***Învăţământul profesional şi tehnic în domeniul TIC***

**Proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013**

Beneficiar – Centrul Naţional de Dezvoltare a Învăţământului Profesional şi Tehnic

str. Spiru Haret nr. 10-12, sector 1, Bucureşti-010176, tel. 021-3111162, fax. 021-3125498, [vet@tvet.ro](mailto:vet@tvet.ro)

**SISTEME DE OPERARE ÎN REŢEA**

**Material de predare I**

**Familia Microsoft Windows Server**

**Domeniul: Informatică**

**Calificarea: Tehnician infrastructură reţele de telecomunicaţii**

**Nivel 3 avansat**

**2009**

**AUTOR:**

**IORDACHE FLORIN**

**COORDONATOR:**

**LADISLAU SEICA**

**CONSULTANŢĂ:**

**IOANA CÎRSTEA** – expert CNDIPT

**ZOICA VLĂDUŢ** – expert CNDIPT

**ANGELA POPESCU** – expert CNDIPT

**DANA STROIE** – expert CNDIPT

Acest material a fost elaborat în cadrul proiectului *Învăţământul profesional şi tehnic în domeniul TIC,* proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013

**Cuprins**

[I. Introducere 4](#_Toc235152346)

[II. Documente necesare pentru activitatea de predare 6](#_Toc235152347)

[Tema 1. Familia Microsoft Windows Server 7](#_Toc235152348)

[Tema 2 Protocoale de reţea 11](#_Toc235152349)

[Fisa 1. Protocoale de rețea 11](#_Toc235152350)

[Tema 3. Servicii de rețea 16](#_Toc235152351)

[Fișa 1 Servicii de reţea 16](#_Toc235152352)

[Fișa 2. Active directory - Serviciul de catalog 17](#_Toc235152353)

[Fișa 3. Instalarea serverului DHCP 21](#_Toc235152354)

[Fișa 4 Instalarea serverului DNS 24](#_Toc235152355)

[Tema 4 Instalarea sistemului de operare Windows 2003 server 26](#_Toc235152356)

[Fișa 1. Operațiuni pregătitoare 26](#_Toc235152357)

[Fișa 2 Instalarea sistemului de operare 28](#_Toc235152358)

[Tema 5 - Configurarea sistemelor de operare în rețea 31](#_Toc235152359)

[Fisa 1. Configurarea Active Directory 31](#_Toc235152360)

[Tema 6: Securitatea NOS 41](#_Toc235152361)

[Fisa 1. Securizarea sistemului 41](#_Toc235152362)

[Fișa 2 Utilitare pentru monitorizarea sistemului. 47](#_Toc235152363)

[Fişa rezumat 51](#_Toc235152364)

[Bibliografie 53](#_Toc235152365)

# I. Introducere

Materialele de predare reprezintă o resursă – suport pentru activitatea de predare, instrumente auxiliare care includ un mesaj sau o informaţie didactică.

Prezentul material de predare, se adresează cadrelor didactice care predau în cadrul şcolilor postliceale, domeniul **Informatică**, calificarea **Tehnician infrastructură reţele de telecomunicaţii**

El a fost elaborat pentru modulul **Sisteme de operare în reţea**, ce se desfăşoară în 93 ore, din care laborator tehnologic 31

| **Teme** | **Fise suport** | Competenţe/Rezultate ale învăţării |
| --- | --- | --- |
| Tema 1. Familia Microsoft Windows Server | Fisa 1 | * C1, C2, C3, C4 |
| Tema 4 Protocoale de reţea | Fişa 1 | * C1, C2, C3, C4 |
| Tema 5: Servicii de reţea | Fişa 1  Fişa 2  Fişa 3  Fişa 4 | * C1, C2, C3, C4 |
| Tema 7: Instalarea WIN2003/ WIN2008 server | Fişa 1  Fişa 2 | * C1, C2, C3, C4 |
| Tema 8: Configurarea sistemelor de operare in retea | Fişa 1 | * C1, C2, C3, C4 |
| Tema 9: Securitatea NOS | Fişa 1  Fişa 2 | * C1, C2, C3, C4 |

C1. Pregateste sistemul de calcul pentru instalare

C2. Analizează sistemele de operare de reţea.

C3. Utilizează sistemele de operare în reţea

C4. Administrează sistemele de operare în reţea

# I. Documente necesare pentru activitatea de predare

Pentru predarea conţinuturilor abordate în cadrul materialului de predare cadrul didactic are obligaţia de a studia următoarele documente:

* *Standardul de Pregătire Profesională* pentru calificarea Tehnician echipamente de calcul, nivelul 3 avansat – [www.tvet.ro](http://www.tvet.ro), secţiunea SPP sau [www.edu.ro](http://www.edu.ro) , secţiunea învăţământ preuniversitar
* *Curriculum* pentru calificarea Tehnician echipamente de calcul, nivelul 3 avansat – [www.tvet.ro](http://www.tvet.ro), secţiunea Curriculum sau [www.edu.ro](http://www.edu.ro) , secţiunea învăţământ preuniversitar

# Tema 1. Familia Microsoft Windows Server

Familia de sisteme de operare Windows 2003/2008 server oferă o gamă variată de servicii care poate acoperi majoritatea cerințelor în materie de servere de pe piața IT. Are în componență următoarele sisteme de operare:

1. **Standard edition** - sistem de operare de reţea, care oferă soluţii simple şi rapide pentru firme. Windows Standard Server 2003/2008 oferă servicii pentru partajarea fişierelor şi imprimantelor, conectarea securizată la Internet, desfăşurarea centralizată a aplicaţiilor din spaţiul de lucru Windows Standard Server 2003/2008 permite multiprocesare simetrică pe 2 căi şi până la 4 GB de memorie.
2. **Enterprise edition** – sistem de operare de rețea destinat rețelelor mari de calculatoare. Oferă funcţionalitatea necesară pentru infrastructura întreprinderii, aplicaţiile tip linie de afaceri şi tranzacţiile de comerţ electronic. Windows Enterprise Server 2003/2008 este un sistem de operare complet, care acceptă până la 8 procesoare, cluster cu 4 noduri şi până la 32 GB de memorie. Este disponibil şi pentru platformele de calcul pe 64 de biţi.
3. **Datacenter edition** - Conceput pentru activităţile care necesită un nivel ridicat de scalabilitate şi disponibilitate, Windows Datacenter Server 2003/2008 oferă o bază solidă pentru construirea soluţiilor critice de baze de date, software de planificare a resurselor întreprinderii (ERP), prelucrarea în timp real a volumelor mari de tranzacţii şi consolidarea serverelor. Este cel mai puternic şi mai funcţional sistem de operare pentru server din familia windows 2003/2008 server, permiţând multiprocesare simetrică cu până la 32 de căi (SMP), având drept caracteristică standard atât clusterul cu 8 noduri cât şi serviciile de load-balancing. Windows Datacenter Server 2003 este disponibil şi pentru platforme de calcul pe 64 de biţi.
4. **Web edition** - Este un server Web orientat pe funcţii, optimizat astfel încât să furnizeze firmelor o platformă cuprinzătoare şi stabilă pentru servire şi găzduire pe Web. Uşor de instalat şi de administrat.
5. **For Itanium based systems -** Windows Server 2008 pentru sistemele Itanium-Based este optimizat pentru baze de date mari, linie de afaceri și aplicații specifice oferind disponibilitate mare precum și scalabilitate până la 64 de procesoare.
6. **HPC server -** Windows HPC Server 2008, reprezintă următoarea generație de high-performance computing (HPC), oferind unelte enterprise pentru un mediu HPC extrem de productiv. Construit pe platforma Windows Server 2008, cu tehnologie 64-bit, Windows HPC Server2008, poate scala eficient până la mii de nuclee de procesare incluzând console de administrare care vă ajuta să monitorizați proactiv starea generală a sistemului. Programarea operațiunilor, interoperabilitatea și flexibilitatea vă permit integrarea între platforme HPC Windows și Linux, suportând aplicații SOA. Productivitate sporită, performanțe scalabile, ușurință în utilizare, sunt doar câteva din capacitățile care fac din Windows HPC Server 2008 unul din cele mai reușite sisteme de operare server.

