



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE,
ZNANOST IN ŠPORT

Center
Republike Slovenije
za poklicno
izobraževanje



EVROPSKA UNIJA
EVROPSKI
SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST



worldskills Slovenia

Testna naloga

SloveniaSkills 2020 - IKT

24., 25. januar 2020

N-Sim

Simulated Experiences



Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega socialnega sklada Operacija se izvaja v okviru Operativnega programa 2014-2020, prednostna os 10 – Znanje, spretnosti in vse življenjsko učenje za boljše zaposljivost, prednostna naložba 10.2.- Izboljšanje relevantnosti izobraževalnih sistemov in sistemov usposabljanja za trg dela, olajšanje prehoda iz izobraževanja v zaposlitev ter krepitev sistemov poklicnega izobraževanja in usposabljanja in njihove kakovosti, tudi z mehanizmi za napovedovanje potreb po spretnostih, prilagoditvijo učnih načrtov ter vzpostavitev in razvojem sistemov za učenje na delovnem mestu, vključno z dualnimi učnimi sistemi in vajeniškimi programi.



UVOD

N-Sim, d.o.o., je mlado hitrorastoče start-up podjetje, ki v okviru digitalne transformacije letalske industrije proizvaja simulatorje letenja. Najnovejša različica njihovega simulatorja, N-Sim-Fly je na uvodni predstavitvi dosegla tako močan odziv strokovne javnosti, da so se odločili poleg prodaje posameznih simulatorjev postaviti še prvi »show-off« simulacijski center v državi.

Kot start-up je N-Sim odprl svoje prve poslovne prostore na Kajuhovi ulici 32U, 1000 Ljubljana. Do sedaj so imeli le preprosto internetno povezavo do ponudnika storitev, z razvojem podjetja pa je prišlo do novih potreb tudi v glavni pisarni. Za prvi simulacijski center, ki zahteva zelo hitro in varovano povezavo z glavno pisarno, so kupili poslovne prostore v velikosti 500 m² na Vokmerjevi 19, 2250 Ptuj. Otvoritev je predvidena v roku dveh dni.

N-Sim vas je preko razpisa zaposlil za nedoločen čas kot omrežnega administratorja. Vaša prva naloga na novem delovnem mestu je, da pripravite in prilagodite novo in obstoječo informacijsko-komunikacijsko infrastrukturo v skladu z načrti podjetja in pripravite vse potrebno, da bo tudi med in po otvoritvi novega centra podjetje lahko delovalo nemoteno.

NAČIN DELA

Testna naloga je pripravljena za izvedbo v dveh tekmovalnih dneh. Drugi dan predstavlja nadaljevanje prvega. Po končanem prvem dnevu bodo sodniki ocenili vaše delo. Velik del tega, kar je bilo potrebno storiti prvi dan, je pomemben tudi za delovanje v drugem dnevu, a to ne pomeni, da bo ta del ponovno ocenjen po koncu drugega dne. Izjemo predstavljajo zgolj tiste naloge, ki so integrirane v prejšnje. Skladno s tem bodo sodniki po koncu drugega dne ocenili delovanje rešitve kot celote, ne samo določene postavke, ki so bile zahtevane tekom drugega dne. Rešitev ob koncu tekmovanja mora biti torej skupek vseh zahtevanih nalog, ki morajo delovati druga z drugo. Sodniki bodo ocenili vaš končni produkt.

Dostop do interneta je med tekmovanjem (ne pa npr. med kosilom) strogo prepovedan. Tekmovalci nimajo dostopa do komunikacijskih naprav, ki bi bile povezane v zunanje omrežje. Svoje naprave, ki bi bile tega zmožne, morate pred začetkom tekmovanja pustiti v za-to namenjenih garderobah. Na tekmovališče vam ni dovoljeno prinašati ničesar. Kar potrebujete, boste našli tam.

Testna naloga je zastavljena na način, da določi cilje vsakega dne, a hkrati prepusti vam, katere izmed teh boste uresničili, glede na vaše zmožnosti.

