Raport Științific și Tehnic
Hub inovativ pentru tehnologii avansate de securitate cibernetică (ATLAS)
Contract Nr. 17PCCDI/2018
- Etapa IV -

Introducere

Etapa IV s-a desfășurat în perioada 01/01/2021 - 30/09/2021 și a avut ca obiective principale:

- achiziția ultimului lot de echipamente;
- testarea platformei cyber range prin organizarea în comun a unui exercițiu de apărare cibernetică;
- diseminarea rezultatelor cercetării prin publicarea de articole în jurnale și la conferințe și prin intermediul site-ului Web de prezentare a proiectului (https://security-hub.ro/);
- organizarea unui workshop tematic pentru prezentarea rezultatelor obținute în cadrul proiectului complex către potențialii beneficiari;
- elaborare program comun de cercetare-dezvoltare și inovare.

Pentru atingerea acestor obiective, au fost planificate două activități în cadrul proiectului component 3. Proiectele componente 1 și 2 au fost finalizate la sfârșitul etapei III, toate obiectivele propuse fiind atinse sau depășite. În continuare, sunt prezentate în detaliu rezultatele științifice și tehnice obținute în urma derulării activităților specifice proiectului component 3 precum și acțiunile întreprinse pentru dezvoltarea în continuare a soluțiilor realizate în cadrul proiectelor componente 1 și 2.

Proiect Component 1 - Metode formale și tehnici de învățare automată pentru securizarea aplicațiilor și sistemelor de operare

În cadrul proiectului component 1 au fost dezvoltate două produse noi: *Platformă online pentru analiza binarelor* și *Framework de securitate bazat pe metode formale și învățare automată*.

Platforma online pentru analiza binarelor are la bază framework-ul KOBOLD (https://github.com/malus-security/kobold). După finalizarea Etapei III, KOBOLD a continuat să fie dezvoltat în următoarele direcții:

1. Investigarea scurgerii de date (https://github.com/malus-security/ios-privacy-leaks) pentru aplicațiile iOS:
    a. Am investigat politicile de confidențialitate pentru cele mai folosite aplicații de pe App Store. Acestea specifică ce date colectează aplicațiile și cu cine le partajează. Din analiza noastră am observat că aplicațiile colectează date ce pot fi considerate confidențiale. De exemplu, numele, data de naștere sau locația sunt informații prezente în majoritatea politicilor de confidențialitate. De asemenea, regăsim în unele politici informații biometrice, despre sănătate sau religie. Colectarea acestor informații (ex: biometrice) nu ar trebui să fie permisă.

b. Am creat o configurare în care captăm și analizăm traficul de pe dispozitiv către serverele externe. Am confirmat că o parte din informațiile menționate în politicile de confidențialitate părăsesc telefonul (ex: nume, data naștere, ID telefon și chiar locația).
c. Am realizat un studiu pe 230 de persoane cu vârste cuprinse între 10 și 70 de ani, cu nivel de educație divers, în care am pus întrebări pentru a afla cât de importantă este confidențialitatea datelor pentru ei. Întrebările au fost despre conștientizarea datelor colectate, motivele colectării și citirea politicilor de confidențialitate ale aplicațiilor. Răspunsurile arată că oamenii știu despre colectarea de date însă doar jumătate fac ceva în această privință. 20% dintre utilizatori citesc politicile de confidențialitate. Cel mai frecvent motiv este că politica de confidențialitate este prea mare și greu de citit.

2. Dezvoltarea soluției de verificare a UI (https://github.com/malus-security/ios-ui-exerciser) pentru iOS. În acest modul am dezvoltat o soluție de investigație și testare a interfeței cu utilizatorul fără a fi nevoie de codul sursă. Acest modul oferă adaptabilitate și se adresează atât aplicațiilor simple, cât și aplicațiilor de socializare. Modulul se adresează telefoanelor fizice, nu emulatoarelor. UI-Exerciser creează un arbore de stări pentru aplicația testată, iar apoi analizează exhaustiv fiecare stare. UI-exerciser a reușit să detecteze o anomalie ce poate duce la vulnerabilități de acces, denumită de noi *Dot Artefact* și raportată la Apple în Mai 2021.

Framework-ul de securitate bazat pe metode formale și învățare automată este format din două componente: *RIVER* (detecție de vulnerabilități bazată pe analiză dinamică) și *MALID* (detecție de malware bazată pe analiză statică).

RIVER (https://river.cs.unibuc.ro/) este un framework creat special pentru a testa programe cu ajutorul căruia se pot găsi intrări problematice care pot conduce la descoperirea de vulnerabilitati. Acesta funcționează la nivel binar și include următoarele componente: analiză dinamică de tip taint, poate marca părțile din intrare care au fost folosite în timpul execuției, sistem de execuție simbolică și sistem de execuție concolică.