O analiză comparativă a sistemelor de operare din familia Windows 2003/2008 Server este dată în tabelul de mai jos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Caracteristică** | **Web Server** | **Standard Server** | **Enterprise Server** | **Data Center** |
| **Tehnologii de clustere** | | | | |
| Echilibrarea încărcării reţelei (NLB) | da | da | da | da |
| Protecţie la defecţiuni în cluster | nu | nu | da | da |
| **Communicaţii şi servicii de reţea** | | | | |
| Suport pentru Reţea privată virtuală (VPN) | parțial | da | da | da |
| Serviciul Protocol de iniţiere a sesiunii (SIP) | nu | da | da | da |
| Serviciul de autorizare Internet (IAS) | nu | da | da | da |
| Network Bridge | nu | da | da | nu |
| Partajare conexiune la Internet (ICS) | nu | da | da | nu |
| **Directory Services** | | | | |
| Active Directory | nu | da | da | da |
| Suport pentru servicii Metadirector (MMS) | nu | nu | da | da |
| **Servicii de fişiere şi imprimare** | | | | |
| Sistem de fişiere distribuite (DFS) | da | da | da | da |
| Sistem de criptare fişiere (EFS) | da | da | da | da |
| Shadow Copy Restore | nu | da | da | da |
| SharePoint Team Services | nu | da | da | da |
| Suport stocare la distanţă | nu | da | da | da |
| Serviciul de fax | nu | da | da | da |
| Servicii pentru Macintosh | nu | nu | da | da |
| **Servicii de management** | | | | |
| IntelliMirror | nu | da | da | da |
| Resultant Set of Policy (RSoP) | nu | da | da | da |
| Windows Management Instrumentation (WMI) Command Line | nu | da | da | da |
| Servicii de instalare la distanţă (RIS) | nu | da | da | da |
| **Servicii de securitate** | | | | |
| Internet Conection Firewall | nu | da | da | nu |
| Certificate Services | nu | parțial | da | da |
| **Servicii de terminal** | | | | |
| Spaţiu de lucru la distanţă pentru administrare | da | da | da | da |
| Terminal Server | nu | da | da | da |
| Sesiuni Terminal Server | nu | nu | da | da |
| **Servicii multimedia** | | | | |
| Servicii Windows MediaT | nu | da | da | nu |
| **Scalabilitate** | | | | |
| Suport de 64 biţi pentru computere bazate pe IntelR ItaniumT | nu | nu | da | da |
| Hot add memory.1 | nu | nu | da | da |
| Acces neuniform la memorie (NUMA)1 | nu | nu | da | da |
| Control procese | nu | nu | da | da |
| Suport | nu | nu | nu | da |
| **Servicii pentru Web şi aplicaţii** | | | | |
| .NET Framework | da | da | da | da |
| Internet Information Services (IIS) 6.0 | da | da | da | da |
| ASP.NET | da | da | da | da |
| 1 Poate să fie limitat datorită lipsei de suport hardware OEM. | | | | |

Familia windows 2008 server aduce facilități suplimentare:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Facilități noi / îmbunătățite** | **Enterprise Server** | **Datacenter Server** | **Standard Server** | **Web Server** | **Itanium Server** | **HPC Server** |
| AD Rights Management Services (RMS) | da | da | da | nu | nu | nu |
| Criptare a datelor (CNG) | da | da | da | da | da | da |
| Opțiuni suplimentare pentru politica de grup (Group Policy) | da | da | da | da | da | da |
| Virtualizare - Hyper-V | da | da | da | nu | nu | da |
| Internet Information Services (IIS) 7.0 | da | da | da | da | da | da |
| NEW: Protecția accesului la rețea (NAP) | da | da | da | nu | nu | nu |
| Controllere de domeniu read only (RODC) | da | da | da | da | nu | da |
| Server Core | da | da | da | da | nu | nu |
| Server Manager | da | da | da | da | da | da |
| Servicii de terminal și aplicații la distanță | da | da | da | nu | nu | nu |
| Servicii de instalare în rețea - (WDS) | da | da | da | nu | nu | da |

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 10-15 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

# Tema 2 Protocoale de reţea

## Fisa 1. Protocoale de rețea

În Internet se folosesc protocoale care fie se bazează pe TCP/IP, fie utilizează protocolul TCP/IP. Vom prezenta în continuare cele mai folosite protocoale utilizate în mediul Internet.

**Protocolul ARP** – protocol de rezoluție a adresei

Pentru ca două sisteme de calcul să poată comunica într-o rețea este necesară cunoașterea atât a adresei MAC, cât şi a adresei IP. În cazul în care numai una dintre adrese este disponibilă se apelează la un protocol dedicat care pe baza acesteia va determina cealaltă adresă.

Stiva de protocoale TCP/IP conține două protocoale de nivel rețea pentru a servi acest scop: ARP (Address Resolution Protocol) şi RARP (Reverse Address Resolution Protocol). ARP este protocolul ce va oferi adresa MAC a unui dispozitiv de rețea, dată fiind adresa sa IP. ARP se bazează pe construirea şi menținerea unei tabele ARP. O tabela ARP are rolul de a oferi o corespondență între adresele IP şi cele MAC. Acestea sunt construite dinamic şi sunt stocate în memoria RAM. Deși există mecanisme pentru adăugarea sau eliminarea unei intrări într-o tabelă ARP acestea sunt rareori folosite. Fiecare computer sau dispozitiv de rețea își păstrează propria sa tabelă ARP.

**Protocolul ICMP** – protocolul mesajelor de control

Arhitectura internetului implică o serie de probleme atunci când o maşină anume nu funcţionează. Dacă funcţionează, totul e bine. Dacă nu, intervine ICMP: Internet Control Message Protocol.

ICMP este protocolul responsabil cu determinarea eventualelor probleme datorate "căderii" unei maşini. Nu-i aşa că ați folosit comanda ping? Aşa trimiteți un pachet. Ţinta va răspunde - în cazul în care va primi pachetul. Dacă totul e în ordine, rezultatul este un pachet identic. Dacă nu, veți primi un pachet ICMP. Acesta conţine, în header-ul său, informaţiile de care are nevoie pentru a determina o eventuală problemă.

Protocolul ICMP este unul de mare importanţă, în primul rând pentru administratori. Ei îşi pot da seama dacă cineva a scos din uz o maşină în mod intenţionat - spre exemplu dacă o maşină funcţionează perfect, dar portul 80 (HTTPD) nu este accesibil, avem un indiciu al unui eventual atac.

**DHCP** – protocol pentru alocarea dinamică a adreselor IP

În primele zile ale reţelelor TCP/IP, administratorii defineau adresa fiecărui dispozitiv într-un fişier text sau într-o casetă de dialog. Din acel moment, adresa rămânea fixată până când cineva o modifica. Problema era că administratorii, ocazional, atribuiau din greșală adrese contradictorii altor dispozitive din rețea, provocând multe și mari neplăceri. Pentru a rezolva această problemă şi pentru a facilita atribuirea adreselor TCP/IP a inventat un serviciu numit Dynamic Host Configuration Protocol (DHCP).

Serviciile DHCP rulează pe un server DHCP, unde controlează un domeniu de IP, denumite domeniu de acoperire. Când dispozitivele se conectează la o reţea contactează serverul DHCP pentru a obţine o adresă atribuită pe care să o poată folosi. Se spune că adresele de la un server DHCP sunt închiriate clientului care le folosește, cea ce înseamnă că rămân atribuite unui anumit dispozitiv pentru un interval de timp înainte de a expira şi devin disponibile pentru utilizare de către un alt dispozitiv. Perioadele de închiriere sunt de numai câteva zile, dar administratorii de reţea pot folosi orice perioadă de timp doresc.

**HTTP** - Hypertext Transfer Protocol

World Wide Web este alcătuit din documente care folosesc un limbaj de formatare denumit HTML, abreviere de la Hypertext Markup Language (limbaj de marcare prin hipertext). Aceste documente sunt compuse din text de afişat, imagini grafice, comenzi de formatare şi hiperlegături spre alte documente situate altundeva în Web. Documentele HTML sunt afişate cel mai frecvent folosind browsere Web, precum Internet Explorer, Safari sau Mozilla Firefox.

Un protocol denumit Hypertext Transfer Protocol (protocol de transfer prin hipertext) controlează tranzacţiile dintre un client Web şi un server Web. HTTP este un protocol destinat stratului aplicaţie. Protocolul HTTP face uz în mod transparent de DNS şi de alte protocoale Internet pentru a forma conexiuni între clientul și serverul Web astfel încât utilizatorul cunoaşte numai numele domeniului şi numele documentului însuşi.

HTTP este, în esenţă, un protocol nesigur. Informaţiile pe suport text sunt transmise „în clar", între client şi server. Pentru a satisface necesitatea unor reţele Web sigure există alternative precum Secure HTTP (S-HTTP) sau Secure Sockets Layer (SSL).

Cererile unui client Web către un server Web sunt orientate spre conexiune, deci sunt persistente. Odată ce clientul a primit conţinutul unei pagini HTML, conexiunea nu mai este activă. Executarea unui clic în documentul HTML reactivează legătura fie către serverul original (dacă într-acolo indică hiperlegătura), fie către un alt server, situat altundeva.

**FTP** – protocol pentru transferul fișierelor

Abrevierea FTP simbolizează două lucruri: File Transfer Protocol (protocol de transfer al fişierelor) şi File Transfer Program (program de transfer al fişierelor).

FTP este un protocol de nivel aplicaţie folosit pentru trimiterea şi recepţionarea fişierelor între un client FTP şi un server FTP. De regulă, aceasta se realizează cu programul FTP sau cu un alt program care poate de asemenea folosi protocolul. Transferurile FTP pot fi bazate pe text sau sunt binare și pot manipula fişiere de orice dimensiune. Când vă conectaţi la un server FTP pentru a transfera un fişier, vă conectaţi la serverul FTP folosind un nume de utilizator şi o parolă valabile. Totuşi, multe site-uri sunt configurate să permită ceea ce se numeşte FTP anonim, când se introduce numele de utilizator *anonymous* şi apoi introduceţi și adresa dumneavoastră de e-mail ca parolă.

**Telnet** – protocol pentru stabilirea de conexiuni la distanță

Telnet defineşte un protocol care permite stabilirea unei sesiuni terminal de la distanţă la o gazdă din Internet, astfel ca utilizatorii de la distanţă să aibă acces ca şi cum ar sta la un terminal conectat direct la calculatorul gazdă. Folosind Telnet, utilizatorii pot controla sistemul gazdă aflat la distanţă, executând operaţii precum gestiunea fișierelor, rularea aplicaţiilor sau chiar (cu permisiuni corespunzătoare) administrarea sistemui aflat la distanţă.

