Mis on sõnastikrünne (*dictionary attack*)?

Sõnastikrünnet kasutatakse parooliga kaitstud süsteemidesse sissemurdmiseks. Häkker katsetab järjekindlalt kõikvõimalikke sõnu, mis võiksid paroolis sisalduda, nagu nimed, kohad vms. „Sõnastik“ viitab ründajale, kes proovib parooli teadasaamiseks ära kõik sõnad sõnastikus.

Tavaliselt tehakse sõnastikrünnet tarkvaraliselt, mitte iga parooli käsitsi katsetades.

Milleks kasutatakse krüptograafias soola (*salt*)?

Krüptograafias nimetatakse soolaks juhuslikke andmeid, mida kasutatakse paroolide räsimisel täiendava sisendina. Peamiselt pakub sool kaitset sõnastikrünnete vastu, mille puhul võrreldakse paroole sõnade räsidega ja rünnakute puhul, milles kasutatakse eelnevalt valmisarvutatud „vikerkaaretabeleid“. Näiteks kasutajakontot luues ja salasõna sisestades, lisab süsteem automaatselt „soola“, et parool ei meenutaks äratuntavaid sõnu.

Mis on parooli räsimine (*password hashing*)?

Parooli räsimisel võetakse avatekst ja kohaldatakse sellele algoritmi, et saada täiesti teistsugune väärtus. See väärtus on alati samasugune, seetõttu võib parooliräsi hoida andmebaasis ja kontrollida kasutaja sisestatud parooli vastu räsi. Räsimisel on mõistlik kasutada „soola“ – veidi lisaandmeid, mis muudavad räsid tunduvalt raskemini murtavaks.

Räsifunktsioonid on näiteks md5, SHA-1, SHA-256, GOST, HAVAL.

hacking

Kuidas töötab jõurünne (*brute force attack*)?

Jõurünne on katse ja eksituse meetodil toimepandav rünne info hankimiseks, näiteks parooli äraarvamiseks. Jõurünne põhineb pigem „toorel jõul“ kui intellektuaalsel strateegial. Jõuründes kasutatakse automatiseeritud tarkvara, millega luuakse suur arv järjestikusi oletusi ihaldatud andmete väärtuse kohta. Progeja loodab arvuti võimsusele ja katsetab kõikvõimalikke kombinatsioone alustades „a, b, c…, aa, ab, ac…, aaa…“ jne.

hacking

Mida ütleb Moore’i seadus (*Moore’s Law*)?

Inteli kaasasutaja Gordon E. Moore pani 1965. a tähele, et mikrokiibil olevate transistorite arv kahekordistub iga kahe aasta järel. Moore’i seaduse järgi see trend jätkub ka tulevikus.

Praegu kulub tavalisel personaalarvutil parooli ”Safety4me” lahtimurdmiseks ligikaudu 39 päeva.

hacking

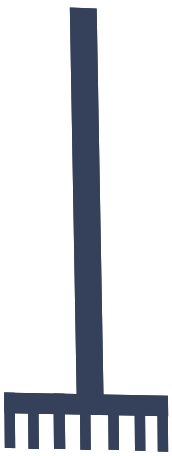
Kirjelda head parooli (*password*) ja nimeta kolm nõrka sageli kasutatavat parooli (salasõna)

Tugev parool on raskesti äraarvatav nii inimesele kui ka arvutiprogrammidele. Tugev parool koosneb vähemalt 14 tähemärgist ning sisaldab nii suur- kui ka väiketähti, numbreid ja sümboleid. Tugev parool ei sisalda sõnu, mida võib leida sõnastikust, kasutaja nime, sünnikuupäeva, aadressi vms. Tihti kasutatavad nõrgad paroolid inglise keele kõnelejate hulgas on näiteks: 123456, password, qwerty, abc123, 111111, iloveyou, adobe123, 123123, Admin, letmein, photoshop, trustno1, 000000.

hacking

Mis on *card skimming* ja *skimmer*?

