HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Proces autentikacije kod Windows 2000 operacijskih sustava

**CCERT-PUBDOC-2003-03-07**

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

U ovom dokumentu opisani su osnovni postupci autentikacije kod Windows 2000 operacijskih sustava te načini na koje se informacije prikupljene ovim postupcima mogu iskoristiti za praćenje i analizu aktivnosti na sustavu. Iako su ukratko opisani LM i NTLM protokoli korišteni kod starijih Windows platformi (Windows 98, Windows NT), naglasak je dan na Kerberos protokolu, procesu autentikacije primijenjenom kod Windows 2000 sustava.
Analizirani su događaji koji se javljaju u različitim scenarijima postupka autentikacije kod mješovitih Windows sustava, zajedno s pripadajućim pojašnjenjima i log zapisima koji potvrđuju pojedine aktivnosti. U svrhu demonstracije pojedinih događaja uspostavljeno je testno okružje bazirano na kombinaciji Windows NT i Windows 2000 sustava, kojim su simulirane različite mogućnosti autentikacije korisnika u mješovitim Windows okruženjima.
Na kraju dokumenta opisan je način na koji je moguće na Windows 2000 sustavu uspostaviti bilježenje željenih log zapisa u bazu podataka, što se pokazalo kao vrlo praktično rješenje kod većih računalnih mreža. Mogućnost pretraživanja i filtriranja prikupljenih podataka prema različitim kategorijama u tom slučaju uvelike olakšava postupke analize log zapisa, a samim time i detekciju sumnjivih događaja koji mogu upućivati na maliciozne aktivnosti na sustavu.
Na kraju dokumenta korisnik bi trebao biti upoznat s osnovnim načelima postupaka autentikacije kod Windows 2000 sustava te značenjem različitih poruka koje se javljaju kao dio ovog postupka. Uz razumijevanje navedenih elementa, analiza aktivnosti na sustavu te uspostava kvalitetnog i pouzdanog sustava za bilježenje i praćenje log zapisa ne bi trebala predstavljati poseban problem.

# 2. Windows 2000 autentikacija

Kod Windows 2000 operacijskih sustava inicijalno se u svrhu autentikacije mrežnih resursa koristi Kerberos protokol. Kerberos protokol razvijen je na MIT (***M**assachusetts **I**nstitute of **T**echnology*) institutu u sklopu *Athena* projekta započetog 1983. godine, s osnovnim ciljem integracije različitih mrežnih računalnih resursa i procesa (SSO *–single sign-on* procedure*,* mrežni datotečni sustavi, imenički servisi, grafička okruženja i sl.).
Smatra se kako je Microsoft odabrao Kerberos kao glavni proces za autrentikaciju kod W2K platformi iz dva razloga. Prvi je taj što Kerberos omogućuje pouzdanu i dobro isprobanu autentikaciju mrežnih resursa, a drugi je razlog što je Kerberos protokol objavljen pod *Open Source* licencom i bilo ga je moguće modificirati i prilagoditi vlastitim potrebama.
Osim Kerberos autentikacije, Windows 2000 platforme radi kompatibilnosti sa starijim proizvodima podržavaju i LM, NTLM i NTLMv2 postupke autentikacije. U nastavku su razmotrene osnovne karakteristike navedenih procesa.

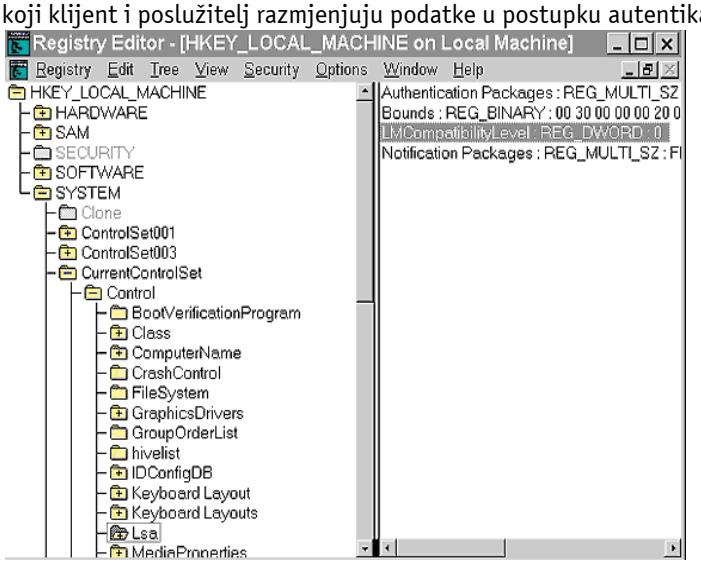
## 2.1. LM, NTLM, NTLMv2 autentikacija

Windows NT 4.0 platforma je do objave SP4 sigurnosne zakrpe podržavala dva načina autentikacije korisnika. To su:

- *Lan Manager challenge/response* autentikacija – postupak podržan radi kompatibilnosti s ranijim *Lan Manager* klijentima na DOS, Windows for Workgroup i Win95 sustavima i,
- *Windows NT challenge/response* autentikacija (NTLM).

Kako bi se omogućila komunikacija sa poslužiteljima koji podržavaju samo LM postupak autentikacije, Windows NT klijenti prije SP4 zakrpe bi istovremeno koristili oba postupka, čak i u situacijama kada bi komunicirali s NT poslužiteljima koji podržavaju noviji NTLM postupak autentikacije.
S obzirom na način na koji LM autentikacija kriptira zaporke i autenticira mrežne resurse, Windows NT platforma je zbog potrebe zadržavanja kompatibilnosti sa starijim Windows sustavima naslijedila i ozbiljne sigurnosne nedostatke.
Iako LM autentikacija koristi *challenge/response* pristup kako bi se izbjegla transmisija korisničke zaporke preko mreže, inherentno su sadržani i propusti koji neovlaštenom korisniku omogućuju da analizom mrežnog prometa (engl. *Sniffing*) kompromitira proces prijavljivanja korisnika u sustav (engl. *Logon*).

Windows NT sustav implementira napredniji NTLM postupak autentikacije, ali zbog problematike kompatibilnosti s ranijim Windows implementacijama sadrži gotovo identične propuste.
Kao potvrda spomenutim sigurnosnim nedostacima može se navesti `L0phtCrack` program od tvrtke *L0pht Heavy Industries*, koji na temelju analize mrežnog prometa pri postupku autentikacije korisnika može rekonstruirati originalnu korisničku zaporku. `L0phtCrack` program se s vremenom razvijao tako da su u novijim inačicama dodane nove mogućnosti i grafičko sučelje koje olakšava korištenje programa manje iskusnim korisnicima.
Objavom SP4 sigurnosne zakrpe za Windows NT operacijske sustave, Microsoft je unio poboljšanja u postojeći NTLM proces autentikacije te novom dorađenom postupku pridijelio naziv NTLMv2. Verzija 2 NTLM postupka unosi brojna poboljšanja vezana uz sigurnost postupka autentikacije sa naglaskom na sigurnosti komunikacijskih veza između klijenta i poslužitelja, povjerljivosti i integritetu podataka, a dodana je i 128-bitna enkripcija.
Navedenim poboljšanjima uklonjeni su neki od propusta unutar samog NTLM protokola, ali su još uvijek ostali problemi vezani uz kompatibilnost s ranijim inačicama, gdje su Windows NT klijenti inicijalno koristili oba postupka autentikacije (LM i NTLM).
Jedini način putem kojeg je bilo moguće utjecati na postupak autentikacije bio je modificiranjem `LMCompatibilityLevel` *registry* ključa (Slika 1). Modificiranjem ove vrijednosti bilo je moguće definirati način na koji klijent i poslužitelj razmjenjuju podatke u postupku autentikacije.




*Slika 1: LMCompatibilityLevel registry ključ*

`LMCompatibilityLevel DWORD` ključ prima vrijednosti od 0 do 5, kojima se može utjecati na nivo kompatibilnosti sa starijim Windows inačicama. Što je veća vrijednost pridjeljenja `LMCompatibilityLevel` parametru to je postignut viši sigurnosni nivo, ali sa manjim stupnjem kompatibilnosti s starijim Windows platformama.
U sljedećoj tablici (**Tablica 1**) dan je kratki opis značenja mogućih vrijednosti `LMCompatibilityLevel` parametra.

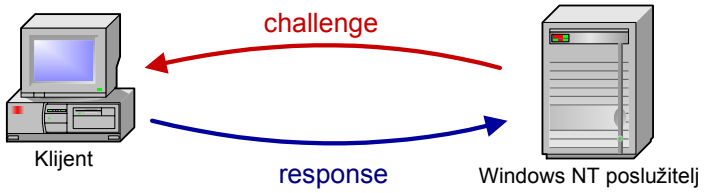
| ***Level*** | **Značenje** |
|---|---|
| *Level 0* | Klijent šalje LM i NTLM *response* nizove. NTLMv2 se nikada ne koristi. |
| *Level 1* | Ukoliko se klijent i poslužitelj dogovore, koristi se NTLMv2 autentikacija. |
| *Level 2* | Koristi se samo NTLM autentikacija. |
| *Level 3* | Koristi se samo NTLMv2 autentikacija. |
| *Level 4* | Domenski poslužitelj (engl. *domain controller*) odbija zahtjeve LM klijenta. |
| *Level 5* | Domenski poslužitelj (engl. *domain controller*) odbija zahtjeve LM i NTLM klijenta. Koristi se isključivo NTLMv2 postupak autentikacije. |

*Tablica 1: Značenje Level parametra LMCompatibilityLevel ključa*

### 2.1.1. Princip rada LM/NTLM/NTLMv2 autentikacije

Postupak autentikacije kod LM/NTLM/NTLMv2 grupe protokola bazira se na *challenge/response* algoritmu. Postupak je sljedeći:

- poslužitelj klijentu šalje slučajni niz znakova (engl. *challenge*);
- klijent kriptira primljeni *challenge* niz sa *hash* funkcijom korisničke zaporke i tako dobiveni niz znakova vraća poslužitelju (engl. *response*);
- poslužitelj dekriptira odgovor i uspoređuje dobivenu vrijednost sa nizom poslanim u prvom koraku;
- ukoliko se nizovi poklapaju, korisnik se smatra autenticiranim.




*Slika 2: LM/NTLM/NTLMv2 postupak autentikacije*

Kao što je ranije spomenuto Windows NT klijenti inicijalno šalju NTLM i LM *response* znakovne nizove kao odgovor na poslužiteljev *challenge* niz, kako bi se održao zadovoljavajući nivo kompatibilnosti s ranijim inačicama.

### 2.1.2. Razlike između LM/NTLM/NTLMv2 autentikacija

- LM (*Lan Manager*) *challenge/response* autentikacija
  LM zaporka bazira se na DOS/OEM skupu znakova, može biti velika do 14 znakova i nije osjetljiva na velika i mala slova. Prije postupka enkripcije svi znakovi se pretvaraju u velika slova.
  Prvih sedam znakova zaporke koristi se za računanje prvih 8 bajtova, a drugih sedam znakova za računanje preostalih 8 bajtova konačne 16-bajtne *Lan Manager One-Way Function* (OWF) zaporke. Ovakav način generiranja zaporke povlači da je zaporke duže od sedam znakova moguće napadati u blokovima od po sedam znakova, što neovlaštenim korisnicima olakšava postupak kompromitiranja zaporke. Za generiranje *OWF* zaporke koristi se DES algoritam u kombinaciji sa korisničkom zaporkom u čistom tekstualnom obliku (engl. *plain text*).
  U prvom koraku postupka autentikacije, poslužitelj klijentu šalje 16-bajtni *challenge* niz. Primljeni *challenge* niz klijent kriptira lokalno pohranjenom 16-bajtnom OWF zaporkom i formira 24-bajtni *response* znakovni niz koji se vraća poslužitelju.
  Programski modul koji je kod NT sustava zadužen za implementaciju postupka autentikacije zove se *Local Security Authority* (`LSA - LSASS.exe`). Spomenuti modul koristi MSV1_0 (`MSV1_0.dll`) paket za autentikaciju koji se sastoji od dva dijela. Prvi dio nalazi se na strani klijenta, dok se drugi dio nalazi na sustavu na kojem je pohranjena SAM (*Security Account Manager*) baza s podacima o mrežnim objektima (korisnički računi, računala, korisničke grupe i sl.). Kod lokalnog prijavljivanja u sustav oba modula MSV1_0 paketa nalaze se na istom računalu.
  Komunikacija između klijenta i poslužitelja prema ranije navedenim koracima odvija se upravo putem spomenutih dijelova MSV1_0 paketa. Klijent poslužitelju šalje podatke o korisničkom računu, domeni zajedno s primljenim *challenge* nizom, nakon čega poslužitelj na temelju primljenog odgovora i vrijednosti pohranjene u lokalnoj SAM bazi provodi autentikaciju korisnika.
- NTLM (NT *Lan Manager*) *challenge/response* autentikacija
  Za razliku od LM zaporke, NT zaporka bazira se na *Unicode* setu znakova i osjetljiva je na velika i mala slova. Maksimalna veličina NT zaporke teoretski je 128 znakova, ali je s obzirom na grafičko sučelje NT sustava ograničena na 14 znakova. Konačni OWF niz dobiva se RSA MD4 enkripcijom.