După finalizarea Etapei III, ne-am concentrat pe două direcții de dezvoltare a tool-ului RIVER:

1. Îmbunătățirea RIVER folosind tehnici de inteligență artificială (*RiverFuzzRL*). Combinația dintre tehnicile de fuzzing și AI este o direcție nouă importantă în domeniu identificării vulnerabilităților software. De aceea, am hotărât să optimizăm rezultatele RIVER folosind metode de ML, în special reinforcement learning, pentru a ghida fuzzing-ul spre zonele cu posibile vulnerabilitati.
2. Adaptarea RIVER la domeniul IoT (*RiverIoT*). În acest caz, obiectivul a fost să valorificăm fundația solidă reprezentată de RIVER pentru dezvoltarea de metode de fuzzing ghidat pentru a testa aplicații IoT. Arhitectura de testare este modelată ca un grafic al conexiunii proceselor desfășurate pe dispozitive fizice. Metodele utilizate extind capacitatea de testare a proceselor individuale. Noul cadru propus permite utilizatorului să testeze interacțiunea proceselor precum și conexiunile dinamice care ar putea apărea în timpul rulării.

Proiect Component 2 - Arhitecturi de securitate pentru IoT

În cadrul proiectului component 2 au fost dezvoltate două produse noi: *Metodologie pentru evaluarea securității IoT* și *Framework de securitate bazat pe reputație pentru IoT*.

Metodologie pentru evaluarea securității IoT, denumită MIST, a fost completată pe perioada etapei 4 prin adăugarea de noi riscuri și vulnerabilități care au fost evidențiate de cercetări recente. De asemenea, a fost definită o metodologie destinată evaluării securității dispozitivelor IoT personale sau de tip Smart Home, de către utilizatorii casnici. Această extensie a metodologiei inițiale, permite o evaluare de tip black-box a securității dispozitivelor IoT apelând la criterii ce pot fi observate sau

evaluate de către un consumator final, fără a necesita un background tehnic. Procesul de evaluare constă în completarea unui chestionar, iar la final, pe baza răspunsurilor înregistrate, dispozitivul evaluat este încadrat într-o clasă de risc din prisma securității. Chestionarul va fi publicat pe site-ul metodologiei, www.mist.ase.ro.

Framework-ul de securitate bazat pe reputație pentru IoT, denumit generic RESFIT, a continuat să fie dezvoltat prin adăugarea de funcționalități noi. Astfel, s-au analizat mecanisme noi pentru calculul reputației nodurilor IoT bazate pe tehnici de Machine Learning (k-nearest neighbors (k-NN), support vector machines (SVM), decision tree) față de clasificatorul bayesian naiv folosit inițial și s-a studiat folosirea framework-ului RESFIT și în alte categorii de aplicații cum ar fi crowd sensing, pe lângă cele de tip smart home și smart city.

Specificațiile de proiectare și dezvoltare pentru framework-ul RESFIT precum și rezultatele experimentale obținute în urma testelor efectuate au fost publicate într-un articol la jurnalul MDPI Electronics [1]. Codul sursa pentru framework-ul RESFIT este open-source fiind disponibil la adresa: https://github.com/atlas-iot/resfit

Experiența acumulată a permis extinderea cercetărilor în domeniul securității IoT și publicarea unui nou articol la aceeași revistă MDPI Electronics având ca temă detecția anomaliilor folosind tehnici de învățare profundă nesupervizată pentru identificarea rețelelor de boți IoT [2].

Proiect Component 3 - Mediu distribuit pentru exerciții și cercetare avansată în domeniul securității cibernetice

Activitatea 4.1 - Evaluarea operațională a platformei cyber range

Exercițiul de apărare cibernetică s-a derulat în perioada 11-13 iunie 2021. La exercițiul au participat 26 de studenți de la licență și master din cadrul universităților partenere în proiect, grupați în 8 echipe. Exercițiul au pus la încercare abilitățile tehnice ale studenților în domeniul securității cibernetice precum securizarea sistemelor de operare și a serverelor de aplicații, securizarea rețelelor, pentesting, forensics și analiză malware. Exercițiul a fost axat pe componenta practică (hands-on) și a constat din două tipuri de scenarii.

În cadrul primului scenariu (red team vs. blue team) studenții au trebuit să securizeze o serie de servere de aplicație pentru a putea face față la atacurile derulate de către instructori. Mașinile virtuale aferente exercițiului au fost active în rețea. Acest lucru a permis validarea soluțiilor adoptate de studenți de pe un sistem dedicat, aflat în rețea cu mașinile virtuale folosite.

Exercițiile au fost proiectate și stocate în repository împreună cu scripturi de implementare și validare. Scripturile de implementare au fost folosite pentru a instala exercițiile pe mașina virtuală inițială, în timp ce scripturile de validare au fost utilizate pe mașina virtuală a atacatorului pentru a recupera starea defectelor și a actualiza scorul.