Card skimming tähendab pangakaardi magnetribal olevast infost illegaalse koopia tegemist, kasutades võlts-kaardilugejaid (*skimmer*) ja klahvistiku katteid või peidetud videokaameraid kaardi PIN-koodi salvestamiseks. Varastatud andmete abil üritavad petturid ohvri pangakontot kasutada.



hacking

Milleks kasutatakse vikerkaare-tabeleid (*rainbow tables*)?

Vikerkaaretabel on eelnevalt valmisarvutatud tabel krüptograafiliste räsifunktsioonide ümberpööramiseks, tavaliselt parooliräside murdmiseks. Tabeleid kasutatakse eelkõige avatekstiparoolide taastamiseks (kuni teatud pikkusega, koosnedes piiratud hulgast tähemärkidest).

Näited:

a - 0cc175b9c0f1b6a831c399e269772661
b - 92eb5ff ee6ae2fec3ad71c777531578f
c - 4a8a08f09d37b73795649038408b5f33
A - 7fc56270e7a70fa81a5935b72eacbe29

Millist tundlikku infot võib peale jäädvustatud kujutise fotost leida?

Metaandmed:

EXIF info (*Exchangeable image file format*), väike ülevaade fotost, mis säilib isegi pärast lõikamist;

Asukohaandmed (GPS koordinaadid);

Näotuvastus;

Objektituvastus (nt autonumber);

Kaamera tootja ja mudel;
Kuupäev ja kellaaeg.

Kuidas erinevad HTTP ja HTTPS?

HTTP-d (*Hypertext Transfer Protocol*) kasutab WWW (*World Wide Web*). HTTP määratleb, kuidas sõnumeid edastatakse ning milliseid toiminguid peaksid veebiserverid ja veebisirvikud tegema. Näide: URL-i sisestamisel veebisirvikusse saadetakse veebiserverile soovitud veebilehe esiletoomiseks HTTP käsklus. **HTTPS** (*HTTP Secure*) muudab häkkeritele kasutajate jälitamise keerulisemaks, luues krüptitud kanali läbi ebaturvalise võrgu. HTTPS tagab, et andmeid ei edastata avatekstina, mis on palju lihtsamini pealtkuulatav.

Mis on ummistusrünne (*DDoS*)?

Ummistusründes ehk teenusetõkestuses (*Distributed-Denial-of-Service*) osaleb tavaliselt palju arvuteid, mis on kas nakatunud (*botnet*'i osa) või milles on protokollid vigaselt rakendatud, s.o kuritarvitatavad. Ründe sihtmärgiks olev server suudab töödelda vaid teatud arvu päringuid korraga, seega koormab häkker serveri üle. Teenusetõkestuseks nimetatakse ummistusrünnet seetõttu, et samal ajal ei ole võimalik serveri pakutavaid teenuseid kasutada.

internet

Mis on robotilõks (*CAPTCHA*)?

CAPTCHA on lühend, mis võtab kokku „Completely Automated Public Turing test to tell Computers and Humans Apart“. Robotilõks on küsimus-vastus-tüüpi test, mida kasutatakse internetis, et kindlaks teha, kas kasutaja on inimene või mitte.

Robotilõksu kasutamine vormide edastamisel vähendab märgatavalt rämpspostitusi veebilehel.

digital safety

internet

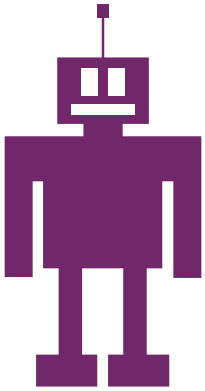
What is cyberbullying? Give an example.

Cyberbullying is bullying that takes place using electronic technology such as cell phones, computers, and tablets as well as communication tools as social media sites, text messages, chat, and websites. Examples of cyberbullying include mean text messages or e-mails, rumours sent by e-mail or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profi les.

internet

Mis on *bot*?

