**Overview: Question 1**
*These are short-answer questions*

1. Give one legitimate use of ARP spoofing.
   *One can use ARP spoofing for backup services. Say a machine goes down, another can be brought up and advertised as having the same IP address as the machine that is down.*

2. In a switched LAN employing star-topology, is DHCP spoofing attack (rouge server replying to DHCP discover/offer messages) possible? Justify.

   *Yes, since DHCP discover/offer messages are broadcast, everyone will receive them including the attacker, who can reply accordingly.*

3. How does IPSec provide protection against source IP address spoofing?

   *As part of IKE, phase-1 the source is authenticated and later this field is integrity checked.*

4. How is a client authenticated in SSH?

   *There are two options: password or publick key based where the client send its public key which is checked by the server against valid stored keys.*

5. Which of the following security goals are addressed by the HTTPS protocol: (a) privacy, (b) confidentiality, (c) availability. Justify.

   *Since content is encrypted, it achieves confidentiality. Some one eavesdropping will not be able to figure out what sites the person is visiting, so privacy to some extent. HTTPS does not do anything to handle availability.*

6. What advantage does a sub-domain DNS attack provide the attacker?

   *It helps him in the race against time from the genuine authoritative server since the latter will not reply for non-existent sub-domains..*

7. Which is worse for an intrusion detection system, false positives or false negatives? Why?

   *False negatives have to be zero, since its role if detecting intrusions. False positives are annoyances that can be tolerated if the rate is very low.*

**Question 2: Firewall**

Supposing a company wants to install a 'stateless' packet filter with the following policies.

1. By default, block all inbound connections.
2. Allow all inbound TCP connections to SMTP (port 25) on mail server 11.22.33.44.
3. Allow all inbound TCP connections to HTTPS (port 443) on web server 11.22.33.55.
4. Allow all outbound connections.
5. Telnet access (port 23) (incoming or outgoing) should not be allowed (because it sends passwords in cleartext).

(a) Using the below syntax, write the firewall ruleset for the company's firewall. For each rule, also provide a brief description of its purpose. Order the rules like in iptables i.e. if a rules matches it will execute the rule and skip all below rules.

| Action | Source address | Dest Address | Protocol | Source port | Dest port | Flag bit |
|---|---|---|---|---|---|---|

*1. Allow * 11.22.33.44 tcp * 25 - [from out interface] (allows SMTP from outside)*
*2.Allow *11.22.33.55 tcp * 443 - [from out interface] (allows HTTPS from outside)*
*3.Drop * * tcp * 23 - [from in interface] (drops telnet connections to outside)*
*4.Allow * * tcp * * - [from in interface] (allows all outbound traffic)*
*5.Allow * * tcp * * ACK-bit-set [from out interface] (allows TCP responses)*
*6. Drop * * * * * - [from out interface] (default deny; drops incoming telnet connections also)*

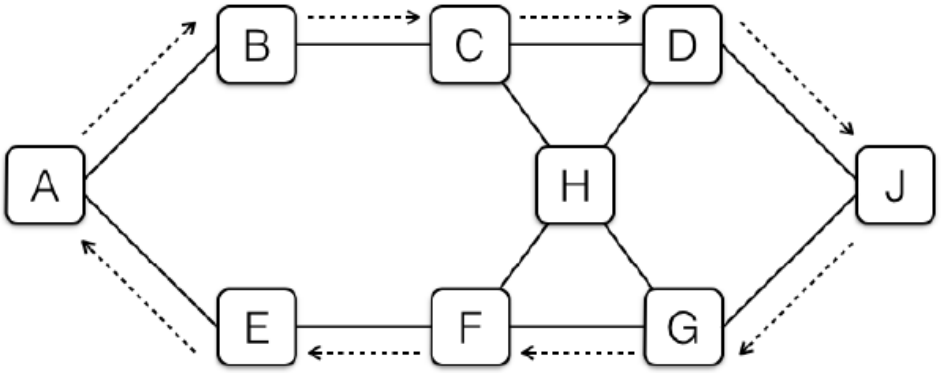
(b) Suppose hackers target this company's network with repeated requests for large images on the company's webserver. The hackers machines are on the 20.1.21.x subnet. How could you change your firewall ruleset to block these attacks? Specify the rule and its position in the above table (part a).

*Add the rule*
*Drop 20.1.21.* * tcp * * - [from out interface]*
*as the FIRST rule in the ruleset.*

(c) Suppose employees in the company start downloading lots of movies from website at 44.33.22.11:80. How could you change your firewall rules to stop employees from accessing the website? Specify the rule and its position in the above table (part a).

