ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Laboratorio di Sicurezza Informatica

Modalità d'esame

Marco Prandini

Dipartimento di Informatica – Scienza e Ingegneria

Workflow

- Il giorno dell'esame, obbligatoriamente nella stessa seduta, si sostengono la prova teorica e, se ammessi, quella pratica
  - per superare l'esame devono risultare singolarmene sufficienti entrambe
- Prova teorica
  - correzione automatica su EOL
  - se superata consente l'accesso alla prova pratica
- Prova pratica
  - correzione manuale (non immediata)
- Calcolo della media tra le prove (stesso peso)
- Dopo qualche giorno: pubblicazione dei voti su AlmaEsami
- A richiesta, solo per modificare un voto già sufficiente: prova orale
  - la prova orale può abbassare o alzare il voto al più di 3 punti
  - può spaziare su qualsiasi argomento trattato nel corso, teorico o pratico
- Entro una settimana dalla pubblicazione dei risultati, chi vuole rifiutare il voto o richiedere la prova orale facoltativa deve contattare via e-mail il docente
- Chi ha in carriera il corso integrato con Lab. Sicurezza otterrà come voto la media dei due; contattare via e-mail il docente per chiedere la verbalizzazione

Prova teorica

- Domande a risposta chiusa su tutto il programma, anche i comandi visti in lab
  - es.: vediamo iptables in laboratorio, potrebbe esserci una domanda che chiede in che catena inserire una regola per ottenere un certo effetto
- Non si può consultare materiale di alcun genere
- Penalizzazione per risposta sbagliata
- Parametri indicativi (di volta in volta potranno oscillare in un intorno di questi valori)
  - Durata: 45 minuti
  - Numero domande: 30-40
  - Risposte: vero-falso o scelta multipla
  - Risultato perfetto: 36 punti
  - Sufficienza: 18 punti

Prova pratica

- 2 ore in totale
- Vengono proposti esercizi simili a quelli svolti in laboratorio, di tipo sia offensive (conduzione di un attacco verso un sistema vulnerabile fornito) che defensive (adozione di meccanismi di protezione delle reti o dei sistemi)
- Si possono consultare appunti, script autoprodotti, materiale del corso, documentazione (non piattaforme di scambio soluzioni)
- Temi:
  - strumenti di enumerazione, brute-forcing e intercettazione dati
  - sfruttamento di vulnerabilità via privilege escalation, su binari, su applicazioni web
  - sicurezza delle informazioni *(questi strumenti potrebbero essere richiesti per interagire con la piattaforma d'esame – vedi esempi)*
    - crittografia con pgp *(es. consegna file firmati)*
    - protezione del traffico con ssh e vpn *(es. accesso a sistema da testare)*
  - configurazione firewall con iptables
  - definizione di regole di monitoraggio host- e network-based