Bot (lühend robotist) on programm, mis automatiseerib või jäljendab inimtegevust internetis. Veebibot on tarkvararakendus, mis jooksutab automaatseid toiminguid üle interneti. Enamasti kasutatakse *bot*-e veebilehtede indekseerimiseks. Vestlusbot võib suhelda kasutajatega, mängubot'id automatiseerivad korduvaid ülesandeid. Mängubot'ide kasutamist peetakse pettuseks (*cheating*).



What does ISP stand for?

An ISP (Internet Service Provider), is a company that provides its customers access to the internet and other web services. ISPs can vary in size - some are operated by one individual, while others are large corporations. They may also vary in scope - some only support users in a particular city, while others have regional or national capabilities.

internet

I will choose and ask you to name two of the following chat acronyms.

AFK	Away from keyboard
AKA	Also known as
BB	Bye bye
BRB	Be right back
CYA	See you!
K	Okay
GG	Good game
IRL	In real life
LOL	Laughing out loud
NP	No problem
OMG	Oh my god
RTFM	Read the f****g manual
TY	Thank you
WB	Welcome back
WTF	What the f***

Mis on URL ja mida see teeb?

URL (*Uniform Resource Locator*) on veebisirvikus kuvatav internetilehe või -faili aadress. Koos domeeninimedega aitab URL nimetada ja leida veebilehti ilma IP-aadressi meelespidamise ja sisestamiseta.

I will choose and ask you to name one of the following worldwide Internet usage fact. (+/-5%)

Note that current world population is 7.3 billion.

How many..

..people are using the Internet? (39%)

..websites content is in English? (55%)

..users use Internet in English language? (27%)

.. adult cell owners use their phones to go online? (63%).

internet

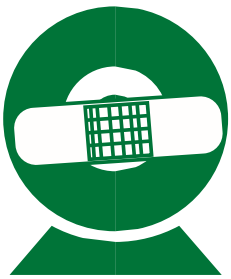
Mis on *botnet*?

Kurjategijad levitavad pahavara, mis võib arvuti muuta *bot*'iks ehk zombiks. *Botnet* on robotvõrk, mis koosneb nakatunud arvutitest, mida kasutatakse omaniku teadmata näiteks rämpsposti saatmiseks, viiruste levitamiseks ja serverite ründamiseks. *Botnet*'i osaks olev arvuti võib muutuda aeglaseks.

malware

Mis on nuhkvara (*spyware*)?

Nuhkvara on tarkvara, mis aitab koguda ja edastada infot ilma arvutikasutaja teadmata. Enamasti liigitatakse nuhkvara järgmiselt: süsteemiseirajad, troojad, reklaamvara ja jälitusküpsised. Nuhkvara olemasolu kasutaja tüüpiliselt ei märka ja seda on keeruline avastada. Nuhkvara võib koguda kasutaja sisselogimisandmeid ja pangainfot. Nuhkvara võib paigaldada täiendavat tarkvara, veebisirvikuid ümber suunata või muuta arvuti seadeid. Nuhkvara võib arvutisse sattuda pahaloomuliselt veebilehelt. Mõnikord tuleb nuhkvara kaasa autentse tarkvaraga.



malware

Mis on klahvikuulaja (*keylogger)*?

Tark- ja riistvaralisi klahvikuulajaid kasutatakse klahvivajutuste (sh paroolide) kinnipüüdmiseks ja salvestamiseks. Tarkvaraline klahvikuulaja on paigaldatud ja peidetud arvutisse. Riistvaraline klahvikuulaja võidakse rakendada BIOSi tasemel või klaviatuuri ja arvuti vahele ühendatud seadme abil. Klahvikuulajad võivad automaatselt andmeid üle interneti klahvikuulaja „peremehele“ saata.

malware

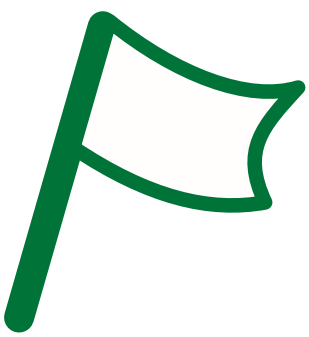
Mis on nullpäeva-rünne (*zero-day exploit*)?