Namen testne naloge je simulirati življenjski scenarij, vsakdanje delo normalnega podjetja, v kolikor je to le mogoče. Naš namen NI zavajanje, ustvarjanje dodatnih trikov ali poustvarjanje situacij, ki so skoraj nemogoče v produkcijskem okolju. Vsekakor obstaja več možnih poti do končne rešitve. Vedite, da v industriji velja za boljše rešitev tista, ki sledi t.i. »best-practice« smernicam. Torej tudi na tekmovanju lahko za enako delujočo rešitev ekipa, ki upošteva te smernice (v okviru certifikatov, ki predstavljajo tvarino tekmovanja), prejme več točk (npr. uporaba naprednejšega AES algoritma za šifriranje prinese več točk kot uporaba zastarelega algoritma DES).



OPREMA

STROJNA OPREMA:

- 1x Cisco 28x1 usmerjevalnik
- 1x Cisco 1841 usmerjevalnik
- 2x Cisco Catalyst 2960 / 3560 / 3750 stikalo
- 1x strežnik (VMware vSphere Hypervisor 6.7): min. 16GB RAM, 250GB SSD, 2x NIC
- 2x prenosni računalnik (Windows 10) + miška

PROGRAMSKA OPREMA:

- Debian 10.1.0 »buster« (DVD-1-3)
- Windows Server 2019
- Windows 10
- VMware vSphere Hypervisor (ESXi) 6.0 + vSphere Client
- Cisco IOS: po seznamu

EKOLOGIJA in NAPOTKI ZA TEKMOVALCE

Tekom tekmovanja se bomo trudili porabiti čim manj papirja in pisal. V skladu z ekološkimi smernicami bomo uporabili čim manj fizičnih naprav, nadomestili jih bomo z virtualizacijo.

Povezave do štirih ponudnikov storitev bomo združili v eno trunk povezavo na delovno mesto na prvi vmesnik stikala S-SC-NET in jo nato razdelili na prve štiri vmesnike istega stikala. Ostali vmesniki omenjenega stikala S-SC-NET služijo kot stikalo v simulacijskem centru. Glej fizično in logično topologijo.

Strežnik ima nameščeni dve mrežni kartici, od katerih naj bo ena uporabljena za priključek naprav v glavno poslovalnico (S-OFFICE; vlani X11, X12 in X13), druga pa naj bo uporabljena za priključek v simulatorski center in zunanje omrežje ISP-SIM (S-SC-NET; vlani X51, X52, X54 in X05). Glej fizično in logično topologijo.

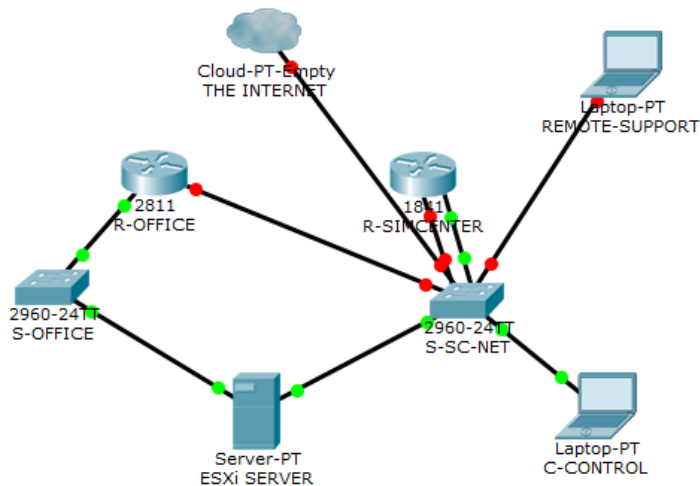
Na strežniku bo v naprej nameščenih 6 virtualnih naprav, od tega 2 Windows strežnika »WDC-1« in »WDC-2«, Debian strežnik »L-WEB«, 2 Debian odjemalca (simulatorja) »SIM-FLY-51« in »SIM-FLY-03« ter Windows odjemalec »STAFF«. Vnaprej nastavljen management IP naslov na strežniku je 192.168.32.5/24.

Kjerkoli v nalogi ni posebej določeno, uporabite uporabniško ime »ict«, in geslo »20skills19«. Vedno uporabite podano geslo! V nasprotnem primeru obstaja možnost, da vašega dela ne bomo zmožni oceniti, torej lahko za svojo rešitev prejmete 0 točk.

