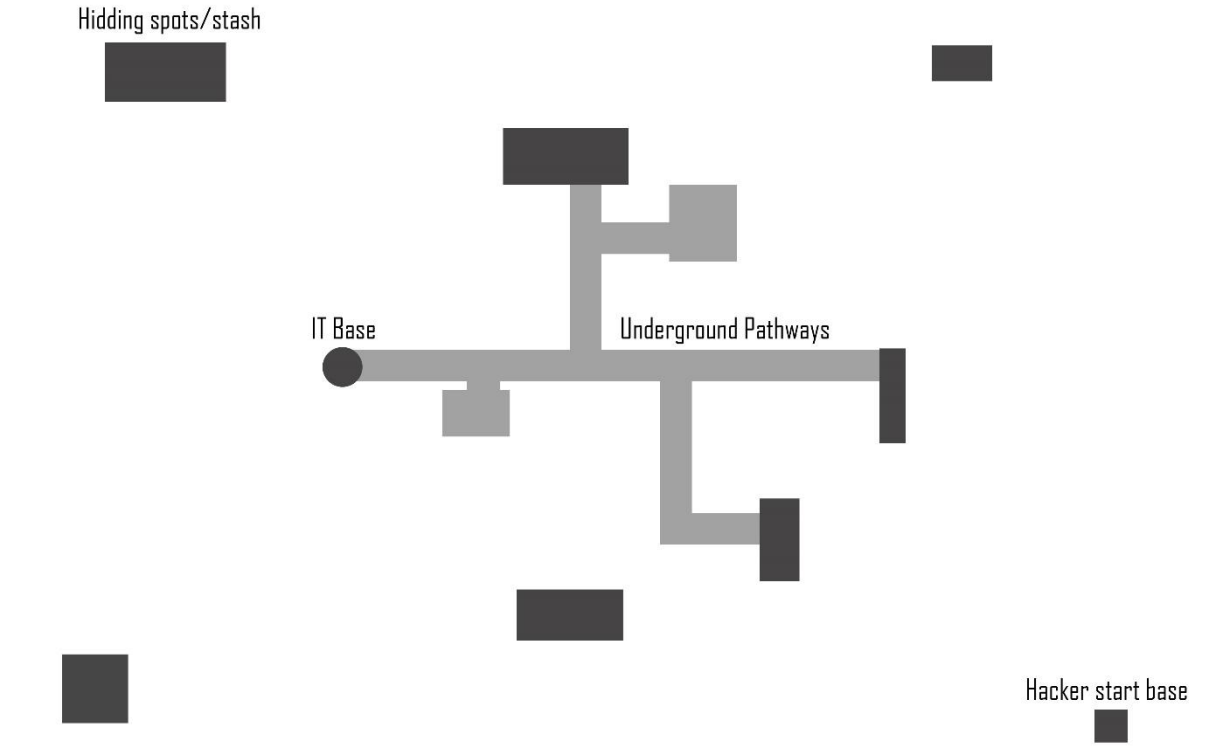
Map Examples

----------IT BASE----------

----------FULL MAP----------



Roles

Hackers

- Tech
    - Specialized in exploiting systems
        - Has improved hacking skills
- Thug
    - Specialized in aggressive encounters and exploring
        - Has basic weapons
- Engineer
    - Specialized in tools for creating new exploits
        - Has different electronics that can be placed

IT staff

- Tech
    - Specialized in preventing attacks
        - Has improved anti hack skills
- Guard
    - Specialized in aggressive encounters and exploring
        - Has basic weapons
- Pentester
    - Specialized in finding exploits
        - Has the ability to find exploits before they are exploited

Gameplay

Hackers

Hack valuable resources in the IT base.

All roles can hack, but tech have increased hacking skills.

Thug have improved combat skills, such as improved stamina, basic weapons and taser to knock out enemies.

Engineers can use different electronics to exploit secure devices or explore hidden areas with wireless camera devices.

IT

Defend valuable resources in the IT base.

All roles can defend from hacks, but tech have increased mechanics to prevent attacks.

Guards have improved combat skills, such as improved stamina, basic weapons and taser to knock out enemies.

Pentesters are able to test systems and find exploits before they are exploited.

Honey pots

Both teams can create honey pots. These works as decoys.

Hackers can create fake threats that looks like real hacks to misleads IT of where attacks are coming from.

IT can setup unsecure devices that are worthless to hack to delay hackers.

IT can setup traps that will alert them of things like the position of the hacker that hacked the device. Guards can then try to find their location and therefore hackers have to find new locations to hide in.

Both teams can create executable programs on some devices that could be useful in different scenarios.

Hacks

Hackers can scan different networks on the map, they can with this technique find valuable, unsecure and potentially interesting devices.