Nullpäeva-rünnet kasutatakse senitundmatu ja veel lappimata turvaaugu ärakasutamiseks. Sellist rünnet nimetatakse nullpäeva-ründeks, kuna progejal on olnud nö null päeva aega olnud vea parandamiseks. Nullpäeva-nõrkuste müük auklike toodete arendajatele või valitsusasutustele on üsna tavaline.

malware

Mis on lunavara (*ransomware*)?

Lunavara on pahavara, mis piirab nakatunud arvutile (andmetele) ligipääsu ning nõuab piirangute eemaldamise eest pahavara loojatele lunaraha. Mõned lunavara vormid krüptivad arvuti kõvakettal olevad failid, kui teised lihtsalt lukustavad süsteemi ning kuvavad sõnumeid, mis peaks kasutajaid maksma meelitama.



malware

Mis on tagauks (*backdoor*)?

Tagauks on vahend arvuti-programmile juurdepääsuks turva-mehhanismidest mööda minnes. Vahel võib progeja paigaldada tagaukse, et programmile probleemide kõrvaldamiseks või muul põhjusel ligi pääseda. Seevastu ründajad kasutavad iseavastatud või -paigaldatud tagauksi mõne nõrkuse ärakasutamiseks ning andmetele volitamata ligipääsuks.

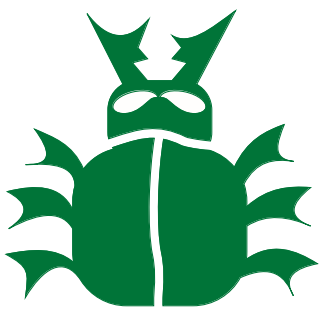
404
.

malware

Mis on pahavara (*malware*)?

Pahavara on üldtermin, mis hõlmab erinevaid vaenuliku tarkvara vorme, sh arvutiviirused, võrguussid, troojad, lunavara, nuhkvara, reklaamvara, hirmutamisvara jne.

Pahavara kasutatakse arvuti tegevuse katkestamiseks, tundliku info kogumiseks või ligipääsu saamiseks arvutile / infosüsteemile. Näiteks võlts-viirusetõrje on info varguseks loodud pahavara, mis matkib päris-turvatarkvara. Kuna võlts-viirusetõrje teeb arvutis muudatusi, on selle eemaldamine keeruline.



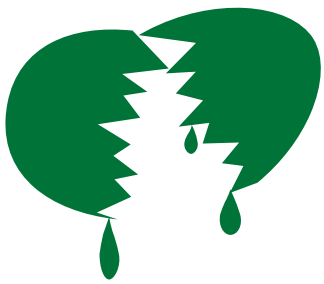
malware

Mis on laadung (*payload*)?

Laadungiks kutsutakse pahaloomulise koodi osa, mis mõjub mingil moel kahjustavalt.

Pahavara, nagu võrguussid, viirused ja troojad, analüüsi korral viitab „laadung“ pahavara kuritahtlikele omadustele. Kuigi mitte kõik viirused ei kanna laadungit, peetakse mõnda neist eriti ohtlikuks.

Laadungi näiteid: andmete hävitamine, solvavad sõnumid, spämmi saatmine nakatatud arvutist.



malware

Kirjelda juurkratti e käomuna (*rootkit*)

Juurkratt on tippklassi pahavara, mis on kavandatud teatud protsesse või programme tavapäraste tuvastus-meetodite eest peitma ja võimaldama jätkuvat privilegeeritud ligipääsu süsteemile. Tegemist on trooja-tüüpi programmiga, mis peidab tõendeid ründaja tegevusest, jäädes ise varjatuks ning luues ründajate jaoks kaugligipääsu süsteemidele tagaukse kaudu. Juurkratt asendab normaalsed programmid ja süsteemiteegid enda omadega.

malware

I will choose and ask you to describe one of the following Wi-Fi glossary terms.

