Feb 24, 2023

Introduction to Computer and Network Security

Part 1

Question 1 [50 points]

The BrokenWare company uses a tool capable of deploying and serving virtual computers. The tool contains a critical flaw that can be exploited to compromise any system. The vendor releases a patch for the vulnerability on 23 February 2021, but BrokenWare does not update its systems.
At the beginning of February 2023, the company is hit by a ransomware that is able to encrypt all the company data by exploiting the unpatched vulnerability.

You are a security expert paid to comment on why it is *virtually* impossible to decrypt BrokenWare's data without paying the ransom. Specifically, you should explain the reason by first defining the notions of

- (a) cryptosystem [5 points];
- (b) Kerckhoffs principle [5 points];
- (c) key management and its purpose [10 points];
- (d) symmetric key cryptography [10 points];
- (e) asymmetric key cryptography [10 points].

Finally, you should describe

- (f) which security architecture and best practices could have mitigated this kind of attack [10 points].

Part 2

Question 2 [40 points]

In the context of the Diffie-Hellman key exchange, describe (a) the protocol, (b) the Men-In-the-Middle (MITM) attack, and (c) how it is possible to mitigate the MITM attack.

Question 3 [10 points]

Define the notions of vulnerability and threat and give (at least) an example for each one.

Please, remember…

Be sure to annotate the following information on each used sheet of paper (possibly, 2 sheets at most)

- Name
- Surname
- Student ID number
- Question number