PROTECŢIE ŞI SIGRANŢĂ ÎN FUNCŢIONARE

GRUPA 443A

OFRIM DRAGOŞ

OFRIM BOGDAN

SĂCĂLEANU DRAGOŞ

CRAINIC DAN

Administratorii de sistem experimentaţi caută în permanenţă breşe în sistemul lor de securitate şi modalităţi de îmbunătăţire a acestuia din cauza faptului că există persoane răuvoitoare ce caută să spargă mecanismele de securitate. Dacă mecanismul de securitate nu este modificat, hackerii vor încerca diferite metode de a-l depăşi până când una va reuşi. Dacă mecanismul de securitate se modifică în timp hackerii vor pierde majoritatea timpului încercând să ajungă în punctul de la precedenta încercare şi astfel sistemul rămâne intact.

Nu există imunitate perfectă la atacurile ce privesc sistemele de securitate deoarece tot timpul răufăcătorii găsesc puncte slabe pe care le exploatează. Scopul urmărit este de a menţine securitatea sistemului la un nivel cât mai ridicat posibil şi informarea imediată asupra atacurilor produse.

Window NT este un sistem de operare Microsoft dedicat serverelor, fiind proiectat pentru a răspunde pieţei în continuă dezvoltare a reţelelor locale. Nivelele de acces la informaţiile stocate în server sunt controlate printr-un mecanism ce se bazează pe sistemul de fişiere NT sau NTFS. Modelul de securitate Windows NT şi sistemul de operare NTFS permit administratorului de reţea să controleze accesul utilizatorului de la un nivel ca acela al unităţii de disc, trecând până la nivelul directoarelor şi ajungând la nivelul fişierelor individuale dintr-un director.

Fiind un sistem remarcabil de unitar, NTFS are doar unele scăpări minore care pot fi totuşi exploatate de hackeri într-o oarecare măsură. Se pot enumera câteva:

- daca pe un server se creează un director pentru un utilizator, acesta poate folosi instrumente de administrare de sistem pentru a permite accesul la directorul respectiv oricărei persoane care accesează serverul, deoarece utilizatorul este posesorul directorului în cauză; dacă un hacker reuşeşte să intre în server ca utilizator cu drepturi extinse, acesta poate partaja directoarele utilizatorului respectiv cu

oricine şi apoi poate ieşi din server, păstrând accesul la directorul nou partajat;

- un hacker poate reporni serverul folosind o dischetă MS-DOS şi poate accesa unitatea server NT cu un utilitar Microsoft denumit ntfsdos.exe; acesta poate vizualiza apoi întreaga unitate server fără a mai avea nevoie de permisiuni de securitate;
- dacă unui utilizator i se acordă control complet asupra unui director, în locul permisiunilor de citire, scriere, ştergere şi creare, utilizatorul primeşte o permisiune ascunsă denumită File Delete Child. Aceasta nu poate fi eliminată şi oferă utilizatorului dreptul de a şterge din director orice fişier care poate fi doar citit. Pentru o implementare Windows NT, capacitatea utilizatorului de a şterge fişiere importante poate fi extrem de periculoasă.

Există mai multe tipuri de atacuri la adresa sistemelor de securitate fiecare având mecanismul specific şi metoda de exploatare a vulnerabilităţii sistemului.
O metodă de atac la adresa securităţii este calul troian, program sau script ascuns în interiorul unui program autorizat. Multe din aceste programe sunt destinate sistemelor Microsoft şi afectează în special programele de gestionare a poştei electronice. Un exemplu de cal troian este programul Love Bug din anul 2000. Acesta se ascundea într-o scrisoare de dragoste şi când era deschis se autoexpedia tuturor persoanelor din agenda de adrese, ştergea fişiere de pe disc şi descărca un alt program de tip cal troian care prelua parolele din sistem. Love Bug a afectat doar sistemele Microsoft Windows. Programele de tip "cal troian" sunt rar întâlnite la sistemele Linux, un exemplu fiind depistat în pachetul "util-linux-2.9g.tar.gz" pe anumite situri web, iar protecţia împotriva acestora este greu de asigurat.

S-au dezvoltat tehnici de verificare a fişierelor descărcate la Red Hat şi alte distribuţii. Pretty Good Privacy (PGP) oferă criptarea asimetrică a datelor

pentru poşta electronică, chei secrete şi criptare simetrică pentru alte tipuri de fişiere. PGP se foloseşte în special pentru asigurarea destinatarilor că mesajele citite nu au fost interceptate, ci au fost trimise chiar de autor. Suma de control reprezintă un tip de semnătură utilizată pentru validarea fişierelor atunci când acestea sunt transferate prin mijloace nesigure. Suma de control se calculează din valorile binare ale octeţilor fişierului creând o amprentă a acestuia. La recepţionarea fişierului se calculează o nouă amprentă care se verifică cu cea calculată anterior.

O altă metodă de atac a sistemelor Linux este "poarta din spate" care reprezintă un cod adăugat la program ce permite accesul neautorizat la calculatorul gazdă. Poarta din spate se poate depista analizând codul sursă a produsului. Unele sisteme care utilizează programe de gestionare a pachetelor (Red Hat Package Manager şi Package Management System din distribuţia Debian) dispun de comenzi ce verifică dacă pachetul a fost sau nu modificat şi de coduri de eroare ce indică modificările aduse.

O vulnerabilitate a sistemelor Linux o reprezintă fişierele care configurează sistemele "de încredere". Aceste fişiere permit utilizatorilor să intre în sistem fără parolă dacă numele lor şi al maşinilor pe care lucrează sunt incluse în fişierele "/etc/hosts.equiv" şi ".rhosts" din directoarele proprii ale utilizatorilor. Majoritatea administratorilor dezactivează comenzile pe care se bazează aceste fişiere şi le înlocuiesc cu pachetul Secure Shell (SSH).

O altă metodă de atac asupra sistemului Linux este tehnica "spoofing" ce presupune falsificarea identităţii unui utilizator cunoscut. Falsificarea face ca mesajele pe care le vede un destinatar să apară ca fiind trimise de un utilizator cunoscut şi ca datele primite să apară ca provenind de la o maşină de încredere. Acest tip de atac poate fi combătut prin configurarea nucleului Linux pentru verificarea adresei sursei.

Un tip de atac des întâlnit este cel asupra parolelor utilizatorilor. Cei care vor să intre într-un sistem pot încerca să găsească parola unui utilizator şi astfel să obţină accesul pe contul respectiv. Acest tip de atac poate fi combătut prin instruirea utilizatorilor de a alege parole greu de găsit şi de a le schimba des.

Sistemul Linux foloseşte un utilitar "cracklib" ce determină gradul de siguranţă al unei parole şi nu permite utilizatorilor obişnuiţi să îşi aleagă o parolă din dicţionarul cracklib, doar superuser-ul având acest drept.

Sistemul Linux are o vulnerabilitate la atacurile fizice. O persoană care dispune de o dischetă de pornire poate reporni sistemul în modul monoutilizator şi în acest fel capătă privilegii de root în acel sistem. Pentru securizarea sistemului trebuie modificată configuraţia implicită prin introducerea unei parole la repornirea sistemului. Pentru ca această parolă să nu fie văzută de intruşi trebuie introdusă o parolă la configuraţia BIOS astfel încât să fie împiedicată pornirea sistemului de pe dischetă sau CD-ROM.

Există atacuri specifice la adresa serverului Windows NT.

Atacul prin "mirosirea" reţelei.

Prin "mirosirea" unei reţele de către un hacker se înţelege interceptarea şi copierea pachetelor care parcurg reţeaua, urmărind eventuale informaţii valoroase incluse în acestea. Una din situaţiile ce facilitează "mirosirea" reţelei o reprezintă utilizarea unei versiuni mai vechi a programului Windows NT *LANMAN LAN Manager*. Parolele trimise pe reţea de către acest program sunt în format de text simplu, ducând la intercepţia lor fără un atac direct asupra sistemului şi fără un acces ulterior în sistem ca utilizator obişnuit. În versiunile Windows NT 3.51 şi ulterioare, parolele sunt trimise în formă criptată, reducându-se riscul decodificării lor.

Pe de altă parte, un hacker poate intercepta orice parolă în clar trimisă de protocoale tradiţionale – FTP sau Telnet. Sunt şanse foarte mari ca parola de utilizator FTP să coincidă cu cea de cont NT şi astfel acest lucru să faciliteze accesul la reţeaua NT. În această situaţie este indicată utilizarea sistemelor de protecţie FTP.

Atacuri prin refuzul serviciului

Transformarea unui serviciu disponibil de la o staţie de lucru sau server într-un serviciu indisponibil este modalitatea cea mai des întâlnită prin care hacker-ii atacă reţeaua. Principalele motive pentru utilizarea acestui tip de atacuri sunt:

- necesitatea reîncărcării sistemului de operare pentru lansarea virusului în cazul instalării de către hacker a unui “cal troian”;
- pentru a da impresia unei simple erori, hackerul doreşte să-şi acopere numele sau să acopere activitatea unităţii centrale de procesare cu o cădere aleatoare de sistem.
- Hackerul doreşte pur şi simplu să provoace căderea serverului.

Se poate întâmpla ca şi administratorul de sistem să utilizeze acest tip de atacuri – pentru verificarea imunităţii sistemului sau atunci când există un proces scăpat de sub control care determină căderea sistemelor utilizatorilor, pune datele în pericol, iar administratorul nu are acces fizic la server.

