORMAL.dot. It also destroys any Word document saved using the Save As function by attaching its macros. [6]

Source:
[5] https://en.wikipedia.org/wiki/Macro_virus
[6] https://www.f-secure.com/v-descs/nuclear.shtml

(e) Explain four different protective measures against malware and describe in your own words what the respective protective measure does.

- **Sciptblocker/Adblocker:** Deactives certain script which may change the behaviour of the site. E.g an adblocker blocks scripts so no advertsing is displayed.
- **Firewalls:** A firewall filters the traffic of a network and blocks possible attackers from unauthorized access.
- **Pentesting:** Pentesting describes the analysis and testing of a system for weaknesses in order to close them.
- **Honeypot:** Honeypots are systems which are suppose to be infected by an attacker in order to study the attackers pattern und observe him. Honeypots are used to distract the attacker from the actual target.

(f) For what reason, from the perspective of an attacker, can a manual attack on a machine make more sense than an automated attack, for example by a virus?

The advantage of manual attacks is that they are much more targeted, e.g. by analyzing the target system or victim. Manual attacks can also be customized, while a virus only executes steps that have already been coded. Infecting a virus is also based of the *competence* of the target or luck. (E.g does a target downloads the file with the virus or not).

Make sure only a specific system is attacked.

Viruses are faster detected.

(g) Research the exact functionality of virus scanners and describe them in your own words.

Manuel monitoring:
Can for patterns in the code, based on a blacklist of viruses/virus patterns.

Realtime monitoring:
Check read write access

Problem: only knows already known malware

(h) How can a user remove malware from an infected system? Describe two different methods and discuss their advantages and disadvantages.

- Backups → use virus scanner to make sure files of backup is not infected
- Try to get rid of malware
- boot from usb stick (linux) with scanner and clean and get rid off infected files

2. Passwords on Linux

(a) In which file can the user passwords be found in the Linux operating system?

The `/etc/passwd` file is the password file where each user account is stored. The `/etc/shadow` file contains the password hash information for the user account and optional aging information. `passwd` stores general user info and `shadow` stores user passwd info. `passwd` is the file where the user information (like username, user ID, group ID, location of home directory, login shell, ...) is stored when a new user is created. `shadow` is the file where important information (like an encrypted form of the password of a user, the day the password expires, whether or not the passwd has to be changed, the minimum and maximum time between password changes, ...) is stored when a new user is created.

Source: https://askubuntu.com/questions/445361/what-is-difference-between-etc-shadow-and-etc-passwd

```
$ cat /etc/passwd
```

(b) Which hash function was used for the passwords?

Usually passwords are stored in the following format `$id$salt$hashed`. The `$id$` indicates the algorithm used.

- `$y$` is yescrypt
- `$1$` is MD5
- `$2a$` is Blowfish
- `$2y$` is Blowfish
- `$5$` is SHA-256
- `$6$` is SHA-512

(c) In this context, explain the so-called salt parameter. What is the value of `salt` for the user `itsec`?

As the same password is always hashed to the same hash value, a random salt is added to the password. Then it's hashed. So when encrypting the hash values of both passwords are different as their salt differ.

```
itsec:$y$j9T$hPjUAImhD7alc6..aX1wd.$...
         ^^^
```

3. Breaking Passwords

Determine the password of user itsec on Linux operating system using a dictionary attack. Document all of your steps (i.e. commands within the command-line interface) and state the duration of your attack.

- Combine `passwd` and `shadow` file so `john` can use them. If it's not done some options of `john` might not be available.
- Remove the unnecessary information so that only the information for the `itsec` user is included in the file.

```
$ sudo unshadow /etc/passwd /etc/shadow > input.txt
```

- Guess the hash using john and the password list
- `--format=crypt` uses yescrypt
- `--show to show the password afterwards`
- `~/Desktop/password.lst` the dictionary
- `~/Desktop/input.txt` the file with the hash

```
$ john --format=crypt --show ~/Desktop/password.lst ~/Desktop/input.txt
itsec:itsec:1001:1003::/home/itsec:/bin/sh

1 password hash cracked, 0 left
```