HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost Samba poslužitelja

CCERT-PUBDOC-2006-08-165

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

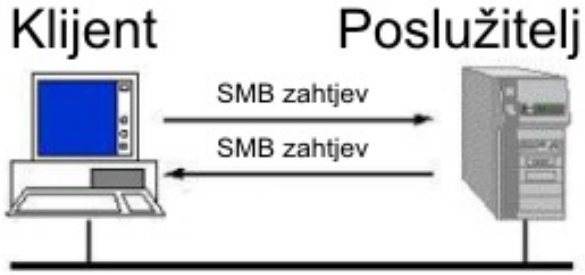
LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Samba poslužitelj predstavlja skup Linux (Unix) modula koji omogućavaju komunikaciju SMB (eng. *Server Message Block*) protokolom Linux operacijskim sustavima. SMB protokol uobičajeno koriste Windows operacijski sustavi za međusobnu komunikaciju te za dijeljenje datotečnih sustava i pisača. Podržavajući SMB protokol, Samba omogućava računalima s Linux operacijskim sustavima sudjelovanje u dijeljenju mrežnih resursa s računalima koja koriste Windows operacijske sustave.

Korištenjem Samba poslužitelja, moguće je dijeliti jedan ili više direktorija, dijeliti više datotečnih sistema, dijeliti pisače u mreži, rješavati probleme na klijentskim računalima preko mreže, provoditi autentikaciju klijenata na Windows domeni ili omogućiti korištenje WINS (eng. *Windows Internet Name Service*) servisa koji kontrolira računala koja međusobno komuniciraju. Za svaku od navedenih stavki postoje različiti oblici prijetnji. Sigurnosne prijetnje mogu biti vanjski zlonamjerni korisnici koji nemaju nikakav pristup u mrežu, ali i unutarnji koji nastoje povećati svoje ovlasti te pristupiti određenim resursima za koje nemaju potrebna ovlaštenja. Stoga Samba mora sadržavati širok spektar zaštitnih mehanizama. U ovom dokumentu opisani su osnovni sigurnosni elementi koje Samba pruža u svrhu sigurnosne zaštite.



Slika 1: Komunikacija računala SMB protokolom

2. Samba poslužitelj

Samba poslužitelj se koristi u situacijama gdje je potrebno međusobno dijeliti računalne resurse u kombiniranoj Windows i Linux (Unix) okolini. On predstavlja skup međusobno povezanih modula koji omogućuju dijeljenje računalnih resursa između Windows i Linux klijenata.

Osnovni razlog zbog kojeg je potrebno korištenje Samba poslužitelja za integraciju Linux sustava u Windows okolinu je taj što Microsoft koristi nešto drugačije protokole i servise koji omogućuju mrežnu komunikaciju među računalima u odnosu na ostale operativne sustave. Osnovni protokol koji omogućuje međusobno dijeljene resursa između Windows računala je već spomenuti SMB protokol koji koristi NetBIOS (eng. *Network Basic I/O System*) te druge protokole niže razine, kako bi se omogućilo lociranje i međusobna komunikacija između pojedinih računala. Takav pristup komunikaciji se bitno razlikuje u odnosu na klasične mrežne protokole (TCP, UDP), koji su implementirani kod većine drugih operacijskih sustava, što je u osnovi izvor svih problema u komunikaciji između Windows i Linux sustava. Razlog tomu je taj što su Microsoft-ovi protokoli bili prvenstveno namijenjeni za korištenje u Microsoft baziranim LAN mrežama.

Samba programski paket se sastoji od više modula koji su određeni za obavljanje dijela poslova:

- Najvažniji modul je `smbd` poslužitelj (radi na TCP portu 137) koji razgovara s klijentima putem SMB protokola te omogućava međusobnu komunikaciju i dijeljenje resursa između računala.
- `nmbd` je drugi po važnosti modul iz Samba programskog paketa, a uloga mu je obavljanje poslova vezanih uz prevođenje NetBIOS imena. Ovaj modul radi na TCP portu 139 i stalno osluškuje mrežni promet te ukoliko na mreži čuje zahtjev za pristup sa svojim NetBIOS imenom, on odgovara svojom IP adresom kako bi računalo koje je uputilo zahtjev zna kome treba slati daljnje pakete.
- `smbclient` je klijentski program za pristupanje resursima drugog računala kojima je dozvoljen pristup. Komande su intuitivne i slične FTP komandama, što olakšava njegovo korištenje.
- `nmblookup` je program koji omogućuje otkrivanje IP adrese računala kojemu se želi pristupiti, na temelju njegovog NetBIOS imena.
- `smbstatus` je programski modul koji omogućuje davanje informacija o trenutnim vezama prema Samba poslužitelju.
- `testparm` je program za provjeru regularnosti napisane ili naknadno modificirane `smb.conf` konfiguracijske datoteke Samba poslužitelja.