*Add the rule*
*Drop * 44.33.22.11 tcp * 80 – [from in interface]*
*before rule 4 in table of part a*

**Question 3: TCP**




Consider the following network topology. The machine A has initiated a TCP connection to machine J. All packets from A to J happen to follow the path indicated by the right-facing dotted arrows, and all packets from J to A happen to follow the path indicated by the left-facing dotted arrows. Machines A and J use modern TCP software and do not have any special defenses against attack.

a) Suppose that Mallory controls (only) machine C. Can she inject RST packets destined for machine J into this TCP connection, such that they will be accepted by machine J? Why or why not?
*Yes. She is on-path and can see the sequence numbers, so she can inject a forged RST packet with the right sequence number.*

b) Suppose that Mallory controls (only) machine C. Can she inject spoofed data into this TCP connection, so machine J will accept the spoofed data thinking that it came from machine A? Why or why not?

*Yes. She is on-path and can see the sequence numbers, so she can inject a forged data packet with the right sequence numbers.*

c) Suppose that Mallory controls (only) machine H. Can she inject spoofed data into this TCP connection, so machine J will accept the spoofed data thinking that it came from machine A? Why or why not?

*No. She is off-path and cannot observe the sequence numbers.*

d) Suppose that Mallory can eavesdrop on all packets that go through machine C (but cannot inject forged packets from C). Also Mallory can run software on machine F that lets her inject forged packets from F to anywhere (but cannot eavesdrop on packets going through F). Can Mallory injected spoofed data into the TCP connection, so that it will be accepted by machine J as though it came from A? Why or why not?

*Yes. She is on-path, so by observing packets traversing machine C, she can observe the sequence numbers. Then, she can inject a spoofed packet from machine F. Note F can inject a packet towards J, nothing stopping it from it.*

e) Suppose that Mallory can eavesdrop on all packets that go through machine F (but cannot inject forged packets from F). Also Mallory can run software on machine C that lets her inject forged packets from C to anywhere (but cannot eavesdrop on packets going through C). Can Mallory injected spoofed data into the TCP connection, so that it will be accepted by machine J as though it came from A? Why or why not?

*Yes. She can see the sequence numbers for both directions (since they're contained in the handshake, and also every packet from J to A contains an acknowledgement that mentions the sequence number of the last packet that J received from A). This is enough that she can inject a forged packet from C that J will accept.*

**Question 4: DOS**

An anti-spam company, GreenMail, uses a vigilante approach to fighting spam. GreenMail's customers report their spam to GreenMail, and the company then automatically visits the websites advertised by the URLs in the spam messages and leaves complaints on those websites. For each spam that a user reports, GreenMail leaves a generic complaint. GreenMail operates on the assumption that as the community grows, the flow of complaints from hundreds of thousands of computers will apply enough pressure on spammers and their clients to convince them to stop spamming. After a short while of operation, GreenMail's public web site comes under a massive DDoS attack that uses SYN flooding.

(a) Briefly describe the type of traffic that an attacker sends to launch a SYN flooding attack.

*A SYN flooding attack sends a stream of TCP initial SYN packets to the targeted server. Each packet appears to represent a request to establish a new connection. Note that the attacker may spoof the source addresses of such SYNs to make them harder for the defender to filter them out, but this is not required. An attack that employs a large botnet, for example, might not use spoofing.*

(b) Briefly describe how the attack can cause a denial-of-service?

*For each incoming SYN packet, the server both responds and consumes memory because it records information (state) associated with the impending new connection. The attack primarily aims to exhaust the server's available memory for keeping this state.*

(c) Can GreenMail use a packet-filter firewall to defend itself against the DDoS that uses SYN flooding? If so, describe what sort of rule or rules the firewall would need to apply, and what collateral damage (side effects) the rules would incur. If not, explain why not. State assumptions made clearly.

*Here are two possible answers:*
*(1) If the flood uses a fixed number (not too large) of IP source addresses in its packets, then the target could install a number of firewall rules that deny traffic from those addresses. In this case, the collateral damage depends on how much legitimate traffic also comes from those addresses.*
*(2) If the flood uses a very large number of IP source addresses, either by employing a large number of different systems (bots) to send the traffic, or by spoofing the IP source address in each SYN packet, then the target will not be able to specify enough firewall rules to defend against the attack. Note that the target cannot use a rule such as drop any incoming TCP SYN sent to our web server without enabling the attack to fully succeed, i.e., the collateral damage would be that no legitimate traffic can reach the server.*

*Solution such as syn cookie will not work since the question is about firewall, not what the GreenMail server can do.*

(d) Explain how the GreenMail service could itself be used to mount a DoS attack.

*An attacker could send a large number of bogus spam reports to GreenMail, falsely indicating some victim site* V *has been sending spam. GreenMail's servers will then visit* V *to lodge complaints, overwhelming* V *in the process if the volume of visits is high enough.*

(e) Briefly describe one approach that victims could use to defend themselves against the attack you sketched.

V *could refuse to accept incoming connections from GreenMail in order to avoid the load from GreenMail's servers registering complaints*