

## IT taristu teenuste turvamine

*Õppeaine nimetus*

Securing IT Infrastructure Services

*Õppeaine nimetus inglise keeles*

Pole veel teada, asendab ainet I385

*Ainekood*

**Aineprogrammi versioon** 2013 Kevad  
Kinnitamise kuupäev

Õppekava(d):

Infosüsteemide analüüs

**X IT süsteemide administreerimine**

IT süsteemide arendamine

Tehnosuhtlus

**Õppeaine eesmärk (tuleneb õppeaine rollist õppekavas ja väljendab mis eesmärgil, mida ja kuidas õpetatakse. Eesmärgis võib kajastada ainega kujundatavaid hoiakuid ja mittehinnatavaid ülekantavaid pädevusi)**

Tutvustada IT taristu teenuste põhimõisteid. Anda oskused põhiliste teenuste paigaldamiseks ja turvamiseks. Anda oskused IT taristu teenuste dokumenteerimiseks.

Eesmärgi saavutamiseks toimuvad laboratoorsed tööd, mille käigus installeeritakse ja konfigureeritakse teenuseid pöörates rõhku teenuse turvalisusele, millele eelnevad loengud alus- ja põhimõistete tutvustamiseks.

**Õpiväljundid - üliõpilase poolt omandatavad erialased ja ülekantavad pädevused**

- sõnastatakse miinimumtasemel;
- väljendavad üliõpilase teadmisi, oskusi, suutlikkust õppe/aine lõppedes;
- on hinnatavad.

(nt. analüüsib probleemi; koostab ettekande; põhjendab valikuid; kirjeldab, võrdleb jne)

**Hindamiskriteeriumid - mitteeristava hindamise puhul õpiväljundi lävendikriteerium ja eristava hindamise puhul hindekriteeriumid.**

<b>Õpiväljund</b>	Oskab seadistada Interneti juurteenuseid (NTP, DNS, DHCP). Oskab seadistada veebi- ja failiservereid apache2 ja SAMBA näitel
Lävend	Õppur suudab praktikumis seadistada õpiväljundis loetletud teenuseid ja kirjeldada teenuste tööd ning põhjendada paigaldatud teenuste seadistamisel tehtud valikuid.
<b>Õpiväljund</b>	Teab Interneti juurteenuste põhi- ja alusmõisteid. Teab veebi- ja

	failiserverite põhi- ja alusmõisteid.				
Lävend	Õppur oskab sõnastada mõistete tähendust ja seost IT infrastruktuuri erinevate teenustega.				
Õpiväljund	Oskab turvata veebi-, failiservereid ja Interneti juurteenuseid. Õppur oskab testida enamlevinud rünnete mõju teenustele.				
Lävend	Õppur oskab seadistada ja kirjeldada erinevaid teenuste turvamehhanisme, mida kasutatakse teenuste turvalisuse tõstmisel ja testimisel.				
Õpiväljund	Teab veebiteenuste vastaseid põhilisi ründeid (injektsiooniründed, XSS, CSRF, DOS ja muud)				
Lävend	Õppur oskab kirjeldada põhiliste rünnete toimemehhanismi ja vastumeetmeid antud ründele.				
Õpiväljund	Oskab seadistada lihtsamaid autentimise ja autoriseerimise teenused juhendi alusel.				
Lävend	Õppur oskab seadistada LDAP ja/või Kerberose põhise autentimise ja autoriseerimise süsteemi ühe konkreetse süsteemi juhendi näitel.				
Õpiväljund	Teab IT infrastruktuuri teenuste põhilisi mõisteid vastavalt õppematerjalis antud nimekirjale. (VPN, virtualiseerimine, SQL, SAN/NAS, monitooring, logiteenus, tulemüüre, IDS ja IPS)				
Lävend	Tudeng oskab sõnastada ja selgitada aines käsitletud teemade sisu ja kasutusvaldkondi.				
Õpiväljund	Õppur oskab dokumenteerida IT infrastruktuuri teenuseid vastavalt aines esitatud juhendmaterjalile.				
Lävend	Õppur koostab nõuetekohase dokumentatsiooni ühe seadistatud teenuse kohta.				
Sihtgrupp		Rakenduskõrgharidusõpe			
Õppeaine maht		6 EAP			
Õppetöö keel		eesti keel			
Õppetöö toimumine erinevates õppevormides					
Õppevorm	Kontaktõpe			Iseseisev töö (sh e-õpe)	Praktika (töökesk-konnas)
	Loeng	Seminar	Labor		
Päevane	32		48	88	
Õhtune					
Kaugõpe	12		30	126	
E-õppe keskkond (link keskkonnale)					
Eeldused (kohustuslikud)			Operatsioonisüsteemide administreerimine ja sidumine		