Kjerkoli v nalogi najdete namesto zapisane številke spremenljivko »X« (npr. IP naslovi, telefonske številke), na tem mestu vnesite številko svojega delovnega mesta. Za preverjanje delovanja storitev bomo sodniki vedno uporabili domenska imena in ne IP naslovov!

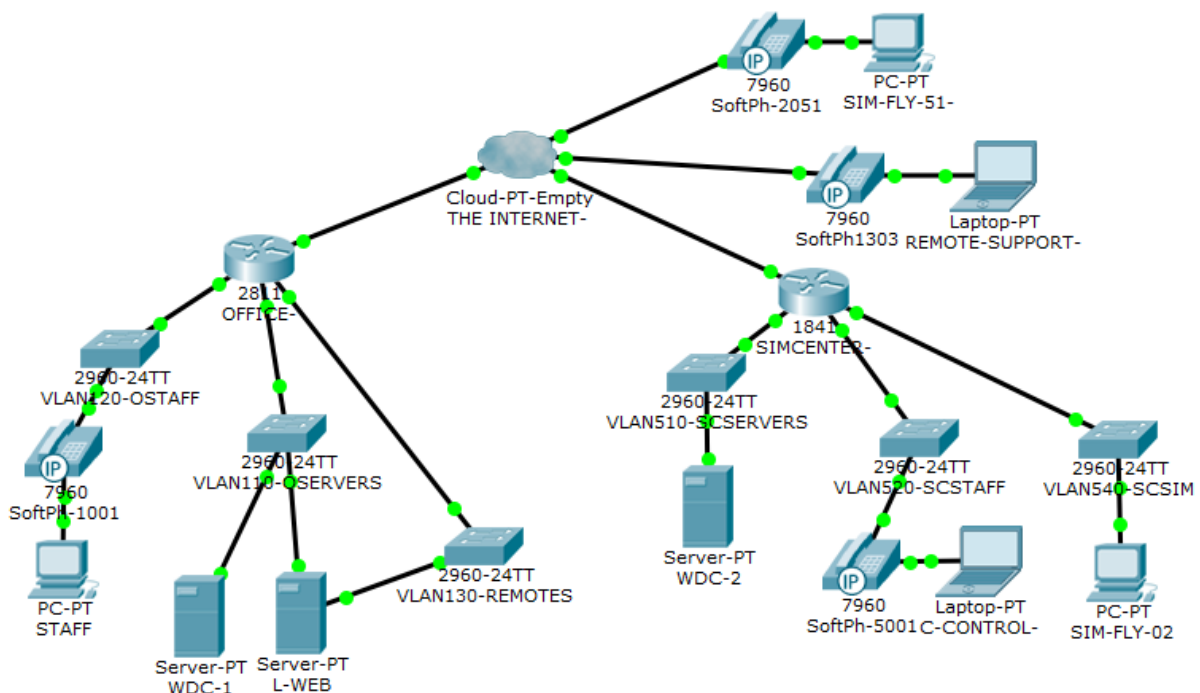
Delujte, kot da je vaša oprema dejansko povezana v internet. V tem duhu izvedite potrebne varnostne ukrepe, da ne bi kdo, pomotoma ali ne, vdrl v vašo opremo (komunikacija med tekmovalci s stališča omrežja ni blokirana, s stališča "fair-play" pa ni zaželenja).

FIZIČNA TOPOLOGIJA



* Z rdečo barvo so označene povezave preko S-SC-NET do ponudnikov storitev.

LOGIČNA TOPOLOGIJA



DAN 1 (7 ur)