Scenariul a fost proiectat astfel încât fiecare echipă să aibă acces complet la un sistem. Sistemul a fost presupus ca fiind compromis, cu multiple probleme de securitate lăsate în urmă de atacator. Mai mult, alte probleme au fost prezente din cauza unor decizii de instalare și configurare imperfecte. Atât defectele rău intenționate, cât și configurarea greșită neintenționată trebuiau descoperite și remediate de către participanți pentru a obține puncte în concurs.

Scenariul a constat din 10 provocări care trebuiau rezolvate de fiecare echipă:

1. *command*: Un server web folosește o vulnerabilitate de intrare neconfirmată pentru a executa comenzi shell.
2. *expired*: Există un certificat expirat pe un server web. Acest lucru trebuie remediat.
3. *admin1*: Serverul bazei de date MySQL este accesibil prin credențialele admin / admin. Aceasta este o parolă administrativă care permite accesul la întreaga bază de date.
4. *admin2*: O cale a serverului web este configurată pentru a utiliza admin / admin.
5. *admin3*: Serviciul LDAP este accesibil prin admin / admin. Aceasta este o parolă administrativă care permite accesul la întreaga bază de date LDAP.
6. *really*: Un serviciu de tip MTA configurat pe sistem ca open-relay, ceea ce permite livrarea mesajelor spam de către sistem, indiferent de sursa lor.
7. *shadow*: Un executabil dat (/usr/bin/rev) este configurat prin capabilități Linux pentru a citi toate fișierele din sistem, aceasta include și fișierul critic /etc/shadow.
8. *sign*: Un serviciu de semnare digitală are o vulnerabilitate de tipul buffer overflow. Executabilul netstat a fost înlocuit pentru a „ascunde” prezența serviciului.
9. *super*: Un utilizator local (fred) poate accesa contul root prin sudo.
10. *todo*: Există o aplicație web NodeJS + mongodb în care utilizatorii pot adăuga articole.

Provocările a fost implementate pe mașinile virtuale puse la dispoziția echipelor participante în concurs (numite mașini *blue*). Scripturile de validare au fost instalate și pornite pe mașina virtuală a atacatorului (numită mașina *red*).

În cel de-al doilea scenariu (digital forensics), studenții au avut de investigat o stație de lucru infectată cu malware și folosită pentru a ataca sisteme de control industrial. Nivelul de dificultate al scenariului a fost unul mediu, timpul estimat de rezolvare fiind de 6 ore.

Scopul scenariului a fost de a identifica acțiunile efectuate de atacatori parcurgând următoarele etape:

- Inițierea procesului de răspuns la incidente;
- Analiza sistemului informatic suspicios și identificarea cauzelor care au generat erorile de funcționare semnalate;
- Analiza artefactelor colectate și documentarea tuturor elementelor malițioase identificate;
- Identificarea vectorului de infecție, metodelor de persistență și a obiectivelor atacatorului, pe baza artefactelor colectate.

Provocările tehnice specifice scenariului au fost complexe, necesitând cunoștințe avansate despre Windows forensics, VBA code review, malware analysis, SCADA forensics.

Scenariile au fost rulate în cadrul platformei cyber range dezvoltată în cadrul proiectului ATLAS. Astfel, platforma a fost evaluată din punct de vedere operațional, performanțele obținute și nivelul ridicat de disponibilitate demonstrând faptul că ea este capabilă să găzduiască cu succes exerciții complexe de apărare cibernetică.

În plus, platforma cyber range realizată s-a dovedit foarte versatilă, fiind folosită cu succes și în alte scopuri. Platforma permite desfășurarea activităților de laborator care necesită instanțierea rapidă de mașini virtuale pentru fiecare student. De asemenea, platforma poate fi folosită pentru emularea unor rețele de tip enterprise pentru a analiza noi tipuri de atacuri și a implementa metode adecvate de protecție.

În perioada următoare, intenționăm să organizăm un *exercițiu la nivel național* la care să fie invitați studenți și cadre didactice de la universitățile din țară care derulează programe de studii în domeniul securității cibernetice pentru a demonstra avantajele unei astfel de soluții. Obiectivul final este de a extinde platforma cyber range la nivelul cât mai multor universități din țară pentru a partaja resursele și a organiza în comun exerciții de apărare cibernetică.