Sam postupak autentikacije identičan je kao i u prethodnom primjeru, s jedinom razlikom što ovdje poslužiteljski dio MSV1_0 paketa procesira i NTLM OWF i LM OWF zaporke (zbog kompatibilnosti s ranijim Windows platformama).
Iako je NTLM proces autentikacije uklonio neke od sigurnosnih nedostataka prisutnih kod ranijeg LM postupka, problematika kompatibilnosti unijela je nove probleme. Pokazalo se da transmisija i lokalna pohrana LM OWF zaporke omogućuje otkrivanje i NTLM zaporke, što predstavlja ozbiljan sigurnosni nedostatak.

- NTLMv2 (NT *Lan Manager version 2*) *challenge/response* autentikacija
  Kod NTLMv2 procesa autentikacije uvedena je mogućnost kontrole nad postupkom autentikacije. Modificiranjem vrijednosti `LMCompatibilityLevel` ključa moguće je definirati da li će se koristiti LM autentikacija od strane klijenta i poslužitelja. Dodatno je uvedena snažnija 128-bitna enkripcija te su dodana još neka svojstva koja pridonose boljoj sigurnosti algoritma.

### 2.1.3. W2K i LM/NTLM/NTLMv2 autentikacija

Windows 2000 operacijski sustavi su zbog potrebe kompatibilnosti sa ranijim sustavima, podešeni da koriste LM/NTLM/NTLMv2 ili Kerberos kao algoritme za autentikaciju. U sljedećoj tablici (**Tablica 2**) prikazane su moguće kombinacije postupaka autentikacije između različitih Windows platformi:

| | **Win 95** | **Win 98** | **Win 95/ 98 sa AD klijentom** | **Win NT** | **Win 2000** |
|---|---|---|---|---|---|
| **Win 95** | LM | LM | LM | LM | LM |
| **Win 98** | LM | LM | LM | LM | LM |
| **Win 95/98 sa AD klijentom** | LM | LM | LM ili NTLMv2 | LM ili NTLMv2 | LM ili NTLMv2 |
| **Win NT** | LM | LM | LM ili NTLMv2 | NTLM ili NTLMv2 | NTLM ili NTLMv2 |
| **Win2000** | LM | LM | LM ili NTLMv2 | NTLM ili NTLMv2 | Kerberos, NTLM ili NTLMv2 |

*Tablica 2: Moguće kombinacije postupaka autentikacije između različitih Windows platformi*

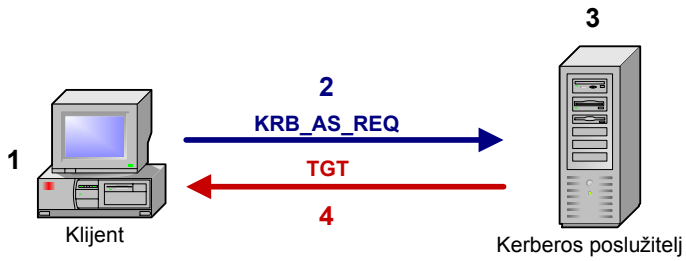
## 2.2. Kerberos

Kerberos je osnovni algoritam za autentikaciju kod Windows 2000 platformi. Prije samog opisa načina na koji Win2000 sustav implementira Kerberos protokol biti će dane neke osnovne napomene vezane uz ovaj "standard".
Kerberos je distribuirani sustav za autentikaciju korisnika i servisa unutar računalnog sustava. Kerberos protokol bazira se na prisustvu trećeg sudionika (engl. *third party*), u ovom slučaju Kerberos poslužitelja, kojem vjeruju svi objekti unutar sustava (korisnici, servisi, itd. - engl. *principals*).
Svi sudionici dijele "tajnu" (engl. *secret*) s Kerberos poslužiteljem i na temelju nje se provodi autentikacia komunikacije s sudionikom. Prednost Kerberos protokola je ta što je isti razvijen s osnovnom pretpostavkom da je računalna mreža nesigurna za transmisiju povjerljivih podataka. Pod tom pretpostavkom razvijen je protokol koji mrežom ne šalje nikakve podatke koje bi neovlašteni korisnik mogao iskoristiti u svrhu kompromitiranja sustava.
Kako je već ranije spomenuto Kerberos je razvijen sredinom 80-tih na MIT Institutu u sklopu *Athena* projekta. Od toga dana Kerberos je prošao kroz brojne dorade i danas se verzija 5 tog protokola smatra *de facto* standardom. Kerberos 5 protokol opisan je u RFC dokumentu 1510.

### 2.2.1. Način rada Kerberos protokola

U ovom poglavlju biti će opisana osnovna načela Kerberos protokola, razložena prema pojedinim fazama komunikacije.

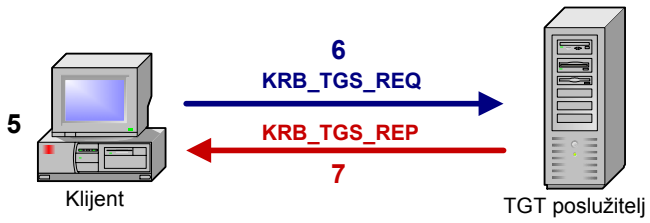
- Faza 1: Zahtjev korisnika za autentikacijom
  Zahtjev korisnika za autentikacijom prvi je korak u postupku Kerberos autentikacije (**Slika 3**).




*Slika 3: Kerberos autentikacija – Faza 1*

1. klijent se prijavljuje lokalno u sustav;
2. Kerberos klijent kreira poruku kombinirajući unesene korisničke podatke zajedno s podacima o Kerberos poslužitelju/ima. Korisnički podaci se nikada ne šalju mrežom u čistom tekstualnom formatu;
3. *Kerberos Authentication* poslužitelj (AS) u lokalnoj *Kerberos Key Distribution Center* (KPC) bazi traži podatke o navedenom korisniku. AS poslužitelj na temelju primljene poruke i lokalno pohranjenih podataka određuje kako će nastaviti s procesiranjem zahtjeva;
4. ukoliko je sve u redu, Kerberos poslužitelj klijentu vraća odgovor (*The Kerberos Authentication Server Reply, KRB_ASREP*), koji uključuje kartu (engl. *ticket*) koju će klijent dalje koristiti za komunikaciju s Kerberos poslužiteljem. Prema Kerberos standardu dobivena karta će se koristiti za izravni pristup aplikacijskom poslužitelju ili za pristup TGT (*Ticket-Granting Server*) servisu koji će generirati odgovarajuću kartu neophodnu za pristup istom.

- Faza 2: *Ticket-Granting* servis razmjena podataka
  Nakon što je klijentu vraćena TGT karta, potrebno je još nekoliko koraka za uspješno prijavljivanje klijenta u sustav. Slijedi opis koraka uključenih u ovu fazu, zajedno s pripadajućim grafičkim prikazom (**Slika 4**):




*Slika 4: Kerberos autentikacija – Faza 2*

5. korisnik pokušava pristupiti mrežnim resursima na proizvoljnom poslužitelju unutar Kerberos sustava;
6. Kerberos klijent TGS poslužitelju šalje TGT kartu primljenu u koraku 4, zajedno sa zahtjevom za novu kartu koja će omogućiti pristup željenom poslužitelju. Ovako formirana poruka nosi oznaku *KRB_TGS_REQ, The Kerberos Ticket-Granting Service Request*.
7. TGS poslužitelj dekriptira primljenu poruku (budući da je ista kriptirana ključem TGS poslužitelja) i provjerava valjanost podataka primljenih u poruci. Ukoliko je zahtjev valjan i ukoliko se poslužitelj za koji je zahtjev upućen nalazi unutar Kerberos domene za koju je TGS poslužitelj odgovoran, klijentu se vraća "karta" koja omogućuje pristup traženom resursu. Odgovor TGS poslužitelja označava se kao *KRB_TGS_REP (Kerberos Ticket Granting Service Reply)*.

- Faza 3: Klijent/poslužitelj autentikacija
  Nakon što je poslužitelj dobio odgovor od TGS poslužitelja, potrebno je dobivene podatke prezentirati poslužitelju kojem se želi pristupati. Na taj način korisnik potvrđuje svoj identitet i pravo pristupa zatraženom resursu.

8. Klijent poslužitelju upućuje zahtjev za pristup resursima (*KRB_AP_REQ*), kojim se utvrđuje identitet i pripadnost klijenta;
9. Poslužitelj dekriptira primljenu poruku (budući da je kriptirana s ključem poslužitelja), provjerava legitimnost zahtjeva i ukoliko je sve u redu dozvoljava konekciju s klijentom.

## 2.3. Kerberos autentikacija kod Windows 2000 operacijskih sustava

Ključan element u implementaciji Kerberos servisa kod Windows 2000 operacijskih sustava je *Kerberos Distribution Center* (KDC) servis. KDC servis pokreće se na poslužitelju domene (engl. *domain controller*) i pohranjuje podatke o svim sudionicima Kerberos domene.
Podaci o korisnicima povezani su s *Active Directory* imeničkim servisom, temeljem Windows 2000 domene. Osim podataka o korisnicima sustava, KDC za svakog od sudionika pohranjuje i tzv. *long term key* koji se koristi u postupku autentikacije.
KDC servis sastoji se od dva dijela:

- *Authentication Service (AS)* servisa i,
- *Ticket Granting Service (TGS)* servisa.

Budući da svi poslužitelji unutar Windows 2000 domene posjeduju svoj vlastiti KDC servis, proces autentikacije može biti proveden od strane bilo kojeg od njih. KDC servis pokreće se u LSP (***L**ocal **S**ecurity **P**olicy*) okružju poslužitelja.
U nastavku je opisana implementacija ranije opisanih faza Kerberos autenikacije (poglavlje 2.2.1) kod Windows 2000 sustava.

- Faza 1: Zahtjev korisnika za autentikacijom
  U ovoj fazi korisnik s KDC servisom razmjenjuje različite podatke koji rezultiraju dogovorenim ključem sjednice između klijenta i KDC poslužitelja, te TGT "kartom" koja klijentu omogućuje identifikaciju kod TGS servisa, neophodnu za daljnji postupak autentikacije.
  1. Korisnik A na W2K sustavu se putem korisničkog imena i pripadajuće zaporke prijavljuje na Windows 2000 domenu. Kerberos klijent na računalu pomoću unesene zaporke generira korisnikov ključ.
  2. Kerberos klijent formira *KRB_AS_REQ (Kerberos Authentication Server Request)* poruku i prosljeđuje je KDC servisu pokrenutom na poslužitelju domene. *KRB_AS_REQ* poruka sastoji se od dva dijela:
     - prvi dio kojim se identificira korisnik A, zajedno s imenom servisa za koji se traže ovlasti pristupa;
     - podaci kojima klijent potvrđuje pripadnost sustavu da zadovoljava uvjete za korištenje servisa. Preciznije, klijent poslužitelju šalje niz autentikacijskih podataka kriptiranih korisnikovim tajnim ključem koji je dobiven iz unesene korisničke zaporke;
  3. KDC pri primanju zahtjeva u lokalnoj bazi (*Active Directory*) pronalazi pripadajući tajni ključ korisnika, dekriptira primljenu poruku te provjerava njezinu legitimnost (vremenske oznake – engl. *timestamps*, podaci o korisniku i sl.).
  4. Nakon što je potvrđen legitimitet primljene poruke i identitet korisnika, poslužitelj klijentu vraća specijalnu potvrdu o vjerodostojnosti (engl. *credential*) koju klijent kasnije koristi u komunikaciji s TGS servisom. U nastavku su opisani dijelovi poruke koju klijent koristi pri komunikaciji s TGS servisom, zajedno s osnovnim postupcima njena kreiranja.
     - KDC servis kreira novi ključ sesije te ga kriptira sa tajnim ključem korisnika A;
     - kopija istog ključa sjednice se zajedno s autorizacijskim podacima korisnika A kriptira tajnim ključem KDC servisa što formira TGT "kartu";
     - KDC servis na temelju spomenutih podataka kreira *KRB_AS_REP* (*Kerberos Authentication Response*) poruku koju vraća klijentu;
     - Pri primanju poruke klijnet dekriptira primljenu poruku te u *cache* memoriji sustava pohranjuje tajni ključ sjednice zajedno s TGT kartom. TGT karta, kao što je već ranije rečeno sastoji se od istog ključa sjednice, zajedno s autorizacijskim podacima korisnika nakon čega je sve kriptirano tajnim ključem KDC servisa.

