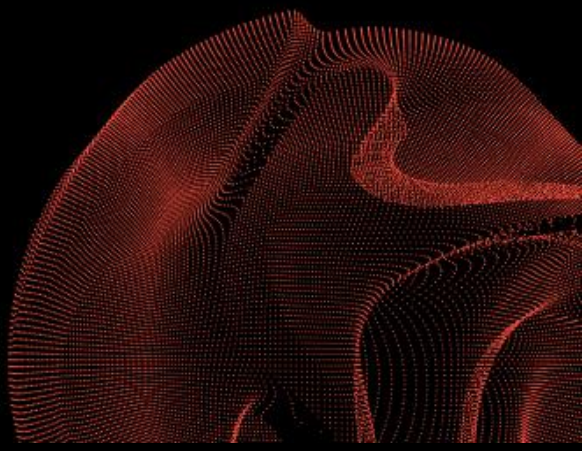
2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



Nacionalinio kibernetinio saugumo (NKSC) prie KAM siūlomos temos:

1. Atvirų šaltinių duomenų analizės įrankis

Atvirų šaltinių analizė – skirta kibernetinių grėsmių žvalgybai ir identifikavimui. Tai yra informacija, kurią naudoja organizacija tam, kad suprastų ir numatytų esamas ir kylančias prieš organizaciją nukreiptas grėsmes. Ši informacija yra naudojama siekiant pasiruošti apsisaugoti, užkirsti kelią ir nustatyti kibernetines grėsmes, kurios galėtų padaryti žalą. Pavyzdžiui: paprasto teksto duomenys internete dalinimuisi yra skelbiami „pastebimi“ tipo tinklalapiuose. Dažnai jie yra naudojami kenkėjiškų programų autorių, turiniui laikyti. Taip pat saugojami „nulaužti“ vartotojų duomenys, kriptovaliutų raktai ir autentifikavimo duomenys bei kita jautri, žalą galinti sukelti informacija.

2. Kibernetinių atakų padarytos žalos apskaičiavimas

Kibernetinis saugumas yra kiekvienos įmonės/įstaigos IT dalis. Dažnai kibernetiniam saugumui neskiriamos lėšos, nes jis negeneruoja“ pelno, tačiau nežinoma, kokią žalą gali padaryti į kibernetiniai incidentai ir kiek kainuoja užtikrinti veiklos tęstinumą. Įvykus incidentui, reikia minimizuoti žalą, atstatyti sistemų veikimą ir atkurti veiklos tęstinumą. Kibernetinės rizikos įskaitant ir atakas yra kaštai, kurias skaičiuoja tiek bankai tiek draudimo kompanijos tiek pačios įmonės. Trūksta įrankių, kurie galėtų padėti įvertinti individualias įmonei kylančias rizikas ir dėl jų prarandamus pinigus. CISO didelėse bendrovėse eskaluoja problemas sukeliamas kibernetinių rizikų, tačiau nėra daug priemonių, kurių pagalba rizikas būtų paaiškinti monetariniais terminais. Užduotis - 2020 m. kibernetinių atakų sukurtos
žalos Lietuvos ūkio sektoriams finansinis įvertinimas.

ORGANIZATORIAI IR PARTNERIAI:

ktu 1922

NORD SECURITY

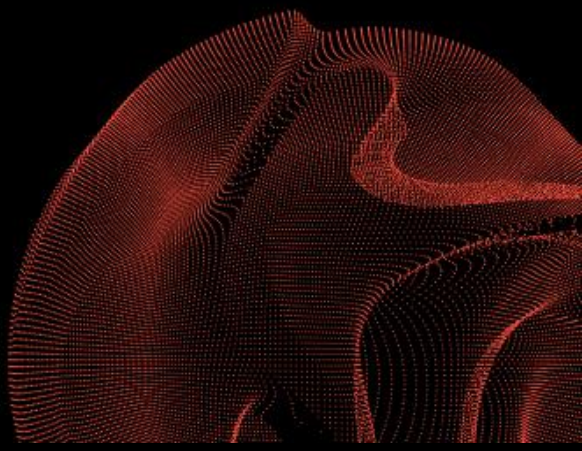
eset CYBERSECURITY EXPERTS ON YOUR SIDE

Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



Nacionalinio kibernetinio saugumo (NKSC) prie KAM siūlomos temos:

3. Turinio valdymo sistemos pažeidžiamumo vertinimas (wordpress, joomla...)

Priešininkai naudoja automatinius įrankius, norėdami nuskaityti interneto tinklalapius, ieškodami saugumo spragų, kad galėtų patekti į interneto serverį. Kai tik randą sprangą turinio valdymo sistemoje, priešininkas gali išnaudoti savo prieigą, kad gautų priėjimą prie autentifikuotų ir privilegijuotų sričių; įkeltų kenkėjiškas programas į interneto serverį, kad palengvintumėte nuotolinę prieigą, įdiegtų kenksmingą turinį į tinklalapius.

