Praktikum 3

PAIGALDUSJÄRGNE SEADISTUS

Paigaldusjärgne kontroll

- Tee ära tarkvarauuendused
- Kontrolli üle, et masinas oleks töötava antiviirus ning sisselülitatud tulemüür
- Kontrolli, et masinas oleks olemas vajalikud riistvaradraiverid
- Vaata üle kasutajaliides
- Vaata üle võimalused, kuidas teha kindlaks, milline on masina riistvaraprofiil ja milline tarkvara on juba paigaldatud.

Windows Update

Settings -> Windows update

Settings -> Delivery optimization

Trikk Windows update peatamiseks:

- Settings -> Network status -> change connection properties –> set as metered connection

Windowsi pakihaldur Chocolatey

Paigaldame PowerShell 7

- https://github.com/PowerShell/PowerShell/releases/tag/v7.1.1

Käivitame PowerShell 7 administraatorina

- Run as Administrator

Paigaldame pakihalduri

- https://chocolatey.org/install

Soovi korral paigaldame pakihaldurile graafilise kasutajaliidese

- Choco install chocolateygui

Tulemüürist

Tulemüür (inglise **Firewall**) on tarkvara või seade, mis turvakaalutlustel piirab ja reguleerib võrguliiklust arvutivõrgus või võrkude vahel vastavalt seadistatud reeglitele. Tavaliselt kasutatakse tulemüüri interneti ja kohaliku kohtvõrgu vahel. Tulemüüri esmane otstarve on väljastpoolt juurdepääsu takistamine ressurssidele, millele pole sellist juurdepääsu ette nähtud. On ka tulemüüre mis piiravad väljuvat liiklust.

https://et.wikipedia.org/wiki/Tulemüür_(informaatika)

Viirusetõrjetarkvara

Viirustõrjetarkvara on tarkvara, mille eesmärgiks on avastada ja elimineerida arvutiviiruseid. Lihtsamad viirustõrjetarkvarad töötavad kasutades tuntud arvutiviiruste definitsioone, mille alusel otsitakse neid viirusi arvutisüsteemi mälust ja salvestatud failidest.

Keerulisemad viirustõrjetarkvarad võivad sisaldada heuristikafunktsioone, mis üritavad tuvastada arvutiviirusi teatud käitumismustrite alusel.

Lisaks võivad viirusetõrjetarkvarad sisaldada lisafunktsioone nagu:

- Ründavat koodi sisaldavate veebilehtede blokeerimine
- Lisaks viirustele ka muu pahavara tuvastamine

Hea viirusetõrjetarkvara

Miks mõni viirusetõrjetarkvara on parem kui teine:

- Pidev viiruste definitsioonide andmebaasi uuendamine
- Võimalikult väike süsteemiressursside kasutus
- Selge ja arusaadav kasutajaliides
- Kasutaja piisav (kuid mitte ülemäärane) teavitamine

NB! Viirused ja pahavara ei ole ainult Windows operatsioonisüsteemide probleem

- https://en.wikipedia.org/wiki/Linux_malware#Viruses
- http://www.welivesecurity.com/2014/03/21/10-years-of-mac-os-x-malware/

Arvutiviirused

Arvutiviirus - Pahatahtliku häkkeri kirjutatud programmijupike, mis on lülitatud mingi normaalse programmi koosseisu ning põhjustab ootamatuid ja sageli kasutajale äärmiselt ebameeldivaid tagajärgi.

vallaste.ee

Arvutiviirus on oma nime saanud omaduse järgi iseseisvalt levida meenutades seejuures bioloogilist viirust. Tegemist on ennast paljundava koodiga.

Esimesed viirused polnud otseselt hävitava iseloomuga tegemist oli akadeemiliste katsetustega.

Troojalased ja juurkomplektid

Trooja hobune - Kasuliku programmi või andmete sisse manustatud kahjulik programmiosa, mis täidab tegelikult mingit varjatud ülesannet, näiteks muudab teatud tingimustel andmeid, rikub kõvakettal failipaigutustabeli (FAT) või teeb arvutis muud kurja. Trooja hobust nimetatakse vahel ka arvutiviiruseks, kui see laialt levib, kuigi erinevalt viirusest see ise ennast ei paljunda. Enamasti kasutatakse terminit "Trooja hobune" siiski ainult nende kuritahtlike programmide kohta, mis ise ei paljune ning isepaljunevaid programme nimetatakse viirusteks.

vallaste.ee

Juurkomplekt (rootkit) - teatud tüüpi Trooja hobune, mis hoiab iseennast ning oma tegevuseks vajalikku failidest, registrivõtmetest ja võrguühendustest koosnevat komplekti peidetuna, nii et arvutikasutajal on võimatu avastada selle olemasolu ja tegutsemist oma arvutis. Et selline jälgede peitmine oleks võimalik, peab Trooja hobune looma endale juurkasutaja õigused.

vallaste.ee

Nuhkvara

Nuhkvara - nuhkvaraks nimetatakse faile, mis installeeritakse teie arvutisse ilma teie teadmata ja mis võimaldavad salaja jälgida teie arvutikasutamist. On palju erinevaid nuhkvara liike: klahvivajutuste registreerijad ja paroolivargad, teie poolt külastatavate veebisaitide ja kasutatavate programmide logerid, e-posti jälgijad ja ümbersuunajad jne.