Scenariile pentru exercițiile de apărare cibernetică dezvoltate pe parcursul proiectului au fost publicate într-un *repository* privat pe GitHub la care au acces toate universitățile partenere (https://github.com/security-hub-ro/cyber-challenges). Pentru fiecare scenariu, în repository se regăsește:

1. Player Instructions Handbook - document adresat participanților la exercițiu, în care este descris contextul, etapele exercițiului, uneltele recomandate a se folosi și livrabilele ce trebuie predate la finalul exercițiului;
2. Exercise Solution - document cu modul de rezolvare a exercițiului pentru evaluarea rezultatelor obținute de fiecare student / echipă în parte;
3. Exercise Deployment - document cu instrucțiuni privind deployment-ul mașinilor virtuale aferente exercitiului în cadrul platformei cyber range;
4. VM Images - Mașinile virtuale aferente exercițiului.

În acest mod, exercițiile pot fi ușor partajate între universități, iar scenariile pot fi reutilizate ori de câte ori este nevoie.

Pentru a simplifica accesul la platformele cyber range din cadrul celor patru universități, a fost dezvoltat un *modul centralizat pentru managementul identității* participanților la exerciții. Modulul a încorporat API-urile de Single Sign-On (SSO) oferite de Google și Microsoft și astfel participanții au putut folosi pentru autentificare conturile de e-mail create de universități pentru accesul la resursele instituționale. Filtrarea participanților s-a realizat pe baza domeniului adresei de e-mail. Soluția este scalabilă, permițând includerea de noi domenii de adrese de e-mail pentru controlul accesului la cyber range.

Cu ocazia exercițiului derulat în comun de universitățile partenere a fost realizat un *sondaj* pentru a colecta feedback de la participanți. Aceasta a avut ca scop să contribuie la îmbunătățirea exercițiilor / scenariilor viitoare, pe de o parte, și să studieze caracteristicile persoanelor interesate de exercițiile de securitate cibernetică, pe de altă parte.

S-au colectat date de la toți cei 26 de participanți. Sondajul a fost anonim și a fost structurat pe trei direcții: (1) informații privind scenariul, (2) date referitoare la pregătirea în securitate cibernetică a participanților și (3) întrebări care pot indica nivelul de cunoștințe generale al participanților cu privire la securitatea cibernetică. Cele 25 de întrebări din chestionarul de feedback sunt prezentate în Anexa 1.

Principalele concluzii rezultate în urma acestui sondaj sunt prezentate mai jos. Ipotezele analizate au fost următoarele:

Ipoteza 1: Concurenții cu note mai bune obțin rezultate mai bune la exercițiile de securitate cibernetică. Participanții sunt de obicei foști studenți sau angajați în domenii conectate la IT. Deoarece securitatea cibernetică este adesea o disciplină secundară în facultățile de oeniu, ne-am uitat la corelația dintre cunoștințele IT generale ale unui student și rezultatele concursului.

Ipoteza 2: Concurenții cu certificări profesionale obțin scoruri mai bune decât cei fără certificări. În prezent, certificările în domeniul securității cibernetice sunt considerate importante în interiorul

organizațiilor și pot oferi un avantaj pentru angajare sau promovare. Am vrut să verificăm în ce măsură certificările profesionale îi ajută pe participanți să obțină rezultate mai bune în astfel de concursuri.

Ipoteza 3: În general, participanții au capacitatea de a se evalua corect. Le-am cerut participanților să-și evalueze singuri nivelul de formare atât în domeniul IT, cât și al securității cibernetice și am corelat răspunsurile cu scorurile obținute în concurs.

Pe lângă ipotezele de mai sus, sunt prezentate o serie de constatări care ajută să înțelegem mai bine particularitățile participanților la concurs și cum putem stimula studenții să studieze securitatea cibernetică.

Majoritatea participanților au fost motivați de dorința de a-și îmbunătăți cunoștințele și abilitățile, 46% s-au concentrat în principal pe securitatea cibernetică, în timp ce 19% au dorit să adune cunoștințe generale de informatică. O parte importantă a participanților a fost condusă de curiozitate (27%) și aproximativ 8% de divertisment. Gradul de dificultate a fost undeva între mediu și crescut, iar timpul alocat pentru eveniment a fost considerat adecvat de cei mai mulți, cu toate acestea 27% dintre participanți au considerat că au nevoie de mai mult timp.

Peste 73% dintre concurenți au considerat calitatea indicațiilor primite medie sau mai bună. 88,5% dintre concurenți au evaluat instrumentele la care au avut acces cel puțin acceptabile, în timp ce 58% au fost foarte mulțumiți. Un aspect important care poate fi îmbunătățit poate fi considerat nemulțumirea unora dintre participanți față de structura sarcinilor, deoarece doar 61,5% dintre ei au fost mulțumiți, în timp ce 23% au fost mulțumiți într-o mică măsură și 15,5 au fost nemulțumiți. Ipoteza noastră este că această cauză este legată de efortul nostru de a crea scenarii cât mai apropiate de cele din practică. Ca atare, structura exercițiului a fost ușor diferită decât în majoritatea evenimentelor similare.

