

Nastavni predmet:	OPERACIJSKI SUSTAVI
Vježba: 07	Sigurnost Windows operacijskog sustava
Cilj vježbe:	Upoznati učenike s ispravnim postavljanjem konfiguracije i sigurnošću Windows operacijskog sustava

PRIPREMA ZA VJEŽBU

Proučiti osnovne pojmove vezane uz sigurnost Windows operacijskog sustava.

IZVOĐENJE VJEŽBE

Postupke, korištene naredbe i dobivene rezultate zadataka zapisivati u bilježnicu te odgovoriti na postavljena pitanja vezana uz vježbu.

Zadatak 1: Korisnički račun bez lozinke

Pokrenuti Windows 7 operacijski sustav.

Ulogirati se kao korisnik koji ima administratorske ovlasti.

U korijenskom direktoriju kreirati direktorij **OS_LV07**.

Za direktorij **OS_LV07** postaviti sva prava za sve korisnike – ako to već nije postavljeno.

a) Kreirati korisnika **ALFA**.

Pokrenite komandnu liniju s **administratorskim ovlastima**:

Start->upisati cmd->desni klik na cmd->odabrati Run as administrator

U komandnu liniju upisati naredbe:

net user ALFA /ADD

U komandnu liniju upisati naredbu:

net user

Da li je stvoren novi korisnik?

Pogledajte trenutne postavke stvorenog računa **ALFA**:

net user ALFA

Izaći iz komandne linije naredbom **exit**.

Zadatak 2: Instalacija Microsoft Baseline Security Analyzer-a

Pozicionirati se u direktorij **OS_LV07**.

U direktoriju **OS_LV07** kreirati poddirektorij **MBSA**.

Pokrenuti instalaciju aplikacije **Microsoft Baseline Security Analyzer 2.3.**

Kliknuti **Next.**

Prihvatite ponuđenu licencu.

Kliknuti **Next.**

Instalirati aplikaciju Microsoft Baseline Security Analyzer 2.3. u poddirektorij **MBSA** koji se nalazi unutar direktorija **OS_LV07.**

Kliknuti **Browse** i odabrati željeni direktorij.

Kliknuti **Next.**

Kliknuti **Install.**

Pojavit će se poruka **Microsoft Baseline Security Analyzer Setup has completed successfully.**

Kliknuti **Ok.**

Zadatak 3: Skeniranje korištenjem Microsoft Baseline Security Analyzer-a

a) Pokrenuti **Microsoft Baseline Security Analyzer 2.3.**

b) Skenirati računalo.

Odabrati opciju **Scan a computer.**

U bilježnicu zapisati opcije koje određuju što će sve biti skenirano.

Ostaviti početne postavke skeniranja.

Kliknuti **Start Scan.**

c) Nakon obavljenog skeniranja pod **Windows Scan Results** pogledati **Local Account Password Test Issue.**

Kliknuti na ponuđene opcije **What was scanned, Result Details, How to correct this.**

U bilježnicu napisati što je navedeno pod **Result Details.**

d) Pogledati **Password Expiration Issue.**

Kliknuti na ponuđene opcije **What was scanned, Result Details, How to correct this.**

U bilježnicu napisati što je navedeno pod **Result Details.**

Zadatak 4: Security Identifier (SID)

a) Ulogirati se kao korisnik koji ima **administratorske** ovlasti.

Kreirati novog korisnika **OMEGA.**

Pozicionirati se u:

Start->Computer-> desni klik miša->odabrati Manage->Local Users and Groups->desni klik na Users->New User

Upisati naziv korisničkog računa: **OMEGA.**

Korisničkom računu dodijelite lozinku **omega**.

Potvrdite dodijeljenu lozinku.

Isključite opciju **User must change password at next login**.

Uključite opciju **Password never expires**.

Odaberite opciju **Create**.

b) Ulogirajte se kao korisnik **OMEGA**.

Pozicionirajte se u direktorij **OS_LV07** i stvorite datoteku **omega** i poddirektorij **OMEGA**.

c) Pogledajte tko je vlasnik stvorene datoteke **omega** i poddirektorija **OMEGA**:

**omega->Properties->odabrati tab Security-> kliknuti na Advanced->otvoriti tab Owner
OMEGA ->Properties->odabrati tab Security-> kliknuti na Advanced->otvoriti tab Owner**

d) Odlogirati se iz računa **OMEGA**.

e) Ulogirati se kao korisnik koji ima **administratorske** ovlasti.

f) Obrisati korisnički račun **OMEGA**:

Start->Computer-> desni klik miša->odabrati Manage->Local Users and Groups->dvoklik na Users-> desni klik na OMEGA ->Odabrati Delete

Pročitati upozorenje!

Kliknuti **Yes**.

g) Pozicionirajte se u direktorij **OS_LV07** i pogledajte tko je sada vlasnik stvorene datoteke **omega** i poddirektorija **OMEGA**.

h) Prepishite broj koji se tamo nalazi.

Taj broj predstavlja **SID** (engl. security identifier), a koriste ga liste pristupa (ACL) za identifikaciju npr. nekog korisnika.

Zadatak 5: Pregled SID-ova

a) Pogledati popis dodijeljenih **SID-ova**:

Start -> upisati regedit -> kliknuti Enter -> odabrati Yes

U **Registry Editoru** odabrati:

Computer -> HKEY_LOCAL_MACHINE -> SOFTWARE -> Microsoft -> Windows NT -> CurrentVersion -> ProfileList

U bilježnicu zapisati što se pojavilo!

b) Kliknuti na jedan kraći i jedan dulji **SID** i pogledati što piše desno pod poljem **ProfileImagePath**.

Možemo li tako identificirati nekog korisnika?

c) Pokušajte pronaći **SID** vezan uz korisnika **ALFA**.