Vulnerabilitatea Windows la atacurile TCP

Windows NT are un grad ridicat de rezistenţă la atacuri TCP cum ar fi atacul prin predicţia numărului de secvenţă. Există totuşi un atac care este eficient împotriva unui server Windows NT şi anume atacul prin deturnarea sesiunii. Acesta se poate efectua împotriva unei reţele Windows NT, dar totodată este mai uşor de întreprins acest atac împotriva unui server Windows NT în comparaţie cu o comunicare prin reţele Unix, datorită modului de examinare a pachetelor TCP în Windows NT.

Sistemul de operare Windows NT a fost creat astfel încât să primească o atestare de clasă minimum C2 în sistemul de evaluare Orange Book al Departamentului American al Apărării. Atestarea a fost primită pentru un sistem de sine stătător, fără unitate de dischetă si fără conexiune de reţea. Cu toate acestea Microsoft a creat un model de securitate pentru Windows NT extensibil, programele pot extinde cu uşurinţă modelele pentru a include noi facilităţi de

securitate, totodată asigurând şi un mediu server de reţea comercial de mare siguranţă. Aspectul cel mai important al evaluării modelului de securitate de clasă C2 îl reprezintă regulile de bază stabilite de acesta pentru accesul la obiectele de sistem. Se poate da ca exemplu suportul Kerberos pe care modelul de securitate Windows NT 4.0 nu-l includea, îin timp ce modelul de securitate Windows NT 5.0 îl conţine. Acest protocol a fost adăugat la lista de protocoale de securitate acceptate de NT în loc de a rescrie întregul model de securitate pentru a fi inclus si suportul Kerberos.

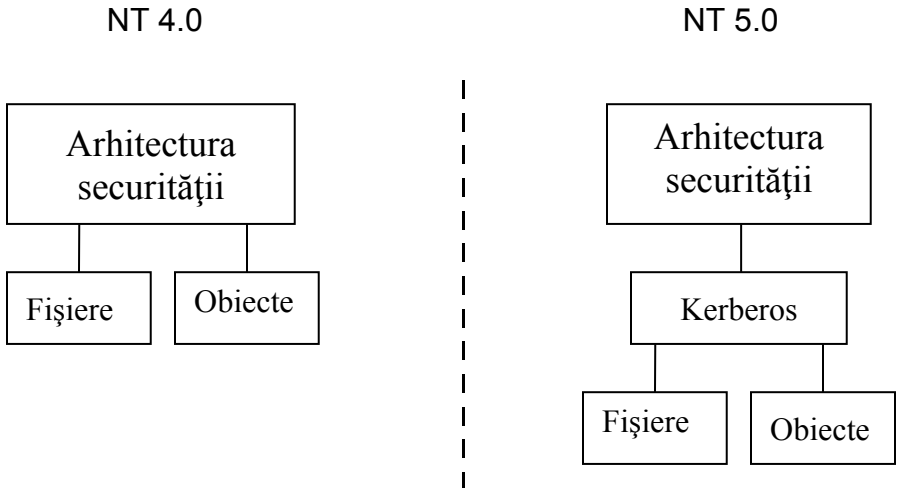


Figura 1 - Spre deosebire de modelul de securitate Windows NT 4.0, modelul de securitate Windows NT 5.0 include protocolul Kerberos

Fiecare obiect Windows NT îşi are propriile atribute de securitate (descriptoare de securitate) care controlează accesul utilizatorului la obiectul respectiv. Descriptorul de securitate este format pe de-o parte dintr-o listă de control al accesului (ACL), impusă de modelul C2, ce conţine informaţii care specifică utilizatorii şi grupurile care au acces la obiect şi nivelul de acces al acestora, şi pe de alta parte informaţii referitoare la obiectul în sine. Grupurile sunt utilizatori asociaţi, în general, printr-o grupare socială sau departamentală. Windows NT instalează mai multe grupuri prestabilite (Everyone, Power Users şi

Administrators) şi acceptă nivele sau tipuri de acces pentru fiecare (grupul Everyone poate avea numai acces de citire la un obiect în timp ce grupul Power Users poate avea acces de citire, scriere, copiere şi ştergere la un obiect).

Lista de control al accesului este formată din două componente: lista de control al accesului discreţionar care controlează utilizatorii care au acces la un anumit obiect (suferă cele mai frecvente modificări) şi lista de control al accesului la sistem care controlează obiectele şi serviciile de sistem care au acces la un anumit obiect.

Informaţii despre obiect	Lista de control al accesului (ACL)	
Nume Locaţie Dimensiune	Lista de control al accesului discreţionar	Lista de control al accesului la sistem (SACL)

Figura 2 - Structura unui descriptor de securitate

Când un utilizator sau un serviciu creează un obiect, Windows NT creează întotdeauna un descriptor de securitate pentru acest obiect. În cazul în care utilizatorul sau serviciul nu îşi ataşează propriile atribute de securitate la fişierul respectiv, Windows NT creează o listă de control al accesului discreţionar fără intrări (Windows NT creează obiectul fără permisiuni explicite şi nimeni nu are acces la el). Permisiunea de a accesa un obiect o au doar utilizatorii şi

grupurile specificate în lista de control al accesului dicreţionar, după ce sistemul a adăugat la obiect permisiuni specifice.

Sistemul de securitate Windows NT are patru componente principale.

Local Security Authority (Autoritatea de securitate locală sau subsistem de securitate) este componenta centrală a securităţii şi se ocupă cu securitatea locală, autentificarea utilizatorilor, generarea şi jurnalizarea mesajelor de verificare (audit).

Security Account Manager (Managerul de securitate a conturilor) gestionează conturile utilizator şi de grup şi pune la dipoziţia autorităţii de securitate locală servicii de autentificare.

Security Reference Monitor (Monitorul de referinţă a securităţii) validează accesul şi verifică (auditing) pentru autoritatea de securitate locală, permite sau refuză utilizatorului accesul la fişier în funcţie de conturile acestuia şi generează mesaje de verificare în funcţie de decizia luată. Monitorul de referinţă a securităţii are o copie de validare a accesului asigurând astfel o protecţie uniformă a resurselor sistemului.

User Interface (Interfaţa utilizatorului) reprezintă ceea ce vede utilizatorul la sfârşit şi execută majoritatea operaţiunilor de natură administrativă .

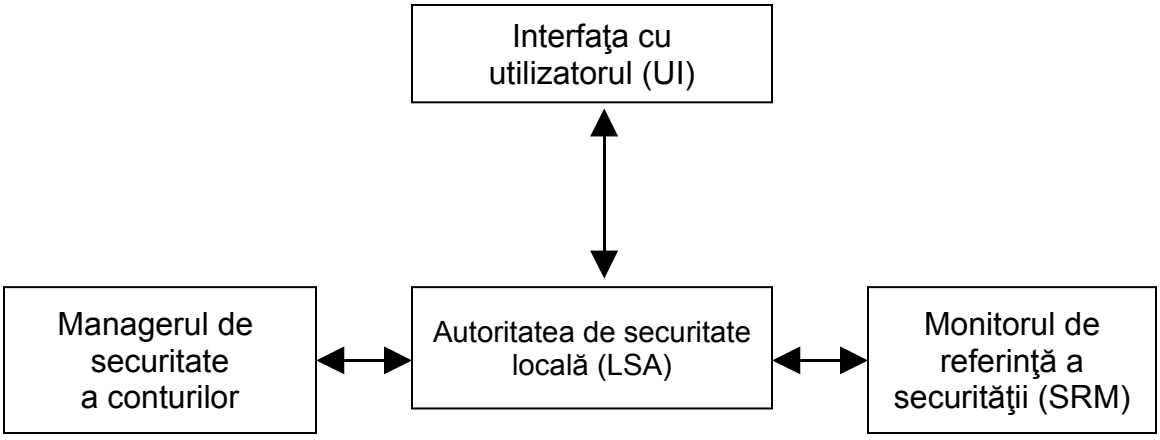


Figura 3 - Natura interactivă a modelului de securitate Windows NT

Fiecare utilizator sau grup trebuie să aibă în mod specific permisiune de acces la un obiect pentru ca sistemul de operare să-i permită accesul la obiectul respectiv. Un sistem Windows NT implementat fără greşeală face mai dificilă spargerea acestuia, însă acest model de securitate nu este unul perfect având puncte slabe indiferent dacă este instalat cât mai bine posibil.

Modul de autentificare a utilizatorilor de către SAM

Windows NT permite accesul unui utilizator dacă recunoaşte numele de cont şi parola acestuia şi creează un obiect jeton (token) care reprezintă utilizatorul în faţa sistemului de operare.

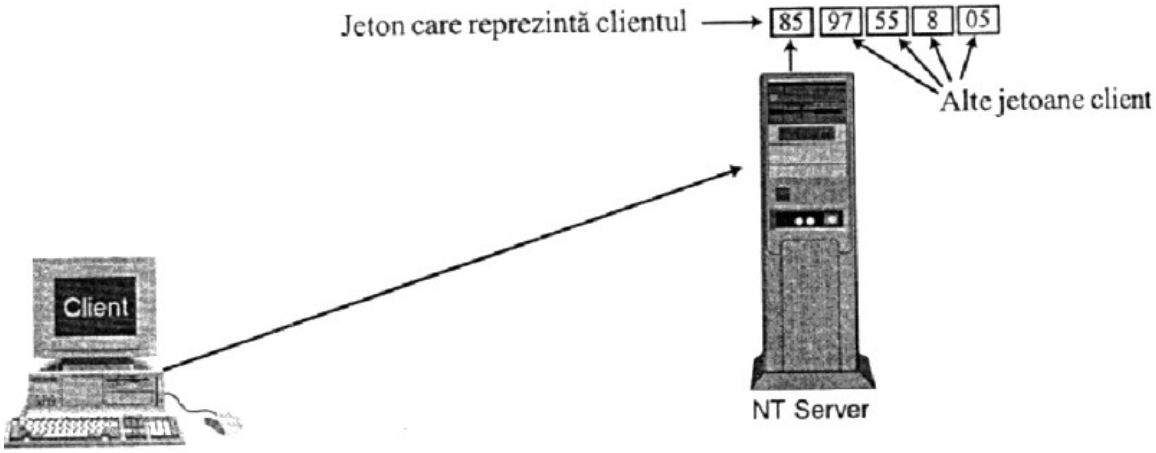


Figura 4 - Sistemul de operare creeaza un jeton pentru a reprezenta utilizatorul

Când utilizatorul rulează un program sistemul de operare creează o asociere între procesul (sau firul) programului şi jetonul acestuia (combinaţia jeton-proces se numeşte subiect) .