1. Za lažje rokovanje z napravami jim nastavite imena, kot so prikazana na fiz. topologiji.
2. Na prvi vmesnik stikala S-SC-NET (Fa0/1) pripeljite kabel s trunk povezavo do ponudnika storitev. Na njem nastavljen VLAN-e nastavite kot access na vmesnike:
 - a. VLAN X02 – ISP-OFFICE, vmesnik Fa0/2, povezava do R-OFFICE
 - b. VLAN X03 – ISP-SIMCENTER, vmesnik Fa0/3, povezava do R-SIMCENTER
 - c. VLAN X04 – ISP-REMOTE, vmesnik Fa0/4, povezava do REMOTE-SUPPORT
 - d. VLAN X05 – ISP-SIM, povezava do SIM-FLY-51, preko povezave na strežnik
3. Preostali del stikala S-SC-NET uporabite kot stikalo v Simulacijskem centru. Na njem ustvarite 4 VLAN-e, ki bodo delovali kot 3 stikala na logični topologiji (+ management):
 - a. Trunk povezava notranjih omrežij med stikalom S-SC-NET in usmerjevalnikom R-SIMCENTER ter med stikalom in strežnikom:
 - i. VLAN 510: SCServers
 - ii. VLAN 520: SCStaff
 - iii. VLAN 540: SCSim
 - iv. VLAN 32: Management
 - b. Poleg omenjenih na trunk povezavi do strežnika dovolite še VLAN X05 za potrebe samostojnega simulatorja pri naročniku SIM-FLY-51.
 - c. Predzadnji vmesnik na stikalu naj pripada VLAN-u SCStaff, nanj naj bo priključen prenosni računalnik SC-CONTROL
 - d. Zadnji vmesnik na stikalu naj pripada VLAN-u Management.
4. Na stikalu S-OFFICE ustvarite 4 VLAN-e, ki bodo delovali kot 3 stikala na log. topologiji (+ management) in jih dovolite na trunk povezavah usmerjevalnik – stikalo – strežnik.
 - a. VLAN110: OServers
 - b. VLAN120: OStaff
 - c. VLAN130: ORemotes
 - d. VLAN33: Management
 - e. Zadnji vmesnik na stikalu naj pripada VLAN-u Management.
5. Ponudnik storitev vam je za omrežje glavne pisarne (OFFICE) podal naslovni prostor:
 - a. IPv4 naslovi: 167.255.X.128/25, privzeti prehod: 167.255.X.129
 - b. IPv6 naslovi: 2a02:faca:X:aa00::/56, privzeti prehod: 2a02:faca:X:aa00::1
 - c. Celotno omrežje glavne pisarne naj deluje v načinu »dual-stack«.
 - d. Za zunanji vmesnik usmerj. R-OFFICE uporabite PRVI uporabni IP naslov.
 - e. DNS strežnik: 1.1.1.1, 2606:4700:4700::1111
6. Na usmerjevalniku R-OFFICE nastavite DHCP strežnik za Management VLAN.
7. Naprave v VLAN-u OServers naj imajo statične javne IPv4 naslove, naprave v VLAN-ih OStaff in ORemotes pa dinamične zasebne IPv4 naslove.
8. Dostop do interneta z naprav z zasebnimi naslovi omogočite z uporabo tehnologije NAT na usmerjevalniku R-OFFICE in bazenom treh prostih naslovov.
9. Usmerjevalnik »R-OFFICE« za notranja omrežja (VLAN 110, 120, 130, 33) nastavite po principu »router-on-a-stick« glede na omrežno topologijo.
10. DNS strežnik pri ponudniku storitev vsebuje naslednje zapise:

Tip zapisa	Ime	Vrednost
NS record	{šola}.n-sim.si	nsX.n-sim.si
A record	nsX.n-sim.si	167.255.X.250
AAAA record	nsX.n-sim.si	2a02:faca:X:aaff::250

Pri čemer velja, da namesto spremenljivke X nastopa zap. št. delovnega mesta posamezne ekipe, namesto {šola} pa nastopa okrajšava posamezne šole, kot sledi iz tabele:

Šola	Okrajšava	Primer zapisa
SŠTS Šiška	siska	siska.si
ŠC Kranj	kranj	kranj.si
ŠC Nova Gorica	ng	ng.si
ŠC Novo mesto	nm	nm.si
ŠC Ptuj	ptuj	ptuj.si
ŠC Velenje	velenje	velenje.si
Vegova Ljubljana	vegova	vegova.si
ZGN Ljubljana	zgnl	zgnl.si