Prilikom korištenja Samba paketa, mogu se javiti problemi u radu uzrokovani nepotpunom kompatibilnošću Windows i Linux mrežnih protokola. Najviše problema u konfiguraciji Samba poslužitelja i međusobne povezanosti Windows i Linux platforme, može biti s problemom kriptiranja korisničkih zaporki. Ukoliko korisnik na Windows računalu koristi kriptiranu zaporku, tad mu se na Samba poslužitelju mora dodijeliti virtualni korisnički račun. Ukoliko se s udaljenog računala želi pristupiti Samba poslužitelju, potrebno se je prvo prijaviti s originalnim Windows korisničkim imenom što će na Samba poslužitelju inicirati poljem za unos naknadno dodijeljene virtualne zaporke u koju se upisuje zaporka na Linux računalu nakon čega se korisniku u potpunosti dozvoljava pristup Samba poslužitelju ili nekom drugom stroju. Pošto Windows i Linux platforma koristi različite algoritme za kriptiranje zaporki, sa strane Linux poslužitelja biti će potrebno generirati posebnu SMBPASSWD datoteku u kojoj su sadržana imena korisnika s kriptiranim zaporkama koje odgovaraju Windows sistemu enkripcije.

Najčešća primjena Samba poslužitelja je u sustavu dijeljenja pisača. Ukoliko je pisač spojen na Samba poslužitelj onda ga mogu koristiti i druga računala u mreži neovisno o operativnom sustavu koji koriste. Svi klijenti u tom slučaju trebaju imati ispravno podešene upravljačke programe za navedeni printer. Veza od računala do pisača odvija se u 4 koraka:

- otvara se veza prema Samba poslužitelju,
- željena datoteka za ispis se kopira preko mreže na Samba poslužitelj,
- zatvara se veza s poslužiteljem,

- Samba poslužitelj šalje kopiju datoteke na pisač i nakon toga ju briše.

Korištenje jednog ili više Samba računala kao poslužitelja za pisače daje fleksibilnost lokalnoj mreži. Pisače se vrlo lako može rasporediti na različite korisnike ili se korištenje može dozvoliti svima. Također, pristup pisaču se može ograničiti samo na par korisnika korištenjem opcije „*valid user*".

3. Sigurnosni elementi Samba poslužitelja

3.1. Kontrola inicijalnog pristupa Samba poslužitelju

Samba poslužitelj podržava široki spektar za kontrolu pristupa klijenata. Poslužitelj može biti konfiguriran s vrlo slabim sigurnosnim restrikcijama, ali isto tako moguće je podesiti vrlo kompleksne sigurnosne politike za kontroliranje klijentskog pristupa.

Postoje dva glavna tipa kontrole pristupa Samba poslužitelju:

- restrikcije bazirane na klijentskom računalu s kojeg korisnik pristupa poslužitelju i
- restrikcije bazirane na korisničkom imenu i zaporci korisnika koji pristupa Samba poslužitelju.

Ukoliko se koriste restrikcije bazirane na korisničkom računalu s kojeg korisnik pristupa poslužitelju, tada mu se dodjeljuju lokalna prava i unaprijed definiraju dozvoljene i nedozvoljene radnje kako bi se smanjila korupcija podataka. Pošto se određenim tehnikama iste restrikcije mogu zaobići, pribjegava se drugom načinu restrikcija baziranim na korisničkom imenu i zaporci korisnika koji pristupa Samba poslužitelju pri čemu se podaci o dozvoljenim i nedozvoljenim radnjama nalaze pohranjeni na Samba poslužitelju. Iako Windows operacijski sustavi koriste drugu metodu, metoda kontrole pristupa preko klijentskog računala može biti izuzetno korisna pa je u pravilu uvijek korisno koristiti i ovu metodu kao nadogradnju na kontrolu pristupa preko korisničkog imena i zaporke. U praksi je preporučljivo koristiti oba tipa kontrole sa ciljem povećanja sigurnosti sustava i sprečavanja namjerne ili nenamjerne greške od strane korisnika.

