Kauno technologijos universiteto (KTU) Kibernetinio saugumo kompetencijų centras kartu su KTU Informatikos fakulteto (IF) Kompiuterių katedra praėjusį šeštadienį surengė vienos dienos „Kibernetinio sprinto 2025“ intensyvią vienos dienos stovyklą.

KTU „M-Lab“ erdvėse (Studentų g. 63a, Kaunas) vyko intensyvios Lietuvos „Paimk vėliavą“ (*angl. – Capture the flag, CTF*) „CyberSprint 2025“ rinktinės treniruotės, atviros dirbtuvės ir demonstracijos kibernetinio saugumo entuziastams.

Bandė įvairius įsilaužimo būdus

CTF – tai varžybos, kuriose dalyviai sprendžia įvairias užduotis (pvz., išnaudoti pažeidžiamumą, iššifruoti duomenis, analizuoti tinklo srautą), kad „paimtų vėliavą“ – specialų kodą ar žymą. Tokios varžybos padeda mokytis įsilaužimo technikų ir apsaugos metodų.

Renginys buvo nemokamas, o intensyvi vienos dienos stovykla subūrė dalyvius, norinčius tobulinti komandinius ir techninius įgūdžius. Čia buvo galima praktiškai išbandyti sudėtingas CTF užduotis: nuo steganografijos iki tinklo srauto ir atminties analizės, susitikti su Lietuvos komanda, kuri atstovaus šaliai „European Cybersecurity Challenge 2025“, bei apžiūrėti parodą su „lockpick“ rinkiniais, tinklo srauto analizatoriais ir kitais kibernetiniais prietaisais.

Po registracijos ir atidarymo vyko įvadinė interaktyvi paskaita „Kas yra CTF ir kaip sprendžiamos užduotys?“, ekspozicijoje pristatyta paroda „Skaitmeniniai šešėliai: kibernetinių įsilaužėlių įrankiai“, o praktinius komandinius įgūdžius stiprino paskaita–dirbtuvės „Lyderystė ir komandinis darbas“.

Pagrindinėje sesijoje dalyviai sprendė realaus sudėtingumo CTF iššūkius, paraleliai vyko „CyberPlay“ mini dirbtuvės („CTF medžioklė“ ir „Pirmas įsilaužimas: išbandyk įrankį pats“). Popiet – interaktyvios fizinės-loginės užduotys „Hakaton‘as: jėga + logika!“ ir demonstracija „0xDEAD: gyvas nulaužimas“.

Saugioje, kontroliuojamoje aplinkoje dalyviai stebėjo, kaip bandoma įsilaužti bei tikrinamos apsaugos naudojant USBKill, „Flipper Zero“, „HackRF“ ir kitus testavimo įrankius, o taip pat išbandytos „Meshtastic“ tinklų (mesh) galimybės ryšiui be infrastruktūros.

Padeda mokytis atsparumo

Patirčių apsikeitimus papildė fizinės pratimų estafetės – nes kiekvienas „hakeris“ čempioniškos formos neįsivaizduoja be ištvermės ir greitos reakcijos. Norintys galėjo „pasipuošti“ savo įrenginį – specialiai tam įrengtame lipdukų stale laukė dešimtys lipdukų.

Interaktyvioje parodoje dalyviai galėjo praktiškai išbandyti „Flipper Zero“ NFC ir RFID žymų nuskaitymą, 433/868 MHz radijo signalų paiešką, atlikti „HackRF“ spektro analizę, pamatyti USB „Rubber Ducky“ ir „Bash Bunny“ automatizuotus scenarijus, Wi-Fi ir LAN paketų paieškos („snifferių“) darbą, bei išsiųsti žinutes „Meshtastic“ tinkle.

„Mūsų tikslas – išauginti komandą, kuri ne tik greitai sprendžia užduotis, bet ir supranta,

kaip veikia įranga, radijas, tinklai ir žmonės. Tokie įrankiai kaip „HackRF“, „Flipper Zero“ ar USBKill laboratorijoje padeda saugiai mokytis ribų ir atsparumo, o „Meshtastic“ parodo, kaip veikti be įprastos infrastruktūros. CTF – tai praktika, disciplina ir komanda,“ – sako KTU prof. dr. Šarūnas Grigaliūnas, KTU Kibernetinio saugumo kompetencijų centro vadovas.

Laukia tarptautinės varžybos

Pasak renginyje dalyvavusių Nacionalinio kibernetinio saugumo centro (NKSC) atstovų, „Kibernetinis sprintas“ augina ir stiprina Lietuvos kibernetinio saugumo ekosistemą.

„Su partneriais buriame nacionalinę komandą, kuri rudenį stos į „Europos kibernetinio saugumo iššūkį 2025“ – tai tramplinas į prasmingą karjerą jauniems talentams“, – pabrėžė NKSC atstovas Povilas Klėgeris.

Komandinius dalyvių gebėjimus stiprino ir mentorė Indrė Kudrevičė su interaktyvia paskaita „Lyderystė ir komandinis darbas“.

„Tokios stovyklos įgalina veikti: iš čia dalyviai išeina su aiškiu tikslu, atsakomybe ir pirmu laimėjimu. Komandinė drąsa gimsta iš mažų žingsnių, kuriuos darome kartu – šiandien, ne rytoj“, – sakė I. Kudrevičė, tikslų siekiančių žmonių mentorė ir asmeninio augimo programų autorė.

„Kibernetinio sprinto 2025“ stovykla – kibernetinių saugumo kompetencijų ugdymo dalis, kurios metu sujungiamos akademijos, valstybės ir pramonės pajėgos. Tai erdvė, kur Lietuvos CTF rinktinė lavino įgūdžius prieš tarptautines varžybas, o bendruomenė gavo progą praktiškai prisiliesti prie šiuolaikinių saugumo technologijų ir metodikų.

Intensyvi stovykla vyko „DigiDefence“ projekto rėmuose, kurio tikslas – didinti Lietuvos kibernetinį atsparumą, kurti ir diegti inovatyvius kibernetinio saugumo sprendimus bei stiprinti tyrimų ir inovacijų ekosistemą.

Renginį organizavo KTU Kibernetinio saugumo kompetencijų centras ir KTU Informatikos fakulteto Kompiuterių katedra.