I prova dell'esame per il corso di Sicurezza Informatica A.A.: 18/19

Ai fini delle seguente prova lo studente deve:

1. Scaricare il file *binario* (https://homes.di.unimi.it/sisop) e sfruttare la vulnerabilità in esso contenuta per realizzare un attacco che consenta di caricare sulla macchina vittima uno shell code che svolga TUTTE e SOLO le seguenti attività:
   a. Copiare il file delle passwd presente sulla macchina vittima nel file `pswd` sotto la directory corrente;
   b. Visualizzare i processi in esecuzione;
   c. Stampare l'elenco dei file nella directory corrente.

   L'attacco deve essere effettuato assumendo che il codice da attaccare risieda su una macchina remota. A seguito di questa attività lo studente deve predisporre una relazione in formato digitale che:
      i. descriva la vulnerabilità presente nel programma, la tecnica di exploit utilizzata e le motivazioni che hanno indotto al suo uso **(5 pt.)**;
      ii. descriva l'exploit, le modalità con cui è stato costruito e le principali difficoltà che si sono dovute superare per renderlo operativo **(7pt)**;
      iii. contenga gli screenshot in cui sia visibile la fase di iniezione dell'exploit ed il relativo risultato **(4 pt.)**
      iv. descriva due contromisure per rendere inefficace il suddetto attacco, motivandone la scelta **(4 pt.)**

2. Sfruttare la vulnerabilità di cui al punto 1 per caricare e mandare in esecuzione uno shell code che visualizzi il file delle password residente sul sistema vittima. L'attacco va effettuato sempre assumendo che il codice da attaccare risieda su un sistema remoto. A seguito di questa attività lo studente deve predisporre una relazione in formato digitale che contenga :
   a. una descrizione dell'exploit e delle modalità con cui è stato realizzato (**5 pt.)**
   b. gli screenshot in cui sia visibile la fase di iniezione dell'exploit ed il relativo risultato **(3 pt.)**
   c. una descrizione del sistema di protezione noto con il termine Propolice, in cui siano descritte le contromisure adottate da Propolice e le corrispondenti vulnerabilità considerate (**2 pt.)**

3. Definire cosa si intende per side channel attack e definire i principi su cui si basano rispettivamente: timing channel attack e power channel attack. (**3 pt.)**

I voti riportati sono un limite superiore e saranno assegnati nel caso di risposte che non contengano imprecisioni e siano sufficientemente esplicative.

Il testo dell'esame deve essere redatto in formato digitale e inviato al seguente indirizzo: danilo.bruschi@unimi.it entro le 12.30 della data corrente.