AP (Access Point) - A device that acts as the bridge between wireless clients and the network.

Captive Portal - AP can interc ept clients who must agree to terms of service.

WPA2 (Wi-Fi Protected Access v2) - is currently the strongest encryption protocol available to wireless networks.

WPS (Wi-Fi Protected Setup) - makes it easier for users to add WiFi clients to wireless networks. It is vulnerable to a brute-force attack and should be disabled.

network

Mis on IP-address? Too näide

IP (*Internet Protocol*) aadress on nelja- või kaheksaosaline elektrooniline seerianumber. IP-aadress võib esineda näiteks kujul 193.40.56.90 (IPv4) või ’2001:7d03:8240:b201:8d73:3604:38b9:2e40’ (IPv6). Iga arvuti, telefon või muu seade, mis ühendub internetiga, saab identifitseerimise eesmärgil endale IP-aadressi. See tähendab, et iga toiming internetis on seostatav selle toimingu taga oleva seadmega / kasutajaga.

127.0.0.1 sweet
127.0.0.1

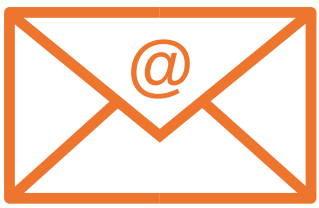
network

Name the three protocols that are used to deliver and receive e-mail.

IMAP (Internet Message Access Protocol) - e-mail is received and held for you by your Internet server. As this requires only a small data transfer.

POP3 (Post Offi ce Protocol 3) - all your e-mail messages will be downloaded from the mail server to your local computer.

SMTP (Simple Mail Transfer Protocol) protocol is used to deliver your e-mail to the recipient's mail server. The SMTP protocol can only be used to send e-mails, not to receive them.



What is NFC

(Near Field Communication) and how can it be used?

Technology used most often with mobile devices to exchange data based on proximity contact. NFC technology is being built into mobile phones for data transfer, touch to pay technolog ies, and smartcard reading.

What is the FTP (File Transfer Protocol) used for? Name one FTP client application.

The File Transfer Protocol (FTP) software is used to receive or send fi les from one computer to another. FTP is built on a client-server architecture. FTP connection can be anonymous but is commonly account based. Popular FTP Client progams are Cyberduck, FileZilla, FireFTP, Smart-FTP, Windows FTP, WinSCP, WS_FTP

What is P2P (Peer-to-peer) fi le sharing?

P2P is a decentralized communi-cations model in which each party has the same capabilities and either party can initiate a communication session. P2P fi le sharing allows users to access media fi les music, movies, and games using a P2P software program that searches for other connected computers on a P2P network. Example of these programs are Torrent clients, Kazaa, Emule, Soulseek.

network

Mis on DNS kaaperdamine (*DNS hijacking*)?

DNS (*Domain Name System / Service / Server*) kaaperdamise korral muudetakse arvuti DNS seadeid kas arvuti ümbersuunamisega liba-DNS serverile või usaldusväärse DNS serveri käitumist modifitseerides nii, et tulemus võib olla veebilehel reklaamide asendamine, hasartmängusaitide blokkimine vms. Selliseid muudatusi võidakse teha pahatahtlikult, näiteks õngitsemiseks või tsenseerimiseks ja jälgimiseks.

network

What is the utility ping used for?

Ping is a computer network utility used to test the reachability of a computer on an network. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an response. In the process it measures the time from transmission to reception and records any packet loss.

network

I will choose and ask you to name one service for one of the these ports.

21 File Transfer Protocol (FTP)

22 Secure Shell (SSH) service

23 Telnet

25 Simple Mail Transfer Protocol (SMTP)

53 Domain Name System (DNS)

80 Webserver, Hypertext Transfer Protocol (HTTP)

443 Secure Hypertext Transfer Protocol (HTTPS)

993 Mail IMAP SSL

network

Mida teeb küpsis (*cookie*)?

