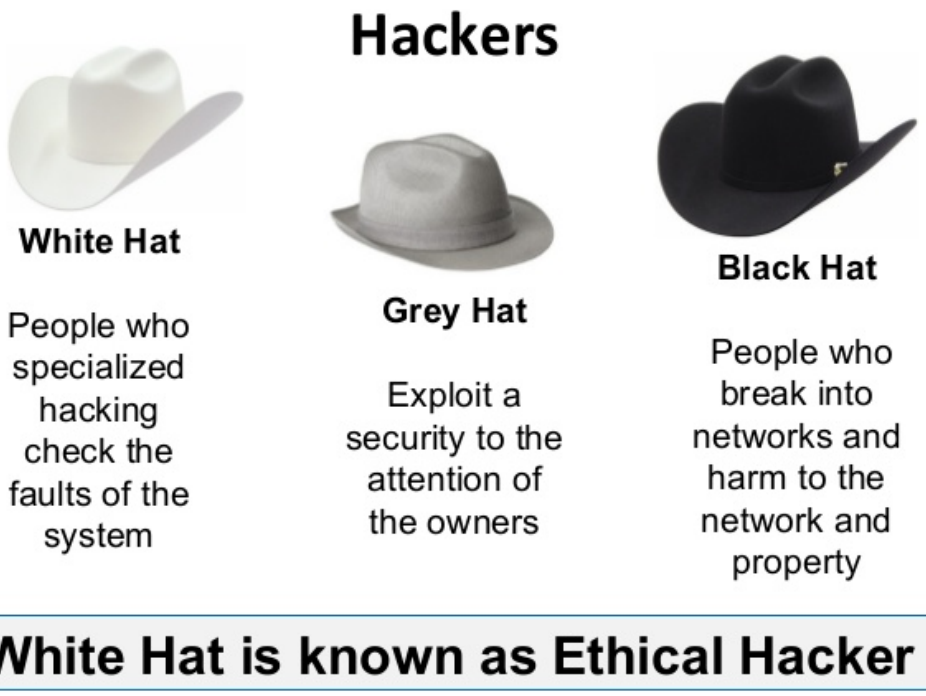
Reading material O5

Actors (heroes and villains) in cyber realms

In the world, people are mostly divided into two: thugs and angels, i.e. people who bring good or evil to order. However, in the world of cyber defense, players are divided into three:

- **“white hats”** are those who do good things. Their goal is to find security bugs in the system and report them or fix them. They are also called ethical hackers.
- **"gray hats"** are those who, depending on the situation, can do so much good or can also act for their own benefit, i.e. if, for example, when a security error is discovered, it is possible to get a benefit for it, they will definitely take it out.
- **“black hats”** or "backhats" are characters who have rather evil motives and are feared because their goal is only self-interest and doing harm to others.



Videos:

- Differences of black, gray and white hackers https://youtu.be/E6S3-XGrZAE
- Story of Anonymous https://www.youtube.com/watch?v=M0gTCTXr0ig

A huge variety of people have been involved with computers and the Internet. The following is just a short list of some interesting names - it's definitely worth looking for more interesting people yourself.

- **Robert Tappan Morris** (born November 8, 1965) is known as the creator of the world's first computer virus. He created his so-called "Morris worm" as a first-year student at Cornell University in 1988. A year later (1989) he became the first person to be convicted of a virtual

crime. Morris was accused of creating and spreading the so-called Morris worm. The Morris worm is considered to be the first computer worm to spread on the Internet. He sent the worm out of the computers at the Massachusetts Institute of Technology to avoid suspicion of Cornell. Morris later claimed that he created the program out of pure scientific interest and that his goal was instead to measure the size of the Internet. However, there may have been a bug in the worm's transmission system, as a result of which some infected computers started reproducing the worm over and over until they became unusable. The Morris worm corrupted a number of systems in this way. The data on the extent of the damage is unclear, and it is also not known exactly, many systems and computers were directly damaged. What is known, however, is that Morris was fined $10,000 and sentenced to 3 years probation. However, the Massachusetts Institute of Technology seems to have forgiven him - Morris is now an assistant professor there.