3.1.1. Ograničavanje pristupa prema mrežnim sučeljima

Neki Samba poslužitelji posjeduju više od jednog mrežnog sučelja. Jedno preko kojeg je poslužitelj spojen na mrežu za koju mora biti dostupan, a ostala za mreže za koje nije dostupan. U tom je slučaju poželjno vezati (eng. *bind*) poslužitelj samo uz ona mrežna sučelja koja ga stvarno trebaju. Za ovakve potreba Samba podržava dva globalna parametra koja omogućavaju ovakvu konfiguraciju:

- **interfaces** – ovim parametrom je moguće specificirati mrežna sučelja uz koja će se vezati Samba poslužitelj,
- **bind interfaces only** – prethodni parametar **interfaces** sam po sebi nema učinka ako se ovaj parametar ne postavi na istinitu vrijednost (`bind interfaces only = yes`) kako bi se onemogućio pristup poslužitelju s drugih mrežnih sučelja.

Kako neki mrežni poslužitelji posjeduju mogućnost komuniciranja preko više od jednog mrežnog sučelja, tako tu mogućnost posjeduje i Samba. Ukoliko je u radu potrebno koristiti više od jednog mrežnog sučelja, tada je to potrebno u Samba poslužitelju dodatno specificirati. Sličan efekt može se postići i korištenjem vanjskih alata kao što je `iptables`, alat za filtriranje mrežnih paketa. U pravilu je poželjno koristiti više slojeva zaštite, tako da u slučaju kada jedan sloj zakaže, ostali još uvijek mogu spriječiti neautorizirani pristup poslužitelju.

3.1.2. Ograničavanje pristupa računalima

Kada klijentsko računalo uspostavi konekciju sa Samba poslužiteljem, ono poslužitelju mora proslijediti svoju IP adresu kako bi poslužitelj znao kamo mora vratiti podatke. Ovo omogućava konfiguriranje poslužitelja tako da ne odobrava pristup s neautoriziranih IP adresa.

Parametri koje je moguće koristiti prilikom konfiguracije pristupa klijentskih računala su:

- **allow trusted domains** – kada je ovaj parametar postavljen na `Yes` Samba poslužitelj prihvaća konekcije sa svih klijenata koji se nalaze u domenama kojima vjeruje domenski kontrolor. Ako je ovaj parametar postavljen na `No`, Samba poslužitelj prihvaća samo konekcije s računala koja se nalaze u istoj domeni kao i sam poslužitelj. Ukoliko Samba

poslužitelju pristupi računalo izvan navedenog opsega IP adresa uskraćuje mu se pristup i o tome se vodi zapis u log datoteci iz koje se naknadno mogu dobiti podatke o eventualnim pokušajima ulaza u sistem.

- **host equiv** – ovim parametrom se mogu specificirati računala ili korisnici kojima će Samba poslužitelj vjerovati bez da ih pita za korisničko ime i zaporku pa stoga ovu opciju sa sigurnosnih aspekata nije preporučljivo uključivati. Ovim parametrom minimalno se povećava brzina Samba poslužitelja, ali se istovremeno narušava stupanj sigurnosti i ukoliko se doista želi koristiti, onda je to preporučljivo samo na lokalnoj mreži do par računala koja po mogućnosti nisu spojena na Internet.
- **use rhost** - u slučaju kada je ova opcija postavljena na `Yes`, individualni korisnici mogu kreirati svoje `.rhost` datoteke unutar kojih mogu specificirati IP adrese računala za koje će pristup biti omogućen bez daljnje autentikacije. Jednako kao i `host equiv`, ovu opciju se iz sigurnosnih razloga ne preporuča koristiti.
- **hosts allow** – ovim parametrom moguće je specificirati jedno ili više računala kojima će biti omogućen pristup Samba poslužitelju (eng. *whitelist*), dok će svim ostalim računalima pristup biti zabranjen. Ovom opcijom se sprečava opterećenje Samba poslužitelja, a povećava se njegova učinkovitost i stupanj sigurnosti. Ovaj način zaštite je preporučljiv u kompleksnim mrežnim sistemima kako bi se povećala učinkovitost i smanjila redundancija podataka uzrokovana velikim brojem upita.
- **hosts deny** – ovim parametrom moguće je eksplicitno zabraniti pristup poslužitelju s nekih određenog klijentskog računala (eng. *blacklist*). U praksi se ova naredba koristi ukoliko je korisnik s navedenog računala prekršio politike za pristup podacima i na neki način korumpirao podatke. Time se povećava brzina Samba poslužitelja i povećava opći nivo sigurnosti.