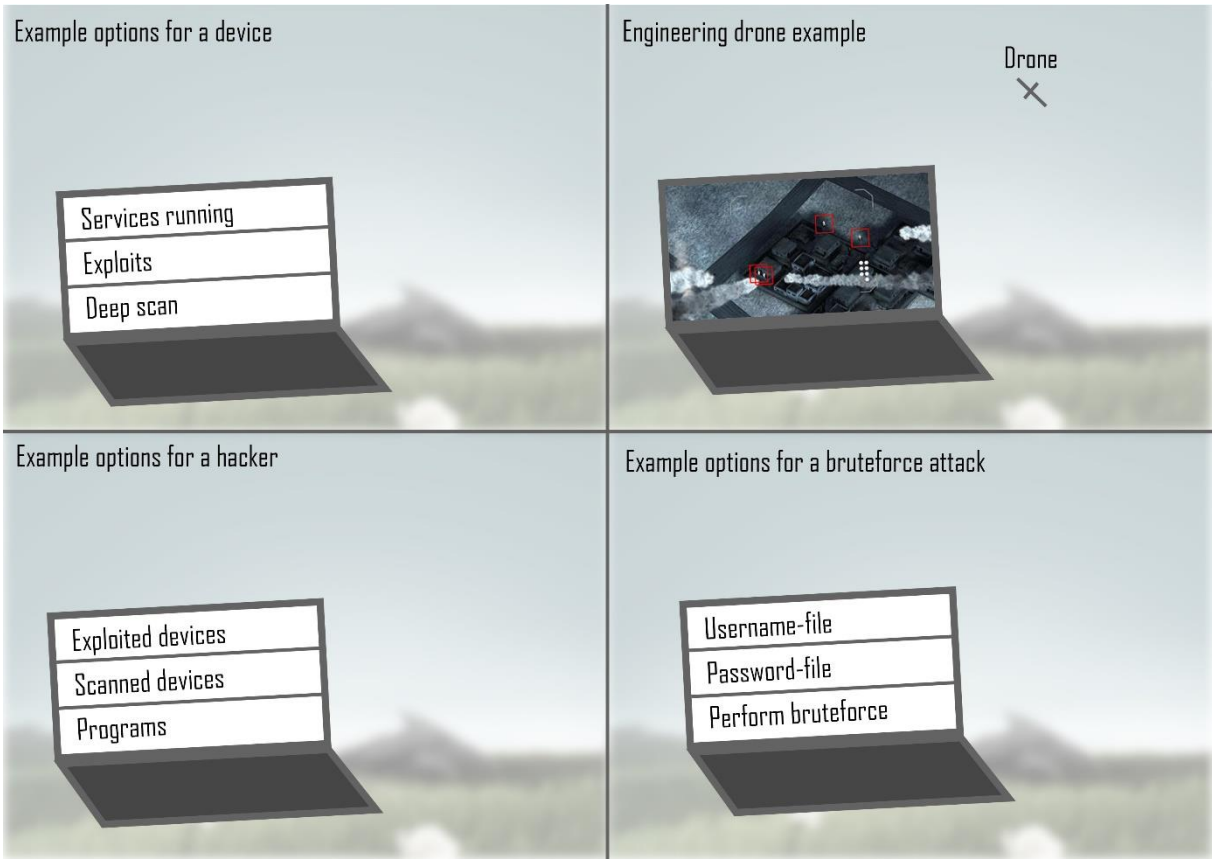
They usually have to deep scan interesting devices to find out more information about it.

Hackers can keep crawling through a network of connected devices when they've exploited a device, they can with this technique open new unsecure devices, this also means that IT can shutdown paths to specific networks completely if they manage to secure all devices on the network. Hackers are however still able to exploit these devices through engineering tools or invading, this is riskier for hackers though since they have to get close to the IT base to use these features.

Some hacks require extra information, for example password brute-forcing, this information can be obtained by exploring and digging in personal data of the IT employees (fake NPCs).

IT have cameras in their IT base that can be unsecure and therefore hacked. This means that hackers can find valuable position information of IT staff but also shutdown cameras to cut off important information for IT.

Devices may have interesting programs that could help both teams get important information. These features may be dangerous to execute though since someone on either team may have tampered or created the program.