Küpsis on väike tekstifail, mis paigaldatakse veebilehe külastamisel kasutaja arvutisse. Küpsist kasutatakse veebilehe külastaja „mäletamiseks“ järgmistel kordadel, eelistuste salvestamiseks või veebilehitsemise jälgimiseks. Küpsised lihtsustavad veebiostlemist, saitide isikupärastamist ja suunatud reklaami. Küpsised ei ole tarkvara, ei saa lugeda andmeid arvuti kõvakettalt ega arvutit kahjustada. Jälgimisküpsised ei ole pahaloomulised nagu pahavara, võrguussid või viirused, kuid võivad osutuda privaatsusprobleemiks.

privacy

Describe the difference between dark internet and darknet.

A dark Internet refers network hosts on the Internet that no-one can reach. According to some estimates, only 0,03% of the web is searchable, hence leaving 99,97% of all data being dark Internet. The data on the dark Internet is generally harmless in nature, being kept off the internet simply because it is data which most people won't need or search for anyway. Deep web or darknet is distributed fi lesharing, which refer to hard-to-find websites and secretive networks that span the Internet.

privacy

What is a BCC (blind carbon copy)? Name some reasons for using it.

BCC allows you to hide recipients in e-mail messages. There are a few main reasons for using BCC:

Privacy - If sending e-mail on behalf of an organization, it is important to keep lists of clients confi dential.

Tracking - you want to make someone, such as a supervisor or team member, aware of the e-mail.

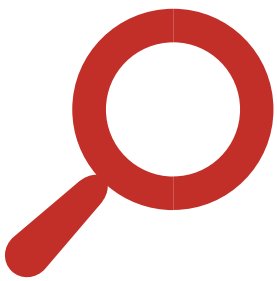
Respect for your recipients - People often forward e-mail without removing the addresses of previous recipients. Spammers may collect and target those addresses.

~~Tallinn~~
~~ESTONIA~~

privacy

What is FinFisher (aka FinSpy) and who uses it?

FinFisher or FinSpy is a piece of computer spyware designed to allow law enforcement to spy on a computer or mobile phone. FinFisher malware is installed in various ways, including fake software updates, e-mails with fake attachments, and security fl aws in popular software. FinSpy backdoors have been found in a total of 25 countries. Including Australia, Canada, Czech Republic, Estonia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Netherlands, Serbia, Singapore, United Kingdom, United States.

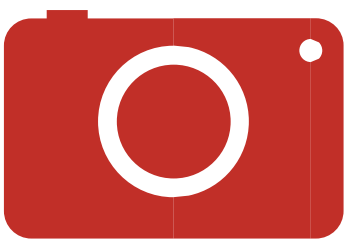


privacy

What steps can you take to avoid having compromising photos of you published online?

Do not take pictures of yourself in any compromising position. Don't get photographed in compromising positions when partying. Do not post, send or upload intimate pictures onto any website.

Always try to imagine your loved ones or employers viewing this ima ge. If someone takes a private picture of you ask them to delete it. Friend ships relationships are not always forever. Disgruntled friends are often posting undesirable images.

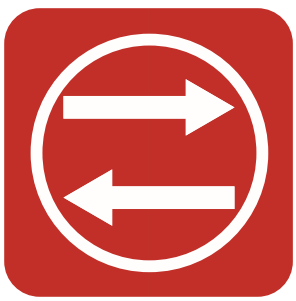


How does identity theft happen?

Someone pretends to be someone else by assuming that person's identity, to gain access to resources in that person's name. The victim of identity theft can suff er consequences if they are held responsible for the perpetrator's actions. Criminal may be able to impersonate you to purchase items, open new accounts, or apply for loans. Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available.

What is a proxy server?

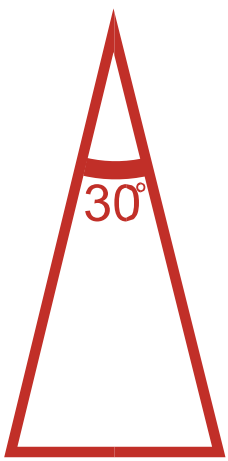
A proxy server is a computer that off ers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a resource available on a diff erent server. The proxy provides the resource either by connecting to the specifi ed server or by serving it from a cache. Today, most proxies are web proxies, facilitating access to Internet and providing anonymity.



privacy

What is the PRISM (a surveillance program)?