- Faza 2: *Ticket-Granting* servis razmjena podataka
  Nakon što je KDC servis klijentu vratio podatke opisane u fazi 1, slijedi postupak kojim klijent zahtjeva ovlasti pristupa bilo kojem drugom servisu unutar Kerberos domene.
  5. Klijent A slanjem *KRB_TGS_REQ (Kerberos Ticket-Granting Service Request)* poruke zahtjeva od KDC servisa "kartu", kojom će mu se omogućiti pristup željenom resursu B. *KRB_TGS_REQ* poruka sastoji se od sljedećih dijelova:
     - identitet servisa B kojem klijent želi pristupiti i za koji zahtjeva poruku o vjerodostojnosti (engl. *credential*);
     - autentikacijske podatke korisnika A kriptirane njegovim tajnim ključem;
     - TGT kartu dobivenu u koraku 4 faze 1.
  6. KDC servis dekriptira TGT ključ svojim tajnim ključem (što je moguće, budući da je u koraku 4 faze 1 klijentu vraćena TGT karta koja sadrži podatke kriptirane tajnim ključem KDC servisa) i pomoću njega dekriptira poruku klijenta koja sadrži tajni ključ sjednice. Budući da se u TGT karti nalazi isti ključ kojim je kriptirana poruka klijenta ovaj postupak ne predstavlja problem za KDC servis. Metodom usporedbe provjerava se legitimnost primljenih podataka te ukoliko je sve u redu generira se novi tajni ključ koji će klijent koristiti za komunikaciju s servisom B. Dvije kopije novog ključa sesije (slično kao i kod dogovaranja u fazi 1) kriptiraju se i šalju klijentu na sljedeći način:
     - jedna kopija kriptirana je tajnim ključem klijenta A koji je poznat samo KDC servisu i klijentu;
     - druga kopija je zajedno s podacima o korisniku koji zahtjeva pristup servisu kriptirana tajnim ključem servisa B (koji je poznat samo KDS poslužitelju i servisu B) i na taj način formira "kartu" koja omogućuje pristup servisu B.
  7. Klijent A svojim tajnim ključem dekriptira prvu kopiju tajnog ključa sesije i pohranjuje ga u *cache* memoriju sustava. Klijent također u memoriju pohranjuje i "kartu" kriptiranu tajnim ključem servisa B. Treba napomenuti kako klijent nije u mogućnosti dekriptirati "kartu" koja je kriptirana tajnim ključem servisa B, budući da je ključ za dekripciju poznat samo KDC i B servisu.
- Faza 3: Klijent/poslužitelj autentikacija
  U zadnjoj fazi klijent koristi podatke primljene u fazi 2 za autentikaciju kod servisa B. Koraci su sljedeći:
  8. Klijent inicira autentikaciju kod servisa B slanjem *KRB_AP_REQ (Kerberos Application Request)* poruke koja se sastoji od:
     - autentikacijskih podatak klijenta A kriptiranih tajnim ključem sjednice dogovorene s KDC servisom;
     - "kartu" primljenu u koraku 6 faze 2, koja sadrži podatke o klijentu i isti tajni ključ sjednice kriptiran tajnim ključem servisa B;
     - zastavicu kojom klijent potvrđuje da li želi obostranu autentikaciju;
  9. Servis B svojim tajnim ključem dekriptira primljenu "kartu" iz koje saznaje tajni ključ sjednice dogovoren između klijenta A i KDC servisa. S istim ključem servis B dekriptira autentikacijske podatke klijenta A i uspoređuje dobivene vrijednosti. Ukoliko je poruka legitimna slijedi ispitivanje zastavice kojom se želi utvrditi da li klijent zahtjeva obostranu autentikaciju. Ukoliko je zastavica postavljena, servis B istim tajnim ključem kriptira dio autentikacijskih podataka primljenih od strane klijenta A i vraća ih klijentu u *KRB_AP_REP (Kerberos Application Reply)* poruci.
  10. Klijent A dekriptira primljenu poruku i primljene podatke uspoređuje s onima poslanim u prethodnom koraku. Ukoliko je poruka legitimna, klijent je uvjeren u autentičnost komunikacije s servisom B.

### 2.3.1. Okružje sa više Windows 2000 domena

Implementacija Kerberos autentikacije kod Windows 2000 sustava omogućuje autentikaciju resursa između više domena. Ovaj postupak omogućuje se kreiranjem posebnog ključa (engl. *interdomain key*) koji pojedine domene međusobno razmjenjuju. Ovakav ključ kreira se u trenutku kada dvije domene dogovore međusobnu vezu (engl. *trust*). Slijedi kratki opis postupka:

- klijent u domeni A želi ostvariti pristup servisu u domeni B. U tom slučaju klijent šalje zahtjev za autentikaciju TGS servisu u njegovoj matičnoj domeni (domena A);
- TGS servis domene A ustanovljava da traženi servis ne pripada domeni A, već da se nalazi u domeni B;
- TGS domene A kreira TGT "kartu" kriptiranu tajnim ključem koji domene A i B međusobno dijele i vraća ga klijentu (engl. *referral ticket*);
- klijent koristi primljenu *referral* "kartu" i putem nje od TGS servisa u domeni B traži tajni ključ sjednice potreban za komunikaciju sa servisom u domeni B;
- TGS servis domene B dekriptira odgovarajućim ključem poruku, provjerava njezin legitimitet nakon čega klijentu šalje "kartu" koja sadrži tajni ključ sjednice koji je potreban za pristup traženom servisu;
- klijent koristi primljenu "kartu" za pristup servisu u domeni B.

### 2.3.2. Miješana Windows okruženja

U miješanim Windows okruženjima iz razloga kompatibilnosti podržani su i stariji protokoli (NTLM), kako bi se starijim klijentima omogućio pristup željenim resursima. Čak i u slučajevima gdje Windows 2000 domena radi u *Native* modu rada, zbog problema kompatibilnosti ili mogućih problema u radu Kerberos sustava, podržane su starije inačice autentikacijskih protokola.
U ovakvim situacijama aplikacije mogu inzistirati na korištenju najsigurnijeg protokola ili se može omogućiti dogovaranje na nivou sustava, koje će prema principu zajedničkog nazivnika, rezultirati korištenjem najprikladnije metode.

# 3. Sigurnosni događaji u postupku Windows 2000 autentikacije

Windows NT i Windows 2000 operacijski sustavi mogu se vrlo detaljno nadzirati ukoliko se na nivou sustava omoguće odgovarajuće postavke. Omogućavanjem bilježenja uspješnih (engl. *success*) i neuspješnih (engl. *failure*) pokušaja prijavljivanja u sustav moguće je detektirati sljedeće događaje:

| Kod greške | Opis |
|---|---|
| 528 | Successful Logon |
| 529 | Logon Failure: Reason: Unknown user name or bad password |
| 530 | Logon Failure: Reason: Account logon time restriction violation |
| 531 | Logon Failure: Reason: Account currently disabled |
| 532 | Logon Failure: Reason: The specified user account has expired |
| 533 | Logon Failure: Reason: User not allowed to logon at this computer |
| 534 | Logon Failure: Reason: The user has not been granted the requested logon type at this machine |
| 535 | Logon Failure: Reason: The specified account's password has expired |
| 536 | Logon Failure: Reason: The NetLogon component is not active |
| 537 | Logon Failure: Reason: An unexpected error occurred during logon |
| 538 | User Logoff: |
| 539 | Logon Failure: Reason: Account locked out |
| 540 | Successful Network Logon |
| Događaji prisutni samo kod Windows 2000 sustava: | |
| 541 | IPSec security association established. |
| 542 | IPSec security association ended. |
| 543 | IPSec security association ended. |
| 544 | IPSec security association establishment failed because peer could not authenticate |
| 545 | IPSec peer authentication failed. |

| Kod greške | Opis |
|---|---|
| 546 | IPSec security association establishment failed because peer sent invalid proposal. |
| 547 | IPSec security association negotiation failed. |
| 672 | Authentication Ticket Granted |
| 673 | Service Ticket Granted |
| 674 | Ticket Granted Renewed |
| 675 | Pre-authentication failed |
| 676 | Authentication Ticket Request Failed |
| 677 | Service Ticket Request Failed |
| 678 | Account Mapped for Logon |
| 679 | Account could not be mapped for logon |
| 680 | Account Used for Logon |
| 681 | The logon to account: <client name> by: <source> from workstation: <workstation> failed. The error code was: <error> |
| 682 | Session reconnected to winstation |
| 683 | Session disconnected from winstation |

*Tablica 3: Poruke postupka autentikacije kod Win NT i Win 2000 sustava*

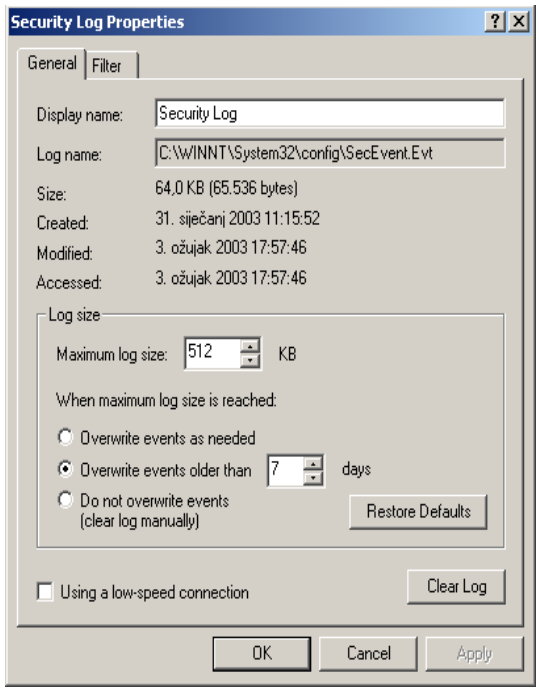
# 4. Prikupljanje sigurnosnih događaja na Windows 2000 sustavima

U inicijalnoj konfiguraciji Windows 2000 i Windows NT operacijski sustavi ne bilježe sigurnosne događaje (engl. *security log events*). Kako bi se omogućilo bilježenje i praćenje događaja vezanih za sigurnost sustava, potrebno je na odgovarajući način podesiti sustav za bilježenje i arhiviranje log zapisa (*Event Log*). Ovaj postupak nije nimalo jednostavan i vrlo često zahtjeva iterativne modifikacije na konfiguraciji kako bi se postigao optimalan rad sustava.

Kod Windows 2000 platformi, sustav za bilježenje log zapisa zove se *Event Log* i podijeljen je na tri dijela:

- *Application Log*;
- Security *Log*;
- *System Log*.

