

Odprta koda in informacijska varnost

četrtak od 8:00 do 12:00, predavalnica 24

Študijsko leto 2007/2008, 4. letnik, 60 ur.

Nosilec: asist. dr. Matej Kovačič

1. VSEBINA SEMINARJA

S povečano stopnjo uporabe informacijske tehnologije se uporabniki soočajo z čedalje večjo odvisnostjo od informacijskih sistemov. Napake v tehnologiji lahko privedejo do resnih osebnih, ekonomskih in celo družbenih posledic, saj se sodobna tehnologija uporablja tako v sferi elektronskega poslovanja, na področju elektronskih volitev, v izobraževanju, itd. Namen seminarja je seznanitev študentov z nekaterimi tehnikami informacijske varnosti in uporabo odprte kode, saj je uporaba odprte kode eden izmed pogojev za transparentnost in posledico večjo stopnjo varnosti informacijskih sistemov.

Študentje se bodo seznanili:

- z osnovami informacijske varnosti in varovanjem informacijskih sistemov pred hekerskimi napadi;
- z avtorsko pravno zakonodajo in odprtimi licencami;
- s konkretno uporabo odprte kode v vsakdanjem življenju.

Poudarek bo na praktičnem delu z Ubuntu Linuxom in uporabi nekaterih varnostnih orodij, študentje pa bodo v okviru seminarja s pomočjo odprtokodnih programov postavili ustrezno zavarovano delovno postajo.

2. OBVEZNOSTI ŠTUDENTOV TER OBLIKE PREVERJANJA IN OCENJEVANJA ZNANJA

Aktivna udeležba na seminarju in sodelovanje pri končnem skupinskem poročilu izvedbe postavitve varne delovne postaje. Poročilo naj obsega 10-20 strani in vsebuje opis sistema ter postopkov nameščanja sistema vključno z zaslonskimi posnetki. Poročilo je potrebno oddati v tiskani in elektronski obliki.

Obvezna je tudi 70% prisotnost na predavanjih in vajah.

3. TEDENSKI DELOVNI NAČRT

zap. št.	datum	predavanja
1.	14. februar 2008	Lastništvo, odprto in prosto programje. Stroški odprtokodne programske opreme. Primeri odprtokodne programske opreme. Kaj je Linux? Distribucija Debian in Ubuntu Linux.
2.	21. februar 2008	Jedro sistema, grafični strežnik in uporabniški vmesnik. Jedrni moduli (podpora strojni opremi). Razdelki. Naprave v Linuxu (/dev). Ubuntu živi CD in alternativni namestitnik Nameščanje poleg operacijskega sistema Windows. Priprava Windows razdelka (pregled in defragmentacija) ter spreminjanje razdelkov z GParted. Praktična namestitev Ubuntu Linuxa. Uporabniška podpora v odprtokodni skupnosti.
3.	28. februar	Nameščanje programske opreme v Ubuntu. Programski viri. Prosti in ne-prosti programski paketi.