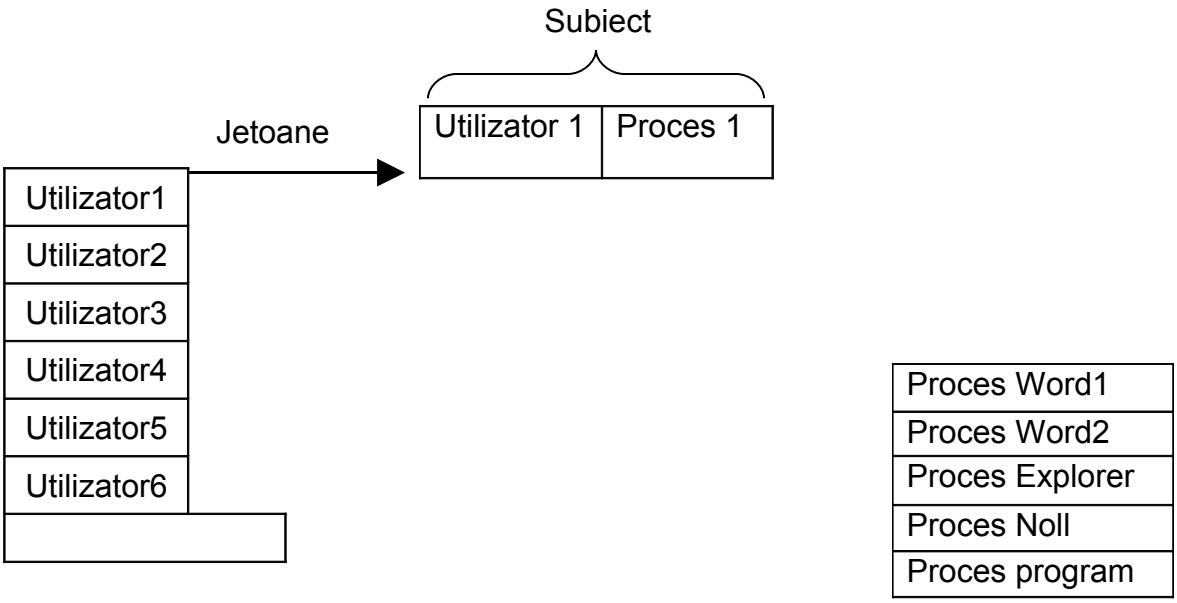


Figura 5 - Sistemul de operare creează un subiect dintr-un proces şi jetonul unui utilizator

Când subiectele accesează obiecte (fişiere sau directoare) Windows NT permite sau nu accesul subiectului la obiect după ce verifică jetonul subiectului în lista de control al accesului şi poate afişa un mesaj de verificare (audit) dacă serverul este astfel configurat.

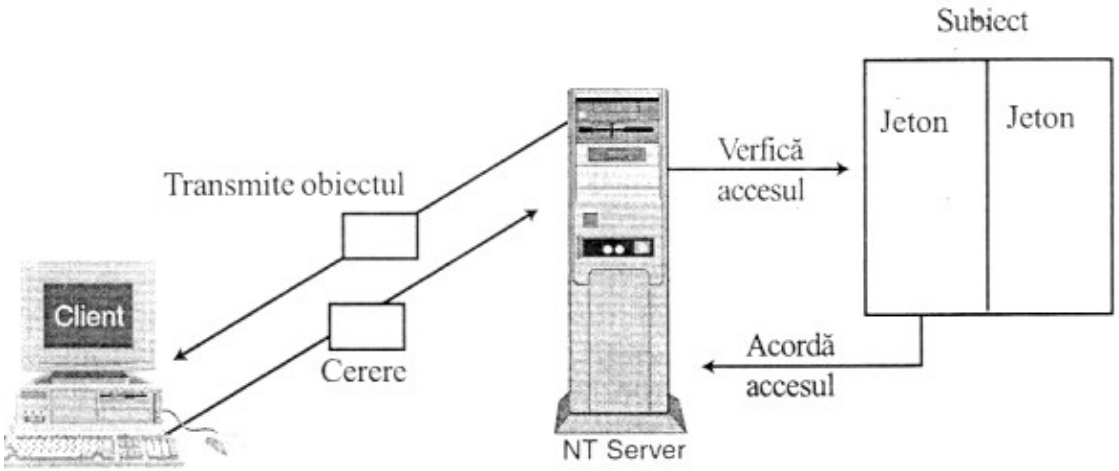


Figura 6 - Sistemul de operare citeşte jetonul subiectului înainte de a-i acorda acces la obiect

Securizarea grupului administrators

În cazul în care un hacker care a încercat să ajungă la un calculator cu un cont de administrator pentru a avea acces la întregul server sau domeniu şi nu a reuşit, conturile fiind suficient de bine asigurate, va încerca să intre în sistem cu un cont de nivel mai redus şi să-şi acorde statutul de membru al grupului Administrator (atac progresiv de securitate – security step-up attack) .

Una dintre cele mai bune modalităţi de protecţie împotriva unui atac progresiv este de a elimina sau modifica drepturile grupului Administrators şi de a se crea un nou grup cu drepturi de acces complete astfel încât hackerul să nu ştie care este grupul ale cărui drepturi vrea să le obţină .

Modalitatea de stocare a parolelor în Windows NT

Pentru verificarea identităţilor utilizatorilor ce accesează sistemul, fiecare sistem de operare utilizează o bază de date cu parole de anumit tip. Pentru sistemul de operare Windows NT această bază se află la adresa "\winnit\system32\config\sam" din serverul Windows NT. La această locaţie sunt de fapt memorate valorile hash unisens ale parolelor utilizatorilor.

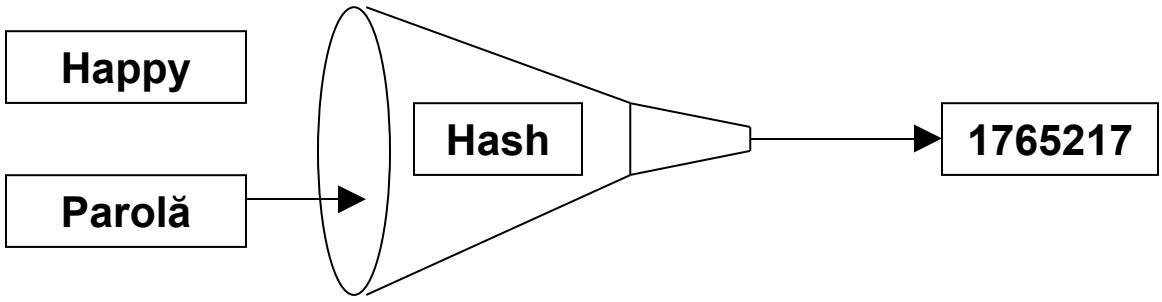


Figura 7 - Sistemul de operare converteşte o parolă într-o valoare hash

O funcţie hash unisens are rolul de a reduce la o formă unică datele de intrare procesate. În Windows NT parola text este convertită într-o serie de octeţi şi apoi convertită într-o valoare hash unisens prin algoritmul MD4 (Message Digest-4).

La încercarea utilizatorului de a accesa serverul, acesta se comportă asemenea sistemului de operare, trecând parola prin funcţia hash unisens MD4. Ulterior, serverul compară valoarea hash unisens a parolei primită de la staţia de lucru cu valoarea hash din baza de date cu parole. În caz de răspuns afirmativ, utilizatorul este acceptat în reţea.