Na sljedećoj slici (**Slika 5**) prikazan je prozor unutar kojeg je moguće podešavati svojstva *Security Log* modula:

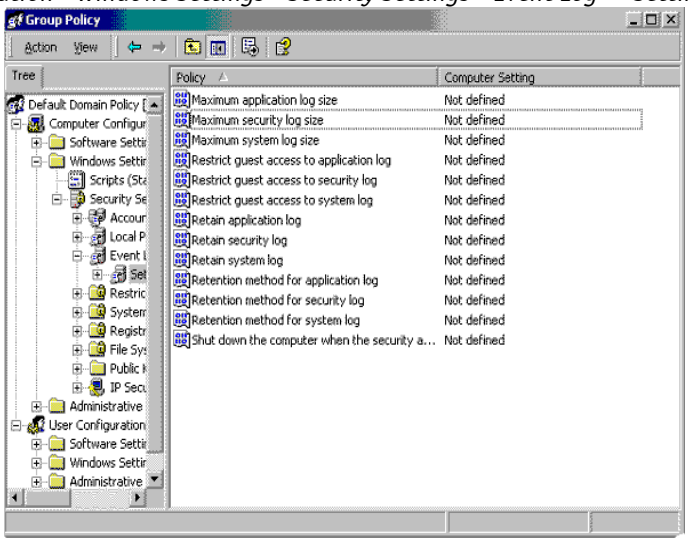


*Slika 5: Security Log Properties*

## 4.1. Veličina i arhiviranje log zapisa

Kod W2K sustava *Group Policy* modul (engl. *snap-in*) zadužen je za kontrolu *Event Log* sustava.
U nastavku je prikazan primjer konfiguracije log sustava u kojem je maksimalna veličina log zapisa podešena na 4032 KB i period čuvanja 2 dana. Postupak je sljedeći:

- unutar *Management Console* (`mmc`) konzole otvoriti *Active Directory Users* and Computer modul;
- otvoriti svojstva (engl. *Properties*) za domenu koja se želi administrirati;
- otvoriti *Group Policy* karticu;
- odabrati *Default Domaain Policy* GPO (*Group Policy Object*) te pritisnuti karticu *Edit*;
- unutar lijevog prozora (**Slika 6**) odabrati uređivanje postavki log sustava (*Computer->Configuration->Windows Settings->Security Settings->Event Log -> Settings*);



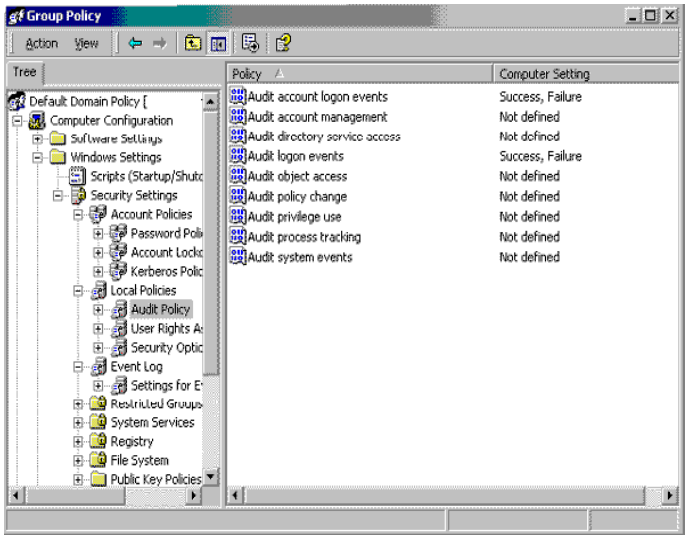

*Slika 6: Podešavanje parametara log sustava*

- unutar desnog prozora odabrati polje *Maximum security log size*, kliknuti desnim gumbom miša te unutar sekcije *Security* podesiti vrijednost 4032 (moguća je i bilo koja druga vrijednost, ovisno o specifičnosti okružja u kojem se sustav podešava);
- na identičan način unutar polja *Retain Security Log* podesiti vrijednost *2 days;*
- učitati unesene promjene pritiskom na karticu *Reload* pod sekcijom *Security Settings* unutar desnog okvira prozora prikazanog na slici.

## 4.2. Podešavanje *Audit Policy* parametara

Budući da W2K i Win NT sustavi inicijalno ne bilježe sigurnosne događaje, unutar *Security Log* modula neće se bilježiti događaji, dok se ne aktivira sustav njihovog bilježenja. Definiranje parametra bilježenja log zapisa za sva računala unutar domene moguće je postići uređivanjem GPO modula. Postupak je sljedeći:

- unutar *Default Domain Policy* modula slijediti stazu *Computer Configuration->Windows Settings->Security Settings->Local Policies->Audit Policy*;




*Slika 7: Podešavanje parametara bilježenja log zapisa*

- desnim gumbom kliknuti na željeno polje vezano za podešavanje bilježenja log zapisa i odabrati polje *Security*;
- definirati situacije u kojima se bilježe log zapisi (uspješno – engl. *success* ili neuspješno – engl. *failure* prijavljivanje u sustav, ili i jedno i drugo);
- ponovno učitati unesene promjene na način kako je to opisano u prethodnom poglavlju (4.1);

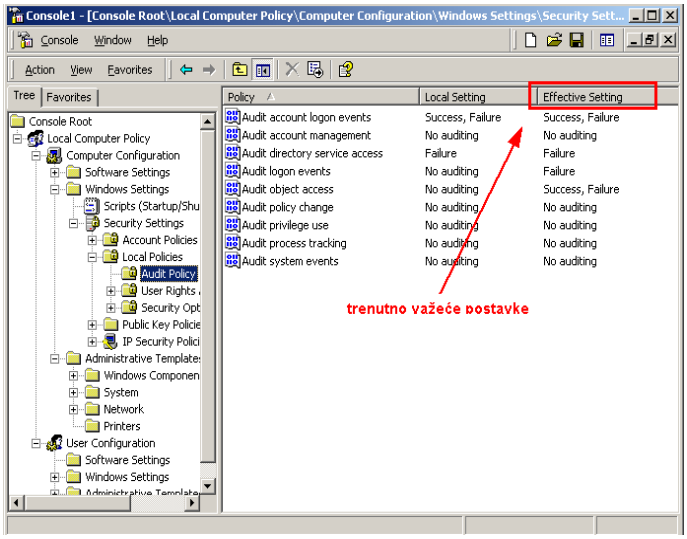
U danom primjeru definirane postavke odnose se na sva računala u domeni. U slučaju potrebe moguće je definirati različite politike bilježenja log zapisa za pojedine grupe računala.
Novo definirana politika bilježenja log zapisa počet će se primjenjivati prilikom sljedećeg prijavljivanja u sustav i dalje u regularnim intervalima (60 do 120 minuta za *Member* poslužitelje, a 5 minuta za poslužitelje domene). Trenutno primjenjivanje politike može se inicirati zadavanjem sljedeće naredbe u naredbenom retku:

```
C:\ secedit /refreshpolicy machine_policy
```

Budući da je sigurnosnu politiku W2K sustava moguće podesiti na različitim nivoima (lokalno, na nivou domene, *site*-a ili organizacijske jedinice (OU)), konačna pravila dobivaju se preklapanjem svih ovih definicija, prema određenim prioritetima. Hijerarhija je sljedeća:

- primjenjivanje lokalno definirane politike;
- primjenjivanje politike definirane na nivou *site*-a;
- primjenjivanje politike na nivou domene;
- primjenjivanje politike na nivou OU-a.

Uz ovakav hijerarhijski način primjenjivanja politike, gdje pojedine definicije imaju veći prioritet od drugih, ponekada je teško utvrditi koja se točno pravila u danom trenutku primjenjuju.
Stanje sustava, s obzirom na sigurnosnu politiku koja se trenutno primjenjuje, moguće je dobiti na sljedeći način. Unutar MMC konzole (modul *Local Security Policy*) potrebno je odabrati polje *Security Setting->Local Policies->Audit Policy,* gdje se nalaze parametri kojima se definiraju događaji koje sustav bilježi (**Slika 8**).
Unutar desnog prozora pod stupcem *Effective Setting*, prikazane su trenutno važeće postavke na sustavu.




*Slika 8: Trenutno važeće postavke*

Windows 2000 platforma u odnosu na starije inačice Windows sustava donosi nekoliko novih događaja koje je moguće pratiti. To su: *Audit logon events, Audit account logon events,* i *Audit directory service access.*

*Audit logon events* parametar omogućuje praćenje lokalnih prijavljivanja u sustav, slično kao i *Logon/Logoff* parametri kod Windows NT sustava. *Logon Type* polje u opisu *Audit logon events* zapisa sadrži numerički vrijednost koja detaljnije opisuje tip događaja. Moguće vrijednosti su:

- (2) – *interactive* – interaktivno prijavljivanje u sustav korisniku omogućuje ili lokalno ili prijavljivanje na domenu, ovisno o karakteristikama navedenog korisničkog računa. Prilikom prijavljivanja na domenu korisnik se prijavljuje poslužitelju domene putem *Active Directory* imeničkog servisa. Kod lokalnog prijavljivanja korisnički podaci provjeravaju se unutar lokalno pohranjene SAM baze*;*
- (3) – *network* – kod mrežnog prijavljivanja u sustav, korisnik se identificira kod svih mrežnih servisa kojima pokušava pristupiti. Ovaj postupak identifikacije je transparentan za korisnike koji se prijavljuju na domenu, za razliku od lokalno prijavljenih korisnika koji pri svakom pristupu mrežnim resursima moraju ponovno unijeti odgovarajuće podatke (korisničko ime i zaporku)*;*

Ostali načini prijavljivanja nisu detaljnije razmatrani, budući da njihov način rada nema značajniju važnost u području obuhvaćenom ovim dokumentom.

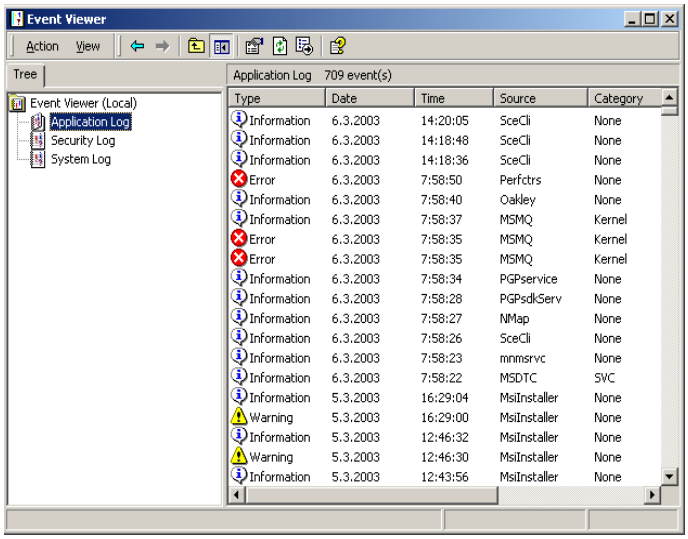
- (4) – *batch;*
- (5) – *service;*
- (7) - *unlocked workstation;*
- (8) - *network logon using a cleartext password;*
- (11) - *impersonated logons.*

Preostala dva parametra (*Audit account logon events,* i *Audit directory service access*) vezana su za poslužitelje domene te kao takvi nemaju lokalni značaj.

*Audit account logon events* parametar omogućuje centralizirano bilježenje događaja vezanih za autentikaciju korisnika na poslužitelju domene.

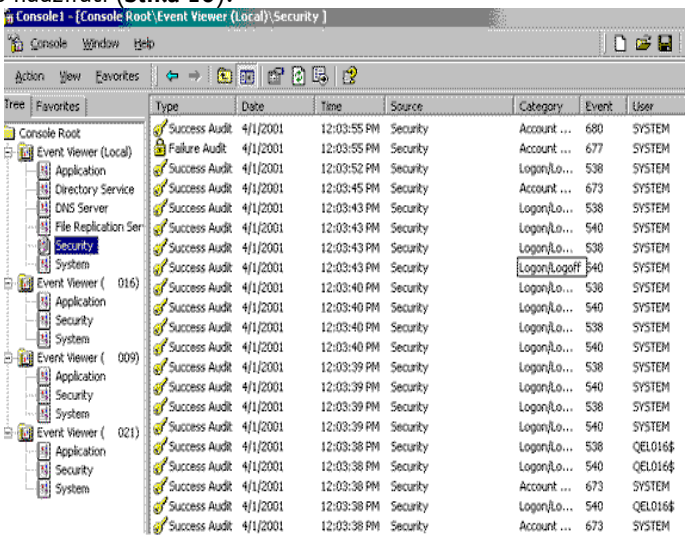
# 5. Praćenje i analiza događaja

Praćenju i analizi log zapisa na W2K sustavu predviđena je *Event Viewer* aplikacija (*Start->Administrative Tools ->Event Viewer*), **Slika 9**.