3.1.3. Autentikacija korisnika pomoću korisničkog imena i zaporke

Samba poslužitelj koristi uobičajenu metodu autentikacije korisnika putem njihovog korisničkog imena i zaporke. Prilikom autentikacije korisnika postoje dva osnovna sigurnosna modela koja definiraju način na koji će Samba poslužitelj štititi pristup dijeljenim resursima. Prvi je tzv. *share* model kod kojeg se svaki dijeljeni resurs štiti individualno, sam za sebe, dok je drugi tzv. *user* model kod kojeg se ispravno autenticiranom korisniku daje pristup svim dijeljenim resursima. Opcija kojom je moguće definirati metodu autentikacije i autorizacije korisnika je `security`, a njene moguće vrijednosti su:

- `Share` – prilikom pristupa korisnika dijeljenom resursu Samba zahtijeva samo zaporku, tj. korisnik ne mora unositi i svoje korisničko ime. Ako je zaporka valjana korisniku se odobrava pristup traženom resursu. Ovakav način rada indicira da Samba mora sama saznati koje korisničko ime klijent treba koristiti. Pri tome Samba može koristiti eventualno poslano korisničko ime, neko od prethodnih korisničkih imena, klijentovo NetBIOS ime, naziv direktorija kojem se pristupa ili neko od korisničkih imena iz `smb.conf` konfiguracijske datoteke. Ukoliko lista mogućih korisničkih imena nije dostupna, Samba obavlja sistemski upit kako bi saznao kojem korisniku odgovara zaprimljena zaporka. Pri tome se provjeravaju datoteke poput `/etc/passwd` i `/etc/group`, a ako one nisu raspoloživi tada se provjeravaju drugi izvori poput NIS (eng. *Network Information Service*) ili LDAP (eng. *Lightweight Directory Access Protocol*).
- `User` – ukoliko se koristi ovaj model, korisnik zajedno sa svojom zaporkom mora Samba poslužitelju proslijediti i svoje korisničko ime. Svaki korisnik kojem se želi omogućiti pristup dijeljenim resursima mora imati svoj korisnički račun na poslužitelju.
- `Server` – u ovom modelu rada Samba se ponaša jednako kao i kad se koristi opcija `User`, s tom iznimkom da se zahtjevi za autentikaciju prosljeđuju domenskom kontroloru. Samba poslužitelj klijentu javi kako radi u `User` modu te potom primljeni par korisničkog imena i zaporke prosljeđuje poslužitelju za autentikaciju koji može biti Windows ili Samba poslužitelj. Ovo doduše ne znači da korisnici kojima je potreban pristup Samba poslužitelju ne moraju imati otvorene korisničke račune. Korisnički računi su i dalje potrebni, samo što je posao autentikacije korisnika prebačen na drugi poslužitelj.

- `Domain` – ovaj model rada jednak je `Server` načinu rada samo što je u ovom slučaju Samba poslužitelj sastavni dio NetBIOS domene. Isto tako, u ovom modu rada koriste se neke naprednije funkcije NetBIOS protokola kao što su tokeni koji se izdaju klijentima nakon autentikacije pa nema potrebe za ponovnom autentikacijom prilikom pristupa nekom drugom dijeljenom resursu. `Domain` način rada omogućava mehanizam za spremanje svih korisničkih i grupnih računa na centralizirano dijeljeno mjesto koje je dijeljeno između domenskih kontrolora. Primarni domenski kontrolor (eng. PDC - *Primary Domain Controller*) je poslužitelj koji je zadužen za osiguravanje integriteta baze s korisničkim računima. Pomoćni domesnki kontrolori (eng. BDC - *Backup Domain Controller*) zaduženi su samo za proces prijave i autentikacije.
- ADS (eng. *Active Directory Services*) – ovaj način rada pretpostavlja uključivanje Samba poslužitelja u ADS sustav (omogućava pristup pomoću protokola poput Kerberos i LDAP-a), korištenjem NT4 RPC bazirane sigurnosti.