vallaste.ee

Windows 10: antiviirus ja tulemüür

Vaikimisi antiviirus: Windows Defender (*Settings– Update & Security - Windows Defender*)

- Kontrolli, et on uuendatud
- Kontrolli, et on sisselülitatud

Vaikimisi tulemüür: Windows Firewall (*Control Panel – Windows Firewall*)

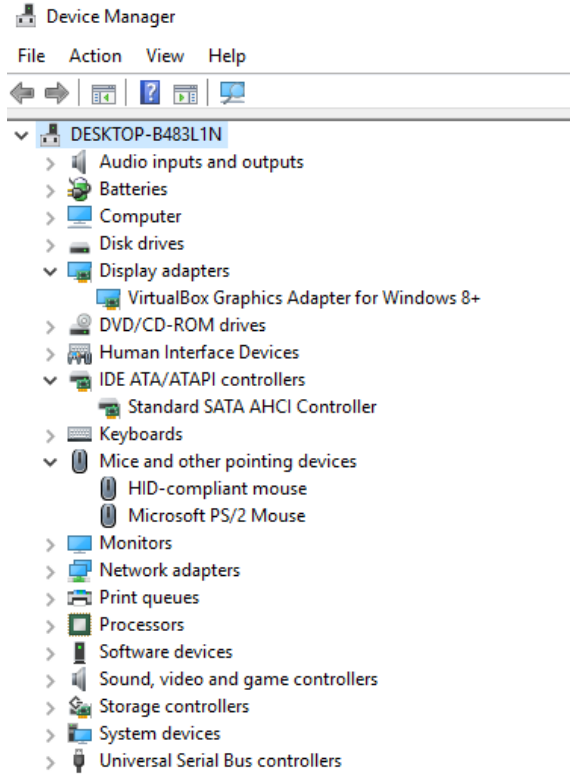
- Kontrolli, et on sisselülitatud

Windows 10: riistvaradraiverid

Control Panel – Device Manager

Riistvaraseadme saab tuvastada Hardware ID põhjal:

Properties – Details – Hardware IDs



Harjutus: tuvasta riistvaraseadmed

USB\VID_04E6&PID_E001\50500194

HDAUDIO\FUNC_01&VEN_11D4&DEV_1984&SUBSYS_17AA20D7&REV_1004\4&30E64BEC&0&0001

ACPI\PNP0303\4&374CCB25&0

SCSI\CDROM&VEN_BE6382V&PROD_GDB834Q&REV_1.0\5&36E5972&0&000

ACPI\IBM0057\4&374CCB25&0

Windows 10: ülevaade riistvarast ja tarkvarast

System Information – msinfo32.exe

Sisoftware Sandra - http://www.sisoftware.co.uk/

Belarc Advisor - http://www.belarc.com/free_download.html

Ubuntu: tulemüür

Kontrollime, kas tulemüür on installitud:

- systemctl status ufw.service

Kui tarvis, siis paigaldame tulemüüri:

- sudo apt install ufw

Seadistame tulemüüriteenuse automaatselt käivitatavaks:

- systemctl enable ufw.service

Käivitame tulemüüriteenuse käsitsi:

- systemctl start ufw.service

Ubuntu: antiviirus

Paigaldame antiviiruse ClamAV
- Sudo install clamav clamav-daemon

Uuendame käsitsi antiviiruse andmebaasi:
- sudo systemctl stop clamav-freshclam
- sudo freshclam
- Sudo systemctl start clamav-freshclam

Seadistame tulemüüriteenuse automaatselt käivitatavaks:
- systemctl enable clamav-daemon.service

Terve failisüsteemi kontrollimiseks
- Sudo clamscan --infected --recursive --remove /

Paigaldame graafilise kasutajaliidese:
- Sudo apt install clamtk

Ubuntu: ülevaade riistvarast ja tarkvarast

Ülevaade riistvarast: lshw

- sudo apt install lshw
- sudo lshw –html > [väljundfail.html]

Üleapt list vaade tarkvarast pakihalduri abil: yum

- sudo apt list --installed > [väljundfail.txt]

Loe lisaks:

http://www.tecmint.com/commands-to-collect-system-and-hardware-information-in-linux/

Kasutajaliidese seadistamine

Sõltub kasutaja eelistustest …

- Aga on mõned kasulikud seadistused

Ubuntu Graafiline kasutajaliides

Kohe on olemas

- Settings->Appearance
- Settings->Background
- Files -> Preferences

Lisaks saab paigaldada

- Gnome-tweaks
- sudo apt install gnome-tweaks

Teistsugune failihaldur

- sudo apt install crusader
- Sudo apt install mc

Windows kasutajaliidese seadistamine

Desktopilt paremklõpsuga

- Display settings
- Personalize

Settings menüüst

- Notifications and actions
- Tablet mode
- Lock screen
- Colors

Start menüü välimuse seadistamine

Settings -> start

Kolmanda osapoole lahendus

- Classic shell
- http://www.classicshell.net/