Programul etapei naționale

Programul competiției interne:

– 30 iunie – 02 iulie 2017 – prima sesiune de calificare (on-line);
– Sfârșitul lunii iulie 2017 – a doua sesiune de calificare (on-site), va dura 8 ore, incluzând exerciții A/D;
– Septembrie 2017 – prima sesiune de training (bootcamp);
– Octombrie 2017 – a doua sesiune de training (bootcamp).

Reguli testare:

– orice tentativă de atac prin metode de tip Denial Of Service a scoreboard-ului sau a celorlalte servicii va conduce la descalificare;
– clasificarea câștigătorilor se face după punctajul total la sfârșitul competiției naționale;
– în caz de egalitate, departajarea se va face după timpul de execuție a task-urilor.

Informații testare:

– task-urile testează următoarele capitole de securitate: Reverse Engineering, Exploitation, Forensics, Web Application hacking, Crypto;
– anumite taskuri pot avea componente din mai multe capitole;
– scopul fiecărui task este de a obține o informație (denumită în mod tradițional "flag") la care nu am avea acces, în mod obișnuit, dată fiind protecția oferită de sistemele de securitate. În fiecare task există o problemă de securitate care ne permite (prin analiza de cod și exploatarea sa) să ajungem la flag;
– un flag poate fi recunoscut după forma următoare: flag{.....};
– fiecare task are un număr de puncte în funcție de dificultatea sa;
– unele task-uri ar putea fi blocate în prima fază, dar vor fi pornite ulterior (până la încheierea perioadei de competiție);
– descrierile task-urilor și fișierele aferente fiecăruia vor putea fi copiate de pe un site anex numit scoreboard;
– de pe scoreboard se vor introduce flagurile și se va putea vizualiza progresul fiecărei persoane înscrise;
– vor exista task-uri offline (care se pot rezolva pe calculatorul personal, pentru validare, trimițându-se doar flagul pe scoreboard) și task-uri online (va exista un IP și un PORT prin care sa se faca interacțiunea cu server-ul).

Materiale educaționale recomandate:
– Criptografie
– https://class.coursera.org/crypto-preview
– http://cryptopals.com/

– Web application hacking
– The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws de Dafydd Stuttard

– Reverse Engineering
– Practical Malware Analysis de Michael Sikorski
– http://beginners.re/

– Exploitation
– Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition de Daniel Regalado
– Hacking: The Art of Exploitation, 2nd Edition de Jon Erickson

– Alte cursuri
– http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html
– https://github.com/isislab/Hack-Night
– http://www.opensecuritytraining.info/Exploits1.html
– http://ocw.cs.pub.ro/courses/cns

Tool-uri recomandate:
– Reverse Engineering
– Ida Freeware / Radare
– Exploitation
– Gdb + Peda (https://github.com/longld/peda)
-Web application hacking
– Burp Suite Free Edition

Concursul final se va desfășura în Spania, în orașul Malaga pe parcursul a cinci zile (30 octombrie – 3 noiembrie). Programul cuprinde atât desfășurarea concursului propriu-zis, precedat de efectuarea unor exerciții pentru acomodare, cât și evenimente de socializare și vizite turistice.

Participanţii între 16 – 18 ani selectaţi pentru a participa la concursul final nu vor putea părăsi ţara fără acordul părinţilor sau tutorelui legal, dat prin declaraţie notarială autentificată.

Pentru informații suplimentare accesați site-ul oficial al competiției: ECSC 2017

Ce exerciții trebuie să rezolvi în cadrul competiției ?

Echipele vor trebui să se transpună într-un scenariu care presupune dezvoltarea și apărarea unei infrastructuri. Partea cea mai importantă va rămâne dezvoltarea și apărarea propriei infrastructuri, dar atacarea celorlalte echipe aduce puncte.
Vor fi 3 nivele de dificultate a testelor: greu, mediu și ușor.

Echipele vor trebui să rezolve un scenariu care presupune dezvoltarea și apărarea unei infrastructuri. De asemenea, aveți șansa să strângeți puncte prin atacarea celorlalte echipe. Partea cea mai importantă va rămâne dezvoltarea și apărarea propriei infrastructuri. Mai mult, este foarte important să cunoști punctele tari și slabe ale echipei tale, pentru a distribui sarcinile în mod optim. Vor fi 3 nivele de dificultate a testelor: greu, mediu și ușor. Testele sunt din următoarele domenii:

– Securitate web;
– Criptografie;
– Inginerie inversă și investigații;
– Programare;
– Teste de penetrare;
– Atac și aparare;

– Securitate Linux/windows/macOS;
– Securitate telefoane mobile.

Condiții de înscriere

Fiecare țară participantă va avea o echipă selecționată în urma fazei naționale a concursului. Participanții care vor să se înscrie în competiţie trebuie să îndeplinească următoarele criterii:

– vârsta cuprinsă între 16 și 25 de ani
– cetățeni ai ţării pentru care participă sau locuiesc şi urmează o formă de învățământ în această ţară

Componența echipelor și categorii

Echipele sunt formate din 2 (maxim 3) antrenori și maxim 10 concurenți din 2 categorii: 5 juniori (între 16 și 20 ani) și 5 seniori (între 21 și 25 ani). Vârsta de referință este vârsta concurentului la sfarsitul anului calendaristic.

Concurenții selecționați în echipa României vor beneficia de:

- Recunoastere nationala si promovare in media;
- Două stagii specializate de pregătire;
- Mentorat cu specialisti din domeniu;
- Oportunitati de angajare in domeniu;
- Toate costurile asigurate de sponsori;
- Premii oferite de sponsori;
- Participare la competitii internationale.
- O invitatie pentru scena Cyber pe durata celor 2 zile ale evenimentului IMWorld (4-5 Octombrie / Romexpo) pentru toti cei care se vor califica in echipa care va reprezenta Romania in etapa finala a competitiei.

Toate persoanele inregistrate in competitie (cei peste 20 ani) vor primi un Pass de acces gratuit in zona Expozitionala IMWorld si pe urmatoarele scene: Enterprise Solutions Stage si Digital&E-commerce Stage.