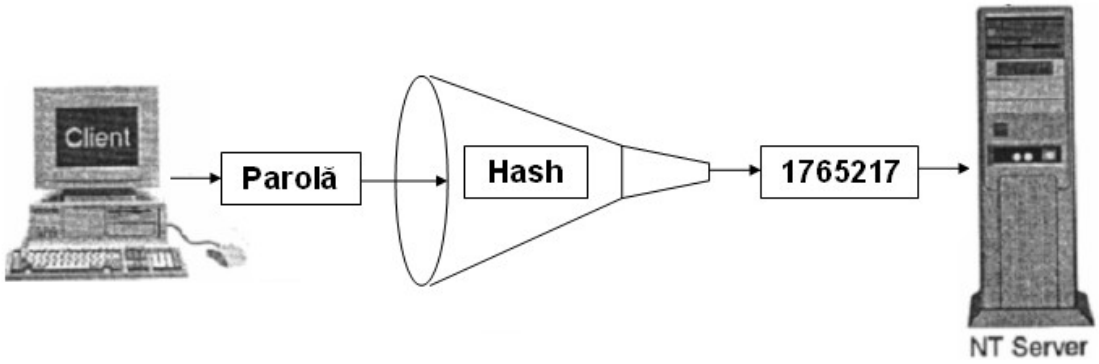
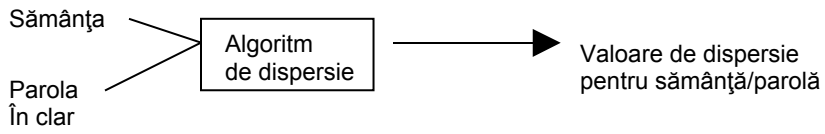


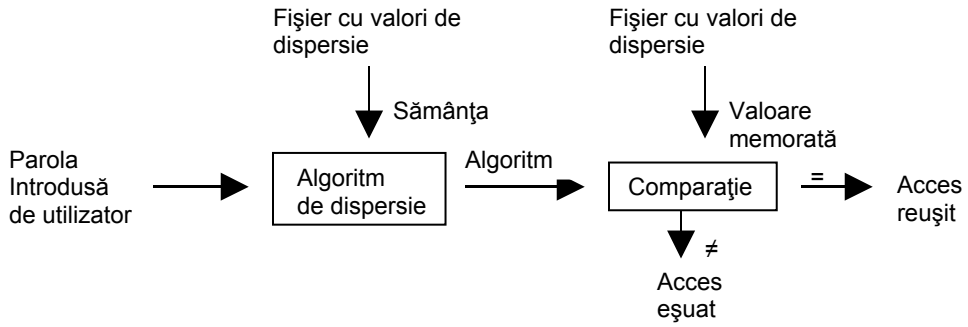
Figura 8 - Sistemul de conversie şi transmisie a parolelor folosit de Windows NT

O cale de pătrundere în sistem ce trebuie protejată este procesul de autentificare al utilizatorilor. Sistemul Linux foloseşte două sisteme de autentificare a parolelor utilizatorilor: DES (Data Encryption Standard) şi MD5 (Message Digest Algorithm, versiunea 5). Parolele criptate cu algoritmul MD5 sunt mai lungi decât cele criptate cu algoritmul DES şi încep cu secvenţa 1. Orice parolă care nu începe cu secvenţa 1 este de tip DES. Algoritmul DES poate lucra cu parole MD5, dar algoritmul MD5 nu poate lucra cu parole DES.

În sistemele Linux parolele sunt codificate într-un mod ce nu permite decriptarea. Atunci când un utilizator îşi schimbă parola, şirul introdus de la tastatură şi un şir "sămânţă" generat de sistem sunt trimise unui algoritm DES modificat sau unui algoritm MD5 pentru a se genera o valoare de dispersie. Algoritmul DES produce o valoare de dispersie de 13 caractere, primele două fiind sămânţa iar celelalte 11 reprezentând parola codificată, iar algoritmul MD5 creează un cod de 32 de caractere care începe întotdeauna cu secvenţa 1. La autentificare, parola introdusă de utilizator şi valoarea sămânţă determinată sunt trimise algoritmului DES generându-se o valoare de dispersie. La algoritmul MD5 primele două caractere ale codului sunt $1 urmate de sămânţă, caracterul $ şi parola codificată. Codul generat se compară cu valoarea de dispersie memorată şi dacă cele două valori coincid atunci parola introdusă este corectă.



Crearea unei parole



Accesul în sistem

Figura 9 - Modul de realizare a dispersiei parolelor de către sistemul Linux

Slăbiciunea acestui sistem de autentificare este dată de necesitatea ca parolele memorate să poată fi citite de toate programele care au nevoie de ele. Chiar dacă codurile memorate nu pot fi decriptate ele pot fi comparate cu o listă de valori generată pentru a se detecta asemănări ce pot fi exploatate ulterior. Spărgătorii de parole codifică un dicţionar de cuvinte şi parole uzuale folosind toate cele 4096 de combinaţii de sămânţă, compară valorile generate cu valorile de dispersie memorate. Orice potrivire a codurilor determină aflarea unei parole cu care se accesează contul unui utilizator al sistemului. Pentru a se elimina această vulnerabilitate se foloseşte o tactică de ascundere a parolelor. Valorile de dispersie memorate sunt transferate într-un fişier ce poate fi citit şi scris doar de superutilizator. În acest mod se împiedică accesul utilizatorilor la valorile memorate şi se pot efectua anumite operaţii asupra parolelor. Se pot obliga utilizatorii să-şi schimbe parola la un anumit interval, se poate interzice schimbarea parolelor într-un anumit interval sau se pot dezactiva conturile neaccesate într-o anumită perioadă de timp. Aceste operaţii pot fi determinate şi efectuate pentru fiecare utilizator în parte.

S-a ajuns în timp la concluzia că identitatea utilizatorilor nu poate fi cunoscută doar pe baza parolei introduse la intrarea în sistem. Astfel, utilizatorii nu trebuie să aibă acces la toate resursele sistemului doar prin simpla autentificare la intrarea în sistem. Linux foloseşte un sistem de autentificare cu module PAM. PAM este un sistem de module de biblioteci care permit administratorului de sistem să configureze un sistem de autentificare pentru fiecare aplicaţie individuală. PAM conţine patru module care realizează următoarele operaţii: autentificarea utilizatorilor, gestiunea conturilor, gestiunea parolelor şi gestiunea sesiunilor de lucru. Pentru a putea lucra cu PAM, aplicaţiile sunt realizate pentru a nu depinde de nici un sistem de autentificare. Administratorul sistemului poate schimba schema de autentificare a unei aplicaţii compatibile PAM fără a rescrie codul aplicaţiei, ci modificând doar fişierul de configurare PAM care poate fi specific aplicaţiei sau global, folosit pentru toate aplicaţiile din sistem. Dacă modulele din fişierul de configurare PAM nu pot

realiza schema de autentificare dorită se pot scrie module noi care sunt apoi inserate în schemă.

Grupurile de domeniu prestabilite pentru Windows NT

La instalarea serverului Windows NT sistemul de operare creează automat şase grupuri prestabilite.

Administrators au dreptul de acces complet la orice fişier sau director atât din server cât şi din interiorul domeniului.

Backup Operators pot evita controlul de securitate într-o operaţie de backup. Drepturile acestora prezintă un risc mare pentru reţea deoarece un hacker poate intra în fişiere off-line prin efectuarea unui backup de reţea.

Guests pot intra în domeniu şi vizualiza majoritatea fişierelor, dar nu le pot accesa în alt fel.

Power Users au toate drepturile utilizatorilor, au drepturi extinse faţă de directoarele date şi pot partaja directoarele şi imprimantele cu alţii.

Replicator poate copia fişiere dintr-o locaţie în alta, dar nu poate deschide sau modifica fişierele copiate fără drepturi suplimentare de acces.

Users au acces home directory (director iniţial propriu) la aplicaţii şi eventual la un director partajat de date.

Grupuri locale prestabilite pentru Windows NT

Administratorii au toate drepturile într-o reţea, însă membrii următoarelor grupuri au unele drepturi suplimentare.

Server Operators pot închide serverul chiar de la distanţă, pot reseta ceasul de sistem al serverului şi pot efectua operaţii de backup şi restabilire.

Backup Operators pot închide serverul şi efectua operaţii de backup şi restabilire .

Account Operators şi Print Operators pot închide serverul.

Este necesară securizarea şi monitorizarea privilegiilor de acces membrilor acestor grupuri întrucât un hacker poate obţine un cont Server

Operator, introduce un virus de tip cal troian în server care se activează după o închidere de la distanţă şi care poate da hackerului privilegii de administrator.

Permisiunile prestabilite pentru directoare din Windows NT

La instalarea sistemului Windows NT se creează permisiuni pentru directoare prestabilite pentru fiecare grup prestabilit după cum urmează.

Server Operators şi utilizatorii pot citi şi executa fişiere, pot afişa permisiunile pentru fişiere şi pot modifica atributele unor fişiere din directoarele "winnt", "\system 32", "\win32app".

Toţi utilizatorii pot lista numele de fişiere din directorul "\system32\config".

Server Operators au drepturi de acces complete (citire, scriere, ştergere, execuţie şi creare), iar toţi utilizatorii au drepturi de citire din directoarele "\system32\drivers" şi "\system\repl".

Server Operators şi Print Operators au drepturi de acces complete, iar toţi utilizatorii au drepturi de citire din directorul "\system32\spool".

Server Operators pot citi şi executa fişiere, pot afişa permisiunile pentru fişiere şi pot modifica anumite atribute de fişiere, iar Replicator au drepturi de citire din fişierul "\system32\repl\export".

Server Operators şi Replicator pot citi şi executa fişiere, pot afişa permisiunile pentru acestea şi pot modifica atributele unor fişiere, iar utilizatorii au drepturi de citire din directorul "\system32\repl\import".

Account Operators pot citi, scrie, şterge şi executa fişiere, iar utilizatorii pot lista numele de fişiere din directorul "\users".

Toţi utilizatorii pot citi, scrie şi executa fişiere din directorul "\users\default".

Fişierele din Linux pot fi securizate prin asocierea unui şir de permisiuni ce determină tipul accesului pentru proprietarul fişierului, membrii grupului de care aparţine fişierul şi ceilalţi utilizatori ai sistemului. Tipurile de acces la fişiere ce pot fi acordate sunt citire, scriere şi execuţie. La stabilirea nivelului de acces pentru un fişier trebuie să se ia în consideraţie utilitatea fişierului. Astfel, pentru ca un utilizator să poată vizualiza un fişier ce se găseşte într-un anumit director trebuie

ca utilizatorul sau grupul din care face parte să aibă drepul de citire al fişierului activat şi directorul să permită de asemenea accesul la fişier. Şirurile de permisiuni asociate fişierelor sunt o metodă bună de protecţie a informaţiei din sistem, însă intruşii nu trebuie lăsaţi să ajungă atât de departe.