zap. št.	datum	predavanja
	2008	Nameščanje programskih paketov za udobno delo z računalnikom. Osnovne nastavitve sistema.
4.	6. marec 2008	Razgled po Linuxu: podrobne možnosti nastavitvev, učinki namizja, upravljalnik omrežja, tiskanje. Dodajanje uporabnikov. Lastniške pravice. Nastavljanje pravic uporabnikom. Ukaz "sudo". Optimizacija z Boot-Up Managerjem.
5.	13. marec 2008	Povezljivost z Windows sistemi: pisanje na NTFS razdelke, uporaba VNC in RDP, samba, MS Office datotečni formati (doc, docx). Povezljivost iz Windows sistemov.
6.	20. marec 2008	Emulacija in virtualizacija. Povezljivost ter izvajanje nevarne programske kode v virtualnem okolju in preiskovanje programske opreme v virtualnem okolju. Predstavitve emulatorja wine ter VmWare in VirtualBox.
7.	27. marec 2008	Informacijski napadi (klasifikacija) in zaščita pred njimi. Upravljanje z varnostnimi tveganji. Razpoložljivost, celovitost in zaupnost informacijskega sistema. Varno uničevanje podatkov. Simetrično in asimetrično šifriranje.
8.	3. april 2008	Verodostojna zatajitev (ang. <i>plausible deniability</i>) in steganografija. Šifrirni algoritmi ter generatorji naključnih števil. Gesla. Uporaba programov za šifriranje elektronske pošte. Nastavljanje in spreminjanje gesel šifrirnih ključev. Delo z javnimi ključi.
9.	10. april 2008	Požarni zid. VPN. Varnostne ranljivosti in varnostni popravki. Varnostne kopije. VPN odjemalec. Varno povezovanje s ssh. ssh -x. Reverzni ssh. Požarni zid.
10.	17. april 2008	Kiberkriminal. Kazniva dejanja iz področja kiberkriminala in praktični opis kiberkriminalnih dejanj.
11.	24. april 2008	Ukazna vrstica (konzola) in predstavitve nekaj najbolj pogostih konzolnih ukazov. Varnost brezžičnih omrežij (WEP, WPA). Kratka predstavitve operacijskega sistema BusyBox.
12.	8. maj	Uporaba nekaterih varnostnih orodij (nmap, WireShark). Varnostni certifikati in napad s posrednikom.
13.	15. maj	Šifriranje trdih diskov v okolju Linux in Windows. Cryptsetup z LUKS podporo, Truecrypt in FreeOTFE.
14.	22. maj	Vzpostavitev v celoti šifriranega sistema.
15.	29. maj	Predstavitve končnega poročila o postavitvi ustrezno zavarovane Linux delovne postaje. Debata na temo prehoda na odprto kodo.

4. TEDENSKI DELOVNI NAČRT VAJ IN OBVEZNOSTI ŠTUDENTOV NA VAJAH

Vaje 1

Študentje naj si ogledajo spletišče mobilnih aplikacij <http://portableapps.com> in si prenesejo ter namestijo dve odprtokodnih aplikacij.

Študentje morajo prebrati esej Richarda Stallmana Pravica brati, ki ga poiščejo na internetu.

Študentje pripravijo kratko poročilo, ki vsebuje opis aplikacije ter uporabniško izkušnjo. Poročilo je dolgo 2 do 3 strani in lahko vsebuje tudi zaslonske posnetke opisane aplikacije.

Študentje napišejo kratek povzetek prebranega eseja in refleksijo na eni strani.

Vaje 2

Študentje bodo dobili originalen namestitveni Ubuntu CD ter si ogledali namestitveni CD-ja z alternativnim namestitelnikom.

Študentje se seznanijo s spletnimi stranmi, ki nudijo pomoč pri namestitvi in uporabi Ubuntu sistema, kot npr. <http://www.ubuntu.si/>, <http://wiki.cybersoc.info>, <http://ubuntuguide.org/>, <http://www.ubuntu.com/> ter sistemom za prijavo napak (<https://bugs.launchpad.net/>).

Študentje zaženejo Ubuntu sistem iz živega CD-ja ter nastavijo omrežje, nato pa zaženejo namestitveni program ter Ubuntu namestijo na računalnik.

Vaje 3

Študentje bodo dokončali namestitev Ubuntu sistema, dodali ustrezne programske vire ter poiskali in namestili programske pakete za udobno delo z računalnikom (Flash predvajalnik, dodatne pisave, dodatne kodeke za predvajanje multimedijskih vsebin, Java, Adobe Acrobat bralnik, podporo za RAR arhive). Naučili se bodo nameščati ter odstranjevati nameščene programe.

Študentje bodo poleg vgrajenega sistema za nameščanje uporabili tudi neposredno namestitev .deb paketa. Na tak način bodo namestili brskalnik Opera. Študentje se bodo tudi seznanili s spletiščem GetDEB.