**SMTP –** protocol simplu de transfer de poștă

Poşta electronică a avut un început cam nesigur pe Internet; primele programe de e-mail partajau puţine standarde cu alte programe de e-mail, mai ales în ceea ce priveşte manipularea datelor binare ataşate. În ziua de azi, toate programele curente de e-mail recunosc toate standardele acceptate pe scară largă.

Simple Mail Transfer Protocol (SMTP) este folosit pentru trimiterea şi recepţionarea mesajelor de e-mail de la un server e-mail la celălalt. Detalii despre SMTP se pot găsi în RFC 821. Protocolul SMTP defineşte un dialog între un sistem emiţător şi unul receptor. Un dialog SMTP începe când un sistem emiţător se conectează la portul 25 al unui sistem receptor. După stabilirea conexiunii, sistemul emiţător trimite o comandă HELO, urmată de adresa sa. Sistemul receptor confirmă comanda HELO, alături de adresa sa proprie. Apoi, dialogul continuă; sistemul emiţător trimite o comandă prin care se arată că sistemul doreşte să trimită un mesaj şi se indică destinatarul căruia îi este destinat mesajul. Dacă sistemul receptor cunoaşte destinatarul, confirmă cererea şi apoi sistemul emiţător transmite corpul mesajului, alături de eventualele fişiere ataşate. În final, conexiunea dintre cele două sisteme este încheiată odată ce sistemul receptor confirmă recepţionarea întregului mesaj.

**POP3 –** protocol de poștă electronică

Post Office Protocol, pe scurt, POP, este primul protocol de poștă electronică şi încă este folosit în zilele noastre. Pentru utilizatorii ce folosesc sisteme care fie nu sunt capabile să ruleze un server complet de tipul Simple Mail Transfer Protocol (SMTP) fie nu sunt conectate perma­nent, este utilizată o maşină de tip „Post Office". Această maşină Post Office este conectată permanent la Internet şi primeşte e-mail-urile destinate utilizatorului prin SMTP. Mesajele sunt trimise într-o căsuţă electronică de pe maşina Post Office ca şi cum ar fi fost maşina folosită de utilizator din modelul vechi. Cândva, mai târziu, utilizatorul se conectează de pe staţia de pe care operează cu ajutorul unui client de e-mail la serverul POP existent pe maşina Post Office şi face transferul mesajelor care aşteaptă pe staţie. Din acest moment, utilizatorul îşi poate citi sau procesa după cum doreşte mesajele în staţia locală. Acest sistem foarte simplu a servit şi serveşte foarte bine utilizatorii de ceva timp încoace.

**IMAP –** protocol interactiv de poștă electronică

Internet Message Access Protocol, pe scurt, IMAP, a fost proiectat pentru a depăşi câteva dintre limitările protocolului POP. În loc să transfere toate mesajele pe staţia clientului, IMAP reţine aceste mesaje pe server. Metoda folosită de POP este denumită câteodată „offline" deoarece, după ce v-aţi transferat mesajele, teoretic, puteţi să vă deconectaţi în timp ce vă citiţi e-mail-ul. Metoda principală folosită de către IMAP este considerată a fi „online" deoarece presupune conectarea pe toată perioada cât vă citiţi mesajele. Atunci când vă conectaţi la un server IMAP, iniţial doar anteturile noilor mesaje sunt descărcate în clientul de e-mail pentru vizualizare şi în momentul selectării unui mesaj este descărcat şi conţinutul acestuia. La final, sunt trimise înapoi la server mesaje pentru setarea unor flaguri ce determină starea mesajelor (citit / necitit).

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare – învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 10-15 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

# Tema 3. Servicii de rețea

## Fișa 1 Servicii de reţea

Un sistem de operare de rețea trebuie să constituie o platformă puternică, o bază pentru serviciile care pot rula într-o rețea de calculatoare. Principalele servicii de care este nevoie într-o rețea sunt:

* Servicii de catalog (autentificare a utilizatorilor) - active directory
* Servicii de suport pentru utilizatorii mobili – remote access
* Servicii de mesagerie - mail server
* Servicii de tipărire - print server,
* Servicii de fișiere - file server:
* Servicii de infrastructură - DNS, DHCP

## Fișa 2. Active directory - Serviciul de catalog

Utilizarea unei rețele include și utilizarea resurselor unei rețele. Deoarece resursele unei rețele pot fi extrem de variate (autentificare, redirecționare cereri, securitate, partajare resurse) s-a simțit nevoia unei centralizări a acestor resurse. Aici apar așa numitele servicii de catalog.

Catalogul este de fapt o bază de date ce conține:

* + Lista cu utilizatorii ce au permisiunea de a se conecta în sistem
  + Lista cu permisiuni pentru fiecare utilizator / resursă
  + Lista cu dispozitivele din rețea care au acces la resursele rețelei

Deoarece o asemenea bază de date poate ajunge la milioane de înregistrări s-a simțit nevoia unei ierarhizări. Această ierarhizare presupune existența unui domeniu și a unui controller de domeniu (fig 1).

Domeniu.ro

Fig. 1

De asemenea dacă baza de date este mare sau foarte mare, respectiv dacă cerințele de proiectare ale domeniului o cer putem avea situații în care vom avea arbori (fig. 2) sau păduri de domenii (fig. 3).

Contabilitate.domeniu.ro

Secretariat.domeniu.ro

Cercetare.domeniu.ro

Domeniu.ro

Fig. 2

**Domeniunou.ro**

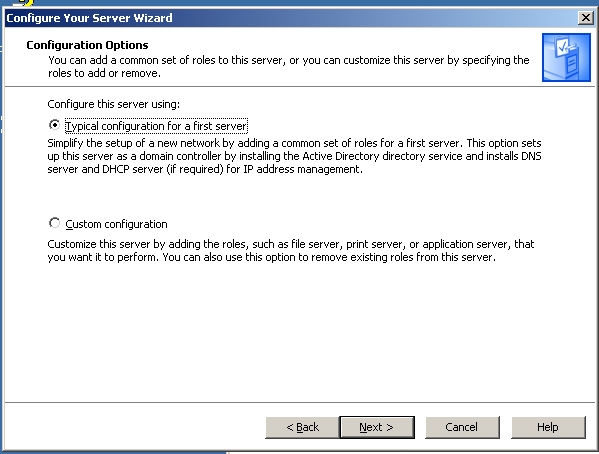
Contabilitate.domeniu.ro

Secretariat.domeniu.ro

Cercetare.domeniu.ro

**Domeniu.ro**

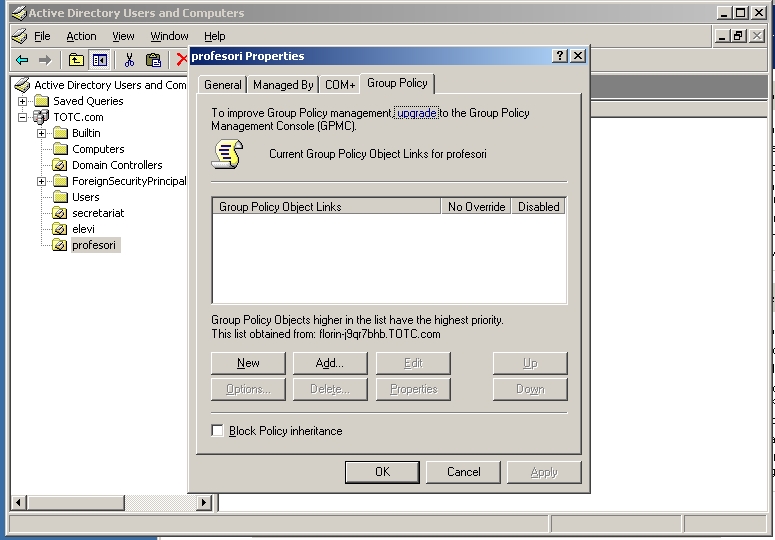
Fig. 3

Instalarea Active Directory în sistemul de operare Winows 2003 server se realizează uşor şi intuitiv cu ajutorul vrăjitorului existent în fereastra Manage Your Server alegând opţiunea Add a role, apoi Active Directory. Dacă este prima dată când instalaţi un controller de domeniu cel mai bine e să lăsaţi vrăjitorul să vă îndrume în instalare şi să instalaţi atât Active Directory, cât şi serverul DNS şi serverul DHCP.

Pe măsură ce instalarea avansează vor fi cerute informaţii vitale pentru organizarea şi buna funcţionare a controllerului de domeniu:

* + Numele de domeniu: poate fi .local dacă dorim ca domeniul creat să fie „local” (să fie separat de domeniul de internet)
  + Numele din DNS al domeniului şi numele din Netbios pentru clienţii non windows

În continuare vom face prezentarea celei mai importante componente din **Active Directory** şi anume **Active Directory Users and Computers**

**Active Directory Users and Computers** pentru domeniul curent conţine, în mod implicit, 5 categorii:

• Builtin - care conţine un set de utilizatori predefiniţi cu diferite roluri în cadrul domeniului d-voastră.

