Number: Name:

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC-AL, MEIC-TP, MEEC, MSIDC

1st Test Recovery, January 25th, 2016

- The duration of the test is of 1:00 hours.
- **Identify all sheets with your student number. Use clearly distinguishable digits.**
- Read all paragraphs of each question before you answer the first one. Some questions are divided into several paragraphs.
- Be **objective** and **concise** in your answers. Use only the space given for each question. Use medium size readable handwriting.
- A wrong answer in a multiple choice question will subtract 1/N of the value of the question, where N is the number of presented options.
- The exam can be answered in Portuguese or in English.
- **Justify all answers.**

1. What is a "script kiddie" attacker? Should security be concerned with this kind of attacker?

2. Consider the Layer 2 (Data Link) of a wired local area network using IP over Ethernet. Alice and Bob are connected to this network.
   a. What is the purpose of ARP tables?

   b. Describe how an attacker (Eve) connected to the network can perform an ARP poisoning attack to intercept traffic between the machines of Alice and Bob.

   c. Describe one approach that could help prevent ARP poisoning.

d. How would you classify the ARP poisoning threat using the STRIDE classifiers?

S -
T -
R -
I -
D -
E -

3. Keys are very important for the effective use of cryptography, and should be generated with good random number generators.
   a. Consider a vulnerability where the generated bits are predictable. How can it be exploited by an attacker?

   b. Disregard the previous vulnerability. Consider another vulnerability where the generated bits are not equiprobable. How can it be exploited by an attacker?

4. Consider the Diffie-Hellman (DH) algorithm between Alice and Bob for shared key generation.

> The values α and q are public:
> A and B generate random and secret values: a and b
> A computes $\mathbf{y_A = \alpha^a \bmod q}$
> B computes $\mathbf{y_B = \alpha^b \bmod q}$

   a. How can A and B compute a shared key $\mathbf{K_s}$?

   b. What prevents an attacker (Eve) from computing $\mathbf{K_s}$? Consider that Eve was able to listen to all the messages exchanged between Alice and Bob in the public channel.

   c. DH is susceptible to man-in-the-middle attacks. Describe how an attacker can perform such an attack.

d. Describe one generic approach that could be used to prevent the man-in-the-middle attack.

e. How can DH be used to ensure Perfect Forward Secrecy?

5. Consider a security system based on X.509 Public Key Certificates. Alice and Bob each have their own public key certificate, issued by the single Certification Authority (CA).

   a. Who should have generated Alice's key pair? Where should each key be stored?

   b. Bob presents Alice with his certificate. What are the validation steps that Alice should take before accepting Bob's certificate?

   c. If Bob discovers that his private key has been leaked, how should he proceed to minimize the damage?

Grading:

1:	1					T= 1
2:	a) 1	b) 1.5	c) 1	d) 1.5		T= 5
3:	a) 1	b) 1				T= 2
4:	a) 1.5	b) 1	c) 2	d) 1.5	e) 1.5	T= 7.5
5:	a) 1	b) 2	c) 1.5			T= 4.5