Marea majoritate a participanților erau absolvenți de universitate (81%), în timp ce alți 11,5% erau în faza de absolvire. 85% dintre studenți au absolvit cu media 8 sau mai mare și 35% cu nota 9 sau mai mare. Majoritatea studenților activaseră în domeniul IT (92,3%), totuși 57,7% dintre ei aveau foarte puțină experiență (0-2 ani). 69% dintre ei aveau experiență profesională într-o poziție care includea sarcini de securitate cibernetică, în timp ce 38,4% au obținut cel puțin un certificat de securitate cibernetică. 84,6% au participat în trecut la concursuri de tip CTF sau evenimente similare.

Din totalul de 26 de concurenți, 15 au obținut un scor între 20% și 40%, opt dintre ei au câștigat între 40% și 60%, doi au obținut scoruri în intervalul 60% -80% și un participant a rezolvat corect mai mult de 80% din sarcini.

Există un mare interes în rândul participanților în domeniul securității cibernetice, deoarece mai mult de 2/3 folosesc publicații specializate în securitate cibernetică pentru a studia informații actualizate cel puțin o dată pe săptămână.

În general, profilul participantului părea potrivit pentru eveniment, deoarece include scenarii atât în sistemele de operare Windows, cât și în Linux. O constatare interesantă a fost că mai mulți participanți erau destul de familiarizați cu Linux Kali decât cu orice altă distribuție Linux în general. Deoarece Linux Kali este considerat o distribuție special concepută în scopuri de securitate cibernetică, acesta este un alt indiciu al interesului participanților pentru securitatea cibernetică.

Pe baza sondajului, am creat un profil de participant care ar putea fi util deoarece (1) putem identifica cu ușurință ce studenți ar putea fi interesați să participe la competiții de securitate și care nu și (2) putem identifica cu ușurință ce studenți ar putea fi interesați de domeniul securității cibernetice.

Deși majoritatea studenților sunt mai degrabă pregătiți în domeniul IT în general decât în securitatea cibernetică în special, 70% sunt puternic interesați de domeniul securității cibernetice. De obicei sunt studenți bine pregătiți, 85% având note medii peste 8 și o treime peste 9 (din 10). Majoritatea participanților păreau să aibă abilități bune de lucru în echipă, deoarece peste 88% dintre ei erau mulțumiți de coeziunea echipei lor.

O treime dintre concurenți dețin deja certificări profesionale și 85% au participat la evenimente similare, cum ar fi concursuri CTF. Majoritatea au cunoștințe solide de programare, în special în limbile C / C ++, Python, Java, C #, JavaScript și PHP. De asemenea, peste 50% sunt familiarizați cu limbajul de asamblare.

În ceea ce privește cunoștințele de securitate cibernetică, participanții tind să fie mai bine pregătiți teoretic decât practic, deoarece sunt mai familiarizați cu concepte care pot fi înțelese studiind teoretic, dar mai puțin familiarizați cu concepte care necesită mai multă practică.

Concluzionând, ipotezele 1 și 3 au fost validate, în vreme ce ipoteza 2 nu a demonstrat o corelație între certificări și rezultate la concurs.

Experiența acumulată în urma derulării exercițiului precum și rezultatele sondajului au stat la baza elaborării unui nou articol trimis spre evaluare la CSEDU 2022 (The International Conference on Computer Supported Education) [5].

Activitatea 4.2 - Diseminare și organizare workshop

Pentru prezentarea și promovarea rezultatelor proiectului ATLAS a fost organizat un workshop tematic în data de 23 Septembrie 2021 la care au fost invitați să participe reprezentanți ai mediului academic și specialiști din partea agențiilor guvernamentale și companiilor private din domeniul securității cibernetice. Workshopul s-a desfășurat online, prin intermediul platformei Microsoft Teams. Lista participanților la eveniment este prezentată în continuare:

1. Academia Tehnică Militară
    - Ion BICA
    - Constantin GRUMĂZESCU
2. Universitatea Politehnica din București
    - Mihai CHIROIU
    - Costin CARABAȘ
    - Radu MANTU
3. Universitatea din București
    - Alin ȘTEFĂNESCU
    - Bogdan GHIMIȘ
4. Academia de Studii Economice din București
    - Cătălin BOJA
5. Universitatea Politehnica din Timișoara
    - Bogdan GROZA
6. Universitatea “Aurel Vlaicu” din Arad
    - Dominic BUCERZAN