• Computers - conţine toate staţiile incluse în domeniul curent.

• Domain Controllers - include toate serverele din domeniul curent care au instalat şi configurat serviciul Active Directory.

• ForeignSecurityPrincipals - conţine identificatorii de securitate (security identi-fiers - SIDs) asociaţi obiectelor Active Directory din alte domenii decât cel curent.

• Users - conţine informaţii despre toţi utilizatorii şi grupurile de utilizatori implicite.

**Active Directory Users and Computers** poate gestiona informaţii despre calculatoare, grupuri de utilizatori, grupuri organizaţionale, imprimante, utilizatori şi directoare puse la dispoziţie în reţea (shared folder).

Recomandabil este ca înainte de crearea unui utilizator să creaţi întâi un nou grup organizaţional care poate include şi staţii de lucru, şi asupra căruia se poate crea o politică de securitate centralizată.

La proprietăţile unui grup organizațional putem specifica următoarele informaţii:

• informaţii generale (General). Conţine informaţii privind descrierea grupului şi adresa la care poate fi localizat acesta;

• informaţii despre persoana / utilizatorul care gestionează grupul respectiv (Managed By).

• politicile de securitate aplicate grupului respectiv (Group Policy) unde avem posibilitatea de creare a unei noi politici de securitate sau importul unei politici deja existente. Nu activaţi opţiunea Block Policy inheritance pentru că aceasta nu se va mai propaga automat asupra altor subsisteme organizaţionale din grupul respectiv.

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

## Fișa 3. Instalarea serverului DHCP

Instalarea şi configurarea de principiu a serverului DHCP se realizează cu ajutorul vrăjitorului care poate fi rulat din fereastra Manage my computer, Add remove roles.

Vrăjitorul ne va ajuta printr-o serie de paşi simpli să configurăm un server DHCP funcţional şi foarte util în dezvoltarea şi managementul reţelei.

Ce informaţii trebuie dumneavoastră să-i daţi vrăjitorului:

1. Numele „rezervorului de adrese” şi o scurtă descriere a acestuia (ex. adrese pentru laboratorul de informatică)
2. Apoi trebuie să ştim adresa de început, adresa de sfârşit şi masca de subreţea. Dacă în această gamă de adrese avem adrese pe care dintr-un motiv sau altul nu dorim să le alocăm dinamic, la pasul următor vom fi întrebaţi care sunt acestea.
3. „Închirierea” de adrese de IP se face pe perioadă determinată (8 zile implicit).
4. Deoarece un server DHCP trebuie să lucreze împreună cu un server DNS vom fi întrebaţi de adresa sau numele serverului DNS respectiv.

În ceea ce priveşte proprietăţile generale ale serverului, este deosebit de important să cunoaşteţi următoarele trei lucruri:

♦ cum se activează jurnalul pentru serviciul DHCP;

♦ cum este implicat serviciul DHCP în actualizarea înregistrărilor DNS pentru clienţii DHCP;

♦ cum se configurează detectarea con­flictelor.

atentie.jpgPe pagina de proprietăţi Advanced puteţi activa proprietatea Conflict Detection Attempts. Această configurare defineşte de câte ori serverul DHCP lansează în reţea comanda PING pentru a obţine un răspuns la o adresă pe care urmează să o aloce unui client. Dacă este detectat un răspuns, atunci serverul DHCP ştie că un alt client uti­lizează adresa şi încearcă să aloce alta. Prin opţiune prestabilită, această proprietate nu

este activată (este stabilită la valoarea 0), dar dumneavoastră puteţi să măriţi această va­loare pentru a verifica adresele. Într-o reţea LAN, o singură încercare trebuie să fie suficientă pentru a controla existenţa unei adrese duplicat în reţea.

Pentru a configura opţiunile Server TCP/IP, efectuaţi clic dreapta pe linia Server Options şi selectaţi opţiunea Configure Options din meniul care apare.

Opţiuni:

♦ ruter;

♦ server DNS;

♦ numele domeniului DNS;

♦ server WINS;

♦ tipul de nod NetBIOS.

În plus, clienţii DHCP Windows 2000 acceptă şi configurarea opţiunilor Perform Router Discovery şi Static Route. Toate cele­lalte setări ale configuraţiei vor fi ignorate de către clienţii Microsoft.

atentie.jpgSe pot configura anumite calcula­toare care să obţină anumite adrese atunci când cer o adresă de la serverul DHCP. Aceste alocări de adrese se numesc rezervări. Printr-o rezervare se realizează o corespondenţă între adresa MAC a unei plăci de reţea şi o adresă TCP/IP. Aceasta are ca efect crearea unei configuraţii statice, fără a fi necesară, de fapt, modificarea proprietăţilor TCP/IP de pe client. Rezervările de adrese sunt utile în mai multe situaţii. De exemplu, dacă aveţi o imprimantă de reţea, care obţine adresa TCP/IP prin intermediul unui server DHCP, dar trebuie să aibă întotdeauna aceeaşi adresă, atunci puteţi utiliza o rezervare. În plus, dacă doriţi să stabiliţi explicit adresa TCP/IP a unui calculator, deoarece acesta are insta­lat un anumit serviciu, dar dumneavoastră doriţi să beneficiaţi de parametrii de confi­gurare oferiţi de serverul DHCP, atunci puteţi utiliza de asemenea o rezervare.

Pentru a crea o rezervare, este necesară adresa hardware (MAC) a plăcii de reţea pen­tru care doriţi să rezervaţi adresa. Aceasta este uşor de obţinut; adresa TCP/IP poate fi obţinută fie local, pe calculatorul cu placa de reţea, fie de la distanţă. În ambele cazuri, calculatorul trebuie să aibă instalat protocolul TCP/IP şi trebuie să aibă o adresă TCP/IP. Local, dacă lansaţi comanda IPCONFIG/all de la un prompt de comandă, va fi afişată o linie cu eticheta Physical Address şi un număr de tipul 00-60-97-D5-22-CA aso­ciat acesteia. Aceasta este adresa MAC şi, dacă ştergeţi liniuţele, obţineţi numărul pe care serverul DHCP îl doreşte asociat cu rezervarea.

Dacă nu puteţi accesa local calculatorul, atunci puteţi determina adresa de la distanţa, folosind comanda PING şi utilitarul ARP. Utilitarul ARP descoperă şi păstrează adresa hardware asociată unei adrese TCP/IP contactate de către calculatorul local. Dacă lansaţi comanda PING pentru calculatorul pe care încercaţi să-l configuraţi şi apoi veri­ficaţi memoria cache pentru utilitarul ARP, atunci veţi descoperi adresa MAC.

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

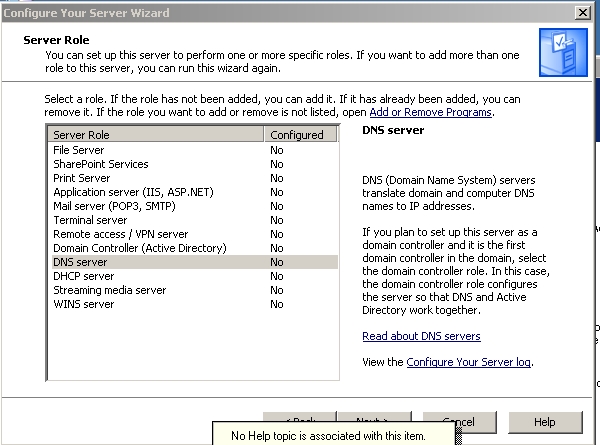
Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

## Fișa 4 Instalarea serverului DNS

Serverul DNS este unul din cele mai importante servere, server fără de care internetul şi reţelele de calculatoare, aşa cum le ştiţi dumneavoastră, ar fi un coşmar.

Închipuiţi-vă doar că ar trebui să ţineţi minte toate numerele de telefon din memoria telefonului dumneavoastră mobil! Acelaşi lucru se întâmplă şi în calculatoare: închipuiţi-vă că ar trebui să ţineţi minte câte o adresă IP pentru fiecare site care vă place!

Instalarea preliminară a unui server DNS se realizează relativ simplu în Windows 2003 Server urmând ca setările de fineţe să fie făcute ulterior. Aşa cum v-aţi obişnuit adăugarea rolului de server DNS se realizează tot din fereastra Manage Your Server.

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

# Tema 4 Instalarea sistemului de operare Windows 2003 server

## Fișa 1. Operațiuni pregătitoare

Windows Server 2003 solicită în cazul minimal un hardware relativ modest. Pentru prioritatea ediţiilor, îl puteţi instala la calculatoarele pe care altfel nu le-aţi putea utiliza ca staţie de lucru. Pentru un server folosit efectiv în producţie ar fi mai bine să utilizaţi un calculator destinat să fie folosit ca server. Calculatoarele de clasa server sunt proiectate şi construite astfel încât să fie mai fiabile şi mai serviabile decât calculatoarele desktop.

Pentru **Web Edition** a Windows Server 2003, iată configuraţia minimală recomandată pentru hardware:

- Procesor de clasă Pentium (doar) cu frecvenţa minimă de lucru de 133 MHz (Microsoft recomandă 550 MHz).

- Cel puţin 128MB de RAM. (Microsoft recomandă cel puţin 256MB)

- Cel puţin 1,5GB de spaţiu liber pe disc.