4. Socialinės inžinerijos vektoriai

Silpniausia vieta kibernetinio saugumo grandinėje yra žmogus, kurį lengva paveikti naudojantis socialinės inžinerijos metodais. Socialinės inžinerijos metodai naudojami siekiant manipuliuoti žmonių emocijomis ir naudojant psichologinį poveikį priversti naudotojus atlikti potencialiai žalingus veiksmus (paspausti nuorodas, atverti svetaines, parsisiųsti bylas, įgalinti veikti žalingą kodą, pateikti asmens ar prisijungimo duomenis). Socialinė inžinerija turi daug vektorių, kurie gali būti išnaudojami prieš skirtingo tipo organizacijas. Tai apima sukčiavimo el. laiškų naudojimą, , telefono skambučių „fishingą“, „žvejojimą“, atviro kodo žvalgybos duomenų rinkimą ir, žinoma, fizinį prieigą. Sukčiavimo el. laiškai gali būti siunčiami keliems žmonėms arba skirti konkretiems vartotojams "ieties sukčiavimo" atveju. Užduotys: 1. Socialinių Inžinerijos vektorių desaugumizavimas/dekonstravimas atpažinimo įrankiu. 2. Socialinės inžinerijos atakų vektorių, nukreiptų prieš Lietuvos MVĮ, galimybių studija.

ORGANIZATORIAI IR PARTNERIAI:

ktu 1922

NORD SECURITY

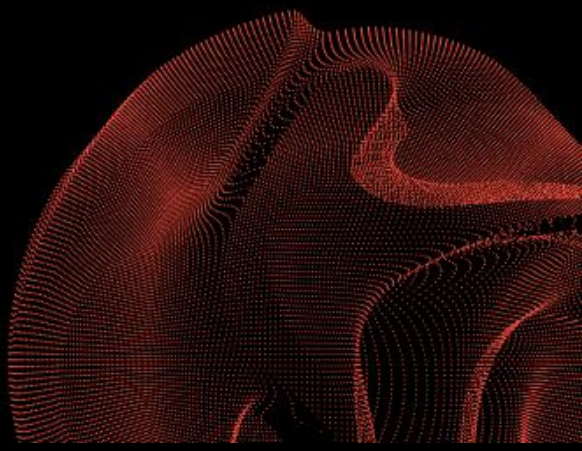
eset CYBERSECURITY EXPERTS ON YOUR SIDE

Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



TV3 kanalų grupės siūlomos temos:

1. Go3 turinio piratų paieška

Saugant Go3 turinio kūrėjus nuo piratų vienas iš kertinių elementų yra atrasti naujus portalus, vietas internete, kur turinys ką tik pradėtas dalintis. Kuo mažesnis atrastas „piratų projektas“, tuo lengviau jį sustabdyti.

Užduotis: Kaip rasti „Piratų projektus“ kol jie dar tik startuoja?

2. Kaip apsaugoti vartotojus, kai jie naudoja vieną prisijungimo duomenų kombinaciją viskam?

Žmonių prisijungimų duomenys patenka į internetą ir piktavaliai pasinaudodami tais duomenimis bando įvairias paslaugas, tame tarpe ir Go3. Ką galima padaryti iš paslaugų teikėjų pusės, kad vartotojai būtų apsaugoti?

Užduotis: Kokie sprendimai išlaikytų balansą tarp 2FA ir problemos ignoravimo?