Windows NT acceptă protocoale de securitate multiple

Microsoft a creat un răspuns cu privire la problemele de securitate ridicate de protocoale. Ea se numeşte Security Service Provider Interface – SSPI şi asigură o modalitate standard de acces la serviciile de securitate distribuite. Microsoft a conceput această interfaţă pentru Windows NT. Furnizorii de servicii de securitate – SSP implementează protocoale de securitate în interfaţa furnizor de servicii de securitate – SSPI. Firme terţe au început crearea de SSP-uri suplimentare care se vor include în Windows NT. În esenţă, protocoalele comunică cu SSP-urile, care la rândul lor comunică cu SSPI, iar acestea comunică cu API-urile pentru a implementa cererea de protocol.

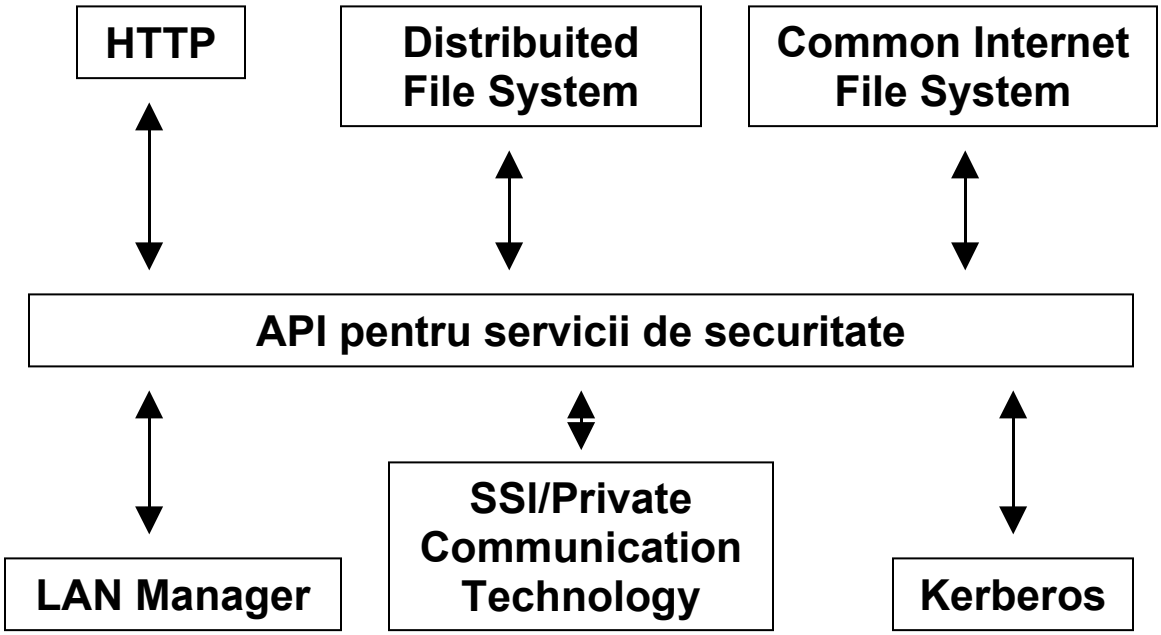


Figura 10 - Modelul Security Service Provider Interface

Despre serviciile protocolului Secure Message Block

Controlul accesului la reţea şi al accesului de la distanţă la serviciile serverului se face de către Windows NT cu ajutorul protocolului Secure Message Block (SMB – bloc de mesaje sigure). Utilizatorilor li se permite accesul de la distanţă la directoarele partajate, la Registry şi la alte servicii sistem. Windows NT controlează accesul folosind nume de utilizatori şi parole. Totuşi, un hacker poate încerca să ghicească nume de utilizatori şi parole folosind atacuri prin forţă brută sau prin dicţionar. Pentru a diminua efectele acestor atacuri, utilizatorilor li se cere crearea de parole de minimum opt caractere, iar cel puţin unul dintre acestea să fie un număr sau simbol. Există de asemenea încă un element de securitate, utilizatorul având un număr limită de login-uri ratate, depăşirea acestuia ducând la blocarea pentru minimum 24 de ore a contului acestuia.

Un cont *Administrator* nu va avea număr limită de login-uri ratate deoarece sunt posibile atacuri prin refuzul serviciului (prin care erorile repetate de login dezactivează toate conturile din calculator). Astfel, parola trebuie să fie lungă şi greu de ghicit. Administratorul poate intra în reţea numai din server sau din controllerul de domeniu. Astfel, un hacker trebuie să fie prezent fizic pentru a putea intra în sistem cu drepturi de administrator.

Protecţia totală a reţelei împotriva accesului la partajările NETBIOS

Partajarea presupune un fişier, un director sau o resursă partajată. O partajare NetBios este creată de către NT la instalarea sistemului de operare. NT foloseşte accesul la partajare în mod prestabilit şi astfel partajările cu acces complet activat devin frecvente. Partajările pot fi folosite de către un atacator pentru determinarea căderii sistemului, în aceste condiţii putându-se opta între elimiarea partajării şi stabilirea de permisiuni explicite pentru corectarea pemisiunilor excesive.

Securitatea serviciului LAN MANAGER

În cazul în care se doreşte conectarea la un server NT, clienţii NetBIOS non-NT pot apela la serviciul Windows LAN Manager ce rulează pe Windows NT. Se utilizează mai ales la conectarea calculatoarelor cu sisteme de operare anterioare.

Un discomfort al acestei soluţii este o siguranţă redusă faţă de autentificarea normlă NT-NT. Mai mult, din cauza posibilităţii de creere a unor breşe suplimentare de securitate în reţea de către LAN Manager, cea mai sigură reţea Windows NT este cea care utilizează staţia de lucru NT 4.0 atât pe partea de client cât şi pe cea de server.

O problemă majoră privind securitatea sistemului o reprezintă protejarea reţelei împotriva accesului neautorizat atunci când este conectată la internet. Există mai multe metode de protecţie, dar pentru a maximiza şansele de stopare a intruşilor se folosesc combinaţii ale acestor metode.

NT şi securitatea serverelor FTP

Având în vedere că cel puţin un server dintr-o instalaţie de reţea Windows NT se va conecta la internet, securitatea din acest punct de vedere este extrem de importantă. Un server FTP inclus în Windows NT are numeroase probleme. Semnificativ mai sigur este serverul FTP Internet Information Server şi se recomandă utilizarea acestuia în dauna unui server standard inclus în Windows NT. Faptul că nu jurnalizează în mod prestabilit accesul la reţea defineşte unul din cele mai mari dezavantaje ale unui server standard FTP.

Securitatea Windows NT Remote Access Services (RAS)

În cadrul serviciilor de asigurare a accesului la distanţă – RAS, Microsoft Remote Access Services este printre cele mai des folosite deoarece gestionează login-urile utilizatorilor de la distanţă la reţeaua NT, inclusiv login-urile telefonice şi prin internet. Pentru conectarea la reţea a utilizatorilor de la o locaţie ce nu

este fizic conectată la reţea, RAS colaborează cu autoritatea locală de securitate, cu managerul de securitate a conturilor şi cu monitorul de referinţă a securităţii.

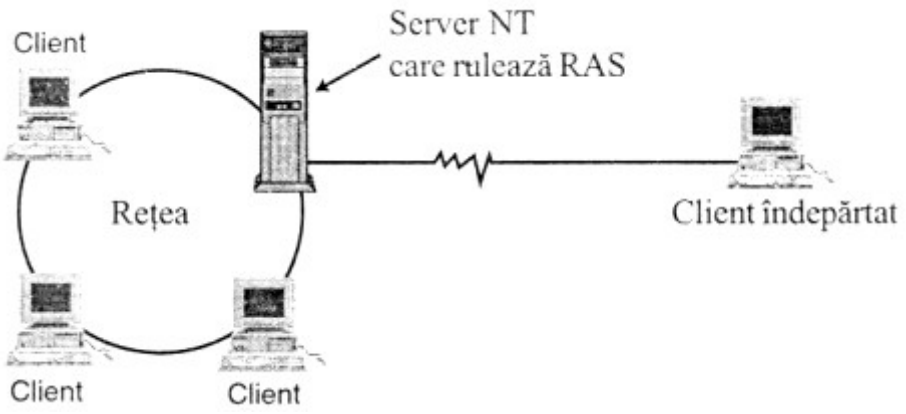


Figura 11 - Utilizatorul se conectează la un server care rulează Remote Access Services

În cazul unei conectări la un server prin RAS, calculatorul aflat la distanţă, utilizând funcţia hash MD4, trece parola de login şi o trimite împreună cu numele utilizatorului la serverul NT. Acesta compară valoarea hash cu valorile din baza de date cu parole, RAS criptând însă numai parola.

Sistemul RAS este un sistem dintr-un domeniu extins, iar aceasta duce la compromiterea calculatoarelor RAS în cazul accesului unui hacker la nivel de reţea. Probleme semnificative de securitate apar în cazul unui server simplu WEB sau FTP, utilizatorii cu drepturi de acces credibile putând citi şi scrie fişiere din sistemul RAS.