Uz ove osnovne načine autentikacije, Samba pruža mogućnost podešavanja i nekih drugih parametara koji utječu na autentikaciju korisnika. To su:

- **min password length** – ovom opcijom se podešava minimalni broj znakova koje Samba prihvaća za korisničke zaporke koje nisu kriptirane. Predefinirana minimalna vrijednost je 5 znakova.
- **null passwords** – ako je ova opcija postavljena na `Yes`, pristup korisničkim računima koji nemaju podešenu zaporku je omogućen bez korištenja zaporke.
- **password level** – SMB/CIFS (eng. *Common Internet File System*) kod Windows 9x i Me sustava koristi zaporke kod kojih se velika i mala slova jednako prezentiraju (npr. zaporka = ZaPoRkA) što nije slučaj i s Linux operacijskim sustavima. Stoga je parametar **password level** potreban kako bi uskladio tu razliku, ali je primjenjiv samo na nekriptiranim zaporkama. Kad primi zaporku Samba poslužitelj isprobava sve moguće kombinacije velikih i malih slova dok ne pogodi pravu.
- **username level** – ovaj parametar omogućava istu funkcionalnost kao i prethodni s tim da se ne odnosi na zaporku već na korisničko ime.
- **restrict anonymus** – ako je ovaj parametar postavljen na `Yes`, Samba ne dozvoljava anonimne konekcije na poslužitelj.
- **revalitade** - ovaj parametar može se koristiti samo ako je opcija `security` postavljena na `User`. Ako je ovaj parametar postavljen na `No`, korisnik se neće morati ponovno autenticirati prilikom uspostave konekcije na novi dijeljeni resurs. U protivnom je prilikom svakog novog pristupa nekom dijeljenom resursu potrebno obaviti autentikaciju korisnika. Time se može povećati mrežni promet koji je uzrokovan ponovnim autentikacijama, a u slučajevima kad korisnikov preglednik ne čuva zaporku, korisnik ju mora ponovno unositi.

3.2. Kriptirane i nekriptirane korisničke zaporke

Samba poslužitelj može raditi kako s nekriptiranim korisničkim zaporkama tako i s kriptiranim korisničkim zaporkama. Nekriptirane zaporke se prilikom slanja mrežom ne kriptiraju već se šalju kao običan ASCII tekst. Kriptirane zaporke se s druge strane prije slanja mrežom kriptiraju i samim time štite od krađe. Neke od prednosti korištenja kriptiranih zaporki su:

- **poboljšana sigurnost** – ako se zaporka prije slanja mrežom kriptira, uvelike se otežava njena krađa što je vrlo značajna, ali i potrebna karakteristika ukoliko se pristup Samba poslužitelju mora omogućiti i iz vanjske mreže,
- **manje opterećenje Samba poslužitelja** – ukoliko je korištenje zaporki moguće samo u nekriptiranom obliku, tada se ne koristi opcija **password level** opisana u prethodnom poglavlju pa time Samba poslužitelj ne mora prolaziti kroz sve moguće varijante unesene zaporke,
- **odvajanje Linux i Samba zaporki** – korištenje kriptiranih zaporki omogućava korištenje drugačijih zaporki za Samba poslužitelj te za sam operacijski sustav na kojem se Samba poslužitelj nalazi,

- **Windows kriptiranje zaporki** – u novim verzijama Windows operacijskih sustava kriptiranje zaporki je postavljeno kao dio uobičajene konfiguracije pa se noviji Windows klijenti neće moći spojiti na Samba poslužitelj koji ne koristi kriptirane zaporke ukoliko nisu re-konfigurirani nakon instalacije,
- **potrebno za domene** - domene funkcioniraju s kriptiranim zaporkama i to se ne može promijeniti tako da je u slučaju korištenja domena kriptiranje zaporki nužno.

Unatoč velikim prednostima kriptiranih zaporki, postoje i neki nedostaci:

- **odvajanje Linux i Samba zaporki** – premda ovo može biti prednost, može biti i nedostatak zato što je potrebno održavati dva nezavisna seta zaporki za istu skupinu korisnika,
- **podrška starijih klijenata** – neki stariji klijenti ne podržavaju kriptirane zaporke.

3.2.1. Politike enkripcije

Većina opcija kojima se definira kako će Samba koristiti kriptirane zaporke definirana je u `smb.conf` konfiguracijskoj datoteci. Neke od opcija koje se češće koriste su:

- **encrypt passwords** – ako je ovaj parametar postavljen na `Yes`, Samba će koristiti kriptirane zaporke spremljene u `smbpasswd` datoteci ili na eksternom autentikacijskom poslužitelju (da li će se koristiti eksterni poslužitelj ili `smbpasswd` datoteka, određeno je sa `security` opcijom). Ako je ovaj parametar postavljen na `No`, koriste se nekriptirane zaporke.
- **smb passwd file** – ovim parametrom podešava se ime `smbpasswd` datoteke.
- **update encrypted** – ovaj parametar je namijenjen kao alat za prijelaz sa sustava u kojem su se koristile nekriptirane zaporke na sustav u kojem se koriste kriptirane zaporke. Ukoliko je ovaj parametar postavljen na `Yes` prilikom svakog spajanja korisnika na Samba poslužitelj, pokreće se `smbpasswd` program koji kriptira korisničku zaporku i sprema je u `smbpasswd` datoteku. Ideja je da se prilikom prijelaza sa sustava nekriptiranih na sustav kriptiranih zaporki inicijalno ovaj parametar postavi na `Yes` i drži tako neko vrijeme dok sve korisničke zaporke nisu kriptirane automatski unesene u `smbpasswd` datoteku. Jednom kad je `smbpasswd` datoteka ažurirana sa svim korisničkim zaporkama, ovaj parametar se postavlja na `No` i prelazi se na sustav korištenja kriptiranih zaporki.
- **unix password sync** – ako je ovaj parametar postavljen na `Yes`, Samba će prilikom svake promjene korisničke kriptirane zaporke pokušati promijeniti i korisnikovu Linux zaporku.
- **passwd program** – ovim parametrom se specificira kompletni put do programa koji Linux koristi za mijenjanje korisničkih zaporki.
- **passwd chat** – tipični Linux programi za mijenjanje korisničkih zaporki koriste interaktivni pristup, tj. korisnik preko interaktivnih dijaloga mijenja svoju zaporku. Ovim parametrom se definiraju odgovori na upite Linux programa za promjenu zaporki potrebni za dovršavanje promjene zaporke.

Zajedno sa Samba poslužiteljem dolazi i `smbpasswd` program namijenjen za kreiranje i promjenu kriptiranih korisničkih zaporki. To je ekvivalent Linux `passwd` programu. Program se pokreće iz komandne linije, a opcije koje je pritom moguće koristiti su:

- **-a** – dodaje korisnika u `smbpasswd` datoteku. Program s ovim parametrom može pokrenuti samo administrator (*root* korisnik).
- **-d** – isključuje određeno korisničko ime. Svaki pokušaj spajanja korisnika koji je isključen neće uspjeti. Samo administrator može pokrenuti program s ovom opcijom.
- **-e** – suprotno od **–d** opcije. Ovim parametrom se ponovno omogućava pristup određenom korisniku. Samo administrator može pokrenuti program s ovim parametrom.
- **-D** *razina_analize* – ovim parametrom se podešava razina log poruka `smbpasswd` programa (0-najniža, 10-najviša). Opcija može biti korisna ukoliko dođe do problema u korištenju programa.
- **-n** – ovaj parametar može koristiti samo administrator, a on omogućava da se određenom korisniku pridijeli prazna zaporka (korisnik ne mora unositi zaporku prilikom spajanja na poslužitelj).
- **-r** *ime_računala* – korištenjem ovog parametra može se podesiti zaporka na udaljenom stroju koji može biti ili drugi Samba poslužitelj ili Windows poslužitelj.

- **-U** *korisničko_ime* – ovaj parametar koristi se zajedno s **–r** parametrom i njime se specificira korisničko ime korisnika čija zaporka se želi modificirati.
- **-h** – ako je `smbpasswd` program pokrenut s ovom opcijom na ekranu se ispisuje sažetak svih opcije koje je moguće koristiti (eng. *help*).
- **-s** – ako se koristi ovaj parametar, `smbpasswd` će koristiti standardni ulaz i izlaz umjesto `/dev/tty` (tipkovnica i zaslon). Ovaj parametar je koristan u slučaju kada je potrebno automatizirati promjene korisničkih zaporki pomoću skripti.

Prilikom konfiguracije Samba poslužitelja za korištenje kriptiranih zaporki potrebno je obaviti nekoliko koraka:

- kreirati `smbpasswd` datoteku,
- popuniti `smbpasswd` datoteku korisničkim zaporkama,
- rekonfigurirati Samba poslužitelj da koristi smbpasswd datoteku (postavljanje opcije `encrypt passwords=Yes`),
- konfigurirati mrežne klijente da koriste kriptirane zaporke (za novije verzije Windows klijenata ovo je standardna opcija tako da ih nije potrebno modificirati).

3.3. Vlasništvo i dozvole nad datotekama

Jedan od važnijih aspekta sigurnosti Samba servera je dodjela vlasništva i dozvola nad datotekama. Samba koristi mnogo parametara kojima se određuju prava pristupa. U ovom dijelu su opisani ti parametri.