PRISM is a electronic surveillance data mining program known to have been operated by the United States National Security Agency (NSA) since 2007. Its existence leaked by NSA contractor Edward Snowden. The Prism program collects stored Internet communications based on demands made to Internet companies such as Google Inc. It's predecessor was ECHELON at Menwith Hill.

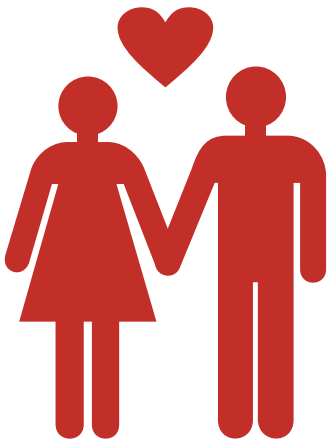


privacy

What is sexting and why is it dangerous?

Sexting (sex and texting) is the act of sending sexually explicit messages or photographs, usually between mobile phones.

Social danger with sexting is that material can be very easily and widely propagated, over which the originator has no control therefore sexting can ruin one's reputation.



privacy

Mis on suhtlus- ehk manipu-leerimisrünne (*social engineering*)?

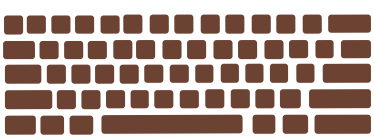
Suhtlusrünnet iseloomustab inimese usaldava loomuse osav käsitsemine. Häkker kasutab teesklust, valesid vm veenvaid nippe, et saada ohver (tihti heauskselt) salajast teavet avaldama. Väljapetetud andmeid kasutades tungib häkker oma tehniliste teadmiste abil organisatsiooni infosüsteemi ning pääseb ligi organisatsiooni infovaradele.

social engineering

Mis on kirjavearünne (*typosquatting*)? Too näide

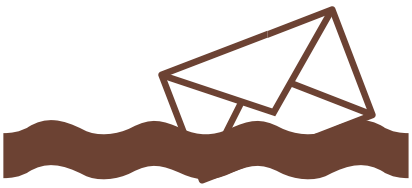
Kirjavearünne, mida nimetatakse ka URL kaaperdamiseks (URL *hijacking*), põhineb interneti-kasutajate eksimustel veebi-sirvikusse aadressi sisestamisel. Kui kasutaja sisestab juhuslikult vigase aadressi, võidakse ta suunata võlts-URL-le, kus halvemal juhul serveeritakse ohtlikku sisu, nagu pahavara, õngitsusvormid jms.

Näiteid: evnir.ee, tallin.ee.



Mis on rämpspost (*spam*)? Kirjelda tüüpilise rämpskirja sisu.

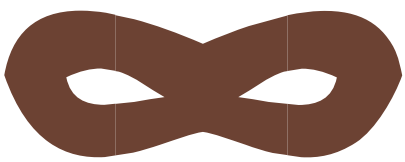
Rämpspost e spämm tähendab soovimatuid, pealesunnitud e-kirju, mida tavaliselt saadetakse paljudele juhuslikele saajatele, kes selliseid kirju muidu ei saaks. Enamiku spämmist moodustab reklaam; spämm on tihti seotud kahtlaste toodete, rikastumisskeemide, liba-teenuste või andmeõngitsustega. Rämpsposti hulka saab vähendada meilifiltreerimise tarkvara kasutades. Üks meetod, millega meelitatakse inimesi kirju avama, on e-kirja saatja võltsimine – näiteks jäetakse mulje, et kirja on saatnud kirja saaja ise või tuntud teenusepakkuja.



social engineering

Mis on *pretexting*?