- Kevin Mitnick (born August 6, 1963) made famous the attack on people related to IT systems and gave a new meaning to the term social engineering (in Estonian, techno-social hacking, communication attack, manipulation of people, etc.). Mitnick found that tricking/influencing people is often the easiest way to get into the system. Mitnick has served multiple prison terms for his illegal activities. Now, however, he is officially the head of a self-named company (Mitnick Security Consulting LLC) that performs security tests.
- Steve Wozniak (born August 11, 1950) Steve Wozniak, who co-founded Apple with Steve Jobs (born February 24, 1955), was interested in hacking phones before programming the first Apple computers. The "blue boxes" used for making free calls (Blue box, https://en.wikipedia.org/wiki/Blue_box) were made by the Steves for their own use and sold to others at a price of approximately 170 dollars a piece.
- Edward Snowden (born June 21, 1983 in North Carolina) is a former CIA and DIA employee and later NSA contractor at Dell who became world famous as a whistleblower when he leaked information about the NSA and CIA's top-secret PRISM surveillance program. The disclosure of PRISM caused a global scandal. Snowden has been declared wanted by the United States and is accused of several crimes, including treason and espionage. Snowden's actions have created two camps: one side sees him as a traitor who should be tried, while the other side thinks he is a hero and deserves respect as a whistleblower of illegal government surveillance.
- Julian Assange (born Julian Paul Hawkins; born 3 July 1971 in Townsville, Queensland) is an Australian internet activist and journalist, founder and editor-in-chief of WikiLeaks. Previously worked as a programmer. In the 1980s, it allegedly infiltrated the information systems of the following agencies: the Pentagon and other US Department of Defense agencies, MILNET, the US Navy, NASA, Citibank, Lockheed Martin, Motorola, Panasonic, Xerox, and several universities. At this point, it is worth noting that the information systems of large institutions are large and complex - so breaking into one subsystem does not mean that all parts of the system are under the attacker's control.
- **Deidre Diamond** - Cyber Security Network (CyberSN) Administrator. Started his career through a StartUp accelerator called Rapid7. the company deals with cyber defense training on non-technical topics. Is the initiator and leader of networks, the creator of a positive work culture.
- **Alissa Johnson** - Head of Information Security at Xerox, previous position at the US White House. His goal was to connect the business and policy communities to make the best cyber defense decisions. In his work at the White House, he was also responsible for budgeting and ensuring the integrity of the infrastructure in various locations, also using the capabilities of cloud technology.

- **Katie Moussouris** is a US cybersecurity researcher. He created Microsoft's Bug Bounty support program. His company is Luta Security. He has also been involved in the creation of the US Department of Defense's bug-finding program for hackers.
- **Paige Bailey** - aka DynamicWebPaige. A Google Artificial Intelligence developer who previously worked at Microsoft on the same topic and also working on making Azure more secure.
- **Krisina Svechinskaya** - is a former Russian hacker who defrauded people with passport and bank forgeries. He hacked the Zeur Trojan to get money from the banks.

Gamer types and roles

As our project is about developing a game there are several things you need to know about the cyber security game types, but also what kind of gamer you are. When you find a match for your interest, gamer type and role in the game, then you will come back to learn again and again.

VIDEO: 5 types of gamers https://www.youtube.com/watch?v=cRnz5LvN4xI

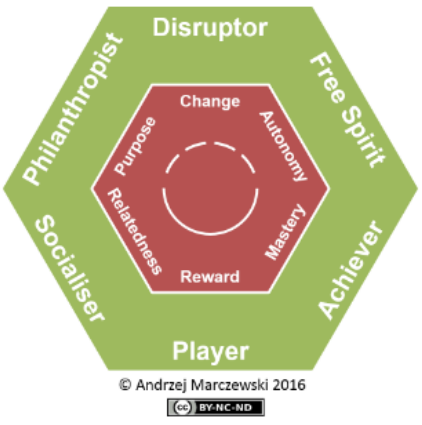
Exercise 1 - find your gamer type
Open up the website https://gamified.uk/UserTypeTest/user-type-test.php?lid=
Take the test and learn who you are!

Example

Overview of the types

- **Socialisers** are motivated by Relatedness. They want to interact with others and create social connections.
- **Free Spirits** are motivated by Autonomy. They want to create and explore.
- **Achievers** are motivated by Mastery. They are looking to learn new things and improve themselves. They want challenges to overcome.
- **Philanthropists** are motivated by Purpose. This group are altruistic, wanting to give back to other people and enrich the lives of others in some way.
- **Players** are motivated by Rewards. They will do what is needed of them to collect rewards from a system.
- **Disruptors** are motivated by Change. In general they want to disrupt your system, either directly or through other users to force positive or negative change.