Pentru a îmbunătăţi securitatea unui astfel de sistem există mai multe etape:

1. pentru blocarea accesului între serverul RAS şi calculatoarele din interiorul parafocului pe o parte a subreţelei se va utiliza un ruter de ecranare. Pe cealaltă parte a subreţelei se va instala un alt ruter de ecranare pentru blocarea anumitor activităţi (ex. FTP);

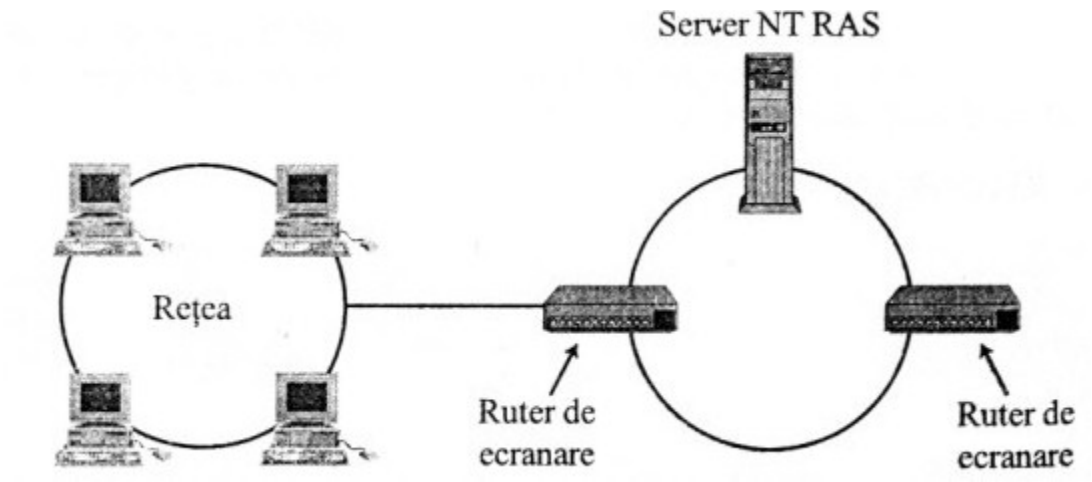


Figura 12 - Un parafoc cu subreţea ecranată care include serverul RAS

2. opţiunea de verificare pentru Remote Access Services trebuie activată. Pentru aceasta se accesează Start-Programs-Administrative Tools-User Manager for Domains-Policies-Audit şi astfel se activează serviciile de verificare normale pentru Windows NT. Odată activate aceste servicii, se editează Windows Registry pentru activarea serviciilor de verficare RAS. Se rulează programul "regedit" şi se setează următoarea valoare de cheie la 1:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters\Logging

   Urmează închiderea serviciului RAS şi reîncărcarea serverului.
3. se semnează obligatoriu fiecare pachet trimis serverului de către utilizatorul de la distanţă, protejând împotriva simulării pachetelor deoarece o modificare a pachetului de către un hacker va altera semnătura digitală;
4. se activează opţiunea de criptare a sesiunii. Astfel, după un login reuşit al unui utilizator, serverul RAS îi va trimite acestuia o cheie de sesiune. Serverul RAS generează pentru fiecare login o nouă cheie, deşi foloseşte criptarea simetrică, ceea ce crează o protecţie împotriva tentativelor de reutilizare a cheilor de sesiune. Criptarea RAS în

Windows NT 3.51 şi NT 4.0 prezintă o deficienţă şi anume faptul că serverul transmite cheia de sesiune în clar, fiind astfel posibilă utilizarea ei de către un hacker pentru interceptarea transmisiunii utilizatorului în timpul sesiunii curente;

5. se activează funcţiile de dial-back. Pentru utilizatorii ce accesează un server RAS cu această opţiune activată, login-ul va fi verificat şi conexiunea întreruptă. Ulterior, serverul RAS se va reconecta la sistemul utilizatorului aflat la distanţă apelând un număr programat anterior al utlizatorului. Astfel se verifică atât locaţia cât şi identitatea utilizatorului;
6. crearea restricţiei cu privire la intervalul de timp în care accesul la server este permis. Este posibilă utilizarea RAS între anumite intervale orare.

Un instrument care protejează sistemul conectat la internet este firewall-ul. Acesta are scopul de a ţine la distanţă potenţialii intruşi şi de a nu lăsa utilizatorii locali să iasă în exterior. Dacă pe calculatoarele unei reţele există informaţii particulare ce trebuie protejate se poate bloca accesul la sistem de pe toate adresele de IP ce nu aparţin reţelei. Accesul poate fi blocat şi în sens invers dacă nu se doreşte accesarea anumitor situri de pe adresele de IP ale reţelei. Un pachet TCP/IP conţine un antet şi date. Antetul conţine adresa IP a expeditorului, destinatarul şi alte informaţii despre pachet. Astfel, firewall-ul examinează doar antetul pachetului pentru a depista destinaţia, nu consumă timp pentru a analiza datele expediate.

Există mai multe tipuri de firewall-uri folosite în acest moment. Un model este firewall-ul cu filtrare de pachete care are rolul de a examina pachetele de date şi de a le expedia la adresele corespunzătoare.

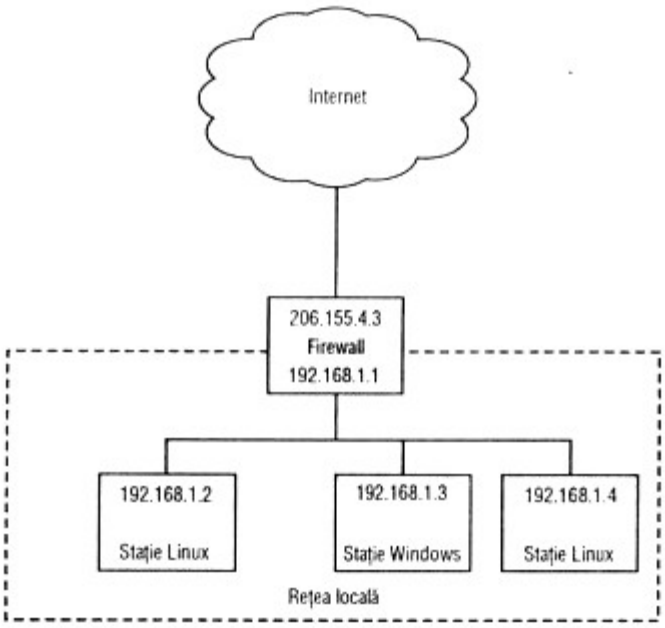


Figura 13 - Configuraţie simplă de firewall

Firewall-ul este conectat atât la internet cât şi la reţeaua locală, astfel având două adrese IP. Pachetele trimise de la staţiile locale la adrese exterioare reţelei şi invers sunt analizate de către firewall care stabileşte care are dreptul de a fi trimis mai departe. Pentru a putea fi trimis la destinatar, un pachet de date trebuie să îndeplinescă un set de reguli configurat în Linux folosind pachetul IP Chains. Un lanţ IP este un set de reguli care trebuie îndeplinite de fiecare pachet pentru a putea trece de firewall. Configuraţia IP Chains foloseşte trei tipuri de lanţuri: de intrare, de ieşire şi de redistribuire. Lanţul de intrare verifică pachetele primite, cel de ieşire verifică pachetele trimise de sistem, iar pachetele destinate altor hosturi sunt analizate de lanţul de redistribuire. Operarea IP Chains este ilustrată în figura de mai jos.

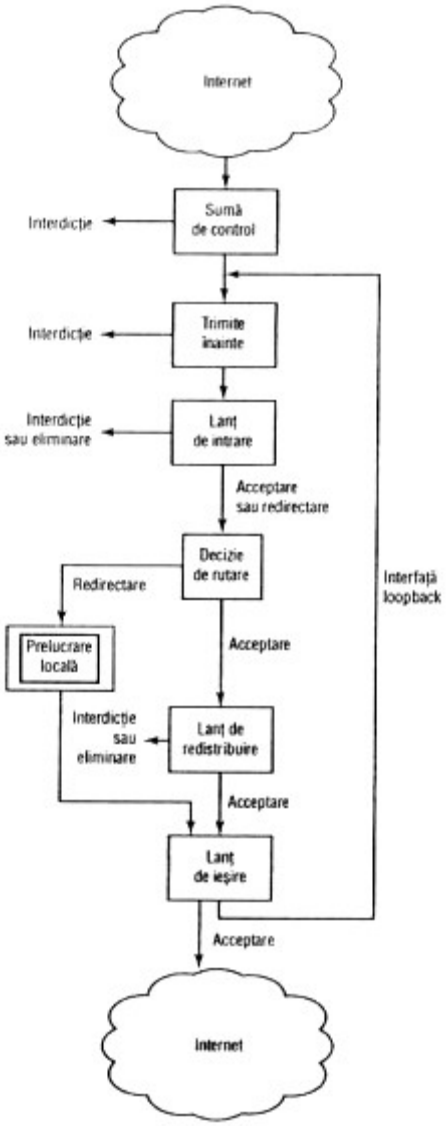


Figura 14 - Operarea IP Chains

Pachetul primit de sistem este trecut printr-un filtru care verifică suma de control. Dacă suma de control este corectă atunci pachetul este trimis unui modul care verifică dacă are un format corect. Dacă acest test este trecut pachetul ajunge în lanţul de intrare unde poate fi acceptat şi trimis lanţului de redistribuire, interzis şi distrus fără a se genera nici o eroare, respins şi returnat expeditorului cu un cod de eroare, sau trimis mai departe unui lanţ creat de utilizator pentru a fi prelucrat. În lanţul de distribuire pachetul poate fi interzis,

eliminat sau trimis lanţului de ieşire. În lanţul de ieşire pachetul este verificat şi poate fi interzis, eliminat sau trimis către o destinaţie din internet. În lanţul de ieşire mai pot intra pachete prelucrate local ce au ca destinaţie o adresă locală. Acestea se întorc în lanţul de intrare prin interfaţa loopback.

