6. SSH/SSL
(a) Someone claims that SSH does not require the use of a Public Key Infrastructure (PKI) and, as a consequence, partners who want to communicate must have pre-configured shared keys. Is this claim correct? Explain!

- Note that the question includes two statements: "SSH does not require ..." and "partners who want to communicate ...".
  A simple yes / no answer can therefore never be correct.
- Let's start investigating the first statement ("SSH does not require ...")
  . A PKI is needed to find authentication and encryption keys.
  . SSH has different authentication algorithms for server and user
  . SSH server authentication is based on "server host keys". The client stores these keys in a local databse, which can be filled in in different ways. One of the ways to fill this database is "best effort" (accept key first time server is being accessed, after that check at each subsequent access if the key is still the same). For this kind of server authentication, a PKI is indeed not needed.
  . SSH user authentication supports multiple methods (one of them being PKI), but can also use "keyboard interactive" authentication. A PKI is also not needed for this.
  -> Conclusion: the first statement ("SSH does not require ...") is therefore correct
- Let's now investigate the second statement ("partners who want to communicate ...")
  This statement is NOT correct. You can use public-keys without the use of a PKI.

(b) The same person claims that SSL/TLS requires the use of a Public Key Infrastructure (PKI). Therefore the data transferred between a SSL/TLS client and a SSL/TLS server will be encrypted using a public key encryption algorithm. Is this claim correct? Explain!

- Note again that the question includes two statements.
- The statement that "SSL/TLS requires the use of a Public Key Infrastructure (PKI)" is too simple:
  . According to the RFCs, server authentication is optional
  . If server authentication is used, a PKI is generally required to check whether the certificate is authentic
  -> In practice this first statement is therefore true; in theory not
- The statement that "therefore the data transferred between a SSL/TLS client and a SSL/TLS server will be encrypted using a public key encryption algorithm" is wrong:
  . the initial key exchange may be based on public keys, which are included in certificates
  . to check these keys, a PKI may be used.
  . however, also diffie-hellman may be used, which means that no PKI is needed
  . The important observation, however, should be that after the negotiation phase is over, symmetric key encryption is used
  -> The second statement is therefore wrong.

7. Network Address Translators (NATs)
Assume you have a PC directly connected to the Internet. All applications work without problems. A few days ago, however, you discovered that there are other computers scanning some ports on your PC. Since you do not like this, you decided to take measures and you bought a (full-cone) NAT.

(a) Will the full-cone NAT be able to prevent that future scan attempts reach your computer? Explain.
- All NATs will be able to block scans to all ports that have not been previously used for transmission. If you don't send anything, you will not receive any scans
- For ports that have previously been used for transmission, a full cone NAT accepts traffic from all other IP addresses from all ports.
-> therefore you may still receive scans on previously used ports. In general this may be only a fraction of all ports, so you are relatively save.
   In addition, you do not ususally send from "server ports" (<1024), so you're even saver.

(b) Someone tells you that, as opposed to NATs, firewalls were designed to block unwanted traffic. To block scans to your computer, it would therefore be better to buy a firewall. Is that correct? If yes, what kind of firewall. If no, why not.
- The following kind of scans exist: TCP, UDP and ICMP
- The following kind of firewalls exist:
  . network firewall / personal firewall -> no difference with resepct to this question
  . stateless firewall / stateful firewall
  . network / transport / application level firewall
    network level firewalls can not block scans
    transport level firewall can block TCP scans (block incoming SYN), but can not block UDP / ICMP scans
    application level firewalls can easily block scans
  -> A stateless network level firewall can not block TCP / UDP scans. It may block ICMP scans

-> A stateful network level firewall can be configured to accept traffic flows initiated by local users
and deny traffic flows initiated by remote users. It can therefore block scans
-> A stateless transport level firewall can block incoming TCP connections, but can not block UDP scans
-> A stateful transport level firewall can block scans
-> A stateless application level firewall does not realy make sense (applications are generally stateful)
-> A stateful application level firewall can block scans
-> Any stateful firewall can be configured to block scans
-> A stateless network level firewall can block ICMP scans, but not TCP and UDP scans
-> A stateless transport level firewall can block ICMP and TCP scans, but not UDP scans

8. Detecting Scans
Assume your next job will be a network manager at a large Internet provider. Your first task is to set-up
a measurement infrastructure to detect scans.

(a) How would this measurement infrastructure look like? Explain.
There are two fundamentaly different approaches:
1) monitor all network traffic (for example using netflow) and search for "scan patterns".
Because of the enormous amount of data transfered over the network, monitoring all traffic may be quite difficult, however.
2) Therefore an easier approach would be to "monitor" traffic going to unused IP addresses, since such traffic will primarily consist of scans. A honeypot will be able to monitor such unused addresses.
Horizontal scans usually "visit" IP addresses in a sequential way, which means that they wll also "pass"
the honeypot. Vertical scans may not be detected by the honeypot, however.
Such honeypot can be seen as a special kind of IDS (not hosts based / not network based)

(b) What kind of protocols do you expect the scans will be based on; do you expect these protocols to be TCP, UDP or another protocol? Explain why you expect this.
-> From the sheets we've seen that a study at the Lawrence Berkeley National Laboratory (LBL) from 2004 revealed that between 56% (LBL-P) and 95% (UW-1) of the background radiation is TCP traffic, between 0.8% (UW-1) and 11.3% (Class A) is UDP, and between 0.3% and 39% is ICMP.
It seems reasonable to assume that much of this traffic is formed by scans.