Learn more about Marczewski's User Types



Exercise 2 - think of what kind of role you would like to take on the game? Make a list of 3 potential roles that relate your competence and interest.

For starting at the cyber security games you need to have skills to search internet, problem solving and technology use at a beginner level. It helps if you know different languages (english, russian to chinese to whatever). And if you have special deeper skills or interest in something from the next list you are ready to go!

Are you a:

- A LEADER OF PEOPLE - Deals with strategy and planning and risk analysis. Dealing with ethical and legal issues, creating and conducting presentations, dealing with people and managing communications. The human aspects also include knowledge of techno-harvesting.
- ADMINISTRATOR (DEFENDER) - Deals with administration and improvement of systems and services. In most cases, developers are divided into systems (win/linux/web/mobile) and network administrators (firewalls, network construction). According to skills, administrators are divided into initiators (can manage and solve simple problems), intermediate (can create rules), advanced (can create a system, e.g. be an architect). An important skill is to identify problems and collect evidence (English forensics).
- THE SCRIPTER - Deals with code analysis and script automation. Can program safely.
- PENTESTER (ATTACKER) - Deals with finding and attacking weaknesses. He has diverse knowledge of operating systems (Windows, Linux, smart devices), web/database programming and their vulnerabilities, scripts to exploit vulnerabilities. You may come across rootkit malware, reverse engineering, intelligence and analysis of public sources, or OSINT (open source intelligence).
- HARDWARE WEAKNESS FINDER - Deals with finding hardware weaknesses and collecting evidence (English forensics). Mobile devices, smart cards, Arduino, locks, etc. breaking devices, using digital logic. The skills are related to the electrician profession, but at a higher level, at the level of a new product developer.
- CRYPTOGRAPHER - Deals with creating and solving ciphers at different levels (algorithms, public/secret key, etc.), logic problems, hashing and blockchain, and steganography.

Every role is usually needed in a cyber game (CTF and Attack-Defence based). Attack and defense skills are the same, but used from different sides (RED or BLUE). Leadership and Crypto go deep on their level separately. Good leaders know about tech, but also know how to lead people, be a team player, but also know how to present the finding example for company higher staff or sponsors.

<table>
<tr><td colspan="3">Leadership</td></tr>
<tr><td>Applications</td><td>Applications</td><td rowspan="4">Crypto</td></tr>
<tr><td>Operating system</td><td>Operating system</td></tr>
<tr><td>Network</td><td>Network</td></tr>
<tr><td>Hardware</td><td>Hardware</td></tr>
</table>

Types of games

There are four types of cyber security games: tests, table top-, video games, capture the flag (puzzles and attack/defense) style games and real simulation attacks of real systems or real missing persons searches or OSINT challenges. Some are interactive and some are like just taking a test in school. But all of them activate your brain and teach different concepts or skills.

- **Tests** - these games are usually like educational surveys or tests that one can take at school, at the workplace. Tests are easy to make and take and share. Teachers and companies usually develop a lot of them to execute. Example Google Phishing test. In our Cyber4Schools game we provide puzzle options between simulations.
- **Card Games and tabletop games** - these are usually gamified discussions that are helped to visualize with paper based simulation of cards. Table tops help adults to understand issues on their current processes or learn new concepts. In our Cyber4Schools game we provide a play on paper concept game before entering the real simulation.
- **Video Games** - there are several video games that you can run on PC or gaming console to learn about cyber security. These game developments take a lot of time and funds to make as it uses gaming motors, visualization and game story needs to be at a high level. Videogames list of examples. In our Cyber4Schools game we provide some visualizations of our game that will raise the motivation to play the game.
- **Capture the Flag (CTF)** games are divided into two categories
    - Puzzles/Jeopardy - you need to find the flag (correct answer). In our Cyber4Schools game we provide exercises that use the solution in a visual way.
    - Attack-Defense games - you need to defend your systems or attack someone else's systems. In our Cyber4Schools game we provide simulation for these events.
- **Real simulation attacks** - example phishing exercise on a real company. Usually they are done by the company IT service or ordered by the professionals. In our Cyber4Schools game we provide simulation for these events.
- **Real missing persons searches or OSINT challenges** use online searches for finding needed information about the company or persons. In our Cyber4Schools game we provide simulation for these challenges inside the game.

Video European Cyber Security Challenge https://www.youtube.com/watch?v=xk389TbtGIk

Examples for games and training materials - reading material

- EU Legislation
- Materials and games
- Examples of CTF environments, CTF environments