7. Universitatea din Craiova
    - Marius MARIAN
8. Universitatea “Ovidius” din Constanța
    - Alexandru BOBE
9. Universitatea “Alexandru Ioan Cuza” din Iași
    - Anca NICA
10. Universitatea Tehnica ”Gheorghe Asachi” din Iași
    - Ștefan ACHIREI
11. Universitatea Tehnica din Cluj-Napoca
    - Adrian COLESA
12. Universitatea ”Babes-Bolyai” din Cluj-Napoca
    - Darius BUFNEA
13. CERT-RO
    - Nelu MUNTEANU
    - Alina VASILESCU
14. Centrul Național CYBERINT
    - Daniel RĂDAN
15. Serviciul de Protecție și Pază
    - Mihai CUJBĂ
16. CertSIGN
    - Valentin HLODEC
    - Marius RADA
17. SecureWorks
    - Alin PUNCIOIU
    - Ionut GEORGESCU
18. Pentest-Tools
    - Adrian FURTUNĂ
19. Atos Convergence Creators
    - Titus BĂLAN
20. Oracle Romania
    - Silviu TEODORU
    - Alin CIUPERCA

Participanții și-au manifestat interesul pentru soluțiile dezvoltate în cadrul proiectului ATLAS, în special pentru platforma cyber range, și s-au arătat deschiși pentru a colabora în vederea extinderii „hub”-ului de securitate cibernetică.

Programul Comun de Cercetare-Dezvoltare și Inovare

În cadrul acestei etape a fost elaborat și adoptat Programul Comun de Cercetare-Dezvoltare și Inovare (CDI) ce are ca scop valorificarea rezultatelor obținute în cadrul proiectului ATLAS și consolidarea colaborării dintre universitățile partenere. În acest sens, au fost agreate următoarele obiective:

- Valorificarea produselor noi dezvoltate în cadrul proiectului prin promovarea și adaptarea acestora în vederea transferului către agenții economici;
- Dezvoltarea de servicii științifice şi tehnologice de înalt nivel, în domenii prioritare precum securitatea cibernetică, inteligența artificială, cloud și IoT;
- Participarea în comun la competițiile de proiecte naționale/internaționale sau finanțate de agenții economici;

- Continuarea publicarii de articole în colaborare în jurnale cotate ISI cu factor mare de impact și la conferințe științifice de prestigiu;
- Extinderea și consolidarea colaborărilor și parteneriatelor cu mediul academic și economic;
- Creşterea vizibilității și recunoașterii la nivel național și internațional;
- Menținerea cercetătorilor noi angajați și ridicarea pregatirii profesionale a acestora.

Pentru atingerea acestor obiective, au fost stabilite următoarele direcții de acțiune:

- Transferul produselor noi realizate către mediul academic / economic
- Participarea în comun la proiecte de cercetare
- Publicarea în comun de lucrări științifice
- Integrarea în spațiul european de cercetare-dezvoltare și inovare

Susținerea hub-ului digital inovativ ”CyberSecurity Hub - CSH” (https://www.cybersecurity-hub.ro/), creat la inițiativa universităților partenere în proiectul ATLAS, reprezintă un alt obiectiv major asumat prin programul comun de cercetare-dezvoltare și inovare. ”CyberSecurity Hub - CSH” a fost înființat cu scopul de a asigura un cadru unitar de cooperare pentru realizarea unor obiective de interes comun și de a contribui la dezvoltarea economică prin soluții ce vizează creșterea nivelului de securitate cibernetică al serviciilor digitale oferite de autoritățile locale și de mediul privat.

”CyberSecurity Hub - CSH” a participat la procedura națională de selecție a centrelor care vor avea posibilitatea să devină membre ale Rețelei Europene de Centre de Inovare Digitală (Rețeaua EDIH) și fost declarat admis. Prezența ”CyberSecurity Hub - CSH” în rețeaua EDIH (https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-tool) va crește vizibilitatea consorțiului și va permite realizarea de viitoare colaborări/parteneriate cu hub-uri similare.

Programul comun de cercetare-dezvoltare și inovare poate fi consultat pe site-ul proiectului la adresa: https://security-hub.ro/wp-content/uploads/2021/04/ATLAS_Program_Comun_CDI_17PCCDI.pdf

Publicarea rezultatelor proiectului

Rezultatele activităților de cercetare derulate în cadrul etapei IV au fost publicate în jurnale și în volumele unor conferințe internaționale indexate ISI/BDI. În total, au fost elaborate **5 articole științifice**, după cum urmează:

1. S-C. Arseni, B.-C. Chifor, M. Coca, M. Medvei, I. Bica, and I. Matei, “RESFIT: A Reputation and Security Monitoring Platform for IoT Applications,” Electronics, vol. 10, no. 15, p. 1840, Jul. 2021;
2. I. Apostol, M. Preda, C. Nila, and I. Bica, “IoT Botnet Anomaly Detection Using Unsupervised Deep Learning,” Electronics, vol. 10, no. 16, p. 1876, Aug. 2021;
3. I. Bica, R. L. Unc, and S. Turcanu, “Virtualization and Automation for Cybersecurity Training and Experimentation,” Innovative Security Solutions for Information Technology and Communications, Lecture Notes in Computer Science, Vol. 12596, pp. 227–241, Springer, 2021;
4. C. Toma, M. Popa, M Doinea, “Cloud Authentication using FIDO compliant Java Card Technology Secure Elements,” The 20th International Conference on Informatics in Economy, Online Conference, Bucharest, Romania, 2021.
5. R. Deaconescu, T. Georgescu, A. Bălțoiu, A. Puncioiu, “Using cybersecurity exercises as essential learning tools in universities,” The 14th International Conference on Computer Supported Education, Prague, 2022 (sub evaluare)