Pentru **Standard Edition**:

- Procesor de clasă Pentium (doar) cu frecvenţa minimă de lucru de 133 MHz (Microsoft recomandă 550 MHz). Ediţia standard poate utiliza până la 4 procesoare de clasă Pentium.

- Cel puţin 128MB de RAM. (Microsoft recomandă cel puţin 256MB şi personaj recomand cel puţin 512MB.) Ediţia standard poate utiliza până la 4GB de RAM instalat.

- Cel puţin 1,5GB până la 2GB de spaţiu liber pe disc.

Pentru **Enterprise Edition**:

- Procesor de clasă Pentium (doar) cu frecvenţa minimă de lucru de 133 Mhz (Microsoft recomandă 550 MHz). Ediţia Enterprise poate utiliza până la opt calculatoare echipate procesoare de clasă Pentium sau Itanium.

- Cel puţin 128MB de RAM. Ediţia Enterprise poate utiliza până la 32GB de RAM instalat.

- Cel puţin 1,5GB pentru calculatoarele echipate cu procesoare de clasă Pentium şi 2GB de spaţiu liber pe disc pentru calculatoarele echipate cu procesoare de clasă Itanium.

După ce aţi verificat că echipamentul hardware corespunde cerinţelor minimale, ar trebui să vă asiguraţi de asemenea că acel hardware pe care intenţionaţi să-l utilizaţi este atestat a fi utilizat pentru Windows Server 2003. Puteţi face acest lucru fie adresându-vă producătorului echipamentului hardware pe care intenţionaţi să-l utilizaţi, fie căutând în Microsoft Hardware Compatibility List, la adresa http:// [www.microsoft.com/hcl](http://www.microsoft.com/hcl).

Pregătirea calculatorului server

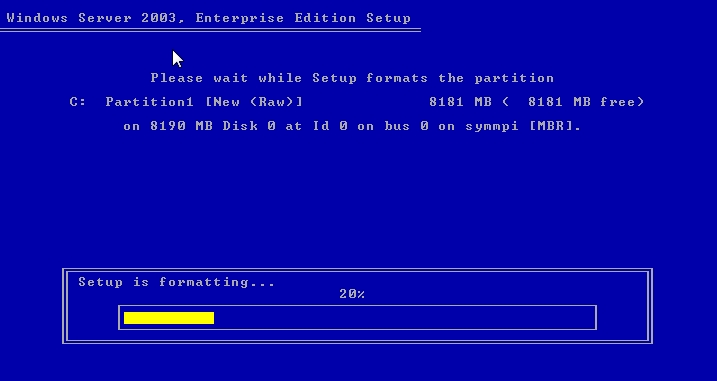
Pentru un server folosit efectiv în producţie, este important să acordaţi o atenţie specială în pregătirea echipamentului hardware. Acest proces presupune următoarele etape:

* + Testarea riguroasă a calculatorului, utilizând programe de diagnoză furnizate de fabricant.
  + Existența unei liste a tuturor componentelor utilizate pe server
  + Existența driverelor pentru componente

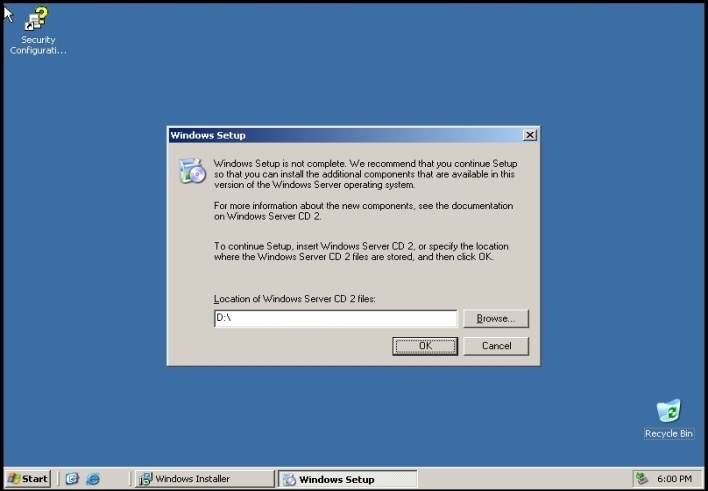
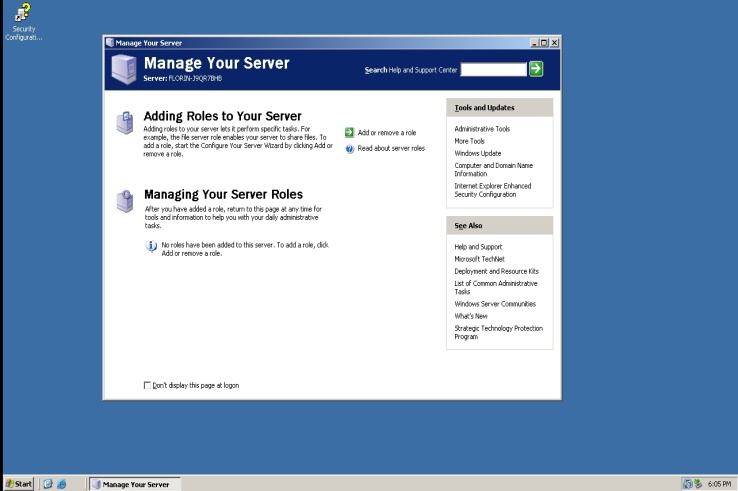
## Fișa 2 Instalarea sistemului de operare

Pentru început trebuie să intrați în BIOS-ul sistemului de calcul și să îl configurați astfel încât să booteze de de CD/DVD. Apoi introduceti CD-ul de instalare Windows 2003 Server in unitatea CD ROM. Cand sistemul porneste, urmariti mesajul “Press any key to boot from CD..” (Apasati orice tasta pentru a boot-a de pe CD)



Daca mesajul apare, apăsați orice tasta de pe tastatură pentru ca sistemul sa booteze de pe CD. Sistemul va începe acum sa inspecteze configurația hardware. Daca mesajul nu apare, unitatea de hard disk este goala şi sistemul va începe sa inspecteze configurația hardware. Va trebui să fim de acord cu termenii de licențiere și apoi dacă totul este în regulă vom avea acces la programul de partiționare și vom realiza partițiile necesare. Datorită avantajelor evidente formatarea partiției se va realiza în sistemul de fișiere NTFS. Va începe apoi procesul de copiere al fișierelor, sisstemul se va restarta și procesul de instalare va continua în mod grafic:

 Vor trebui apoi configurate setările regionale, modul de licențiere (pe server sau pe stație de lucru), numele calculatorului și setările de rețea.

Cu aceasta s-a încheiat prima parte a procesului de instalare. Dacă doriți să instalați Windows 2003 server R2, procesul de instalare va continua cu cererea celui de-al 2-lea CD. După ce instalarea celui de-al 2-lea CD s-a încheiat va apare ecranul binecunoscut

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

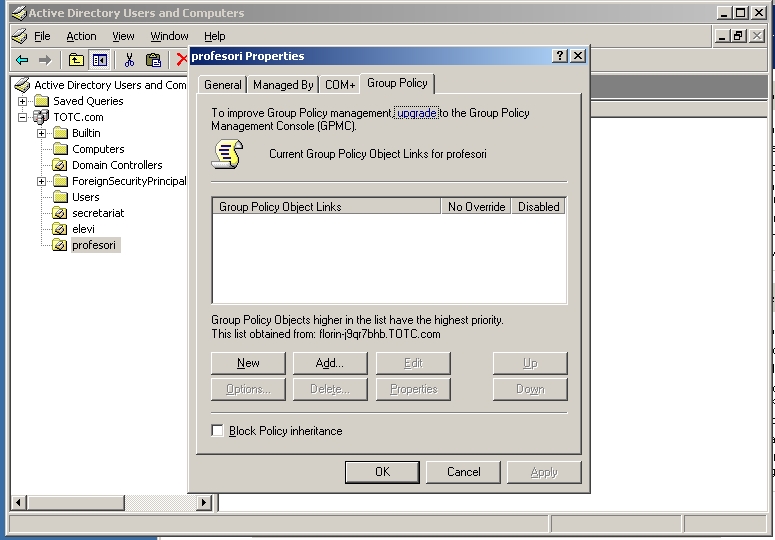
Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

# Tema 5 - Configurarea sistemelor de operare în rețea

## Fisa 1. Configurarea Active Directory

Deoarece securitatea şi managementul securităţii este un element cheie în ceea ce înseamnă Active Directory pentru un domeniu, vom prezenta în continuare, pe scurt, câteva noţiuni şi opţiuni pe care trebuie să le cunoaşteţi atunci când abordaţi un server Windows 2003.

Fereastra Group Policy este împărţită în două mari categorii:

• Computer Configuration (politica staţiilor de lucru şi a serverelor din domeniu);

• User Configuration (politica de securitate pentru utilizatorii din grupul organizaţional respectiv).

Dacă un grup organizaţional conţine numai utilizatori sau numai calculatoare, cealaltă opţiune poate fi blocată din fereastra de proprietăţi a politicii de securitate.

În momentul în care activaţi una dintre cele 2 opţiuni, va apărea pe ecranul d-voastră o fereastră de atenţionare cu privire la consecinţele care pot fi generate în urma acestei operaţiuni, respectiv faptul că staţiilor de lucru din acest grup organizaţional le va fi aplicată politica de securitate locală. Vă recomandăm să creaţi o politică de securitate cu preponderenţă orientată spre utilizator, pentru că pe aceeaşi staţie se pot conecta diferite categorii de utilizatori care pot avea diferite niveluri de acces la aceasta, anumite operaţiuni fiindu-le private de o eventuală politică de securitate eronat specificată.