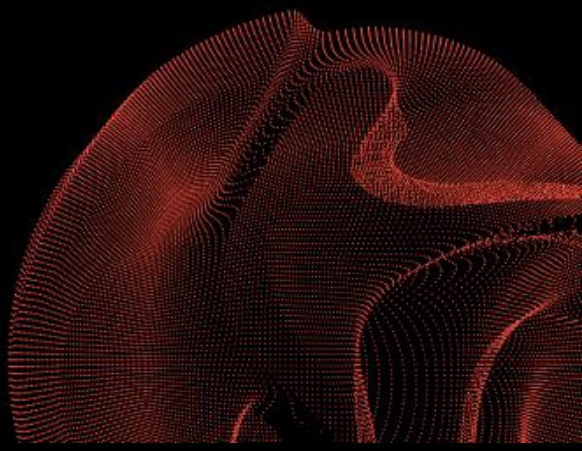
ORGANIZATORIAI IR PARTNERIAI:

ktu 1922 | NORD SECURITY | eset CYBERSECURITY EXPERTS ON YOUR SIDE | Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



NORD SECURITY siūlomos temos:

1. Kibernetinės žvalgybos įrankis pasitelkiant „medaus statinės" (angl. honeypot) metodą

„Medaus statinė" – tai metodas, kai dirbtinai sukuriama saugumo spraga tikintis, kad atakuojanti pusė pasinaudos šiuo pažeidžiamumu. Ši sistema yra paruošiama įsilaužimui taip, kad būtų surinkta kuo daugiau duomenų apie atakuotoją.

2. Algoritmas, kuris atpažįsta duomenų viliojimo internetines svetaines pagal svetainės adresą

Didelė dalis duomenų viliojimo svetainių naudojasi atpažįstamų svetainių adresų pavadinimais kaip patraukliu jauku vartotojams, pvz.: google.com.somesite.lt. Taip sukuriama iliuzija, kad vartotojas jungiasi prie patikimos originalios svetainės. Algoritmas atpažįstantis tokio tipo grėsmes pagal internetinės svetainės adresą užkirstų kelią daliai viliojimo atakų.

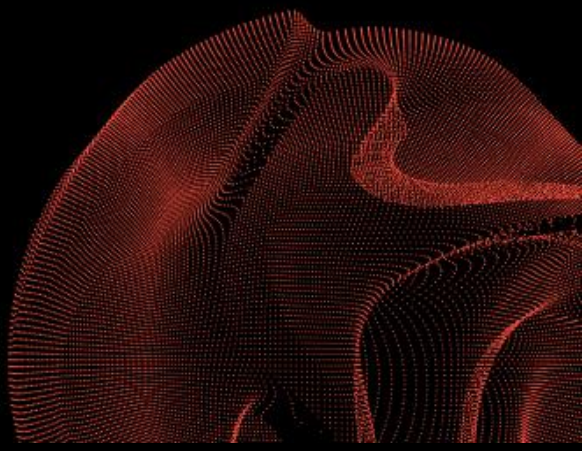
ORGANIZATORIAI IR PARTNERIAI:

ktu 1922 | NORD SECURITY | eset CYBERSECURITY EXPERTS ON YOUR SIDE | Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



LIETUVOS KARIUOMENĖS siūlomos temos:

1. OS paleidimas per bet kokį kompiuterį iš USB laikmenos

Realiuose konfliktuose arba tam tikrose specifinėse situacijose ar specifinių užduočių vykdymo metu dažnai gali nutikti taip, kad nebus galimybės pasinaudoti tarnybinėmis, akredituotomis ar įteisintomis darbo vietomis, dėl ko siekiant maksimaliai užtikrinti duomenų apsaugą būtų galimybė pasinaudoti OS su min. duomenų baze iš USB laikmenų, tai padėtų maksimaliai sumažinti elektroninį pėdsaką, taip pat apsaugo nuo kitokių galimų kibernetinių incidentų, bei palaiko maksimalų efektyvumą vykdant užduotis nestandartinėse situacijose. Reikalingas sprendimas, kuris padėtų paleisti OS per bet kokį kompiuterį (siekiant maksimalių galimybių) tiek su senu UEFI BIOS ar kitais specifiniais BIOS nustatymais, kurie riboją OS paleidimą iš USB laikmenų.

2. Kompleksinis sprendimas saugiam slaptam naršymui internete.

Kadangi Wifi naudojimas yra suprantamas dalykas, todėl mažas nešiojamas Wifi srauto analizatorius gali padėti apsisaugoti nuo išorinių galimų Wifi tinklo atakuotųjų esant už pastovių darbo vietų ribų (pratybos, komandiruotės, užduočių vykdymas ir t.t.). Reikalingas maksimaliai mažas sprendimas su papildomu išorinio maitinimo galimybe (pvz. „PowerBank“). Wifi srauto analizatorius, kuris įspėtų apie kenkėjišką veiklą tinkle, Wifi signalo slopinimus, „Phishing“, „Man in the middle“ ir pan. atakų tipo atvejais. Taip pat turėtų stebėti GPS signalo slopinimą ar klaidinimą, nes Lietuvos kariuomenėje GPS naudojamas įvairiose situacijose ir vietose. Esant galimybei turėtų turėti galimybę atsekti Wifi/GPS slopinimo/trikdymo kryptį, atstumą, o gal net ir vietą priartėjimo būdu pagal signalo stiprumą (kaip variantą).