Site-ul Web al proiectului (https://security-hub.ro/) a fost actualizat în permanență cu informații despre produsele dezvoltate, articolele publicate, programul comun de CDI și evenimentele organizate în cadrul proiectului. Tot pe acest site se află și o scurtă prezentare a hub-ului digital inovativ ”CyberSecurity Hub - CSH”, creat la inițiativa universităților partenere în proiectul ATLAS. Informații detaliate despre CSH se găsesc pe un site-ul dedicat (https://www.cybersecurity-hub.ro/).

Concluzii

Având în vedere cele expuse mai sus, apreciem că au fost atinse toate obiectivele pentru această etapă. Indicatorii de rezultat prevăzuți în contractul de finanțare au fost realizați în întregime. Rezultatele obținute au fost diseminate prin publicarea de articole în jurnale și la conferințe de prestigiu și prin organizarea unui workshop tematic la care au fost invitați să participe reprezentanți ai mediului academic și specialiști din partea agențiilor guvernamentale și companiilor private din domeniul securității cibernetice.

Programul comun de CDI adoptat în cadrul proiectului permite universităților partenere să continue colaborarea pentru valorificarea produselor realizate, participarea în comun la competițiile de proiecte naționale/internaționale sau finanțate de agenții economici, în domenii prioritare precum securitatea cibernetică, inteligența artificială, cloud și IoT.

Data: 30.09.2021

Director Proiect Complex

Prof.univ.dr.ing.

Ion BICA

Anexa 1 - Chestionar de feedback

Prin acest chestionar ne dorim, în primul rând, să aflăm feedback-ul dumneavoastră legat de concursul de tip cyber-range. De asemenea, ne propunem să identificăm cunoștințele și aptitudinile care facilitează obținerea de rezultate bune în astfel de evenimente (concursuri de securitate).

Chestionarul este anonim, iar rezultatele vor fi utilizate în scopul cercetării.

---

* Required

Întrebări legate de concursul cyber-range

1. Care este motivația dumneavoastră de a participa la acest eveniment *

   Mark only one oval.

   - ◯ Îmbunătățirea cunoștințelor și aptitudinilor legate de securitate cibernetică
   - ◯ Dezvoltare în general
   - ◯ Curiozitate
   - ◯ Entertainment

2. Considerați că nivelul de dificultate al evenimentului CTF a fost: *

   Mark only one oval.

   - ◯ Foarte ușor
   - ◯ Ușor
   - ◯ Mediu
   - ◯ Dificil
   - ◯ Foarte dificil

3. Considerați că timpul alocat a fost: *

Mark only one oval.

- Puțin
- Potrivit
- Mult

4. Calitatea indicațiilor primite în cadrul evenimentului a fost *

Mark only one oval.

- Foarte bună
- Bună
- Medie
- Slabă
- Foarte slabă

5. Ați avut acces la instrumentele necesare pentru a vă desfășura activitatea? *

Mark only one oval.

- Da, la tot ce era necesar
- Da, la majoritatea
- Da, la o mica parte dintre acestea
- Nu

6. Considerați că exercițiile au fost structurate adecvat? *

Mark only one oval.

- În foarte mare măsură
- În mare măsură
- Într-o măsură medie
- În mica măsură
- În foarte mică măsură

7. Cum evaluați coeziunea echipei din care ați făcut parte? *

Mark only one oval.

- Foarte bună
- Bună
- Medie
- Slabă
- Foarte slabă

8. Care are fost scorul / procentul de exerciții rezolvate în concurs? *

Mark only one oval.

- 0-20%
- 20,01-40%
- 40.01-60%
- 60.01-80%
- 80,01-100%

Întrebări legate de experiență și studii

9. Care este stadiul studiilor dumneavoastră la licență? *

Mark only one oval.

- Am absolvit
- În curs de absolvire
- M-am înscris și am renunțat
- Nu m-am înscris

10. În cazul în care încă nu ați terminat facultatea, în ce an de studiu sunteți? *

Mark only one oval.

- 1
- 2
- 3
- 4
- an suplimentar
- niciuna dintre variantele de mai sus

11. Care este media dumneavoastră obținută în timpul facultății? (Dacă facultatea este încă în desfășurarea, vă rugăm să alegeți ultimul semestru/an de studiu complet) *

Mark only one oval.