În timp ce firewall-ul cu filtrare de pachete funcţionează la nivel de reţea, serverele proxy lucrează la nivel de aplicaţie. Firewall-ul cu filtrare de pachete cunoaşte doar adresa IP de la care s-a trimis pachetul, în vreme ce serverul Proxy primeşte informaţii direct de la aplicaţia care a fost configurată pentru a comunica prin portul respectiv. Serverul Proxy poate fi situat pe o maşină aflată în interiorul unui firewall (figura 14) sau pe o altă maşină care nu este protejată de un firewall şi este conectată direct la internet şi la reţeaua locală. Dacă serverul Proxy nu este configurat cu un firewall atunci se pot controla doar resursele disponibile utilizatorilor reţelei locale, traficul de intrare nefiind filtrat.

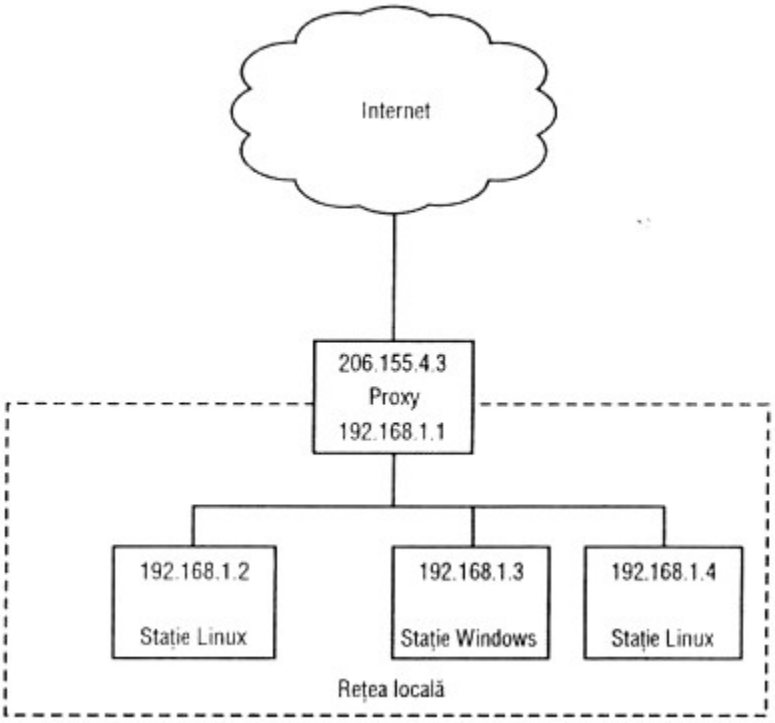


Figura 14 - Configuraţie proxy/firewall

În cazul configuraţiei cu un firewall, serverul Proxy primeşte cererile web ale clienţilor din interiorul firewall-ului şi le compară cu lista siturilor interzise. Dacă pagina cerută nu se află pe această listă, atunci ea este trimisă utilizatorului. Dacă pagina se găseşte în listă, pe calculatorul de pe care s-a trimis cererea se afişează un mesaj care specifică faptul că URL-ul respectiv nu este disponibil sau este scris greşit. Un server proxy utilizează mai multe resurse decât un firewall cu filtrare deoarece creează un proces nou pentru fiecare utilizator ce se conectează prin intermediul său.

O altă metodă de a asigura protecţia sistemului Linux este utilizarea demonului "inetd". "Inetd" are alocate anumite porturi şi lansează doar serviciile asociate porturilor care au solicitări. Această metodă elimină necesitatea ca fiecare proces să aibă propriul demon care să verifice porturile disponibile, în acest fel micşorându-se numărul de porturi deschise prin care spărgătorii pot intra în sistem. Prin utilizarea demonului "inetd" se previne scăderea performanţelor sistemului cauzată de execuţia simultană a demonilor mai multor servicii.

Există mai multe metode de a intra neautorizat într-un sistem, depinde de dorinţa intruşilor de a fi sau nu observaţi. Detectarea intruşilor se poate face destul de uşor în unele cazuri cu ajutorul fişierului "/var/log/secure" din sistemele Red Hat Linux. În acest fişier se stochează toate încercările de accesare a sistemului împreună cu informaţii care arată dacă încercările au avut sau nu succes. Astfel, existenţa mai multor încercări consecutive nereuşite de la acelaşi host sau de la aceeaşi adresă de IP indică faptul că o persoană neautorizată a încercat să acceseze sistemul. Încercările nereuşite de intrare în Telnet sau FTP se observă uşor în fişier. Conţinutul fişierului "/var/log/secure" poate fi şters de către spărgători astfel încât să nu se observe tentativele de accesare neautorizată a sistemului, dar administratorii de sistem îşi pot da seama de această faptă prin observarea zonelor albe din cadrul fişierului.

Detectarea tentativelor de accesare neautorizată a sistemului este o operaţie repetitivă greu de efectuat deoarece necesită timp. Aceste încercări se pot întâmpla oricând şi este greu să fii mereu atent şi să le urmăreşti. În scopul de a uşura şi de a eficientiza detectarea tentativelor de accesare neautorizată s-au dezvoltat aplicaţii care verifică periodic sistemul şi care anunţă activitatea suspectă şi modificările aduse anumitor fişiere.

Tripwire 2.2.1 pentru Linux este o astfel de aplicaţie care face un inventar iniţial al fişierelor din sistem şi compară fişierele curente cu acest inventar de fiecare dată când i se solicită. Inventarul trebuie actualizat periodic sau după ce fişierele din sistem au suferit modificări semnificative.

Deception Tool Kit (DTK) este o aplicaţie ce permite urmărilea intruşilor atunci când aceştia încearcă să intre în sistem. DTK face sistemul să pară vulnerabil după care strânge informaţii despre toate încercările de exploatare detectate. Dacă se încearcă accesarea unui anumit fişier, DTK trimite spărgătorului un fişier fals care îl va face să piardă timp până îşi va da seama că fişierul accesat nu este cel real. Pentru a preveni atacurile, sistemele care folosesc DTK emit un anumit semnal pe portul 365. Dacă spărgătorul recepţionează acest semnal se va gandi mai bine dacă să încerce să acceseze sistemul sau nu.

Serviciile de securitate distribuite din Windows 2000 au fost create pentru o îmbunătăţire a securităţii reţelei, prin oferirea mai multor opţiuni in ceea ce priveşte tehnologia de securitate. Ele oferă o metodă de integrare a reţelei în Internet pentru realizarea de operaţii distribuite în condiţii de siguranţă şi permit de asemenea protejarea datelor aflate într-o reţea LAN sau WAN. Folosirea unei plaje mai largi de protocoale de securitate, a tehnologiei de securitate prin cheie publică şi simplificarea administrării au condus la o mărire a flexibilităţii, oferind mai multe posibilităţi pentru alegerea tehnologiei de securitate ce va fi utilizată în mediul de operare.

Versiunile anterioare ale programului Windows NT beneficiau de elemente de securitate datorită cărora era considerat de utilizatori care operează cu date din întrega lume drept un sistem de operare pentru reţele fiabil. Pe parcurs au intervenit numeroase schimbări şi evoluţii în lumea informaticii, printre cele mai importante numărându-se internetul. Implicaţiile şi riscurile legate de deschiderea către internet au făcut ca atenţia lui Microsoft asupra securităţii să crească astfel încât utilizatorii să se simtă mai în siguranţă lucrând cu Windows 2000 Server în desfăşurarea activităţilor lor pe internet.

S-au introdus îmbunătăţiri cum ar fi Active Directory, protocol de autentificare Kerberos, securitatea prin certificate şi folosirea cartelelor inteligente ce permit criptografierea. Aceste îmbunătăţiri au dus la crearea unui mediu pregătit pentru riscurile legate de securitate ce există pe supermagistrala informatică. Prin apariţia ruterelor, a parafocurilor, a serverelor de intranet şi extranet, securitatea nu se mai rezumă decât la stabilirea permisiunilor corecte pentru accesul la fişierele din server.

Active Directory aduce cu sine un serviciu de directoare mai funcţional şi mai bine organizat decât predecesorul său şi oferă o mare flexibilitate în configurarea reţelei şi în controlul general al securităţii. În cazurile anterioare serviciul de directoare devenea tot mai dificil pe măsură ce creştea domeniul, iar în cazul mai multor domenii era dificil să se realizeze un sistem de securitate fără a configura relaţii de încredere complexe. Un alt avantaj îl constituie şi faptul că serviciile de securitate distribuite de Windows 2000 folosesc Active Directory ca pe un conteiner pentru informaţiile de cont şi gestionare în timp ce predeceorul acestuia folosea o porţiune sigură din Registry, performanţele şi scalabilitatea fiind afectate în mod serios.

Într-un domeniu Windows NT nu se putea decât să organizezi utilizatorii în grupuri locale sau globale, ceea ce limita posibilităţile de administrare a accesului utilizatorilor la resursele de reţea. Prin spaţiul de nume DNS integrat in Active Directory administratorul are posibilitatea să organizeze utilizatorii într-una sau mai multe unităţi organizatorice. Active Directory asigură prin integrarea perfectă cu protocolul LDAP un mecanism pentru o mai mare interoperabilitate cu alte

servicii directoare. Prin introducerea acestuia, complexitatea indusă de necesitatea gestionării numeroselor relaţii de încredere între domenii a dispărut. Încrederea tranzitivă între domenii simplifică gestionarea conturilor de încredere interdomenii. Prin stabilirea unei relaţii de încredere biunivoce cu domeniul părinte din arborele domeniului toate domeniile pot avea în mod implicit încredere în celelalte domenii din arbore, acestă relaţie reducând numărul de relaţii univoce care trebuiau stabilite.