*Slika 9: Event Viewer aplikacija za analizu log zapisa*

Putem MMC sučelja moguće je definirati vlastite konzole za praćenje i analizu log zapisa, prilagođene osobnim potrebama. Na primjer, moguće je dodati kopije *Event Viewer* aplikacije za više sustava koji se žele istovremeno nadzirati (**Slika 10**).




*Slika 10: Korisnički definirana konzola za praćenje log zapisa*

## 6. Testno okružje

U svrhu ispitivanja događaja vezanih za autentikaciju korisnika uspostavljeno je testno okružje sa sljedećim Windows sustavima:

- Windows 2000 poslužitelj domene pod testnim imenom TEST (računalo: TEST034);
- Windows 2000 *member* poslužitelji (računala: TEST016 i TEST009);
- Windows NT 4 *member* poslužitelji (računala: TEST007 i TEST021);
- Windows NT 4 Workstation klijenti;
- Windows 2000 Professional klijenti.

U nastavku je dana analiza detektiranih događaja, zajedno s pripadajućim pojašnjenima.

## 6.1. Uspješna prijavljivanja u sustav

U nastavku poglavlja opisani su događaji na Windows 2000 i Windows NT platformama vezani za uspješno prijavljivanje korisnika u sustav (engl. *Success logon*). Opisani su različiti scenariji unutar testnog okružja baziranog na kombinaciji Windows NT i Windows 2000 operacijskih sustava, zajedno s analizom propadajućih događaja i log zapisa koji na njih upućuju.

### 6.1.1. Interaktivno prijavljivanje u sustav na W2K operacijskim sustavima

Podešavanje *Audit logon events* parametra za bilježenje uspješnih i neuspješnih pokušaja prijavljivanja u sustav dalo je sljedeće rezultate.
Kod lokalnog prijavljivanja na W2K sustav, uspješno prijavljivanje rezultiralo je porukom 528 (tip 2 – interaktivno prijavljivanje u sustav), dok je odjavljivanje sa sustava rezultiralo porukom 538.
Detektirani 528 (*Successful Logon*) i 538 (*User Logoff*) događaji vezani su za lokalno prijavljivanje korisnika sa lokalnim korisničkim računom. Može se uočiti da je kod navedenih zapisa pod imenom domene navedeno ime lokalnog računala, što omogućuje jednostavnu identifikaciju lokalnih pokušaja prijavljivanja u sustav.

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528
Date: 3/18/2001
Time: 12:13:52 PM
User: TEST009\juliole
Computer: TEST009
Description:
Successful Logon:

User Name: juliole
Domain: TEST009
Logon ID: (0x0,0x4874B)
Logon Type: 2
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: TEST009
```

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 538
Date: 3/18/2001
Time: 12:17:11 PM
User: TEST009\juliole
Computer: TEST009
Description:
User Logoff:

User Name: juliole
Domain: TEST009
Logon ID: (0x0,0x4874B)
Logon Type: 2
```

Slijedeći zapisi zabilježeni su u postupku prijavljivana korisnika na Windows domenu:

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
```

```
Event ID: 528
Date: 3/18/2001
Time: 12:56:38 PM
User: TEST\TEST1
Computer: TEST016
Description:
Successful Logon:

User Name: TEST1
Domain: TEST
Logon ID: (0x0,0xAC8F)
Logon Type: 2
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: TEST016
```

Može se primijetiti da svi događaji vezani za autentikaciju korisnika počinju s porukom prijavljivanja u sustav (528), a završavaju porukom odjavljivanja iz sustava (538). Kombinirajući ove podatke s *LoginID* poljem, moguće je voditi preciznu analizu vremena kojeg je pojedini korisnik proveo prijavljen za rad na sustavu.

*Audit Account logon* parametar omogućuje bilježenje događaja vezanih za Kerberos autentikaciju korisnika prilikom prijavljivanja na Windows 2000 domenu.

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 672
Date: 3/18/2001
Time: 12:56:38 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Authentication Ticket Granted:

User Name: TEST1
Supplied Realm Name: TEST
User ID: TEST\TEST1
Service Name: krbtgt
Service ID: TEST\krbtgt
Ticket Options: 0x40810010
Ticket Encryption Type: 0x17
Pre-Authentication Type: 2
Client Address: 10.45.15.16
```

Navedeni događaji generiraju se u trenutku kada klijent kontaktira lokalni poslužitelj domene i preda zahtjev za TGT "kartom". Nakon utvrđivanja legitimiteta primljenog paketa, poslužitelj klijentu vraća odgovor i generira događaj s kodom 672 (*Authentication ticket granted*). Unutar zapisa koji upućuju na Kerberos aurtentikaciju, polje *User* ne odaje previše informacija o korisniku, budući da ovo polje uvijek sadrži vrijednost `SYSTEM`.

U ovom slučaju identifikaciju klijenta moguće je obaviti na temelju *Client Address* polja, koje sadrži IP adresu s koje klijent pristupa poslužitelju. Svi Kerberos log zapisi sadrže ovo polje te je putem njega moguće utvrditi identitet korisnika koji pristupa sustavu.

Kod Windows NT sustava, praćenje neuspjelih pokušaja prijavljivanja u sustav bilo je relativno loše riješeno. Iako je bila moguća detekcija neuspjelih prijavljivanja u sustav, nije bilo moguće utvrditi od kuda su isti inicirani, što predstavlja ozbiljno ograničenje u detaljnoj analizi događaja na sustavu.

Nakon događaja 672 (*Authentication Ticket Granted*) , slijedi događaj 673 (*Service Ticket Granted*):

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
```

```
Event ID: 673
Date: 3/18/2001
Time: 12:56:38 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Service Ticket Granted:

User Name: TEST1
User Domain: TEST.SEC01.LOCAL
Service Name: TEST016$
Service ID: TEST\TEST016$
Ticket Options: 0x40810010
Ticket Encryption Type: 0x17
Client Address: 10.45.15.16
```

*Authentication Ticket Granted* poruke (672) mogu se iskoristiti za praćenje prijavljivanja korisnika u sustav putem dodjeljivanja TGT "karte", dok se poruke *Service Ticket Granted* (673) događaj upućuje na pristup resursu za kojeg je klijent zahtijevao autentikaciju.
U prethodnom primjeru događaj 672 upućuje samo na uspješnu autentikaciju korisnika, bez dozvole za pristup ostalim resursima unutar Kerberos domene. Naknadno generirani 673 događaj upućuje na autentikaciju kojom je klijent dobio "kartu" za pristup željenom poslužitelju.
Pokušaj pristupanja drugom poslužitelju za koji klijent nije dobio "kartu" rezultirao je novim 673 log zapisom:

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 673
Date: 3/18/2001
Time: 12:56:38 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Service Ticket Granted:

User Name: TEST016$
User Domain: TEST.SEC01.LOCAL
Service Name: TEST034$
Service ID: TEST\TEST034$
Ticket Options: 0x40810010
Ticket Encryption Type: 0x17
Client Address: 10.45.15.16
```

Lokalno prijavljivanje na W2K sustav rezultira 680 porukom:

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 12:13:52 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST009
Description:
Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name: juliole
Workstation:  TEST009
```

### 6.1.2. Interaktivno prijavljivanje u sustav kod Windows NT operacijskih sustava

Slično kao i kod Windows 2000 sustava, lokalno prijavljivanje u sustav rezultirati će porukom 528 kod uspješnog prijavljivanja, odnosno porukom 538 prilikom odjavljivanja sa sustava:

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528
Date: 3/18/2001
Time: 1:06:07 PM
User: TEST\TEST1
Computer: TEST021
Description:
Successful Logon:

User Name: TEST1
Domain: TEST
Logon ID: (0x0,0x2DAB42)
Logon Type: 2
Logon Process: User32
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: TEST021
```

Budući da Windows NT platforma ne podržava Kerberos autentikaciju, pokušaj prijavljivanja korisnika na Windows 2000 domenu rezultirati će porukom 680 (*Account Used for Logon*):

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 1:12:33 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Account Used for Logon by:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name: TEST1
Workstation:  TEST021
```

### 6.1.3. Mrežno prijavljivanje u sustav sa W2K poslužitelja na W2K klijent računalo

Omogućavanje *Audit logon events* parametra rezultira generiranjem 540 (tip 3 – mrežno prijavljivanje u sustav) poruke na W2K poslužitelju nakon uspješnog mrežnog prijavljivanja u sustav.
Windows NT sustav generira poruku 528 poruku prilikom svakog prijavljivanja u sustav, neovisno o tipu (interaktivno ili mrežno). Za razliku od Windows NT sustava, W2K sustav generira poruku 540 kod mrežnog prijavljivanja, a poruku 528 kod interaktivnog prijavljivanja u sustav. Na ovaj način moguće je razlikovati interaktivne od mrežnih prijavljivanja u sustav:

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 540
Date: 3/18/2001
Time: 2:17:55 PM
User: TEST\admin
Computer: TEST009
Description:
```

```
Successful Network Logon:

User Name: admin
Domain: TEST
Logon ID: (0x0,0x4AAF2)
Logon Type: 3
Logon Process: Kerberos
Authentication Package: Kerberos
Workstation Name:
```

Iz priloženog log zapisa može se primijetiti da je autentikacija korisnika provedena Kerberos protokolom, budući da se radi o dva W2K računala.
Omogućavanje *Audit Account logon* parametra rezultirati će generiranjem 673 poruke kod uspješne Kerberos autentikacije. Nakon što korisnik posjeduje odgovarajuću TGT "kartu", zahtjev za pristup nekom drugom servisu rezultira 673 porukom:

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 673
Date: 3/18/2001
Time: 2:17:55 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Service Ticket Granted:

User Name: admin
User Domain: TEST.SEC01.LOCAL
Service Name: TEST009$
Service ID: TEST\TEST009$
Ticket Options: 0x40810010
Ticket Encryption Type: 0x17
Client Address: 10.45.15.16
```

### 6.1.4. Mrežno prijavljivanje u sustav sa W2K na NT4 računalo

Omogućavanje *Audit logon event* parametra kod Windows NT poslužitelja rezultirati će 528 (tip 3 – mrežno prijavljivanje u sustav) porukom kod uspješnog prijavljivanja u sustav.

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528
Date: 3/18/2001
Time: 1:50:32 PM
User: TEST\admin
Computer: TEST021
Description:
Successful Logon:
User Name: admin
Domain: TEST
Logon ID: (0x0,0xE139)
Logon Type: 3
Logon Process: KSecDD
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \\TEST016
```

Omogućavanje *Audit Account logon* parametra rezultira generiranjem 677 poruke kod W2K poslužitelja. Korisnik `admin` pokušava pristupiti s W2K klijenta Windows NT poslužitelju, pri čemu klijent inicira Kerberos autentikaciju s TGS poslužiteljem. Budući da Windows NT sustav ne podržava Kerberos autentikaciju, W2K klijent dobija 677 poruku (*Service Ticket Request Failed*) o neuspjelom pokušaju.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 677
Date: 3/18/2001
Time: 1:56:42 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Service Ticket Request Failed:

User Name: admin
User Domain: TEST.SEC01.LOCAL
Service Name: HOST/TEST021
Ticket Options: 0x40810010
Failure Code: 7
Client Address: 10.45.15.16
```

Ova greška će za korisnika biti transparentna, budući da će W2K klijent nakon neuspjele Kerberos autentikacije inicirati NTLM autentikaciju podržanu od strane NT poslužitelja.

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 1:56:42 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Account Used for Logon by:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name: admin
Workstation:  \\TEST016
```

### 6.1.5. Mrežno prijavljivanje u sustav sa NT4 na W2K računalo

U ovom slučaju Windows NT klijent pokušava pristupiti resursima W2K poslužitelja. S obzirom da Windows NT sustav ne podržava Kerberos autentikaciju, koristi se NTLM postupak autentikacije.
Uspješno prijavljivanje Windows NT klijenta zabilježeno je porukom 540 (tip 3 – mrežno prijavljivanje u sustav). Treba primijetiti kako W2K sustav uspješno prijavljivanje u sustav bilježi porukom 540, a ne 528 kao što je to bio slučaj u prethodnom primjeru s Windows NT sustavom.

```
Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 540
Date: 3/18/2001
Time: 2:04:54 PM
User: TEST\admin
Computer: TEST016
Description:
Successful Network Logon:
```

```
User Name: admin
Domain: TEST
Logon ID: (0x0,0x1BFC5)
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: \\TEST021
```

S obzirom da NT platforma ne podržava Kerberos autentikaciju, W2K poslužitelj s omogućenim *Audit Account logon* parametrom će prilikom pokušaja prijavljivanja NT klijenta na domenu generirati 680 poruku.

```
Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 2:04:54 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Account Used for Logon by:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name: admin
Workstation:  \\SANS021
```

U ovom poglavlju opisani su događaji vezani za uspješno prijavljivanje korisnika na sustav. Jednako tako važno je i praćenje neuspješnih pokušaja prijavljivanja u sustav, budući da takvi događaji vrlo često mogu biti pokazatelj neovlaštenih aktivnosti na sustavu.
U nastavku dokumenta opisani su događaji vezani za neuspjele pokušaje prijavljivanja u sustav.

