Purpose of Hacking:

- Hacking may be done to promote social or political agenda eg: anonymous engaged in this form of hacking to take down not good things
- Government actors may engage in hacking to further political agendas or for intelligence purposes eg: NAS (US national security agency) and Russian intelligence directorate (GRU)

- **White hat hackers:** aim to identify security flaws and tell vendors so that they can be fixed so for protection.
    - Security researchers and professionals often engage in this form of hacking (think apple find vulnerabilities to stop jailbreaking)
- **Black hat hackers:** exploit vulnerabilities for personal gains

CIA triangle (triad):

- Three principles and goals used in security or to ensure security
    - Confidentiality- keep data secure from unauthorized people
    - Integrity- prevent tampering with data
    - Availability- make sure the data and services are always available to use

Types of cyber-attacks:

Reconnaissance and info gathering:

- Precursor to some eventual cyber-attack (think gather details for house invasion). Find information regarding a potential target. Type of info
    - What kind of network defences are present
    - Who is in charge of the network and can I mess with them
    - How aware are employees of security practises
- Can be two different types active reconnaissance or passive

- Types:
    - **Passive reconnaissance:** use existing information (public) about target to gain information and build profile → launch cyberattack eg
        - Internet whois queries- who's in charge of network? How can they be contacted?
        - Public websites- who is in charge of company and where are they located
        - Social media presence- where did someone go to school, where do they live
    - **Active reconnaissance:** Use more direct methods of information gathering
        - Network or port scanning- what host are present on network/what application are running
        - Direct interactions- call or email target for more info
        - Use this info to investigate potential vulnerabilities based on version if provided

Social engineering:

- The act of manipulating victim into performing specific actions of providing confidential info
- This can be done through the use of psychological principles such fear mongering

Phishing:

- The act of using a fake email/or website to entice user by offering something they might like.
- Attempts to trick a victim into providing sensitive info (username, password and credit card)
- Spear pshing- form of pshing that target specific group of users

Access and intrusion:

- Aim to gain unauthorised access to a system or network can be done based on the info gained during reconnaissance and figuring out where to gain access
- Can be as simple as guessing password or more complex
- May involve gaining access to less secure host or services then using access to compromise sensitive targets

Viruses:

- Describes a piece of code that attaches itself to file or application and replicates it
- Used to be done by floppy disk sharing or now via emails and websites

Worms:

- Similar to viruses in terms of replicating itself but they are able to exist without attached to file or application
- Deliver a payload (malicious code)
- Done by: exploit network based vulnerabilities

Trojan horse:

- Software that masquerades as harmless application that includes malware
- Eg : free adobe transmits your keystrokes to attacker

Software exploit:

- Software or sequence of inputs that take advantage of a vulnerability in existing software
- Usually mitigated by applying software patches
- Exploits that are used before the vulnerability is publically known is called zero day exploits

Rootkit:

- Software designed to access privileged areas of the system such as root access eg: jailbreaking (includes exploit and kit to make sure it is maintained)
- Usually installed through an exploit, but can be deliberately or unintentionally installed by users
- Difficult to detect and remove due to high level of access gained

Denial of service attacks:

- Aim to impact the availability of a system or network, preventing legitimate access by trying to overwhelm the target with more traffic than it can handle
- Early denial of service attacks could be carried out by a single host (or small number)
- Types-
  - Ping of death: flood large ICMP messages to cause OS to crash
  - Smurf attack: send ICMP as broadcast with a spoofed source address to have all host to respond
  - Tcp SYN flood: continually send TCP synchronisation request to target and create a large number of TCP connection
  - Dns amplification: send dns or ntp servers with a spoofed source address causing servers to send traffic to the target (so all the request get sent to spoofed server to then send to target)

Distributed denial of service attacks:

- Botnets are a grouped of compromised host (think compromised old computers) that are instructed to perform actions an attack by handler
- They will overwhelm a target and cause it to crash.
- More difficult to defend since it may appear legitimate as it is hard to tell difference between real traffic and fake traffic.