Defense

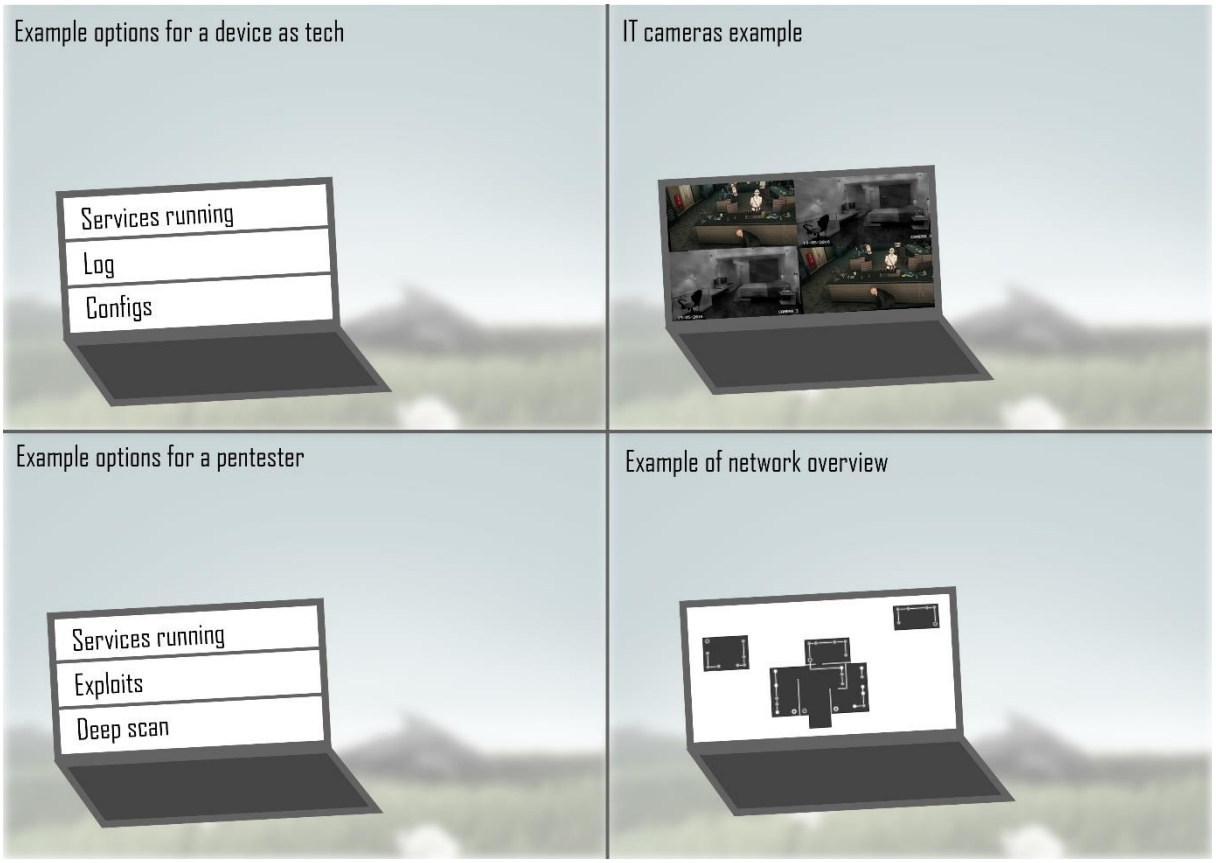
IT will usually not be aware of when they are being attacked. They have to investigate their systems for suspicious changes and entries to decide if they need to take actions.

Some ways for IT to secure their network is to look through config files, analyze log files, search for unsecure or exploitable services and analyze their network structure to figure out where their weaknesses lie.

Pentesters can try to perform exploits on their own systems to detect weaknesses that are hard to detect, if they manage to exploit the system before a hacker does they can patch this exploit before any harm is done by a hacker.

IT usually perform their actions on the physical computer instead of over the network to overcome different security restrictions that are setup on the network. This means that IT have to move around a lot compared to hackers.

IT have security cameras setup over their base, these can be used to detect intruders in the area. They also have full knowledge of their network architecture; therefore, they can navigate through their network easily.



Death System

Instead of dying a player will be heavily injured, teammates can then resurrect this player after a small amount of time. When a hacker is injured the IT-team can take this player as a “hostage”, this means they will be captured until a teammate rescues them.

When a player is kept hostage, they are free to spectate their teammates until they’re rescued.

Exploration

Both teams start with an unexplored map. This map will be filled in when your team discovers different areas on the map.

Hackers

Hackers can find stashes and hiding spots located at different places in the world. These places may contain materials used for engineers to build electronics.

They can also find where devices are located through network scanning.

Hackers should change positions to make sure they are not getting tracked down by IT.

If hackers run out of entry points to hack they must invade the IT base to create new exploits.

IT

IT starts with a fully explored base.

Guards can choose to go out and search for the hackers in the world. This may be risky though since it gives hackers the opportunity to sneak into their base easier.

Some cameras may overload and IT-staff therefore have to visit this location to repair the camera.