O primă subcategorie întâlnită la ambele categorii este Software Settings ce conţine opţiunea Software installation, care presupune instalarea automată a unor aplicaţii împachetate în prealabil în mod administrativ. Pachetele utilizate în acest scop sînt recunoscute sub extensia MSI. Aceste pachete se salvează într-un director pus la dispoziţie în reţea. Instrumentele respective se bazează pe crearea unei imagini (snapshot) a regiştrilor sistemului de operare, instalarea şi configurarea aplicaţiilor, repornirea sistemului, împachetarea aplicaţiei prin preluarea fişierelor de pe disc, precum şi a cheilor introduse în regiştri.

În subcategoria Windows Settings există opţiunea Scripts care, pentru Computer Configuration, include opţiunile Startup şi Shutdown, iar la User Configuration include Log on şi Log off. Aici se pot specifica diferite script-uri care să se declanşeze în momentul în care staţia sau utilizatorul se autentifică în reţea.

O opţiune din politica de securitate poate avea 3 stări:

• Nedefinită/neconfigurată (not defined/not configured);

• Definită/Activă (specificarea unei valori/Enabled);

• Indisponibilă (Disabled).

În continuare, vom încerca să explicăm câteva dintre opţiunile politicii uzuale de securitate, valorile aferente şi, înainte de toate, calea de a ajunge la opţiunea respectivă.

**Computer Configuration\ Windows Settings\ Security Settings\ Account Policies\ Password Policies:**

• Maximum password age (durata maximă de valabilitate a unei parole) - forţează utilizatorul ca după un anumit număr de zile (implicit 70) să-şi schimbe parola. Este în strînsă legătură cu Minimum Password age (durata minimă de valabilitate a unei parole) (implicit 30 de zile).

• Passwords must meet complexity requirements (parola trebuie să aibă un format complex) - care înseamnă că aceasta nu trebuie să conţină o parte sau tot numele de utilizator; să nu fie mai mică de 6 caractere; să conţină caractere mari, mici, numere şi caractere non-alfanumerice (de exemplu, !, $—>, %). De asemenea, se recomandă folosirea caracterelor speciale sau a caracterului spaţiu în crearea parolelor. Activarea acestei opţiuni forţează utilizatorul să nu mai folosească data naşterii, numărul de la maşină sau nume familiare în crearea parolelor.

**Computer Configuration\ Windows Settings\ Security Settings\ Account Policies\ Account Lockout Policy:**

• Account lockout threshold (blocarea contului de utilizator) - se configurează pentru a preveni încercările repetate de conectare la reţea în condiţiile de necunoaştere a parolei. Valorile pe care le poate lua sînt de la 1 la 999. Implicit această opţiune nu este configurată, iar valoarea 0 elimină posibilitatea de blocare a contului. Recomandăm valoarea 3 pentru această opţiune.

• Account lockout duration (timpul de blocare a unui cont) - specifică durata de blocare a unui cont care a fost blocat automat prin opţiunea anterioară. Intervalul de valori este cuprins între 1 şi 99999 minute, valoarea implicită fiind de 30 de minute, configurabilă automat în momentul în care se configurează opţiunea anterioară.

**Computer Configuration\ Windows Settings\ Security Settings\ Local PoIicies\ User Rights Assignment:**

• Add workstations to domain (adăugarea de staţii în domeniu) - se configurează pentru a permite utilizatorilor sau unui grup de utilizatori să adauge staţii de lucru în domeniu. Implicit, grupul de utilizatori care poate adăuga staţii în domeniu este Authenticated Users, dar în această categorie pot intra toţi utilizatorii creaţi în Active Directory, ceea ce diminuează controlul asupra staţiilor din domeniul res­pectiv.

• Change the systern time (schimbarea timpului din sistem) - în mod implicit, fiecare utilizator poate să schimbe data şi ora sistemului, dar nu recomandăm acest lucru pentru că poate duce la înregistrarea greşită din punctul de vedere al timpului a unor evenimente din reţea. Schimbaţi asemănător exemplului anterior această opţiune, definind dreptul de acces grupurilor administrative la nivel de domeniu.

**Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ Security Options:**

• Additional restrictions for anonymous access (Acces limitat conexiunilor anonime). Orice utilizator din domeniul curent sau din alte domenii poate vedea, în mod implicit, resursele puse la dispoziţie în reţea. Pentru a oferi o mai bună protecţie domeniului recomandăm opţiunea Do not allow enumeration of SAM accounts and shares, care înlocuieşte grupul de utilizatori Everyone cu Authenticated Users în definirea politicilor locale de acces la diferite resurse. În acest fel, numai utili­zatorii din Active Directory pot avea acces la resursele domeniului: share-uri, imprimante etc.

• Automatically log off users when logon time expires (Deconectarea automată de la reţea în momentul expirării timpului de lucru). Pentru anumite categorii de utilizatori sau în mod individual poate fi configurat un interval orar de acces în reţea. În momentul în care utilizatorul depăşeşte timpul alocat, acesta este deco­nectat automat de la resursele reţelelor. De asemenea, şi versiunea următoare (local) trebuie activată pentru ca sistemul să deconecteze automat utilizatorul.

• Do not display last user name in logon screen (Neafişarea numelui ultimului utilizator conectat pe staţia curentă). În cazul reţelelor cu mulţi utilizatori, activarea acestei opţiuni aduce un spor de siguranţă la conectarea în reţea, mulţi utilizatori nefiind destul de atenţi la ultimul User Name scris în fereastra de Log On. În cazul în care într-o reţea acelaşi utilizator lucrează cu preponderenţă pe aceeaşi staţie, activarea acestei opţiuni nu este recomandată.

• Message text for users attempting to log on (Mesajul pentru utilizatorii care doresc să se conecteze în reţea). Aici se poate trece un mesaj de informare a utilizatorilor care se conectează în reţea. Opţiunea Message title for users attempting to log on specifică tipul ferestrei de mesaj (de exemplu, Bun venit în cadrul reţelei TOTC).

• Number of previous logons to cache (in case domain controller is not available) (Numărul conectărilor anterioare salvate local în cazul în care serverul de domeniu nu este disponibil) - permite conectarea pe staţii folosind utilizatorii de domeniu chiar şi în cazul în care serverul de autentificare este temporar indisponibil. Această opţiune este recomandabilă numai în cazul în care domeniul conţine puţini utilizatori, şi aceştia se conectează cu precădere pe aceeaşi staţie. În cazul domeniilor cu mulţi utilizatori, crearea profilurilor de utilizatori locali duce la o diminuare a spaţiului disponibil pe disc. Valoarea 0 este corespondentă cazului al doilea.

• Prompt user to change password before expiration (Atenţionarea utilizatorului pentru a-şi schimba parola cu un anumit timp înainte de expirare). Se exprimă în zile, valoarea implicită fiind 14. Vă recomandăm însă o valoare mai mică, 5 sau 7, pentru a nu deranja utilizatorul la fiecare conectare. Schimbarea parolei acestuia duce la anularea apariţiei mesajului de avertizare pînă la următorul termen.

• Restrict CD-ROM access to locally logged-on user only (Blocarea accesului la CD-ROM utilizatorilor autentificaţi de staţie şi nu de serverul de domeniu). Se utilizează pentru prevenirea instalării unor aplicaţii, copierii de fişiere etc. de alţi utilizatori decît cei autentificaţi în domeniu. De asemenea, se poate interzice accesul către unitatea de dischetă prin următoarea opţiune : Restrict floppy access to locally logged-on user only.

**Computer Configuration\ Windows Settings\ Security Settings\ Restricted Groups** este destinată limitării drepturilor anumitor grupuri de utilizatori, prin adăugarea acestora în această categorie

**Computer Configuratiom Windows Settings\ Security Settings\ System Services** este destinat configurării serviciilor care vor rula pe staţiile de lucru din domeniu. Se pot defini modul de pornire a serviciului, precum şi grupurile de utilizatori care au dreptul de pornire a respectivului serviciu.

Atenţie la modul de pornire a anumitor servicii. Testaţi în prealabil pe o staţie obişnuită care dintre servicii vă pot asigura o funcţionalitate optimă şi care pot fi oprite. Este bine cunoscut că un număr mai mic de servicii aduce cu sine şi o memorie RAM suplimentară.

**Computer Configuration\ Windows Settings\ Security Settings\ Registry** este opţiunea prin intermediul căreia administratorii pot defini permisiuni de acces utiliza­torilor pe anumite secţiuni din regiştrii sistemului de operare de pe staţiile de lucru.

**Computer Configuration\ Windows Settings\ Security Settings\ File System** permite administratorilor adăugarea şi definirea politicii de securitate la nivelul directoa­relor şi fişierelor de pe staţiile de lucru.

**Computer Configuration\ Administrative Templates** conţine o serie de şabloane de opţiuni predefinite configurabile. Şabloanele implicite sînt conf, inetres, system.

• încetarea apariţiei ferestrei de bun venit la conectarea în reţea: Computer Configu­ratori Administrative Templates\ System\ Don't display welcome screen at logo.