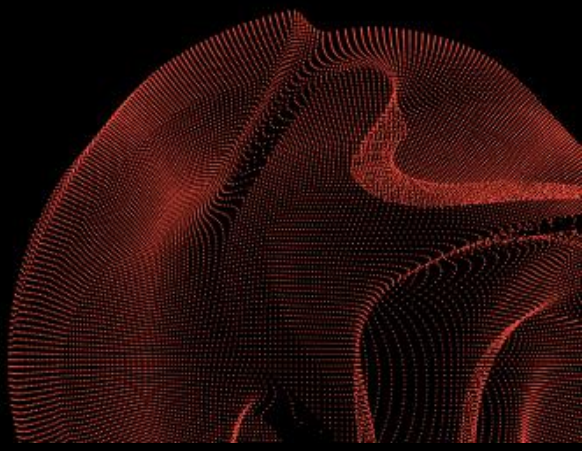
ORGANIZATORIAI IR PARTNERIAI:

ktu 1922 | NORD SECURITY | ESET CYBERSECURITY EXPERTS ON YOUR SIDE | Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



LIETUVOS KARIUOMENĖS siūlomos temos:

3. Kompleksinis sprendimas saugiam slaptam naršymui internete.

Tai turėtų būti vienas iš pagrindinių įrankių tam tikriems specializuotiems vatotojams naršant internetinėse platybėse. Reikalingas sprendimas, kuris maksimaliai apsaugotų minėtus vartotojus nuo galimų kibernetinių atakų bandant identifikuoti konkrečius asmenis, jų buvimo vietą ar kitaip bandyti paveikti jų veiklą ar bandyti nukreipti siekiamus efektus priešinga kryptimi.

4. Saugus apkarpytas Android atvaizdas.

Tam, kad maksimaliai užtikrinti judriojo ryšio saugų naudojimą vykdant įvairias užduotis ar vykstant į komandiruotes tarnybiniais klausimais reikalingi ir maksimaliai saugūs pagrindiniai šiuolaikiniai įrankiai – išmanusis įrenginys. Daugelis šalių pasirenka Android tipo išmaniuosius įrenginius, nes Android OS galima pakoreguoti, kad maksimaliai apsaugotu nuo galimų kibernetinių incidentų. Reikalingas maksimaliai apkarpyto Android OS sprendimas, kuris leistų išnaudoti kertinius Android elementus (programinės įrangos paketus), bet kartu maksimaliai užtikrintų tiek duomenų saugumą bei apsaugą nuo galimų kibernetinių incidentų. Šis atvaizdas neturėtu turėti galimybės lengvam kertinių saugumo nustatymų ir panašių pakitimų pakeitimui. Papildomai ateityje, būtu gerai jog: galima būtu valdyti centralizuotai - tiek pritaikytas taisykles, tiek gal patį įrenginį su apkarpyta Android OS. Taip pat įvykus šios OS pažeidimui, tam tikrų taisyklių apėjimui ar pan. praneštu jog OS nebėra saugus naudojimui.

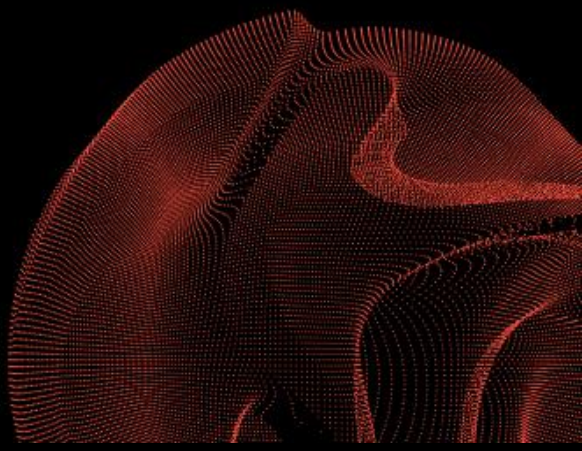
ORGANIZATORIAI IR PARTNERIAI:

ktu 1922 | NORD SECURITY | eset CYBERSECURITY EXPERTS ON YOUR SIDE | Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