- 5-6
- 6-7
- 7-8
- 8-9
- 9-10
- nu am absolvit

12. Câți ani de experiență aveți în câmpul muncii pe o poziție legată de domeniul IT? *

Mark only one oval.

- Nu am
- 0-2 ani
- 2-5 ani
- 5-10 ani
- peste 10 ani

13. Câți ani de experiență aveți în câmpul muncii pe o poziție legată de securitate cibernetică? *

Mark only one oval.

- Nu am
- 0-2 ani
- 2-5 ani
- 5-10 ani
- peste 10 ani

14. Aveți certificări în domeniul securității sau alte domenii conexe (precum rețele de calculatoare)? *

Mark only one oval.

- Nu
- Da, 1
- Da, 2-3
- Da, peste 3

15. Ați mai participat la evenimente de cecuritate cibernetică, precum CTF-uri, cyber-range sau de tip hackathon? Dacă da, la câte? *

Mark only one oval.

- Nu
- Da, 1-2
- Da, 3-5
- Da, 6-10
- Peste 10

16. Ce nivel considerați că aveți în domeniul IT în general? *

Mark only one oval.

	1	2	3	4	5	
Începător						Senior

17. Ce nivel considerați că aveți în domeniul securității cibernetice? *

Mark only one oval.

	1	2	3	4	5	
Începător						Senior

18. Cât de des citiți articole de securitate cibernetică (bloguri, website-uri etc)? *

Mark only one oval.

- Zilnic
- De 2-3 ori pe săptămână
- Săptămânal
- Lunar
- Foarte rar

19. Cum vă evaluați la următoarele discipline? (unde 1 - înseamnă Foarte slab pregătit, 2 - slab pregătit, 3 - mediu, 4 - bine pregătit, 5- foarte bine pregătit) *

Mark only one oval per row.

	1	2	3	4	5
Matematică					
Rețele de calculatoare					
Sisteme de operare					
Hardware					
Structuri de Date					

20. Cu care dintre următoarele limbaje de programare sunteți familiar? *

Check all that apply.

- [ ] C/C++
- [ ] Python
- [ ] Java
- [ ] C#
- [ ] Javascript
- [ ] Ruby
- [ ] PHP
- [ ] Assembly
- [ ] .Net
- [ ] Altele

21. Cu care dintre sistemele de operare de mai jos sunteți familiar? *

Check all that apply.

- [ ] Windows
- [ ] Linux Kali
- [ ] Linux (orice altă distribuție decât Linux Kali)
- [ ] OSX
- [ ] Unix
- [ ] DOS
- [ ] Altele

Aspecte legate cunoștințele în domeniul securității cibernetice

22. Sunteți familiarizați cu următoarele? *

Mark only one oval per row.

	Da	Nu	Am auzit de termen, dar nu stiu prea multe despre acesta
OWASP			
ENISA			
Stuxnet			
SolarWinds attack			
Heartbleed attack			
WannaCry			

23. Cu care dintre instrumentele următoare sunteți familiarizat (ați lucrat cu acestea sau cu unele similare)? *

Mark only one oval per row.

	Da	Nu	Am câteva cunoștințe, dar nu stăpânesc bine conceptul
Wireshark			
Nikto			
Linux Kali			
OpenVAS			
WinDump			
Fortinet			
Acunetix			
Cain & Abel			

24. Sunteți familiarizat cu următoarele concepte? (1) *

Mark only one oval per row.

	Da	Nu	Am câteva cunoștințe, dar nu stăpânesc bine conceptul
Diferențele dintre o cheie simetrică și una asimetrică			
Modelul OSI			
Diferențe dintre TCP și UDP			
Funcție hash criptografică			
Triunghiu CIA (principiile securității)			
Three-way handshake			
Diferențe dintre vulnerabilitate și amenințare			

25. Sunteți familiarizat cu următoarele concepte? (2) *

Mark only one oval per row.

	Da	Nu	Am câteva cunoștințe, dar nu stăpânesc bine conceptul
BYOD			
Clickjacking			
Virtual sandbox			
Lateral attack			
Honeypot			
Buffer overflow			
Rootkit			
Atac SQL			
Atac de tip man-in-the-middle			
Diferențe dintre encryption și hashing			
Cunosc cum se verifica validitatea unui certificat digital			

26. Sunteți familiarizat cu următoarele concepte? (3) (Da/Nu/ Am câteva cunoștințe, dar nu stăpânesc f bine conceptul) *

Mark only one oval per row.

	Da	Nu	Am câteva cunoștințe, dar nu stăpânesc bine conceptul
The concept behind Solarwinds attack?			
Conceptul din spatele WannaCry attack?			
Conceptul din spatele HeartBleed?			
User mode vs kernel mode			
Inteleg cum functioneaza un atac XSS			