Man-in-the-middle attack:

- An attacker intercepts communication between the victim and their destination and the communication can be read or modified
  - This may happen where an attacker acts as a wireless access point and captures packets from nearby users and therefore

Harder defending or attacking: in general, defending against a threat is harder than attacking since with defending you need to secure all potential vulnerabilities while attacking you need to find and exploit only one vulnerability

Defence in depth:

- The practice of implementing multiple layers (not just one) of countermeasures to protect device or network because it is more difficult to defeat a multilayered system than a single mitigation
- For example: an organisation may have a network level firewall, as well as firewalls on end points (like on devices itself)

Security through obscurity:

- Is a measure that doesn't actually boost security? It involves hiding/obscuring technical details from others and assuming that it is secure because it is hidden
- For example: a wireless access point prevented from advertising the presence is generally less secure because if we find it we can access it without no security measures.
- Therefore, we want people/developers to try actively to break through security so that we can fix any vulnerabilities

Securing the network: When we want to secure a network we need to look to secure two layers:

Network edge: point of ingress, usually router (network layer). Method of securing network-

- ***Reducing the attack surface:***
    - The aim is to reduce the number of areas that we can be attack. Ports opened means more entry point into system therefore, more attack surface.
    - So we need to identify unnecessary ports are open. Then terminate applications using the port (think using application opens the port).
    - A firewall can also be used to prevent communication occurring over port

- ***Firewall:***
    - A firewall is a barrier with a set of rules determines which determine which network traffic can pass or not pass. Two approach of firewall:
        - Blacklist: permit everything except traffic specified that can't pass
        - Whitelist: deny everything apart from traffic specified that can pass
    - Therefore, white listing is more secure but requires more maintenance as new applications must be explicitly added to pass list
    - Filtering is based on: source and destination Ip address and port numbers
- ***Intrusion detection and Prevention system: (***for big organisations)
    - More advanced firewalls that actually consider the content of the packets (or series of packets) not application as whole
    - Allows for more advanced detection of threats-
        - Abnormal traffic (spike of traffic) will notify network
        - Signatures of known attacks will be used to identify and alert the network
    - Intrusion detection systems (log the events) vs intrusion prevention system (mitigates attacks)
    - Can be dedicated hardware for this or get a software for your networks

- ADD FROM PREVIOUS SHEET SECURING WIRELESS-WEP ETC

Endpoints devices: security measures for end user devices like pcs or mobile devices. Method of security

- ***Ensure patches are installed:***
    - The older unpatched version of software/application may be prone to vulnerabilities. So both application and software should be updated to latest version.
    - Many security breaches could have been avoided had updates been sooner so within 48 hours
- ***Endpoint firewalls and anti-malware:***
    - Most os have some form of firewall integrated + antivirus and anti-malware are often includes too
    - Make sure to enable and keep them updated
    - Third party anti-virus is also available but requires significant access and may be prone to additional vulnerabilities
- ***Passwords:***
    - Using many endpoint security methods will be useless if an attacker gets physical access that's why we need a password
    - Passwords are stored on every device and in every service, but not in plain text so hackers can't/have a difficult time to decode it
    - National institute of standards and technology guideline:
        - Guessable not, 8 characters, not in dictionary
- ***Two-factor authentication: (Not secure maybe don't study)***
    - Most services use a password as authentication method. Additional paradigms/methods to authenticate(models)
        - A token (something you have)
        - Something you are (biometric like finger tips iphone)
- ***Principle of least privilege:***
    - Consider whether administrative privileges are needed for all users (remove if aren't)
    - Most users will have administrative accounts for operating system by default
    - Administrative users can have the ability to install software and access files without restriction
- ***Backup your data:***
    - Important data should be backed up regularly
        - Protects against hardware failure
        - Allows recovery after an attack
    - Use 3 2 1 rule:
        - Ensure you have three copies of any important data
        - Keep these copies in at least two formats (eg on hard drive and on usb)
        - On copy should be stored off-site
- ***Encrypting data at rest:***
    - Encrypting data on your device renders it unreadable to an attacker that gains physical access
        - Useful if device is stolen

    - Most os have inbuilt full disk encryption
        - Windows bitlocker
    - Used to slow down devices, now limited performance impact due to hardware improvements

Relationship between security and convince:

- Security and convenience are often seen in opposition since making network or endpoint devices more secure reduces usability/convenience as
    - Secure passwords are difficult to remember
    - Having to type in password to install software is annoying
    - Finding phone to login (runescape) to pc is even worse
- Therefore, it is important to find level of security required based on threat model ie: are you defending against nation or nosey housemates. Also identify threats you are trying to defend against will help determine which countermeasures are required

- **Heartbleed (2014):**

- **Black energy (2015):**