1.

a) i.

**Worm:** self-replicating program that infects other machines over the network or removable devices

**Adware:** displays intrusive advertisement

**Drive-by-download:** code executed by visiting a malicious website

Drive-by-download is most likely (as more users are likely to be affected)

a) ii.

1. The botnet acts as a keylogger, stealing banking details

2. The botnet acts as a cryptominer, mining bitcoin

3. Others pay to use the botnet as a service (e.g. for DoS)

a) iii.

* Recruit a new machine for the botnet
  + Infect a new machine with botnet malware
    - Deliver attack vector via Spam email
    - Deliver attack vector as Drive-by-download
    - Deliver attack vector as Worm
  + Prevent instantly being removed
    - Avoid detection by anti-virus software
    - Be inconspicuous (unnoticeable) by user
  + Communicate with C&C (Command and Control)
    - Communicate avoiding IDS/filter

b) i.

Need the VM :(

4.

a) i.

**Spoofing**: access the website as somebody false. E.g. steal a password, login to their account. This violates the privacy of this account and any friends.

This applies to the login/account feature of the architecture.

Mitigate with good password methods i.e. send hash, over TLS, require password complexity etc.

**Tampering**: MITM tamper with information sent across the internet. E.g. Changing password => tampered to become MITM set password, Adding new friend => tampered to become MITM set account, now MITM gets private information only for friends.

Applies to internet communication channel / any features client can use.

Mititgate with TLS, MACs, anti-CSRF tokens.

**Information Disclosure**: social network gives away information that it shouldn’t e.g. user information specific to one account (address, credit card information). Information is private to user, thus violating privacy of social network.

Applies to user data i.e. database of information of architecture.

Mtitigate with TLS, clear policy on who can access what (no loopholes).