<b>Eeldusained</b> (soovituslikud)		Andmeturve	
<b>Õppeaine kontrolli vorm</b>		eksam	
<b>Õppejõud</b>			
Nimi		<b>Margus Ernits</b>	
Kontaktandmed: e-post telefon Skype		<b>margus.ernits@itcollege.ee</b> <b>margus.ernits</b>	
Ametikoht teaduskraad		<b>Õppejõud</b> <b>Rakenduslik kõrgharidus</b>	
<b>Õppejõud</b>			
Nimi		<b>Katrin Loodus</b>	
Kontaktandmed: e-post telefon Skype		<b>katrin.loodus@itcollege.ee</b> <b>katrinloodus</b>	
Ametikoht teaduskraad		külalisõppejõud <b>Rakenduslik kõrgharidus</b>	
<b>Õppeaine programm</b> (teemad loogilises järjestuses)			
<b>Jrk. nr.</b>	<b>Teema</b>	<b>Tunde (kokku)</b>	<b>Kirjandus</b> (K-kohustuslik; T-täiendav)
<b>Loengud</b>			
1	Sissejuhatus ainesse, põhi ja alusmõistete kirjeldus	1	
2	Interneti ajateenuse NTP seadistamine	1	
3	Interneti domeeninimede süsteem DNS ja selle turvalisus	4	
4	DHCP teenuse põhimõisted ja seadistamine	2	
5	Tulemüürid ja VPN	2	
6	Veebiteenuse seadistamine (Näiteks apache2, WordPress ja Varnish baasil)	2	
	Veebirakenduste turvatestimine OWASP (Open Web Application Security Project) baasil Veebirakenduste turvalisus DVWA näite baasil	4	
	Veebirakenduse turvalisuse parandamine rakenduskihi tulemüüride baasil (GreenSql ja mod_security näidetel)	4	
	Autentimine ja autoriseerimine	3	

	Failiserveri teenus	1	
	E-posti teenus	2	
	Syslog – rsyslog ja syslog-ng	2	
	Mõisted SAN/NAS/CAS, RAID ja failisüsteemid	2	
	Dokumentatsiooni koostamine	2	
<b>Praktilised tööd</b>			
0	Ubuntu serveri ja kliendi paigaldamine, Osadmin kordamine	2	
1	NTP paigaldamine ja seadistamine	1	
2	DNS paigaldamine ja seadistamine	4	
3	DHCP paigaldamine ja seadistamine	2	
	Laborite 1, 2,3 kaitsmine (viies ja kuues nädal)	4	
4	Apache2 paigaldamine ja virtualhostide seadistamine	4	
5	Wordpress paigaldamine ja jõudluse testimine	4	
6	DVWA paigaldamine ja OWASP testimine SQL tulemüüri paigaldus ja testimine Veebitulemüüri mod_security paigaldamine ja testimine	16	
	Laborite 3,4,5,6 kaitsmine	5	
7	Zentyal SAMBA4 infrastruktuuri paigaldamine	4	
	Labor 7 kaitsmine	2	
<b>Iseseisva töö kirjeldus, ajakava</b> (ülesanded, kodutööd, orienteeruv maht)			
1. Ubuntu serveri paigaldamine ja Operatsioonisüsteemide kordamine 6h 2. Tulemüüride põhimõistete omandamine (iptables või PF baasil) 4h 3. DNS põhimõistete omandamine 8h 4. HTTP protokollide põhimõistete omandamine (lisaks HTTPS ja TLS) 8h 5. Veebiserverite põhimõistete omandamine Apache2 ja nginx baasil 4h 6. Veebirakenduse jõudluse testimine ja parandamine 4h 7. OWASP top 10 mõistetega tutvumine 8h 8. DVWA paigaldamine ja nõrkustega tutvumine 16h 9. Rakenduslikud tulemüürid (GreenSQL ja mod_security näitel) 16h 10. Dokumentatsiooni koostamine ühele seadistatud teenusele 10h 11. Infrastruktuuri teenuste põhimõistete õppimine 4h			

## Kirjandus

### Kohustuslik kirjandus (K)

Aine kodulehel toodud kirjandus, mis toetab iseseisva töö kirjelduses antud teadmiste omandamist.

### Täiendav kirjandus (T)

**Hindamismeetodid** (nt. kontrolltöö, juhtumi analüüs jm) ja vajadusel nende osakaalud.

Iga õpiväljundi kohta tuleb saavutada minimaalne lävend. Oskuste hindamiseks tuleb teha iga õpiväljundi kohta praktiline laboritöö, mis tuleb praktilises tunnis personaalselt kaitsta.

Teadmiste hindamine toimub praktilise töö kaitsmise käigus. Kui suulisel kaitsmisel hinnet ei saadud, siis toimub teadmiste kontroll kontrolltööna.

Kaitsmisele kuuluvad laborid:

- NTP
- DNS
- DHCP
- Apache2, WordPress, Varnish
- DVWA
- Rakenduslikud tulemüürid - GreenSQL, Mod Security
- SAMBA

Teoreetiliste teadmiste kontrolliks tehakse kaks kontrolltööd õpiväljundites loetletud teemadel.

Arvestus koosneb kahest osast. Praktilisest ja teoreetilisest. Arvestusel tuleb paigaldada ühte loosiga saadud teenust ja vastata 5-10 teooriaküsimusele.

Arvestuse praktiline osa:

Õppejõud teeb katki ühe seadistatud teenustest.

NB Kohe kirja ka järelarvestuse asjad! (Järelarvestusele saamiseks tuleb kaitsta kõik laborid ja saata dokumentatsioon enne järelarvestuse päeva)

**Lisainfo aine kohta** (tehniliste vahendite vajadus, õppetöö korraldus, tasemetestid ja muu)

Aine läbiviimine toimub arvutiklassis. (Nii loengute, kui ka praktikumide raames). Arvutiklass, milles õppetööd läbi viiakse peab jääma kogu semestri jooksul samaks. Arvestuseks vajalik aeg on minimaalselt 6h (kuni 24 õppuri korral). Kui õppureid on rohkem, tuleb iga 24 õppuri kohta arvestada 6h

Aineprogrammi koostaja:  
Margus Ernits

Kuupäev