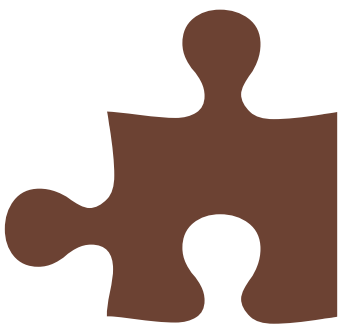
Pretexting'ut kasutatakse sihtmärgiks valitud isiku kolleegi, politsei, IT kasutajatoe või muu autoriteetse isikuna esinemiseks. Sageli piisab selleks vaid usaldustäratavast häälest. *Quid pro quo* meetodi puhul helistab ründaja juhuslikele numbritele organisatsioonis, väites, et ta helistab tehnilisest toest vm. Ründaja „aitab" lahendada probleemi, jõudes lõpuks kellenigi, kel on tõesti mure. „Aidates" juhendab ründaja arvutisse käske sisestama, mis annavad ründajale ligipääsu või käivitavad pahavara.



social engineering

Describe how XSS (Cross-Site Scripting) works.

Attacker exploits a vulnerability in a website that the victim visits by injecting a client-side script that executes malicious JavaScript in another user's browser. As an example attacker inserts javascript in a comments box that redirects to malicious website.



social engineering

Mis on peibutusrünne (*baiting*)?

Peibutusrünne on nagu trooja, mis kasutab füüsilist andmekandjat ja tugineb ohvri uudishimule või ahnusele. Näiteks jätab ründaja pahavaraga nakatatud mälupulga asukohta, kus see kindlasti leitakse. Ühendades mälupulga selle sisu nägemiseks arvuti külge, paigaldab kasutaja teadmatult oma arvutisse pahavara.

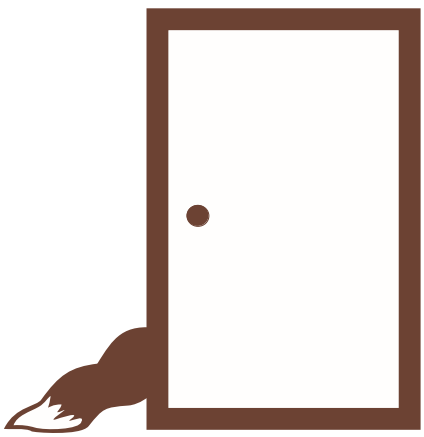
Mis on prügisukeldumine (*dumpster diving*)?

Prügisukeldumine on äri- või eraprügi sõelumine, et leida nt salasõnu, võrguinfot vms teavet, mis on jõudnud prügikasti, kuid võib osutuda kasulikuks. Prügisukeldumine on mõjus ühiskonnas valitsevate tabude tõttu. Prügil on halb „maine“ ning äravisatud kraam unustatakse kiiresti. Samas tekitavad prügikollid ebameeldivaid tundeid, seega vaadatakse neist mööda. Tasub meeles pidada, et pole olemas murdmatut lukku.

social engineering

Kuidas töötab sappahaakimine (*tailgating*)?

Turvavaldkonnas viitab sappa-haakimine, mida nimetatakse ka turjaltassimiseks (piggybacking), olukorrale, mil keegi siseneb õigustatud isiku kannul ligipääsu-piirangutega alale - lipsates näiteks kellegi järel läbi ukse või ühinedes suurema rahvahulgaga. Seda rünnet peetakse üheks lihtsamaks manipulatsioonründe vormiks.



social engineering

Kuidas kasutatakse õngitsust (*phishing*)?

Õngitsus ehk kalastamine on katse omandada tundlikku infot, nagu salasõnad ja krediitkaardiandmed, teeseldes usaldusväärset e-kirja või veebilehte.

Tavaliselt kasutatakse seda trikki e-kirjas, mis oleks justkui saabunud päris-ettevõttelt. Sõnumis on tihti kasutatud ettevõtte veebilehe kujunduselemente. Kirjas püütakse kasutajat veenda, et ta peaks kinnitama oma andmed, sisestades need uuesti.

social engineering

TALLINN UNIVERSITY

Digital Safety Lab