Prilikom postavljanja parametara kojima se određuje vlasništvo i dozvole pristupa datotekama, moguće je postaviti više pitanja koja služe kvalitetnijem postavljanju parametra nad datotekama: Da li korisnik ima potrebu korištenja sustava iz komande linije, može li iz nje stvarati kratice ili brisati datoteke iz mapi sa zabranom brisanja datoteci? Osim toga postavlja se pitanje dodjele privilegija. Ukoliko korisnik preko Sambe dohvaća link, može li pomoću njega dohvatiti neke druge datoteke za koje inicijalno nema dodijeljena prava? Ukoliko se problem shvaća s razine korisnika, postavlja se pitanje koje privilegije Samba korisnici imaju u pristupu računalu? Tu se postavlja pitanje da li korisnici koriste svoj korisnički račun ili virtualni s drugačijim pravima? Sva navedena pitanja mogu uzrokovati česte intervencije administratora sistema ukoliko se ne uzmu u obzir, a posljedice za sistem mogu postati nesagledive. Samba upravo zbog tih problema koristi kontrolne mehanizme kojima definira parametre nad datotekama:

- **read list** – ovim parametrom se određuje popis korisnika koji imaju samo pravo čitanja nad mapom koja je inicijalno određena za čitanje i pisanje.
- **write list** – ovaj parametar je obrnut od **read list** parametra. Korisnici iz ove liste mogu upisivati podatke u datoteke koje su inicijalno određene samo za čitanje. Ukoliko mapa sadrži postavljene parametre za čitanje i pisanje, onda **write** lista ima prioritet.
- **valid user** – ovim parametrom se određuje lista korisnika s punim pravom pristupa, dok ostali korisnici vide samo naziv mape.
- **invalid users** – ovaj parametar je obrnut od **valid user** parametra. Korisnici iz ove liste imaju zabranu pristupa mapi dok ju svi ostali koriste s dodijeljenim pravima. Ukoliko mapa sadrži postavljene parametre za **valid user** i **invalid user**, tada **invalid user** parametar ima prioritet.

Da bi se povećala sigurnost sustava, u praksi se preporuča korištenje više navedenih parametara čime se osigurava veća sigurnost sustava. Zanimljiv primjer bi mogao biti gdje se u radu koristi mapa s pravom čitanja u kojoj su instalacije programskih paketa. Ukoliko bi se na nju dodijelila prava čitanja nastao bi problem zbog brisanja programskih paketa ili njihovih dijelova. Ukoliko se samo jednoj osobi dozvoli pravo zapisivanja i nadogradnje programskih paketa, onda je uklonjen problem brisanja datoteka.

3.4. Integracija ACL-a sa Samba poslužiteljem

Neki Windows operacijski sustavi podržavaju sigurnosni model naziva ACL (eng. *Access Control List*) kojeg predstavljaju korisnici, grupe koji imaju dozvole čitanja ili zapisivanja u mape kao i u Linux sigurnosnom modelu. Zbog kompleksnije strukture ACL-a, u praksi je otežana implementacija potpune kompatibilnosti s Linux sigurnosnim modelom. ACL je mnogo kompleksniji nego Linux sigurnosni

model pa zbog toga Samba ne podržava ACL u potpunosti, ali Samba omogućuje Windows klijentima pristup Linux sustavu pomoću ACL kontrolnih mehanizama:

- **nt acl support** – ovaj parametar određuje hoće li Samba Windows NT klijentima dopustiti pristup Linux sustavu. Pretpostavljeni parametar je `yes`.
- **security mask –** ovaj parametar određuje dozvole pristupa za Windows NT klijente. Kako bi se definirale maksimalne dozvole pristupa, postavlja se parametar `security mask=0777`.
- **directory security mask** – ovaj parametar je identičan prethodnom, no koristi se za dodjelu prava nad mapama, a ne datotekama.
- **force security mode** – ovaj parametar se koristi za inicijalnu dodjelu prava nad datotekama koju može izmijeniti Windows NT klijent. Početna vrijednost se zadaje parametrom `force create mode=0000` koja označava minimalne ovlasti.
- **force directory security mode** – ovaj parametar je istovjetan prethodnome, no odnosi se na mape, a ne datoteke.

3.5. Korištenje Samba poslužitelja sa SSL-om

Pošto je Samba poslužitelj dizajniran u vrijeme kada su zahtjevi za sigurnosnim aspektima komunikacije bili relativno mali, osim kriptiranja zaporki sam poslužitelj ne podržava enkripciju korisničkih podataka koji se prenose preko mreže. Kako bi se riješio ovaj problem moguće je konfigurirati Samba poslužitelj tako da radi u kombinaciji s nekim od SSL (eng. *Secure Socket Layer*) paketa kao što su SSLeay ili OpenSSL.

