1 Which is a treat? (network company)

* 1. Daily courier who drops packages and picks them up.
  2. Former employee who left
  3. Employee travelling on company business
  4. Building management company installs sprinkler system

1. Access servers → internal intruder
2. Beguarded sell information, use information for harm
3. Lose laptop, hacked company would get compromise.
4. Sprinkler system could cause damage

2 Define notion of collision resistance in hash function

H: X → Y is collision resistant → computationally infeasible.

To find 2 points x1, x2 ∈ such that h(x1) = h(x2)

3

|  |  |
| --- | --- |
| A (has pw) | B (has key) |
| Send [conn request] to B  Compute key from pw, then compute X by encrypt([R]) with key  Send [x] to B | Generate a random challenge R sends [R] to A  Compute Y ← decrypt(x) with key. If Y = k → A is authenticated |

Breaking this using brute force

repeat: {

Choose candidate password cpw;

Compute ckey from cpw;

Compute cX with cX = X (Symmetric Key)

}

4 Explain BotNet, Easter Egg, Logic Bomb

BotNet: peer-to-peer network of compromised computers

Easter Egg: unspecified code hidden in a program

Logic Bomb: malicious code activated by such trigger

5 Name ways hackers can compromise computers without code breaking

1. Key catcher (software, hardware)
2. Email executable files
3. Boot CD

6 Firewall does not protect from

1. Malicious code in emails
2. Human error or internal attacks, compromised internal machines or VPN
3. Malicious code injections
4. Open ports
5. Firewall itself
6. DDoS attacks against firewall

7 Download email or web pages with hidden content

TLS and SSL are encryption protocols

→ Security and data protection on internet

→ Encrypt segments of communication at transport layer for end-to-end communication.

8 IP attackers inserts bogus packets into communication. Would this succeed on SSL and IPSec?

IPSec would block the packets and NOT forward to TCP

SSL could break and insert the bogus package

* RSA, Vigenere, PlayFair
* Q’s from past papers.
* Sample Q’s from recommended book

4 Q’s do 3