## 6.2. Neuspješna prijavljivanja u sustav

U nastavku poglavlja opisani su događaji na Windows 2000 i Windows NT platformama vezani za neuspješno prijavljivanje korisnika u sustav (engl. *Failure logon*). Opisani su različiti scenariji unutar testnog okružja baziranog na kombinaciji Windows NT i Windows 2000 operacijskih sustava, zajedno s analizom pripadajućih događaja i log zapisa koji na njih upućuju.

### 6.2.1. Interaktivno prijavljivanje u sustav na W2K operacijskim sustavima

Na W2K sustavu na kojem je omogućen *Audit logon events* parametara, neuspjeli pokušaj lokalnog prijavljivanja u sustav rezultirati će generiranjem 529 poruke (*Logon Failure: Reason: Unknown user name or bad password*). Pod neuspjelim pokušajem prijavljivanja u sustav smatra se unošenje ili pogrešnog korisničkog imena ili zaporke.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/18/2001
Time: 12:20:31 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST009
Description:
Logon Failure:

Reason: Unknown user name or bad password
User Name: fakeuser
Domain: TEST009
Logon Type: 2
```

```
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: TEST009
```

Ukoliko je na sustavu omogućeno praćenje *Audit Account logon* događaja, unošenje pogrešnog korisničkog imena ili zaporke generirati će poruku 681. Poruke će se razlikovati ovisno o razlogu zbog kojeg je poruka generirana.
U slučaju pogrešnog korisničkog imena poruka je:

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/18/2001
Time: 12:20:31 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST009
Description:
The logon to account: fakeuser
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: TEST009
failed. The error code was: 3221225572
```

dok u slučaju pogrešne zaporke poruka izgleda ovako:

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/18/2001
Time: 12:18:20 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST009
Description:
The logon to account: juliole
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: TEST009
failed. The error code was: 3221225578
```

Iako ove dvije poruke na prvi pogled izgledaju identično, razlika se može primijetiti kod `error code` polja. U sljedećoj tablici (**Tablica 4**) su prikazane moguće vrijednosti `error code` polja, zajedno s pripadajućim značenjem.

| error code | hex vrijednost polja | značenje |
|---|---|---|
| 3221225572 | C0000064 | Pokušaj prijave u sustav sa pogrešno unesenim ili nepostojećim korisničkim računom. |
| 3221225578 | C000006A | Pokušaj prijave u sustav sa pogrešno unesenom zaporkom. |
| 3221225583 | C000006F | Pokušaj prijave korisnika u nelegitimnom vremenskom periodu. |
| 3221225584 | C0000070 | Pokušaj prijave sa neautoriziranog računala. |
| 3221225585 | C0000071 | Pokušaj prijave sa zaporkom kojoj je istekla valjanost. |
| 3221225586 | C0000072 | Pokušaj prijave sa korisničkim računom koji je onemogućen od strane administratora. |
| 3221225875 | C0000193 | Pokušaj prijave s korisničkim računom kojem je istekla valjanost. |
| 3221226020 | C0000224 | Pokušaj prijave korisnika s uključenim parametrom "*Change Password at Next Logon*". |
| 3221226036 | C0000234 | Pokušaj prijave s zabranjenim korisničkim računom . |

*Tablica 4: Vrijednosti error code parametra*

Prilikom pokušaja prijavljivanja na Windows 2000 domenu s pogrešnim parametrima, *Audit Account logon* parametar zabilježiti će dva događaja na poslužitelju domene. To su:

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 675
Date: 3/18/2001
Time: 12:54:01 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Pre-authentication failed:

User Name: sans1
User ID: TEST\TEST1
Service Name: krbtgt/TEST
Pre-Authentication Type: 0x2
Failure Code: 24
Client Address: 10.45.15.16
```

i

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 676
Date: 3/18/2001
Time: 1:02:41 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Authentication Ticket Request Failed:

User Name: fakeuser
Supplied Realm Name: TEST
Service Name: krbtgt/TEST
Ticket Options: 0x40810010
Failure Code: 6
Client Address: 10.45.15.16
```

Osim podataka o korisničkom imenu i domeni kojoj se pokušava pristupiti, bilježi se i IP adresa klijenta s kojeg je zahtjev primljen. Na ovaj način omogućuje se identifikacija računala i korisnika koji je pokušao pristupiti sustavu.

### 6.2.2. Interaktivno prijavljivanje kod WinNT operacijskih sustava

Slično kao i kod W2K sustava, neuspjeli pokušaj prijavljivanja u sustav (ili lokalno ili na domenu) rezultirati će porukom 529.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/18/2001
Time: 1:03:08 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST021
Description:
```

```
Logon Failure:

Reason: Unknown user name or bad password
User Name: juliotre
Domain: TEST021
Logon Type: 2
Logon Process: User32
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: TEST021
```

Ukoliko je omogućen *Audit Account logon* parametar na poslužitelju domene biti će zabilježena 681 poruka koja upućuje na detalje o neuspjelom pokušaju prijavljivanja.
U slučaju pogrešno unesenog korisničkog imena poruka je,

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 4/1/2001
Time: 12:21:30 PM
User: NT AUTHORITY\SYSTEM
Computer: QEL034
Description:
The logon to account: admin
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: QEL021
failed. The error code was: 3221225572
```

a u slučaju pogrešne zaporke,

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 4/1/2001
Time: 12:20:53 PM
User: NT AUTHORITY\SYSTEM
Computer: QEL034
Description:
The logon to account: admin
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: QEL021
failed. The error code was: 3221225578
```

Kao i u prethodnom primjeru, uzrok greške moguće je doznati putem vrijednosti `error code` parametra.

### 6.2.3. Mrežno prijavljivanje u sustav sa W2K poslužitelja na W2K klijent računalo

U ovom slučaju neuspjeli pokušaj prijavljivanja u sustav rezultirati će porukom 529 neovisno o tome da li je pogrešno uneseno korisničko ime ili zaporka.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/30/2001
Time: 11:06:47 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST009
Description:
```

```
Logon Failure:

Reason: Unknown user name or bad password
User Name: admxxx
Domain: TEST
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: TEST016
```

*Audit Account logon* opcija, ukoliko je omogućena, rezultirati će bilježenjem 676 i 681 poruka u slučaju pogrešno unesenog korisničkog imena,

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 676
Date: 3/30/2001
Time: 11:06:47 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Authentication Ticket Request Failed:

User Name: admxxx
Supplied Realm Name: TEST
Service Name: krbtgt/TEST
Ticket Options: 0x40810010
Failure Code: 6
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001
Time: 11:06:47 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
The logon to account: admxxx
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: TEST016
failed. The error code was: 3221225572
```

te porukama 675 i 681 u slučaju pogrešne zaporke.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 675
Date: 3/30/2001
Time: 10:56:01 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Pre-authentication failed:

User Name: admin
User ID: TEST\admin
```

```
Service Name: krbtgt/TEST
Pre-Authentication Type: 0x2
Failure Code: 24
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001Time: 10:56:02 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
The logon to account: admin
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: TEST016
failed. The error code was: 3221225578
```

Razlika između slučajeva u kojima je pogrešna navedeno korisničko ime ili zaporka može se primijetiti i kod polja `Failure Code`, kojemu je u prvom slučaju pridjeljena vrijednost 6, a u drugom vrijednost 24.

### 6.2.4. Mrežno prijavljivanje sa W2K na NT4 računalo

Na sličan način, neuspjeli pokušaj prijavljivanja u sustav, bez obzira radi se o pogrešnom korisničkom imenu ili zaporci rezultirati će porukom 529.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/30/2001
Time: 11:03:20 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST021
Description:
Logon Failure:

Reason: Unknown user name or bad password
User Name: admxxx
Domain: TEST
Logon Type: 3
Logon Process: KSecDD
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \\TEST01
```

Ukoliko je omogućen, parametar *Audit Account logon* rezultirati će generiranjem događaja 677 (`Failure Code 7`) na domenskom poslužitelju, koji je posljedica činjenice da W2K računalo zahtjeva Kerberos "kartu" za pristup NT računalu koje ne podržava Kerberos autentikaciju.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 677
Date: 3/30/2001
Time: 11:09:38 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
```

```
Service Ticket Request Failed:

User Name: TEST016$
User Domain: TEST.SEC01.LOCAL
Service Name: HOST/TEST021
Ticket Options: 0x40810010
Failure Code: 7
Client Address: 10.45.15.16
```

*Audit logon* parametar, ukoliko je omogućen, također će rezultirati porukama 681 i 676 kod neuspjelog pokušaja prijavljivanja na domenu. Ovisno o tome da li je pogreška posljedica neispravnog korisničkog imena ili zaporke, poruke će se razlikovati prema `Failure Code` polju.
Neuspjeli pokušaj prijavljivanja u sustav prouzrokovan unošenjem pogrešnog korisničkog imena rezultirati će `Failure Code 6` porukom,

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 676
Date: 3/30/2001
Time: 11:09:38 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Authentication Ticket Request Failed:

User Name: admxxx
Supplied Realm Name: TEST
Service Name: krbtgt/TEST
Ticket Options: 0x40810010
Failure Code: 6
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001
Time: 11:09:38 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
The logon to account: admxxx
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: \\TEST016
failed. The error code was: 3221225572
```

dok će greška prouzrokovana pogrešnom zaporkom rezultirati `Failure Code 24` i porukom 681 na domenskom poslužitelju.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 675
Date: 3/30/2001
Time: 11:25:02 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
Pre-authentication failed:
```

```
User Name: admin
User ID: TEST\admin
Service Name: krbtgt/TEST
Pre-Authentication Type: 0x2
Failure Code: 24
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001
Time: 11:25:02 AM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
The logon to account: admin
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: \\TEST016
failed. The error code was: 3221225578
```

### 6.2.5. Mrežno prijavljivanje u sustav sa NT4 na W2K računalo

I u ovom slučaju neuspjeli pokušaj prijavljivanja u sustav rezultira greškom 529, neovisno o tome da li je pogrešno navedeno korisničko ime ili zaporka.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/18/2001
Time: 2:11:06 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST016
Description:
Logon Failure:

Reason: Unknown user name or bad password
User Name: fakeuser
Domain: TEST
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \\TEST021
```

Na poslužitelju domene, *Audit Account logon* parametar će rezultirati greškom 681.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/18/2001
Time: 2:11:14 PM
User: NT AUTHORITY\SYSTEM
Computer: TEST034
Description:
The logon to account: fakeuser
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
```