Študentje se bodo seznanili tudi s funkcijo in urejanjem zagonskega menija Grub.

Študentje pripravijo poročilo o namestitvi (iz vaj 2 in 3), ki obsega 1 do 3 strani.

Vaje 4

Študentje bodo priključili in nastavili omrežni tiskalnik. Ogledali si bodo delo z datotekami (ustvarjanje, kopiranje, brisanje) ter se seznanili s konceptom lastniških pravic nad datotekami. Naučili se bodo spreminjati razpored tipkovnice in menjati jezik namiznega okolja. Naučili se bodo spreminjati ločljivost zaslona, nastaviti zvočni sistem ter zamenjati prijavno okno. Naučili se bodo tudi nastaviti namizje (dodajanje in spreminjanje elementov namizja) ter urejati sistemske menije. Naučili se bodo nastaviti sistemski čas in vključiti sinhronizacijo s časovnimi strežniki. Naučili se bodo zaganjati programe v administratorskem načinu ter se spoznali z Boot-Up Managerjem s katerim bodo nekoliko optimizirali sistem. Sistem bodo zagnali v varnem načinu ter v njem nastavili izgubljeno geslo. Naučili se bodo spreminjati geslo ter dodajati nove uporabnike in jim dodeljevati pravice.

Vaje 5

Študentje bodo odprli in uredili nekaj obstoječih dokumentov v MS Office formatu. Namestili bodo ODF (docx) pretvornik. V pisarniškem programu OpenOffice se bodo kot privzeti format za shranjevanje dokumentov naučili nastavili MS Office format zapisa. Datoteke bodo iz OpenOffice izvozili v PDF. Odprli bodo tudi nekaj multimedijskih datotek. S pomočjo odjemalca za Terminal Server se bodo povezali na Windows namizje. S pomočjo programov putty in WinSCP se bodo iz Windows okolja povezali v Linux sistem

Študentje pripravijo poročilo (iz vaj 4 in vaj 5) o nastavitvi sistema ter potencialnemu prehodu iz Windows okolja v okolje Linux, ki obsega 1 do 3 strani. V poročilu omenijo tudi možne težave pri prehodu (vključno s težavami pri spremembi uporabniškega vmesnika).

Vaje 6

Študentje bodo iz originalnih skladišč paketov namestili emulator wine ter v Linux namestili enega izmed podprtih Windows programov (npr. WinZip, Pajek,...). Seznam podprtih programov si bodo ogledali na spletni strani projekta Wine.

Študentje bodo tudi namestili virtualizacijski program VirtualBox, ter sestavili virtualni računalnik ter v njem iz ISO slike CD-ja zagnali poljuben Linux živi CD (Slax, Ubuntu,...).

Študentje pripravijo kratek opis virtualizacije in poročilo, ki obsega 1 do 2 strani.

Vaje 7

Študentje se bodo naučili uporabiti nekaj metod varnega uničevanja podatkov (uporaba programov DBAN in dd).

Študentje bodo namestili program za delo in upravljanje s šifrirnimi ključi Seahorse. Ustvarili bodo tudi par GPG ključev.

Seznani se bodo tudi z dodatkom za Firefox Fire Encrypter, ki omogoča generiranje naključnih gesel.

Vaje 8

Študentje se bodo naučili delati z GPG/PGP šifrirnimi ključi (iskanje po strežnikih s ključi, uvoz ključev, izvoz ključev, preklic ključa).

Študentje bodo namestili dodatek za šifriranje e-pošte Enigmail ter šifrirni dodatek za brskalnik Firefox FireGPG. Poslali in prejeli bodo vsaj eno šifrirano sporočilo po elektronski pošti.

Vaje 9

Študentje si bodo ogledali šifriranje in dešifriranje datotek z GPG v programu za delo z datotekami Nautilus.

Študentje se bodo naučili nalagati varnostne popravke sistema. Študentje se bodo seznanili s požarnim zidom Firestarter oziroma z orodjem iptables. Seznanili se bodo tudi z orodjem za arhiviranje rsync.