LIETUVOS KARIUOMENĖS siūlomos temos:

5. Judriojo ryšio įrangos pažeidžiamumo analizatorius

Šiais laikais ir ateities tendencija yra neapsieinama be išmaniųjų įrenginių. Tačiau išmanieji įrenginiai gali būti nesaugūs naudojimui tiek dėl kenkėjiškai (specialiai) paliktų spragų/nustatymų, tiek šiaip pagal nutylėjimą paliktų spragų, tiek dėl pasenusių dalykų, tiek dėl kitų spragų. Todėl reikalingas įrankis ar sprendimo būdas kuris išanalizuotu šias spragas. Tačiau kalbame ne apie fizinį tam tikro įrenginio prijungimą prie pasiūlyto įrankio, o nuotolinį analizatorių. Kitaip tariant įrankis turėtu iš išorės skanuoti įrenginių WiFi, Bluetooth ir kitus įrenginių signalus ir atlikti raportą apie surinktas spragas.

6. Mini nešiojamas IDS galbūt su IPS su LCD ekraniuku.

Vykdant specifines užduotis ar tam tikros situacijos metu gali reikėti jungtis prie nežinomų, nepatikimų ir visokių skirtingų tinklų. Tokiu atveju reikalingas mažas IDS įrenginys su nedideliu LCD ekranu, kuris praneštu apie tinkle vykdomus kibernetinius išpuolius ir atvaizduotu LCD ekrane jog metas atsitraukti/atsijungti nuo tinklo, nes buvimas prisijungus nebėra saugus. Papildoma IPS funkcija galėtu padėti ne tik apsisaugoti nuo kibernetinių išpuolių, apsaugoti svarbią informaciją tinkle, bet ir padidintu galimybę ilgiau išbūti tinkle. Papildomai apie kibernetinės atakos grėsmę būtu galima atpažinti ne tik iš informacijos apie atakos tipą, laiką, kiekį ir t.t. LCD ekrane, bet ir pagal skirtingų spalvų įspėjimas ar garsiniu signalu.

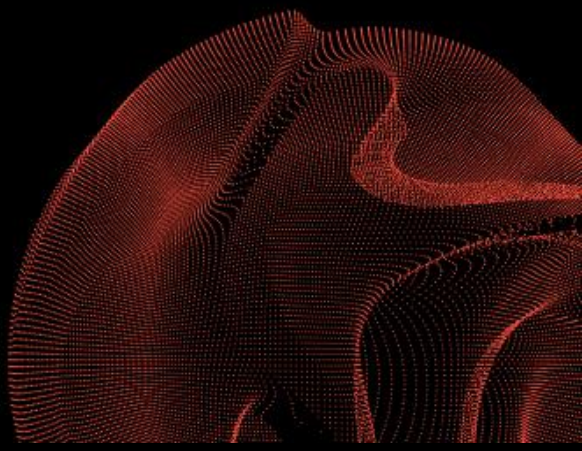
ORGANIZATORIAI IR PARTNERIAI:

ktu 1922 | NORD SECURITY | eset CYBERSECURITY EXPERTS ON YOUR SIDE | Go3

2021 11 12-14

KIBERNETINIO SAUGUMO HAKATONAS

DELTA1



LIETUVOS KARIUOMENĖS siūlomos temos:

7. END mygtukas

Užduočių vykdymo metu gali pasitaikyti atvejų, kai per trumpą laiką gali tekti sunaikinti arba paslėpti jautrią informaciją turimuose išmaniuosiuose įrenginiuose, kad vėliau jos nebūtų galima kibernetiniais arba tardymo (papuolus į nelaisvę) metodais ištraukti. Dėl to reikalingas sprendimas su itin greitu ir maksimaliai ar net „neįmanomu“ užšifravimo būdu. taip vadinamu „END“ arba „KILL“ mygtuku, kurį paspaudus viskas sudėtingai užsišifruotų arba būtų “neįmanoma” atšifruoti jautrios informacijos esančios įrenginyje, nes visokie bandymai informaciją ištrinti arba bandymai sunaikinti įrenginį užtrunka laiko ir dažniausiai būna nesėkmingi.

ORGANIZATORIAI IR PARTNERIAI:

ktu 1922

NORD SECURITY

eset CYBERSECURITY EXPERTS ON YOUR SIDE

Go3