• Blocarea rulării automate a unui CD în momentul introducerii acestuia în unitatea de CD-ROM : Computer Configuration\ Administrative Templates\ System\ Disable Autoplay.

• În cazul în care aveţi mai multe servere de autentificare pentru domeniu, propagarea schimbărilor care se efectuează pe acestea poate fi configurată din: Computer Configuration\ Administrative Templates\ System\ Group Policy\ Group Policy refresh interval for domain controllers. Valoarea implicită este de 5 minute.

**Prezentarea principalelor categorii din User Configuration**

• Personalizarea titlului pentru Internet Explorer şi a imaginii de pe bara cu instrumente: User Configuration\ Windows Settings\ Internet Explorer Maintenance\ Browser User Interface\ Browser Title

• Specificarea unui proxy pentru comunicarea pe Internet: User Configuration\ Windows Settings\ Internet Explorer Maintenance\ Connection\ Proxy Settings

• Personalizarea paginii de start (home page), a paginii de căutare şi a paginii pentru asistenţa tehnică: User Configuration\ Windows Settings\ Internet Explorer Maintenance\ URLs\ Important URLs Această opţiune este foarte importantă pentru configurarea unei pagini HTML drept desktop al staţiilor din domeniu.

• Pentru specificarea altei locaţii directorului My Documents: User Configuration\ Windows Settings\ Folder Redirection\My Documents. În lista Settings există opţiunea Basic - Redirect everyone 's folder to the same location (redirecţionarea tuturor utilizatorilor către aceeaşi locaţie), iar la Target folder location treceţi adresa la care va fi redirecţionat automat directorul My Documents pentru fiecare utilizator în parte.

• Interzicerea schimbării paginii de start (home page): User Configuration\ Admi­nistrative Templates\ Windows Components\ Internet Explorer\ Disable changing home page settings.

• Ascunderea opţiunii Folder Option din meniul Tools din Windows Explorer cu scopul de a nu permite utilizatorilor vizualizarea unor fişiere ascunse, sau fişiere sistem, în scop distructiv, sau a eliminării lor din necunoştinţă de cauză: User Configuration\ Administrative Templates\ Windows Components\ Windows Explo­rer\ Removes the Folder Option menu item from the Tools menu. Opţiunea ascun­derii fişierelor şi eliminarea posibilităţii de dezascundere poate fi depăşită cu utilitarul Command Prompt, comanda attrib.

• Ascunderea anumitor discuri în My Computer, pentru a restricţiona accesul la acestea: User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ Hide these specified drives in My Computer. Foarte multe erori care se întâmplă la utilizarea calculatoarelor sunt cauzate de mutarea accidentală prin drag-and-drop a directoarelor dintr-o locaţie în alta. Pentru protejarea sistemului de operare, dar şi pentru a păstra o ordine în organizarea fişierelor de pe discul C:, vă reco­mandăm să activaţi opţiunea Restrict C drive only. De asemenea, puteţi bloca accesul la discurile A: sau B: pentru a vă proteja şi prin această cale de utilizatorii care pot transporta viruşi pe dischete (Restrict A, B and C drives only). În cazul în care doriţi blocarea accesului la CD-ROM, trebuie să activaţi opţiunea Restrict D drive only, cu specificarea faptului că trebuie să vă configuraţi partiţiile de pe staţiile de lucru (Administrative Tools\ Computer Management\ Disk Management) în aşa fel încît discul de CD-ROM să aibă asignată litera D. Dacă staţia d-voastră face parte dintr-un domeniu public, gen i-cafe, puteţi ascunde toate discurile de pe staţie, prin activarea opţiunii Restrict all drives. Chiar dacă activaţi această politică de securitate, accesul la discuri este posibil din Command Prompt numai dacă nu aţi dezactivat această opţiune.

• Eliminarea iconiţei My Network Places din Windows Explorer pentru a preveni accesul neautorizat în reţea: User Configuration\ Administrative Templates\ Windows Components Windows Explorer\ No „Entire Network" in My Network Places.

• Specificarea numărului maxim de documente stocate în lista documentelor recent apelate: User Configuration\ Administrative Templates\ Windows ComponentsX Windows ExplorerX Maximum number of recent documents (valoare implicită: 15).:

• Eliminarea opţiunii Run din meniul Start: User Configuration\ Administrative Templates\ Start Menu & Taskbar\ Remove Run Menu from Start Menu.

• Ascunderea iconiţei de acces la reţea de pe Desktop : User Configuration\ Admi­nistrative Templates\ Desktop\ Hide My Network Places icon on desktop.

• Interzicerea schimbării destinaţiei directorului sistem My Documents: User Configuration\ Administrative Templates\ Desktop\ Prohibit user from changing My Documents path.

• Ascunderea resursei Active Directory în reţea: User Configuratori Administrative Templates\ Desktop\ Active Directory\ Hide Active Directory folder.

• Interzicerea accesului la tabloul de bord al calculatorului (Control Panel): User Configuratori Administrative Templates\ Control Panel\ Disable Control Panel.

• Dacă doriţi în schimb să păstraţi numai anumite componente în Control Panel, puteţi alege opţiunea Show only specified control panel applets şi specificaţi numele componentelor pe care le doriţi. Componentele pe care le puteţi folosi le găsiţi în directorul în care a fost instalat sistemul de operare, subdirectorul System32, sub forma unor fişiere cu extensia CPL. Pot exista în schimb şi neclarităţi în legătură cu aceste componente pentru că, de exemplu, nu există nici un CPL care să deschidă fereastra de configurare a tastaturii, şi nici a imprimantelor.

• Interzicerea modificării setărilor pentru display : User Configuration\Administrative Templates\ Control Panel\ Display\ Disable Display în Control Panel. Această regulă poate fi considerată una dintre cele mai drastice pentru utilizatorul final. Folosirea acestei politici de securitate diminuează posibilitatea de apariţie a unor cazuri de acest gen, pentru că în utilitarul Paint există încă posibilitatea de setare a unei imagini drept fundal al desktop-ului d-voastră.

• Interzicerea modificării parametrilor TCP/IP : User Configuratori Administrative Templates\ Network\ Network and Dial-up Connections\ Allow TCP/IP advanced configuration

• Blocarea accesului la utilitarul pentru comenzi (Command Prompt): User Configu­ratori Administrative Templates\ System\ Disable the command prompt. În această secţiune, la opţiunea Enabled foarte important este modul în care se vor executa script-urile. Dacă la procesul de autentificare de reţea aveţi script-uri de tip BAT pentru diferite operaţiuni, alegeţi din lista Disable the command prompt script processing also opţiunea No.

• Interzicerea accesului la regiştrii sistemului de operare, activaţi opţiunea Disable registry editing tools.

• Interzicerea accesului către anumite aplicaţii: Do not run specified Windows applications

• Limitarea accesului la aplicaţia de gestiune a proceselor (Task Manager): User Configuratori Administrative Templates\ System\ Logon\ Logoff\ Disable Task Manager; recomandăm această opţiune în momentul în care rulaţi aplicaţii de monitorizare pe staţiile de lucru sub formă de servicii, pentru a preveni oprirea neautorizată a acestora de către utilizatori.

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

# Tema 6: Securitatea NOS

## Fisa 1. Securizarea sistemului

Securitatea se referă la menţinerea sistemului în stare de funcţionare în regi continuu şi la parametri normali. Securitatea nu se referă doar la protejarea împotriva diferitelor tipuri de atacuri, ci şi la protecţia împotriva căderilor hardware (a harddisk-urilor), a ştergerii accidentale a datelor.

Un server este supus permanent riscurilor unor atacuri de diferite feluri, aceste provenind de la distanţă sau chiar de pe propria maşină. Atacurile pot fi:

• atacuri de refuz al serviciilor (Denial of Service), care degradează sau defecteas  
anumite servicii ale programului;

• atacuri în vederea obţinerii de privilegii asupra sistemului;

• atacuri în vederea copierii sau distrugerii de informaţii.

Principalele tipuri de atacuri:

Poate fi stopat prin introducerea în fişierele de configurare a accesului din cadrul MTA a unei directive de refuzare a mesajelor provenind de pe maşina sau de la utilizatorul respectiv. Această soluţie nu rezolva însă problema traficului prin reţea.

2. Spam (e-mail spamming)

De obicei, adresa expeditorului este falsă (pentru a nu putea fi descoperit), astfel că acest tip de  
atac poate fi prevenit configurând serviciul de e-mail pentru a respinge e-mail-urile  
provenite de pe domenii care nu pot fi rezolvate.

3. Falsificarea adresei expeditorului (E-mail spoofing)

Serverul (sau serverele, în unele cazuri) de mail care a transmis mesajul poate fi  
determinat prin analiza antetului mesajului. Se recomandă contactarea administra­  
torului serverului respectiv şi solicitarea de informaţii privind originea mesajului  
(acestea pot fi obţinute din fişierele jurnal ale sistemului)'.

4. Abonarea nesolicitată la liste de discuţii

Reprezintă înscrierea unei adrese e-mail pe una sau mai multe liste de discuţii  
fără ca persoana căreia îi aparţine adresa să fi cerut explicit acest lucru. Nu există  
soluţii rapide pentru stoparea acestor atacuri, ci doar trimiterea de cereri de dez-  
abonare. :

5. Atacuri pentru refuzul serviciilor (Denial of Service) '

Prevenirea atacurilor de tip DoS se poate face prin instalarea de firewalluri (care să filtreze pachetele către porturi care trebuie protejate, precum şi pachetele ICMP) instalarea de conexiuni de siguranţă (backup) şi dezactivarea serviciilor care n necesare (pentru a diminua expunerea acestora la potenţialele atacuri).