11. Ponudnik storitev vam je za omrežje simulacijskega centra podal naslovni prostor:
 - a. IPv4 naslovi: 69.2.X.192/26, privzeti prehod: 69.2.X.200
 - b. IPv6 naslovi: 2a02:faca:X:bb00::/56, privzeti prehod: 2a02:faca:X:bb00::1
 - c. Celotno omrežje simulacijskega centra naj deluje v načinu »dual-stack«.
 - d. Za zunanji vmesnik usmerj. R-SIMCENTER uporabite PRVI uporabni IP naslov.
 - e. DNS strežnik: 1.1.1.1, 2606:4700:4700::1111
12. Na usmerjevalniku R-SIMCENTER nastavite DHCP strežnik za Management VLAN.
13. Naprave v VLAN-u SCServers naj imajo statične javne IPv4 naslove, naprave v VLAN-ih SCStaff in SCSim pa dinamične zasebne IPv4 naslove
14. Dostop do interneta z naprav z zasebnimi naslovi omogočite z uporabo tehnologije PAT na usmerjevalniku R-SIMCENTER.
15. Usmerjevalnik »R-SIMCENTER« za notranja omrežja (VLAN 510, 520, 540, 32) nastavite po principu »router-on-a-stick« glede na omrežno topologijo.
16. Na vseh omrežnih napravah želimo imeti omogočen oddaljen dostop z avtentikacijo s parom javnega in privatnega ključa (key-based).
 - a. Uporabnik naj ob oddaljeni prijavi takoj pristane v privilegiranem izvršilnem načinu (Privileged-Executive Mode).
 - b. Oddaljen dostop naj bo mogoč le iz računalnikov v omrežjih Management – VLAN 32 in 33.
 - c. Datoteka s ključem naj bo na namizjih obeh prenosnih računalnikov, ključ naj bo že vnesen v program PuTTY na obeh prenosnih računalnikih.
17. Ponudnika storitev na lokaciji delavcev, ki izvajajo oddaljeno podporo od doma (REMOTE-SUPPORT) ter na lokaciji samostojnega simulatorja letenja pri naročniku (SIM-FLY-51) ponujata le dinamično nastavitve javnega IP naslova.
18. Za povezavo med poslovalnicama (OFFICE in SIMCENTER) skrbi Site-to-Site IPSec VPN tunnel med usmerjevalnikoma.
 - a. Preverjanje pristnosti naj bo na osnovi ključa.
 - b. Znotraj tunela uporabite privatne IPv4 oz. Link-Local IPv6 naslove.
 - c. Za usmerjanje prometa med lokacijama naj skrbi OSPFv3.
 - d. Ves promet med lokacijama mora biti šifriran.
19. Dohodni promet iz interneta naj bo iz varnostnih razlogov prepovedan, v kolikor ni nujen za delovanje organizacije.
20. Za centralizirano upravljanje z domeno, uporabniškimi računi zaposlenih in njihovimi napravami naj skrbi »WDC-1«.
 - a. Nastavite ga za skrbnika domene {šola}.n-sim.si z uporabo storitev aktivnega imenika (AD) in DNS strežnika.
 - b. Windows odjemalca PC-STAFF in prenosnik SC-CONTROL pridružite domeni.
 - c. Vnesite 3 organizacijske enote (OU) z uporabniki, kot sledi:

Organizacijska enota	Uporabnik
Staff	Aljaž
Staff	Cveto

Staff	Janez
CenterControl	Olga
CenterControl	Jakob
CenterControl	Lado
Remote	Pavel
Remote	Črtomir
Remote	Marta
Remote	France