U bilježnicu zapisati **SID** vezan uz korisnika **ALFA**!

d) Da li je **SID** jedinstven za svakog korisnika?

Sigurnost Windows operacijskog sustava

Komentirati u bilježnicu!

e) Pokušajte pronaći **SID** vezan uz korisnika **OMEGA** kojeg ste obrisali (taj **SID** ste već zapisali u zadatku 4).

Da li je taj **SID** u listi ponuđenih **SID-ova**?

Ako je, komentirati u bilježnicu zašto?

f) Kako to da su neki **SID-ovi** jako kratki, a ostali dulji? Koja je razlika?

Komentirati u bilježnicu?

Zadatak 6: Korisnik OMEGA (SID)

a) Ulogirati se kao korisnik koji ima **administratorske** ovlasti (ako već niste ulogirani kao **administrator**).

Ponovo kreirati korisnika **OMEGA**.

Pozicionirati se u:

Start->Computer-> desni klik miša->odabrati Manage->Local Users and Groups->desni klik na Users->New User

Upisati naziv korisničkog računa: **OMEGA**.

Korisničkom računu dodijelite lozinku **omega**.

Potvrdite dodijeljenu lozinku.

Isključite opciju **User must change password at next logon**.

Uključite opciju **Password never expires**.

Odaberite opciju **Create**.

b) Ulogirajte se kao korisnik **OMEGA**.

c) Pozicionirajte se u direktorij **OS_LV07** pogledajte tko je sada vlasnik stvorene datoteke **omega** i poddirektorija **OMEGA**:

omega->Properties->odabrati tab Security-> kliknuti na Advanced->otvoriti tab Owner

OMEGA ->Properties->odabrati tab Security-> kliknuti na Advanced->otvoriti tab Owner

Komentirati u bilježnicu!

d) Odlogirati se kao korisnik **OMEGA** i ulogirati se kao korisnik koji ima **administratorske** ovlasti.

e) Ponovo pogledati popis dodijeljenih **SID-ova**:

Start -> upisati regedit -> kliknuti Enter -> odabrati Yes

U **Registry Editoru** odabrati:

Computer -> HKEY_LOCAL_MACHINE -> SOFTWARE -> Microsoft -> Windows NT -> CurrentVersion -> ProfileList

Da li je korisnik **OMEGA** dobio novi jedinstveni **SID**?

Komentirati u bilježnicu!

Zadatak 7: Local Security Policy

a) Pokrenuti **Local Security Policy**:

Start -> Control Panel -> Administrative Tools -> dvoklik na Local Security Policy

b) Dvoklik na **Local Policies** -> Dvoklik na **User Rights Assignment**

Na desnoj strani će se pojaviti dva stupca **Policy** i **Security Settings**.

c) **Desni klik na Access this computer from the network -> odabrati Properties -> kliknuti na tab Explain.**

Pročitati čemu služe ove postavke.

Vratiti se na tab **Local Security Setting**.

Uočite da su navedeni tipovi korisničkih računa koji preko mreže mogu pristupiti računalu.

U bilježnicu zapisati da li to predstavlja sigurnosni problem?

Da li bi s liste uklonili neki od navedenih tipova korisničkih računa?

d) **Desni klik na Allow log on locally -> odabrati Properties**

Iz liste navedenih tipova korisničkih računa maknuti **Guest** račun:

Kliknuti na Guest -> Remove -> Kliknuti Apply -> kliknuti OK

U bilježnicu odgovoriti kakav je to **Guest** korisnički račun i da li je potreban!

e) **Desni klik na Allow log on through Remote Desktop Services -> odabrati Properties**

U tabu **Explain** pogledati čemu služe ove postavke.

Vratiti se na tab **Local Security Setting**.

Označite sve navedene tipove korisničkih računa i kliknite **Remove** pa **Ok**.

Da li je ovo poboljšalo sigurnosne postavke računala?

f) **Desni klik na Deny access to this computer from the network -> odabrati Properties**

U tabu **Explain** pogledati čemu služe ove postavke.

Vratiti se na tab **Local Security Setting** te uočiti da je naveden samo **Guest** tip korisničkog računa.

Što ako želimo da nitko ne pristupa računalu preko mreže. U tom slučaju treba na listu dodati **Everyone** tip korisničkog računa.

Kliknuti Add User or Group -> kliknuti na Advanced -> kliknuti na Find Now

Pojaviti će se popis korisničkih računa.

Odabrati **Everyone** i dva puta kliknuti **OK**.

Sada je i **Everyone** račun dodan na listu.

Da li je odabir ove opcije ojačao sigurnost računala?

g) **Desni klik na Deny log on through Remote Desktop Services -> odabrati Properties**

U tabu **Explain** pogledati čemu služe ove postavke.

Dodati **Everyone** na listu.

h) **Kliknuti na Local Policies -> Security Options**

Desni klik na Interactive logon: Do not require CTRL + ALT + DELETE -> odabrati Properties

U tabu **Explain** pogledati čemu služe ove postavke.

Ako ovdje odaberemo opciju Disabled da li je to ojačalo sigurnosne postavke?

Provjera znanja:

- 1) Čemu služi Microsoft Baseline Security Analyzer ? (1 bod)
- 2) Što je SID? (1 bod)
- 3) Od čega se sastoji SID? (1 bod)
- 4) Ostaje li SID nakon brisanja korisnika? (1 bod)
- 5) Mogu li dva korisnika imati isti SID? (1 bod)
- 6) Što je Local Security Policy? (1 bod)

Ocjene: 6 bodova = 5 ; 5 bodova = 4 ; 4 boda = 3 ; 3 boda = 2 ; <3 boda = 1