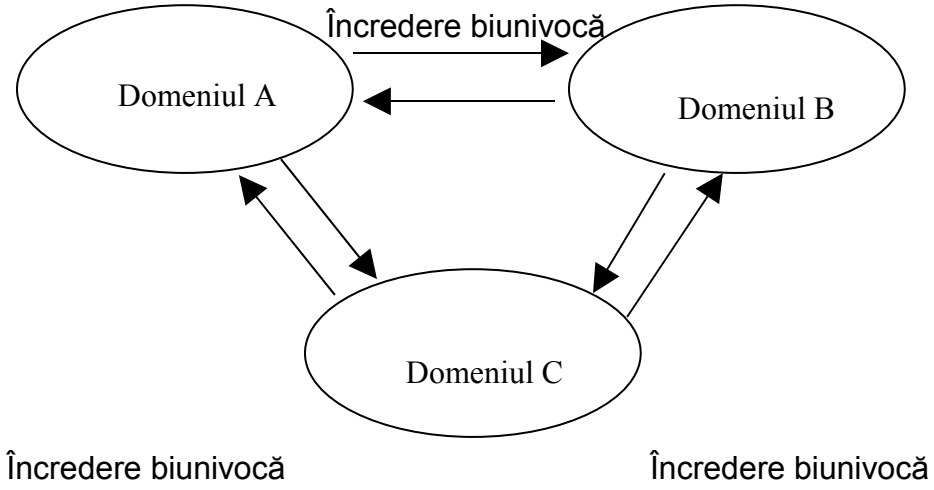


Figura 15 - Relaţie de încredere între mai multe domenii din serviciile de directoare ale mediului NT

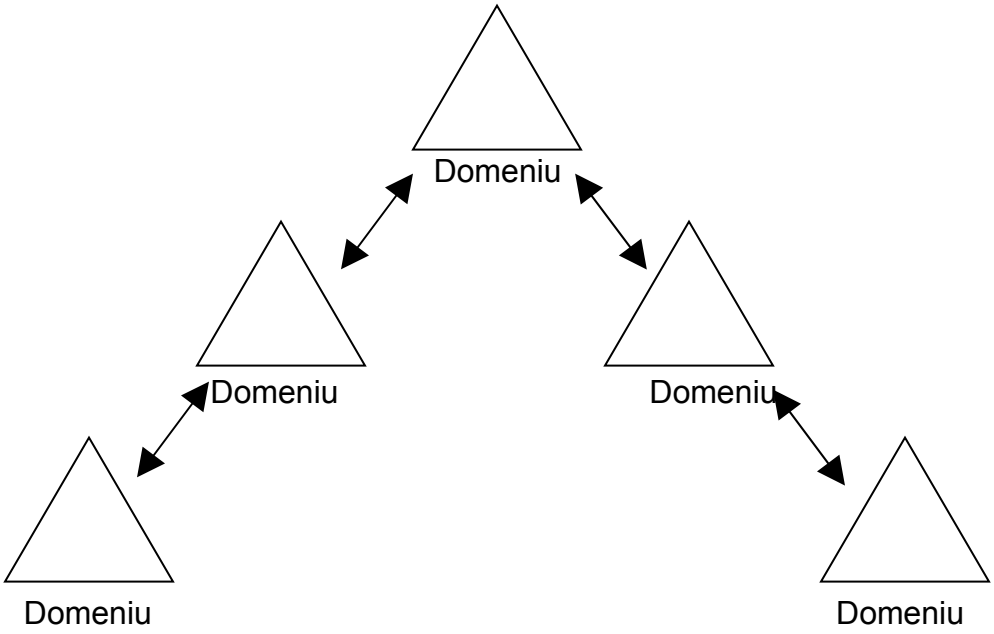


Figura 16 - Relaţii de incredere intre domenii în Active Directory (numar mai mic de relaţii univoce)

Arhitectura sistemului de securitate a obiectelor din Active Directory face posibilă delegarea controlului specific pentru accesul la obiectele din Active Directory şi este determinată de descriptorii sistemului de securitate din Windows 2000. Fiecare descriptor are o listă ACL care acordă sau refuză anumite drepturi de acces pentru utilizatori şi obiecte. Acestea pot fi definite la trei niveluri specifice:

- acordarea drepturilor de acces pentru toate proprietăţile obiectului;
- acordarea drepturilor de acces pentru un grup de proprietăţi ale obietului;
- acordarea drepturilor de acces la o anumită proprietate a obiectului.

Administratorul de reţea trebuie să stabilească o politică de securitate ce va determina modul în care utilizatorii vor putea intra în reţea şi tipul de acces al acestora. Această politică va fi determinată în mare măsură de posibilităţile sistemului de operare. La introducerea ei trebuie avuţi în vedere mai mulţi factori:

- securitatea datelor: reţeaua trebuie protejată astfel incât clienţii să nu poată modifica datele din reţea, în mod voit sau nu; nivelul de securitate pentru date va afecta şi configuraţia sitemului de operare realizată;
- amabilitatea faţă de clienţi: trebuie creată o politică prin care utilizatorul să poată repecta regulile;
- interoperabilitate: modelul de securitate ales trebuie să ia în considerare integrarea şi interoperabilitatea cu alte sisteme; în diferite medii de reţea la nivel de organizaţie trebuie sa fie asigurat utilizatorilor accesul la diferite platforme, de la UNIX la NetWare;
- probleme legate de accesul la distanţă: trebuie permis accesul de la distanţă dar fără deschiderea unor uşi atât de mult încât să poată intra şi persoane nepoftite;
- găsirea unor buni administratori.

Pentru o compatibilitate cu alte sisteme de operare diferite şi pentru o flexibilitate a suprafeţei de lucru, Windows 2000 recunoaşte o serie de protocoale diferite:

1. protocolul de funcţionare Kerberos:
    - a permis mărirea numărului de elemente de securitate ale mediului Windows 2000 şi delegarea autentificării pentru aplicaţiile client-server multietajate;
    - realizarea autentificării este îmbunătăţită, permite autentificarea utilizatorilor în domenii aflate la orice nivel în arborele de domeniu prin relaţiile de încredere trazitive;
    - permite mediului Windows 2000 să se integreze fără probleme într-o reţea de firmă în care sunt folosite platforme diferite;
    - este un protocol de autentificare standardizat şi se bazează pe o tehnică numită "secrete comune";

- principiul este urmatorul: secretul (parola) este cunoscut numai de client şi de server şi pe langă aceasta se mai foloseşte şi codificarea cheie secretă; clientul şi severul trebuie să poată folosi împreună o cheie de codificare care este furnizată de centrele pentru distribuirea de chei (KDC – Kez Distribution Center); aceasta este folosită pentru obţinerea unor tichete pentru obţinerea de tichete (TGT – Ticket Getting Tickets); TGT-urile, centrul KDC şi sectorul din care face parte KDC sunt elemente ale procesului de autentificare prin protocolul Kerberos;

Când se foloseşte un protocol Kerberos clientul trebuie să facă următorii paşi:

- autentificarea iniţială a clientului se face în KDC;
- se solicită centrului KDC un tichet de sesiune pentru autentificarea în serverul de destinaţie;
- tichetul este prezentat serverului de destinaţie în momentul configurării conexiunii de către client;
- serverul de destinaţie verifică tichetul eliberat de centrul KDC.

2. protocolul de autentificare Windows NT LAN Manager (NTLM): se foloseşte atunci când un server sau un client Windows 2000 trebuie să comunice cu un sistem Window NT pentru a realiza o autentificare; oferă o metodă sigură de autentificare în domeniul Windows NT din cadrul reţelelor locale (LAN) şi în reţelele de mare suprafaţă (WAN); în procesul de autentificare au existat si puncte slabe precum:
    - autentificarea ineficientă în servere (serverul de aplicaţii trebuie să se conecteze la un controller de domeniu pentru autentificarea fiecărui client);
    - lipsa autentificării tranzitive de domeniu (când se lucra cu mai multe domenii admnistratorii de reţea erau obligaţi să creeze şi

o reţea complexă de relaţii de încredere explicite; acestea erau necesare deoarece un utilizator nu putea fi autentificat între domenii);

- integrarea reală la nivel de reţea (NTLM nu este un protocol de autenticitate general acceptat; acest fapt limitează posibilitatea de integrare în alte sisteme de operare care sunt folosite în cadrul unei reţele de organizaţie);
- imposibilitatea delegării autentificării;
- autentificarea reciprocă (numai serverul poate verifica identitatea clientului, nu şi invers).

Aceste slăbiciuni fac ca serverul să fie vulnerabil intr-un mediu deschis, cum sunt cele folosite în prezent.

3. protocoale cu cheie publică: asigură confidenţialitatea şi siguranţa în Internet; conexiunea prin SSL (Secure Socket Layer) realizată între browser şi serverul Web foloseşte certificate cu cheie publică pentru autentificarea clientului şi severului;

4. autentificarea prin parolă distribuită (DPA) e folosită ca protocol de autentificare secret partajat pentru accesul la serviciile firmelor care oferă Internet.

Protocoalele de autentificare Kerberos şi NTML sunt două protocoale pentru autentificarea în reţea pe care le recunoaşte Windows 2000, acestea variînd în funcţie de programul client utilizat.

Protocolul de autentificare folosit între client şi server

Sistem de operare	Windows 2000 Server	Windows NT Server
Windows 2000 Professional / Server	Protocolul Kerberos	NTLM
Windows NT Workstation / Server	NTLM	NTLM
Windows 98	NTLM	NTLM
Windows 95	NTLM	NTLM
Windows 3.11	NTLM	NTLM

Se observă că protocolul Kerberos este folosit doar pentru autentificarea unui client Windows 2000 de către un server Windows 2000. Acesta este un protocol sigur şi solid, general acceptat în domeniu, care oferă o metodă mai sigură şi mai bună prin care utilizatorii pot obţine accesul la resursele din reţea.