- d. Želimo, da je »WDC-1« notranji DNS strežnik. Poleg DNS zapisov za odjemalce mora vsebovati tudi zapise za vse omrežne naprave. Poskrbite za naslednje zapise glede na vašo dodelitev IP naslovov:
- l-web.{šola}.n-sim.si
 - wdc-1.{šola}.n-sim.si
 - wdc-2.{šola}.n-sim.si
 - pc-staff.{šola}.n-sim.si
 - sc-control.{šola}.n-sim.si
 - sim-fly-02.{šola}.n-sim.si
 - r-office.dev.{šola}.n-sim.si
 - r-simcenter.dev.{šola}.n-sim.si
 - s-office.dev.{šola}.n-sim.si
 - s-sc-net.dev.{šola}.n-sim.si
- e. Uporabniki iz enote CenterControl naj imajo:
- privzeto nastavljeno ozadje na logotip podjetja,
 - zaklenjeno spreminjanje ozadja,
 - prepovedan dostop do nadzorne plošče,
 - onemogočen ukazni poziv (Command Prompt).
- f. WDC-1 naj bo DHCP strežnik za VLAN OStaff.
21. Strežnik WDC-2 je dodatni redundančni strežnik na drugi lokaciji.
- naj bo pomožni skrbnik domene {šola}.n-sim.si, ki v primeru nedosegljivosti strežnika WDC-1 skrbi za nemoteno delovanje podjetja.
 - WDC-2 naj bo DHCP strežnik za VLAN-a SCStaff in SCSim.
22. »L-WEB« služi kot zunanji DNS strežnik. Vsebuje naj vse potrebne zapise za zagotavljanje funkcionalnosti omrežja iz interneta.
23. Simulatorji letenja med svojim delovanjem proizvedejo ogromne količine podatkov, ki jih je najbolje nemudoma prenesti na strežnike v glavni pisarni. Podjetje se je odločilo za rešitev z oddaljenim dostopom preko navideznega zasebnega omrežja OpenVPN na strežniku »L-WEB«.
- Vzpostavite OpenVPN strežnik na L-WEB.
 - Povezani OpenVPN odjemalci naj bodo vključeni v VLAN ORemotes
 - IP naslove naj dimanično dodeljuje strežnik L-WEB.
 - Za promet OpenVPN odjemalcev naj strežnik L-WEB uporablja omrežno kartico, povezano v VLAN ORemotes. Za preostali promet naj strežnik uporablja omrežno kartico, povezano v VLAN OServers.
 - Vzpostavite OpenVPN povezavo iz odjemalca delavca od doma (REMOTE-SUPPORT) in iz samostojnega simulatorja SIM-FLY-51.
24. Velike količine podatkov s simulatorjev letenja naj se z uporabo NFS avtomatsko shranjujejo na strežnik »L-WEB«.
- Na strežniku ustvarite skupno mapo /var/datashare
 - Vsako minuto naj vsak simulator dopiše svoje ime in trenutni čas v datoteko v skupni mapi z imenom enakim imenu naprave.

25. Za takojšnjo komunikacijo s strankami podjetje potrebuje elektronsko pošto.
- Storitev naj zagotavlja strežnik »L-WEB«.
 - E-poštni naslovi naj bodo oblike »{uporabnik}@{šola}.n-sim.si«.
 - Ustvarite e-poštne predale za uporabnike iz org. enot Staff in CenterControll.
 - Uporabniška imena in gesla naj bodo shranjena na »WDC-1«.
 - Na prenosnem računalniku »SC-CONTROL« v programu »Outlook« nastavite poštni račun za uporabnika »Olga«, če je prijavljen uporabnik »Olga«, ter za uporabnika »Lado«, če je prijavljen uporabnik »Lado«.
 - Na odjemalcu PC-STAFF v programu »Pošta« (»Mail«) nastavite poštni račun za uporabnika »Aljaž«, če je prijavljen uporabnik »Aljaž« ter za uporabnika »Cveto«, če je prijavljen uporabnik »Cveto«.
 - Poskrbite tudi z varnost z uporabo SPF in DKIM.
26. Podjetje za oglaševanje simulatorjev letenja zahteva tudi delovanje spletne strani na naslovih »{šola}.n-sim.si« in »www.{šola}.n-sim.si«. Spletni strežnik s podporo php nastavite na »L-WEB«. Spletna stran naj izpiše ime podjetja ter trenutni datum in uro.
27. Podjetje se je opremilo z moderno IP telefonijo in uporabljajo t.i. SoftPhone rešitve. Omogočite interno IP telefonijo znotraj podjetja.
- Telefonska centrala naj bo na usmerjevalniku R-OFFICE.
 - Telefonske številke naj bodo sledeče:

Naprava	Odjemalec	Tel. št.
PC-STAFF	Cisco IPC	X1001
SC-CONTROL	Jitsi	X5001
REMOTE-SUPPORT	Cisco IPC	X1303
SIM-FLY-51	Jitsi	X2051

- Prijetno bi bilo, če nas v času, ko je naš klic na čakanju, spremlja glasba.

