Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti
Cybersecurity (6 of 9 credits)

Exam of 13 January 2022, a.y. 2021-22. Time: 2 hours
Outcomes will be published in web page within three weeks:
https://sites.google.com/diag.uniroma1.it/cybersecurity/exams

FOR NON-ENGLISH: 2 penalty points (applicable only to courses provided in English)

1. Cryptographic hashing functions

1.1. [2/30] State a minimal but sufficient set of conditions why a hashing function be cryptographic.
1.2. [3/30] Can I use a cryptographic hashing function for a hash table? Motivate.
1.3. [3/30] Can I use the hashing function of a hash table as a cryptographic hashing function? Motivate.

2. Authentication

2.1. [3/30] Username/password based authentication: propose a protocol for having this type of authentication in the LAN, resistant to all types of replay attacks. Can you avoid saving user passwords on the server?
2.2. [3/30] How could an authentication process be based on a public key and what are the relevant weaknesses?
2.3. [3/30] Locate the weakness in this bidirectional challenge-response authentication scheme and mitigate it:

A → B: A, Enc(a, X)
B → A: a, Enc(b, X)
A → B: b

where X is a shared secret key, Enc(y, X) denotes symmetric encryption of y by key X, a is a nonce chosen by A and b is a nonce chosen by B.
2.4. [2/30] Bob is a smart guy and knows how to invent 128-bits random passphrases (typeable on keyboard) that are robust against dictionary attacks. Alice tells him that in spite of such robustness a 128-bits random key is more secure. Bob replies that the security is the same, but the passphrase can be more easily remembered. What's your position? Explain.

3. Access control

3.1. [2/30] Is the HRU (Harrison, Ruzzo, Ullman) model secure against *offline dictionary attacks*? Explain.
3.2. [2/30] Give at least two cases where HRU is decidable. Explain.

4. Firewalls

Assume that the iptables software is running on host *H*, having a network interface eth0 (IP: 192.168.0.2) connected to a LAN (IP: 192.168.0.0/24; the LAN is protected by *H*) and a network interface eth1 (IP: 151.100.4.3) connected to the Internet. Assume that the default policy for all built-in chains is DROP.

4.1. [3/30] Since the LAN contains only local hosts with private IP addresses, it is not possible to directly contact local hosts from the Internet (no IP remapping). However, if *H* accepts, local hosts can establish two-ways communications with remote hosts on the Internet, based on TCP. For this purpose, which rules will you have to define on the perimeter firewall?
4.2. [3/30] Define suitable rules for mitigating a distributed DOS attack to *H*, based on ping-flooding. Avoid blocking/slowing down other protocols.

5. Short answer (at most 4 lines)

5.1. [2/30] Make a comparison between HMAC and digital signing for the purpose of non-repudiation.

Number of homeworks validly (within the proper deadline, or, if on late, explicitly authorized by the prof.) delivered?	

To be delivered with the exam notes written in decent handwriting