```
from workstation: \\TEST021
failed. The error code was: 3221225572
```

Tijekom testiranja primijećeni su u određenim situacijama još neki događaji vezani uz neuspjele pokušaje prijavljivanja u sustav. To su:

- 531 – u slučaju kada je korisnički račun onemogućen;
- 539 – u slučaju kada je korisnički račun zaključan (engl. *locked*);
- 530 – kada se korisnik pokušava prijaviti na sustav u periodu u kojem to nije dozvoljeno;
- 532 – prijavljivanje s korisničkim računom kojem je istekla valjanost;
- 536 – prijavljivanje u trenutku kada *NetLogon* servis nije aktivan;
- 535 – prijavljivanje s korisničkim računom kojem je istekla valjanost zaporke;

# 7. Arhiviranje i analiziranje sigurnosnih događaja

Postoji nekoliko komercijalnih alata na tržištu koji omogućuju analizu i arhiviranje log zapisa. S obzirom na važnost procesa praćenja log zapisa u postupcima redovite administracije sustava, treba ozbiljno razmotriti mogućnosti upotrebe ovakvih alata, iako su neki od njih prilično skupi.
U nastavku dokumenta opisano je nekoliko načina na koje je moguće analizirati prikupljene log zapise.
Nakon što su na sustavu omogućene odgovarajuće metode bilježenja log zapisa na način kako je to opisano u poglavlju 4.2, moguće je u realnom vremenu ili naknadno provoditi analize prikupljenih podataka kako bi se nadzirao rad sustava.

## 7.1. Analize u realnom vremenu

Za analizu log zapisa u realnom vremenu nije potrebno voditi računa o njihovom arhiviranju. Dovoljno je kontinuirano pratiti generirane zapise te, po potrebi, reagirati, ovisno o prioritetu pojedinih događaja.
Kao primjer može poslužiti sljedeći program pisan u *Visual Basic* programskom jeziku, koji se pokreće na poslužiteljima domene i putem e-mail poruke obavještava administratora sustava nakon što je detektiran neuobičajen broj 529 (*Logon Failure: Reason: Unknown user name or bad password*) poruka.
Program koristi WMI (***W**indows **M**anagement **I**nstrumentation*) sučelje za pristup *security event log* događajima, i može biti vrlo koristan za detekciju neovlaštenih aktivnosti na sustavu. Program omogućuje detekciju nelegitimnih pokušaja autentikacije korisnika i ukoliko je instaliran na poslužitelju domene moguće je ovim putem kontrolirati sve pokušaje prijavljivanja u sustav (lokalno i na domenu).
Program izgleda ovako:

```
Private Sub Form_Load()
'*****************************************************************
***
'*****      In order to run this program:
'*****        - Load it in VB
'*****        - Go to Projects -> References
'*****        - Add "Microsoft WMI Scripting V1.1 Library"
'*****      -  Select File -> Make, and save the exe as
Monitor529.exe
'*****      - Run the Monitor529.exe in the servers
'*****
'*****************************************************************
*****
Dim services As SWbemServices
Dim WbemEventSource As SWbemEventSource
Dim strQuery As String
Dim ObjEvent As SWbemObject
Dim Total529 As Integer
Dim AlertMessage As String
```

```
    On Error Resume Next
    Set services = GetObject("winmgmts:{impersonationLevel=
         impersonate,(security)}")
    strQuery = "SELECT * FROM __instancecreationevent " & _
               "WHERE TargetInstance ISA 'Win32_NTLogEvent'"

    Set WbemEventSource = services.ExecNotificationQuery(strQuery)

    Do
    Set ObjEvent = WbemEventSource.NextEvent(120000)  ' Wait 120
seconds

    If Err <> 0 Then
        If Err.Number = wbemErrTimedout Then      ' The call timed
out

            Total529 = 0                          ' reset after
120 seconds

        Else
             AlertMessage = "The program monitoring logon
violations
                            on machine " & _
                            ObjEvent.TargetInstance.ComputerName &
_
                            " failed with error : " & _
                            Err.Number & " " & Err.Description

             Alert (AlertMessage)                 ' alert if
program crashes

             End
        End If

    Else

        If ObjEvent.TargetInstance.eventcode = 529 And _
            ObjEvent.TargetInstance.SourceName = "Security" Then
            Total529 = Total529 + 1
            If Total529 > 5 Then

                AlertMessage = "You got more than 5 logon
violations in a
                                period of 120 seconds on " & _

ObjEvent.TargetInstance.ComputerName

                Alert (AlertMessage)   ' Alert if there is
violation

                Total529 = 0            ' reset after alert
            End If
         End If

    End If

Loop
```

```
End Sub

Sub Alert(AlertMessage)

'********************************************************
' This sub will send an email. Change the email addresses
'
'
' If you don't want an email, you can change this
' sub in order to do something else,
' like for example : Msgbox(AlertMessage)
'********************************************************

Set myMail = CreateObject("CDONTS.NewMail")
myMail.From = "julio.silveira@xyz.com"
myMail.To = "julio.silveira@xyz.com"
myMail.Subject = "You may be having a logon violation"
myMail.Body = AlertMessage
myMail.Send
Set myMail = Nothing

End Sub
```

Na sličan način moguće je nadzirati i druge događaje, uz određene modifikacije na programu. Treba napomenuti kako je ovaj program dan kao primjer i da se ne preporučuje njegovo korištenje u ozbiljnijim aplikacijama.
Kao što je ranije rečeno, program koristi WMI sučelje koje dolazi u osnovnoj instalaciji W2K sustava. Na Windows NT platformama ovaj modul potrebno je zasebno instalirati. Umjesto SMTP protokola moguće je prilagoditi program da koristi drukčije tehnike obavješćivanja administratora (npr. *net send* servis).

## 7.2. Arhiviranje log zapisa i izvješćivanje

Redovito arhiviranje log zapisa vrlo je važan korak u procesu praćenja rada sustava. Velike količine log zapisa, osim što zauzimaju diskovni prostor, dodatno otežavaju analizu i primjećivanje važnijih događaja.
U svrhu automatiziranog arhiviranja *security log* zapisa potrebno je koristiti alat koji omogućuje pohranjivanje prikupljenih log zapisa u datoteku. U tom slučaju moguće je iskoristiti *scheduler* koji će, ovisno o konfiguraciji sustava i količini prikupljenih zapisa, u regularnim intervalima arhivirati starije log zapise.
*Microsoft Resource Kit* jedan je od alata koji putem `dumpel` programa omogućuje pohranjivanje *event log* zapisa u tekstualnu datoteku, u kojoj su pojedina polja odvojena ili *tab* ili *space* znakom. Program omogućuje i filtriranje zapisa što olakšava analizu i pretraživanje pojedinih događaja.
Poznato je još nekoliko programskih alata slične namjene. To su:

- `dumpevt`
- `eventsave`
- `eldump`

U nastavku dokumenta pokazan je primjer kako je moguće pomoću `eldump` programa generirati izvještaj iz *security log* zapisa te arhivirati iste unutar SQL 2000 baze podataka. `Eldump` program moguće je dobaviti sa URL adrese http://www.ibt.ku.dk/.

### 7.2.1. Korak 1: Pohranjivanje log zapisa u tekstualnu datoteku

U prvom koraku potrebno je snimiti log zapise s poslužitelja u datoteku s nastavkom `.evt`. Nakon toga potrebno je pokrenuti `eldump` program s odgovarajućim parametrima:

```
C:\eldump -F c:\TEST009.evt TEST016.evt -l security -e 528 538 -M -t
-c # > sec_log.txt
```

Značenje pojedinih parametar je sljedeće:

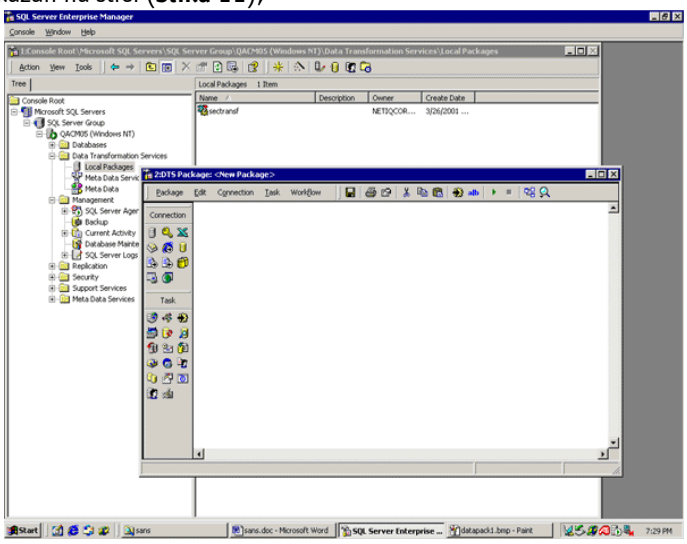
- `-F` – ime datoteke u kojoj su pohranjeni log zapisi;
- `-l` – tip log zapisa koji se želi izvesti. Moguće vrijednosti su: *application*, *system*, *security*;
- `-e` – tip poruka koji se žele filtrirati;
- `-M` – ne izvoziti kompletni sadržaj log zapisa već samo tekstualni opis;
- `-c` – znak kojim će pojedina polja biti odvojena u tekstualnoj datoteci (u ovom slučaju #);

Rezultat izvođenja navedene naredbe rezultirati će `sec_log.txt` datotekom u kojoj će biti navedeni željeni log zapisi u tekstualnom obliku.

### 7.2.2. Korak 2: Učitavanje tekstualnih log zapisa u SQL bazu podataka

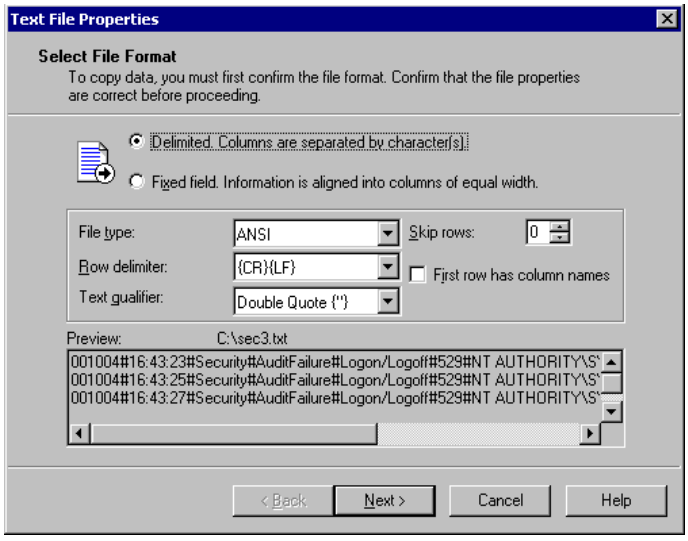
Log zapisi u tekstualnom formatu, dobiveni izvršavanjem `eldump` naredbe u prvom koraku, mogu se učitati u bazu podataka radi jednostavnije analize i obrade. Postupak je sljedeći:

1. Otvoriti `SQL server 2000` Enterprise `Manager`;
2. Otvoriti *Data Transformation Services* direktorij;
3. Desnim klikom na polje *Local Package*, odabrati *New Package* opciju nakon čega se otvara prozor prikazan na slici (**Slika 11**);



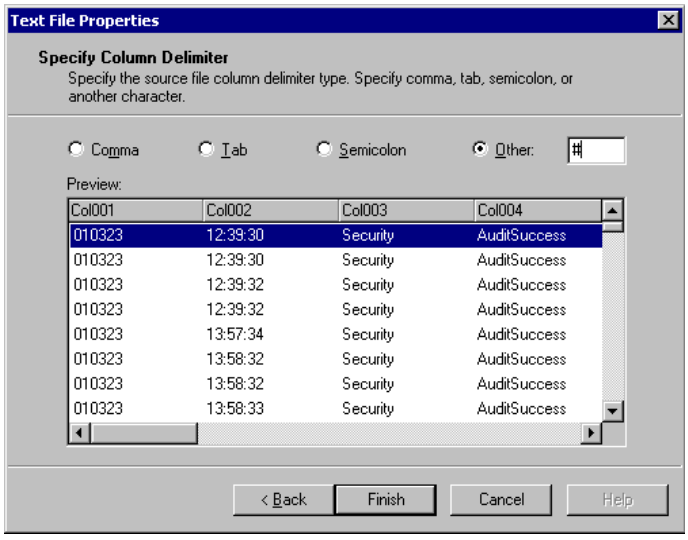

*Slika 11: Učitavanje log zapisa u SQL bazu*

4. Odabrati polje *Connection*;
5. Odabrati željenu tekstualnu datoteku;
6. Odabrati željenu log datoteku;
7. Odabrati polje *Delimited* (**Slika 12**)*;*



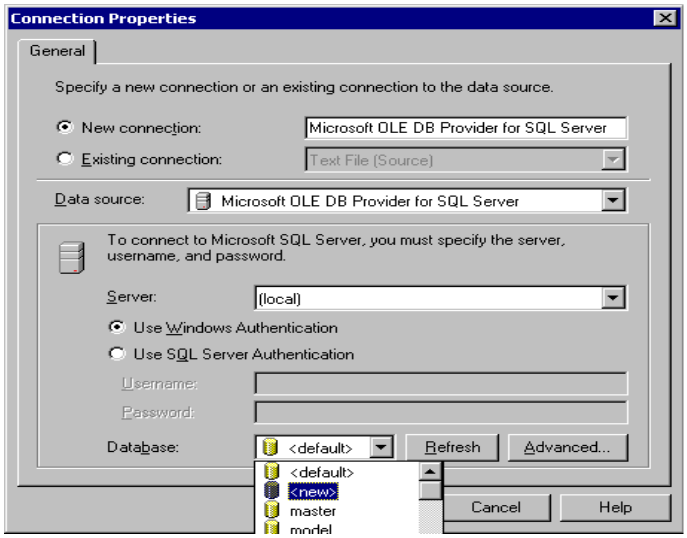

*Slika 12: Učitavanje log zapisa u SQL bazu (2)*

8. Odabrati polje *Other* i navesti znak kojim su polja odvojena u tekstualnoj datoteci (znak #), **Slika 13**;



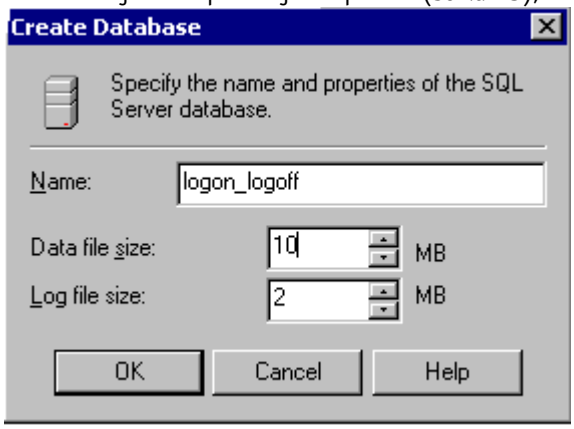

*Slika 13: Učitavanje log zapisa u SQL bazu (3)*

9. Pritisnuti polje *Finish* i *OK*;
10. Unutar DTS stranice, odabrati polje *connections* i *Microsoft OLE DB Provider for SQL Server* (**Slika 14**);



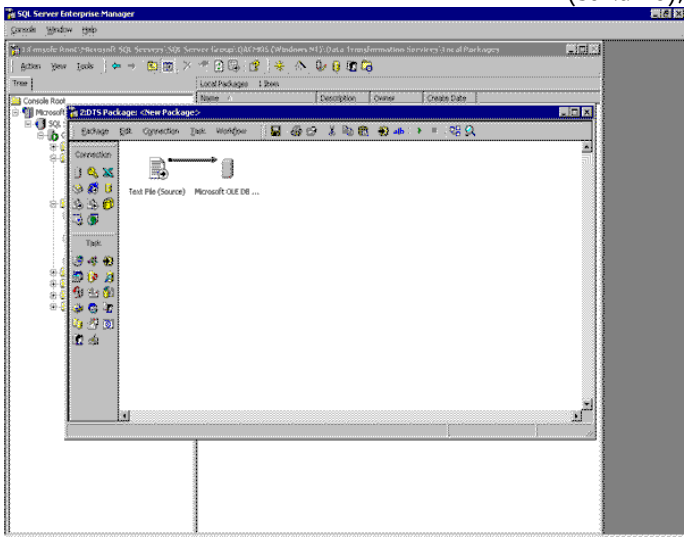

*Slika 14: Učitavanje log zapisa u SQL bazu (4)*

11. Upisati ime nove baze u koje će se pohranjivati podaci (**Slika 15**);




*Slika 15: Učitavanje log zapisa u SQL bazu (5)*

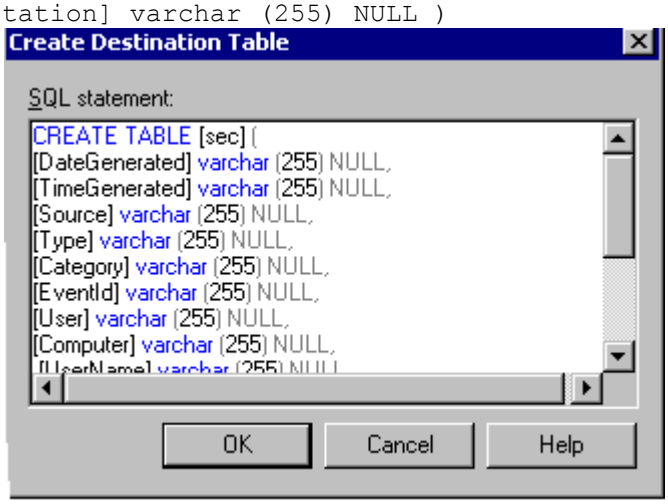
12. Unutar trake s izbornicima odabrati polje *Transform Data Task* s lijeve strane prozora i odabrati tekstualnu vezu kao izvor i OLE DB vezu kao odredište (**Slika 16**);




*Slika 16: Učitavanje log zapisa u SQL bazu (6)*

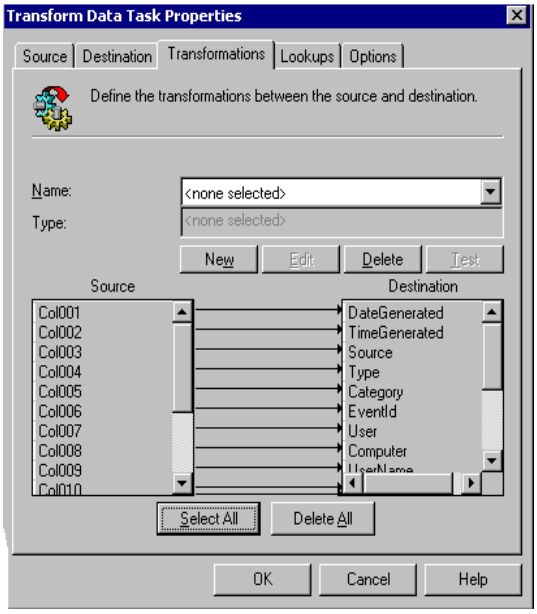
13. Pritisnuti desnim gumbom nad strelicu unutar glavnog prozora i odabrati polje *Properties*;
14. Odabrati odredišni direktorij i definirati SQL naredbe koje će generirati odgovarajuću tablicu;

```
CREATE TABLE [sec] (
[DateGenerated] varchar (255) NULL,
[TimeGenerated] varchar (255) NULL,
[Source] varchar (255) NULL,
[Type] varchar (255) NULL,
[Category] varchar (255) NULL,
[EventId] varchar (255) NULL,
[User] varchar (255) NULL,
[Computer] varchar (255) NULL,
[UserName] varchar (255) NULL,
[Domain] varchar (255) NULL,
[LogonID] varchar (255) NULL,
[LogonType] varchar (255) NULL,
[LogonProcess] varchar (255) NULL,
[AuthenticationPackage] varchar (255)
NULL,
[Workstation] varchar (255) NULL )
```



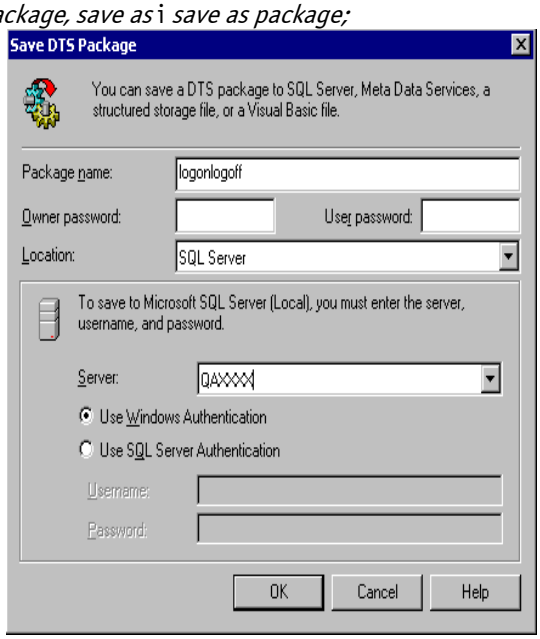

*Slika 17: Učitavanje log zapisa u SQL bazu (7)*

15. Pritisnuti *OK*;
16. Odabrati karticu *Transformation*;
17. Odabrati *Select All* unutar istog prozora;




*Slika 18: Učitavanje log zapisa u SQL bazu (8)*

18. Pritisnuti *OK;*
19. Odabrati polje *Package, save as* i *save as package;*




*Slika 19: Učitavanje log zapisa u SQL bazu (10)*

20. Izvršiti odabrani paket;
21. Ovim koracima kreirana je baza *logon_logoff* sa tablicom *sec* u kojoj se nalaze generirani log zapisi.

### 7.2.3. Korak 3: Generiranje izvještaja

Zadavanjem SQL upita putem *SQL Query Analyzer Tool* sučelja moguće je iz baze filtrirati korisne podatke o događanjima na sustavu. Na primjer, zadavanjem SQL upita,

```
select a.username as Name, a.computer as Computer, a.logontype as
Type, a.datagenerated as Logon_Date,
```

```
a.timegenerated as Logon_Time, b.dategenerated as Logoff_Date,
b.timegenerated as Logoff_Time

from sec as a join sec as b
on a.eventid = 528 and b.eventid = 538 and a.logonid = b.logonid
```

moguće je dobiti podatke o vremenima prijavljivanja i odjavljivanja iz sustava. Korištenjem alata kao što su *MS Access* ili *Crystal Reports* moguće je formatirati dobivene podatke, čime se mogu olakšati postupci njihove analize. Gore navedeni dati će sljedeće rezultate:

| Name | Computer | Type | Logon_Date | Logon_Time | Logoff_Date | Logoff_Time |
|---|---|---|---|---|---|---|
| User1 | TEST009 | 2 | 010323 | 13:58:34 | 010323 | 14:23:00 |
| User2 | TEST009 | 2 | 010223 | 14:24:23 | 010223 | 15:00:04 |
| User1 | TEST016 | 2 | 010223 | 13:58:03 | 010223 | 15:03:08 |

Na sličan način moguće je kreirati i druge tablice koje će pohranjivati ostale događaje na sustavu, prema kojima će se moći obavljati pretraživanje baze i generiranje izvještaja. Primjer događaja koji se mogu pratiti su:

- mrežna prijavljivanja u sustav (engl. *network logons*) (kod 528, tip 3 na NT4 sustavu, kod 540 na W2K sustavima);
- neuspjeli pokušaji prijavljivanja u sustav (kod 529);
- pokušaj prijavljivanja u sustav sa "zaključanog" (engl. *locked*) korisničkog računa (kod 539);
- pokušaj prijavljivanja u sustav s onemogućenog korisničkog računa (kod 531);
- neuspjeli pokušaji prijavljivanja putem Kerberos autentikacije zajedno s pripadajućim uzrokom greške (poruke 675 i 676);
- generiranje "karata" u postupku Kerberos autentikacije – indikacija uspješnog prijavljivanja na domenu (kod 672).

Mogućnost praćenja nekih od upravo navedenih događaja te mogućnosti njihovog pretraživanja i filtriranja prema različitim kriterijima administratorima mogu biti od velike koristi. Prednosti opisanog sustava za praćenje log zapisa još više dolazi do izražaja u većim računalnim mrežama, gdje se svakodnevno generiraju velike količine log zapisa. U takvim slučajevima je proces praćenja i analize log zapisa vrlo težak i zamoran te često rezultira previđanjem važnijih događaja.

# 8. Zaključak

U ovom dokumentu opisani su postupci autentikacije kod Windows operacijskih sustava sa naglaskom na W2K platforme. Opisane su osnovne karakteristike autentikacijskih protokola (LM, NTLM, Kerberos) kako bi se uvidjele prednosti i nedostatci pojedinih algoritama te razlozi za prelazak na novije tehnologije.

U nastavku dokumenta opisani su log zapisi, odnosno događaji, koji se generiraju u procesu prijavljivanja korisnika u sustav zajedno s njihovim značenjem. U svrhu testiranja i analize mogućih događaja, uspostavljeno je testno okružje s kombinacijom Windows NT i Windows 2000 sustava. Ukratko su analizirani log zapisi generirani u različitim scenarijima prijavljivanja u sustav u mješovitim Windows okolinama.

Na kraju dokumenta analizirane su mogućnosti pohranjivanja log zapisa unutar `SQL server 2000 Enterprise Manager` aplikacije te osnovni postupci konfiguracije sustava.