TUTORIAL 1

1) **A DDoS attack prevents you from connecting to your bank website. Which of the security properties will this impact?**

→ Availability

2) **What is the difference between authenticity and integrity?**

→ Authenticity is about being certain tht. the info. received/accessed by us is from the entity we believe it to be from.

→ Integrity is about making sure tht. info. has not been corrupted, changed or added to by human activity either during transit / in storage.

3) **What are the basic elements of a threat model?**

→ WHO is the adversary and what abilities & access do they have.

→ WHERE are they in relation to the objects we are trying to secure.

→ WHAT is the aim of the adversary / what are we trying to prevent them from doing at the high lvl.

→ WHAT particular threats are we trying to prevent that, if successfully taken advantage of, will lead to the adversary achieving their goals

4) **Imagine that you have important data on your laptop. You place a tracking chip inside it in a tamper resistant enclosure. Is this a cost-effective way to protect your laptop? Relate your answer to the different types of defences one could employ to protect their assets. Make sure to include your assumptions.**

→ Are there more than one type of adversary and can they collude.

'Not 'Prevent'!

→ Tracking chip in laptop can be a form of deter and recover defences.

→ It is deter if it is common knowledge tht. your laptop has a chip inside Then the would-be laptop thieves may think twice abt. stealing a laptop.

→ It is recover since once laptop is stolen, you can use the tracking feature to locate it. This assumes tht. chip is still operational and within range of the tracking sys.

→ It may be deflect since the thieves may then steal nearby laptops instead and avoid yours. (Not as strong a defence in this setting as the above two)

→ If a tracking chip is cost-effective depends on cost of laptop, value of the info. it contains, cost of chip and operation of the infrastructure required to track chip once stolen.

→ Also important is the adversary who this chip is supposed to work in the face of

5) **ARP allows address translation between IP and MAC addresses.**

(a). **How many MAC addresses are allocated to each manufacturer for their use (assuming one prefix each).**

e.g. 00-1A-92-D4-BF-86 $\therefore 2^{24}$ addresses

IEEE assigned — Assigned by organizations

(b). **Which of the two address spaces would be exhausted first, MAC or IPv4? Give the (approximate) difference.**

IPv4 → 32-bit addresses

MAC → 48-bit addresses $\therefore 2^{48} - 2^{32}$ more MAC addresses

6) **Recall encapsulation. Imagine that a packet of 10 bytes needs to go through 3 layers of the stack before it is transmitted to another machine. Each layer added 10 bytes of header and 2 bytes of footer.**

(a). **What is the size of the packet that is transmitted?**

(10)

L1 - - - - - - - (10) + (10) + (2)

L2 - - - - - (10) + (10) + (10) + (2) + (2)

L3 - - (10) + (10) + (10) + (10) + (2) + (2) + (2) → 46 bytes

(b). **Imagine that the original 10-byte packet is fragmented into two. Now what is the total size (in bytes) of transmitting that original packet?**

$2 \times (10 + 10 + 10 + 5 + 2 + 2 + 2) = 82$ bytes

7) **NAT is useful to ease the exhaustion pressure on the IPv4 address space. It can also hide the internal information of a private network from external observers.**
Give at least one type of information that could be prevented from being observed?
Give reasons why this is good to protect.

→ Hide no. of machines on the private network.

- By hiding no. of hosts, we do not present as an attractive target for attackers who are looking to maximise their gains given the cost of running the attack
- Size of network could also reveal potential operational capabilities of the network (i.e. dedicated dbase servers or printers) that might give clues on how to best attack the network hosts.

8) **Imagine you want to divert internet traffic to your own knock-off bank website that is a duplicate of the original bank website.**

(a). **What could you do to divert the traffic from the real website to yours (assume that certificates or other forms of authentication are not present)?**

→ Try to poison DNS cache of name servers so tht. they point to my IP address.

→ If we are the ISP / other router on the path of victim, we could divert traffic to fake site by rewriting the destination IP in the packet header.

(b). **Would this be a stealthy attack, or would it be traceable?**

→ DNS cache attack may be noticed by the cache server after the attack since they may keep logs.

→ The diversion may be more stealthy since there is no record of the change except at the network node tht. rewrote the header.

9) **Imagine that an IDS has been trained to detect website-X (that serves malware) and the IDS has a TPR = 95.99% and an FPR = 15%. Suppose that website-X is very popular and 50% of all website visits that the IDS observes are to it. What is the probability that when the IDS detects a visit to website-X it is correct? Show your intermediate steps.**

→ Imagine 1 million visits :

$$TP = 500\,000 \times \frac{95.99}{100} = 479\,950$$

$$FP = 500\,000 \times \frac{15}{100} = 75000$$

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{479\,950}{479\,950 + 75000} = 86.5\%$$