S tem se zaključí 1. dan tekmovanja. Sodniki bomo pri preverjanju VEDNO uporabljali imena storitev namesto IP naslovov. Ocenjuje se funkcionalnost podjetja, ne nastavitve. Močno priporočeno je, da na zadnjih straneh izpolnite tabelo z IP naslovi, saj lahko ta sodnikom pomaga razumeti vašo rešitev.

*"I don't always test my code.
But when I do, I do it on Production Servers."*

DAN 2 (5 ur)

1. Stikalo »S-SC-NET« zavarujte, kolikor se le da. 802.1x
 - a. Na novo ustvarite VLAN BlackHole in vanj dodajte vse neuporabljene vmesnike.
 - b. Neuporabljeni vmesniki naj bodo privzeto ugasnjeni.
 - c. Na predzadnjem vmesniku (povezava do SC-CONTROL) omogočite preverjanje pristnosti z uporabo protokola IEEE 802.1x. V kolikor se na vmesnik na stikalu prijavi uporabnik iz organizacijske enote CenterControll, naj se vmesnik vključi v VLAN SCStaff, sicer naj uporabnika preusmeri v VLAN BlackHole. Preverjanje naj poteka na WDC-1.
2. Dodajte interni spletni strežnik podjetja na L-WEB.
 - a. Dodajte spletno stran »intranet.{šola}.n-sim.si«.
 - b. Iz varnostnih razlogov naj bo dostopna samo preko HTTPS protokola.
 - c. CA za izdajanje certifikatov prav tako nastavite na L-WEB.
 - d. Certifikatu strežnika morajo zaupati vsi odjemalci, certifikati spletnih strani morajo biti podpisani na strežniku.
 - e. Nastavite avtomatsko preusmeritev iz HTTP na HTTPS.
 - f. Za novo spletno stran nastavite preverjanje uporabniških imen in gesel preko strežnika WDC-1.
 - g. Spletna stran naj prikazuje napis "Dobrodošli na intranet!"
3. Site-to-Site VPN tunel iz dneva 1 nadgradite z uporabo certifikatov s strežnika L-WEB namesto uporabe ključa v skupni rabi ("pre-shared key").
4. Vse omrežne naprave naj vsako uro pošljejo back-up svojih nastavitvev na TFTP strežnik na naslovu »tftp.n-sim.si«.
5. Za varnost na strežniku »L-WEB« poskrbimo s požarnim zidom (iptables).
 - a. Dostop do spletnega in poštnega je dovoljen ne glede na izvor.
 - b. Dostop do TFTP strežnika je dovoljen samo iz omrežij podjetja.
 - c. SSH dostop do strežnika je dovoljen le iz omrežij na lokaciji glavne pisarne in preko oddaljenega dostopa (VPN).
 - d. Ostali promet je prepovedan, če nikjer v nalogi ni eksplicitno zahtevan.
6. Nadgradite IP telefonijo z možnostjo:
 - a. Parkiranja klicev na številko X111
 - b. Klicanja navzven: klice na številko 911 preusmerite na naslov »sos.n-sim.si«. V testne namene lahko naročite reševalno vozilo.
7. Na strežniku WDC-2 za nadzor nad Windows strežniki v podjetju namestite Windows Admin Center in vanj dodajte vse strežnike z operacijskim sistemom Windows. Nastavite alarm, ki v primeru uporabe več kot 60% pomnilnika na WDC-1 ali WDC-2 pošlje e-poštno sporočilo vsem uporabnikom organizacijske enote Staff.

S tem se zaključí 2. dan tekmovanja. Sodniki bomo pri preverjanju VEDNO uporabljali imena storitev namesto IP naslovov. Ocenjuje se funkcionalnost podjetja, ne nastavitve. Močno priporočeno je, da na zadnjih straneh izpolnite tabelo z IP naslovi, saj lahko ta sodnikom pomaga razumeti vašo rešitev.

"The Problem with SSL jokes is that you must get someone else to vouch for you before you can tell the joke."



DOKUMENTACIJA / ZAPISKI