Vaje 10

Študentje se bodo naučili povezovati na oddaljeni Linux sistem preko ssh in v grafičnem okolju. Naučili se bodo oddaljeno zaganjati programe z grafičnim vmesnikom preko ssh.

Študentje si bodo nastavili VPN povezavo in se povezali na oddaljeni strežnik preko VPN.

Študentje pripravijo kratek opis zavarovanja Linux sistema oz. poročilo o namestitvi in uporabi varnostnih mehanizmov iz vaj 7, 8, 9 in 10 ki obsega 1 do 3 strani.

Vaje 11

Študentje se bodo seznanili z ukazno vrstico in nekaj napogostejšimi ukazi (ls, cd, mkdir, rm, mv, cp, scp, chmod, chown, cat, ps, kill/killall, sudo, su, w, orodjem apt in dpkg (dpkg -l), prižiganje, ugašanje in ponovni zagon servisov, dpkg-reconfigure xserver-xorg, mount, umount, mkfs, skdisk, df, du, lspci, dmesg, tail -f /var/log/messages, tail -f /var/log/syslog, top in htop, ifconfig, iwconfig in dhclient) ter ukazom man.

Študentje bodo naučili izvajati nekaj ukazov v Linux ukazni vrstici: brskanje po imenikih na disku in pregled vsebine tekstovne datoteke, urejanje tekstovne datoteke z urejevalnikom nano, zagon skripte in zagon programa (npr. brskalnika Firefox), pregled aktivnih procesov in ugašanje programa, ki se je obesil.

Študentje si bodo ogledali nekaj kratkih filmov o varnosti brežičnih omrežij ter se v ukazni vrstici razgledali po napravi (brežični dostopni točki) z nameščenim operacijskim sistemom BusyBox.

Vaje 12

Študentje si bodo ogledali kratek film, ki prikazuje napad s posrednikom (primer napada na GMail).

Namestili bodo dve varnostni orodji nmap in WireShark. Z orodjem za skeniranje vrat bodo pregledali sosednje računalnike.

Če bodo dopuščale tehnične možnosti bomo skupaj s študenti računalnike priključili na koncentrador ter izvedli prestrezanje prometa s programom WireShark.

Vaje 13

Študentje bodo namestili šifrirna programa Cryptsetup z LUKS podporo ter Truecrypt. Namestili bodo tudi ustrezne jedrne module. Ustvarili bodo navaden ter virtualni šifrirani razdelek, ju priključili ter nanj zapisali nekaj podatkov. V programu Truecrypt bodo naredili in uporabili skriti razdelek (praktična uporaba funkcije verodostojne zatajitve).

Vaje 14

Študentje se bodo lotili vzpostavitve v celoti šifriranega sistema.

Vaje 15

Predstavitev končnega poročila o postavitvi ustrezno zavarovane Linux delovne postaje. Sodelovanje v debati na temo prehoda na odprto kodo.

5. ŠTUDIJSKA LITERATURA

1. Kovačič, Matej (2006): Nadzor in zasebnost v informacijski družbi, (Zbirka Znanstvena knjižnica). Ljubljana: Fakulteta za družbene vede.
2. Bogataj, Maja (ed.) (2003): Internet in pravo. Ljubljana: Pravna fakulteta Univerze v Ljubljani. (izbrana poglavja).
3. Geer Daniel, Pfleeger Charles P., Schneier Bruce, Quarterman John S., Metzger Perry, Bace Rebecca, Gutmann Peter (2003): CyberInsecurity: The Cost of Monopoly. <<http://www.ccs.cmu.edu/papers/cyberinsecurity.pdf>>.
4. Stallman, Richard (2002): Free Software, Free Society: Selected Essays of Richard M. Stallman – esej Pravica brati. <<http://slo-tech.com/clanki/06006/>>.
5. Anderson, Ross (2003): 'Trusted Computing' Frequently Asked Questions. <<http://www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html>>.