Uobičajeno se SSL koristi u sprezi sa certifikatima koje izdaje mjerodavna ustanova (eng. CA - *Certificate Authority*). CA pruža garanciju da je neka organizacija ona za koju se predstavlja. U većini konfiguracija nije potrebno korištenje vanjskih CA-ova. Naime, moguće je generirati vlastite certifikate što najčešće nije dovoljno za šire poslovanje.

Prije korištenja Samba poslužitelja u kombinaciji sa SSL-om, potrebno je prevesti Samba poslužitelj s uključenom podrškom za SSL. Nakon što je poslužitelj preveden sa SSL podrškom, osnovne SSL funkcionalnosti mogu se konfigurirati unutar `smb.conf` datoteke. Opcije koje se mogu koristiti unutar `smb.conf` datoteke, a koje omogućuju SSL podršku su:

- **ssl** – postavljanjem vrijednosti ovog parametra na `Yes` omogućavaju se SSL konekcije,
- **ssl server cert** – specificira potpuni put do datoteke sa SSL certifikatom poslužitelja,
- **ssl server key** - specificira potpuni put do datoteke s privatnim ključem poslužitelja,
- **ssl ca certfile** – specificira lokaciju certifikata svih povjerljivih CA-ova,
- **ssl ca certdir** – specificira direktorij sa certifikatima svih povjerljivih CA-ova,
- **ssl client cert** – specificira datoteku koja sadrži certifikat klijenta,
- **ssl client key** - specificira potpuni put do datoteke s ključem klijenta,
- **ssl require clientcert** – određuje hoće li Samba poslužitelj prihvatiti konekciju klijenta koji ne posjeduje certifikat,
- **ssl require servercert** – određuje hoće li se klijent spojiti na poslužitelj koji ne posjeduje certifikat,
- **ssl hosts** – koristi se kako bi se specificirali klijenti koji moraju koristiti SSL konekciju kako bi se spojili na poslužitelj i ako ovaj parametar nije definiran, Samba poslužitelj zahtijeva da sve konekcije idu preko SSL-a,
- **ssl host resign** –specificira listu klijenata koji ne moraju koristiti SSL konekciju kako bi se spojili na Samba poslužitelj,
- **ssl ciphers** – specificira koji će se sve algoritmi za kriptiranje koristiti prilikom pregovora oko uspostave veze između poslužitelja i klijenta,
- **ssl version** – specificira koja verzija SSL protokola (t1s1, ssl2, ssl3 i ssl2or3) će se koristiti,
- **ssl compatibility** – ovim parametrom moguće je konfigurirati Samba poslužitelj da prihvaća neke starije SSL implementacije ali u velikoj većini slučajeva nije ga potrebno koristiti.

4. Zaključak

Samba programski paket je vrlo moćan alat u slučajevima kada postoji potreba za međusobnim dijeljenjem računalnih resursa između različitih operacijskih sustava. S obzirom da se Samba koristi za dijeljenje resursa kao što su datoteke i pisači, istovremeno se pojavljuju različiti oblici prijetnji Samba poslužitelju jer on radi u vrlo mješovitoj radnoj okolini. Samba zbog toga u sebi sadrži sigurnosne mehanizme kako se ne bi narušio neometani rad sustava. Također, veliki dio odgovornosti leži na timu administratora koji se brine o ispravnom funkcioniranju Samba poslužitelja.

Vrlo često se uočavaju propusti kod Samba poslužitelja s razlogom što ga mnogo klijenta koristi pa se greške lakše i brže detektiraju. Stoga je vrlo važno pravovremeno i ispravno održavati Samba poslužitelj jer se u suprotnom mogu ugroziti vitalni resursi organizacije, a to su u današnje vrijeme informacije zapisane u nekom dijeljenom diskovnom prostoru. U tu svrhu potrebno je omogućiti višeslojnu zaštitu Samba poslužitelja korištenjem prethodno opisanih sigurnosnih elemenata zaštite.

5. Reference

[1] Web stranice Samba poslužitelja, http://www.samba.org, kolovoz 2006.
[2] The Official Samba-3 HOWTO and Reference Guide, http://us2.samba.org/samba/docs/man/Samba-HOWTO-Collection/, kolovoz 2006.
[3] O'Reilly & Associates: Using Samba, 2nd Edition, veljača 2003.
[4] SYBEX Inc: Security Complete Second Edition, kolovoz 2002.