6. Depăşirea zonelor tampon

Acest tip de atac nu poate veni însă din afara maşinii, ci din interiorul și nu poate fi prevenit. Pe măsură ce asemenea erori sunt descoperite, sunt generate actualizări ale programelor.

7. Interceptarea reţelei (IP sniffing)

Un asemenea atac se poate preveni doar din interiorul reţelei locale. Pentru a preveni, este bine să utilizăm, cel puţin pentru transmiterea parolelor din protocoale sigure, criptate, cum ar fi SSH.

8. Cai troieni (Trojan horses)

Toate fişierele executabile sau arhivele conţinând programe descărcate de pe Internet (chiar şi de pe şiturile oficiale) trebuie verificate înainte de a fi instalate și executate. De asemenea, se recomandă realizarea periodică de copii de siguranță a sistemelor de fişiere, pentru a putea restaura fişierele executabile originale în alterării acestora de către cai troieni.

9. Uşi ascunse

Uşile ascunse sunt cazuri particulare de cai troieni. Un asemenea program creează o „poartă" (de exemplu, un utilizator nou) care să permită accesul ulterior la calculatorul în cauză sau să acorde unui anumit utilizator privilegii speciale. Spre exemplu, un cal troian poate înlocui fişierul /bin/login, care are rolul de a autentifica utilizatorii, pentru a salva parolele tastate de aceştia într-un fişier ascuns;

10. Viruşi

Viruşii sunt programe care pot efectua operaţiuni nedorite, de obicei distructive, şi care au capacitatea de a se „multiplica", adică de a infecta şi alte programe. Viruşii rezidă în general în cadrul fişierelor executabile. Sistemele UNIX nu sunt vulnerabile la viruşi, datorită gestiunii stricte a memoriei şi a proceselor care se execută. Este recomandat, în orice caz, să nu se execute ca root nici un fişier executabil despre care nu se cunoaşte ce face.

11. Viermi (Worms)

Viermii sunt programe de sine stătătoare, capabile să se multiplice, să se transfere pe alte calculatoare şi, eventual, să efectueze operaţii distructive. Sistemele FreeBSD nu sunt afectate de viermi.

12. Ghicirea parolelor (password guessing)

Acest tip de atac se referă la folosirea unui program pentru a determina parolele prost alese, denumit în genere spărgător de parole (cracker). Un astfel de program poate determina, printr-o analiză comparativă, o corespondenţă între variantele de presupuse parole criptate.

13. Folosirea de anumite vulnerabilităţi (bugs) a programelor / serviciilor existente pe server

De obicei, problema securităţii nu se pune la nivel de nucleu al sistemului de operare, ci la nivelul aplicaţiilor. La anumite perioade de timp sunt descoperite vulnerabilităţi în aplicaţiile instalate în sistem, în servicii, unele dintre ele putând fi folosite pentru a obţine accesul în sistem.

Reuşita atacurilor este de cele mai multe ori cauzată de configurări slabe ale sistemului sau de neglijarea erorilor (bugs) de securitate descoperite şi de lipsa update-uui la timp a programelor ce prezintă vulnerabilităţi. De aceea trebuie acordată o importanţă mare configurărilor de după instalare.

Acțiuni ce trebuie întreprinse pentru a se asigura securizarea unui sistem de operare în rețea:

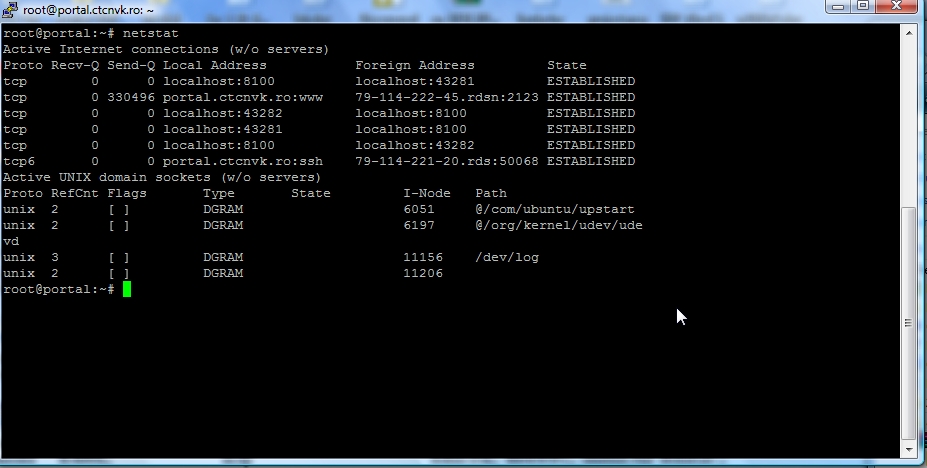
* Siguranţa fizică a sistemului - Instalarea maşinii trebuie realizată într-un loc sigur, să nu fie expusă contactului cu persoane neautorizate. Acestea nu trebuie să aibă posibilitatea sau timpul necesar de a înlătura carcasa, de a modifică configuraţia hardware, de a opri şi apo reporni maşina (eventual în modul single), de a înlocui sau copia informaţiile discuri sau de a inocula programe răuvoitoare (cai troieni). De asemenea, mediile de stocare a salvărilor de siguranţă trebuie să fie păstrate într-un loc închis, fără posibilitate de acces (e.g., un seif).
* Salvările de siguranţă - Se recomandă salvarea periodică cel puţin a fişierelor importante şi, dacă este posibil a întregului conţinut al sistemelor de fişiere.
* Drepturile de acces Ia fişierele importante - Trebuie acordată o atenţie sporită drepturilor de acces la fişierele importante: fişierele de configurare ale diverselor servicii instalate în sistem, fişierele jurnal (log-uri), executabilele care nu trebuie să poată fi apelate de către utilizatorii obişnuiţi, precum şi alte fişiere importante (spre exemplu, baze de date MySQL, PostreSQL etc.), executabilele şi scripturile de iniţializare ale sistemului nu trebuie să poată fi modificate decât de root / administrator.
* Execuţia daemonilor / proceselor - Se recomandă ca numai daemonii / procesele utilizaţi(te) curent să ruleze pe sistem. Mai mulţi(te) daemoni / servicii înseamnă o încărcare mai mare a sistemului, precum şi un nivel de vulnera­bilitate mai mare. De asemenea, o mare parte a daemonilor / serviciilor (care oferă diverse servicii) nu trebuie executaţi sub root / administrator, ci sub utilizatorii speciali (de exemplu, daemonul HTTP rulează sub utilizatorul www).
* Scripturile CGI - Scripturile CGI nu trebuie executate ca root. Acestea trebuie plasate într-un singur director, în care nu se va permite accesul utilizatorilor, iar modificările asupra scripturilor trebuie monitorizate.
* Porturile - Anumite servicii pot fi accesate prin reţea, de pe alte maşini. Pentru aceasta, ele aşteaptă conexiuni pe anumite porturi (e.g., serverul HTTP pe portul 80). Aceste porturi pot constitui puncte vulnerabile ale sistemului (datorită vulnerabilităţilor care pot exista în aceste pro­grame), putând fi detectate de la distanţă cu ajutorul scanerelor. Aceste porturi trebuie protejate fie prin configurarea respectivelor servicii să accepte conexiuni doar de pe o anumită interfaţă de reţea, considerată sigură (e.g., reţeaua locală), fie prin configurarea unui firewall care să nu permită accesarea din exterior a porturilor în cauză.
* Accesul utilizatorului root / administrator în sistem - Din principiu, nu se recomandă permiterea accesului cu root / administrator decât de la consolele sistemului. Accesul de la distanţă (cu SSH) va fi făcut cu un utilizator obişnuit, iar apoi va fi folosită comanda su. Sistemul FreeBSD nu permite accesul la distanţă prin SSH folosind autentificarea ca root şi, de asemenea, nu permite su decât din contul utilizatorilor ce aparţin grupului wheel.
* **Sugestii metodologice**
* Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.
* Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.
* Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,
* personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.
* Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

## Fișa 2 Utilitare pentru monitorizarea sistemului.

**Utilitarul netstat**

Programul netstat afişează informaţii privind starea curentă a conexiunilor de reţea active, tabelele de rutare, statistici despre intefeţele de reţea etc. Aceste informaţii pot fi utile pentru determinarea unor conexiuni dubioase sau care efectuează trafic nejustificat. Spre exemplu, dacă este apelat fără argumente, netstat va afişa conexiunile active:

Sunt utile următoarele argumente pe care le poate primi programul netstat:

• -i - afişează starea interfeţelor de reţea. . .

• -s - afişează o serie de statistici pentru toate protocoalele TCP/IP.

• -r - afişează conţinutul tabelelor de rutare.

Utilitarul tcpdump

Principalul utilitar de interceptare a reţelei este tcpdump, având următoarea sintaxă:

tcpdump [ opţiuni ] [ -i interfaţă ] [ expresie ]

Câmpul expresie specifică ce pachete vor fi afişate. El constă din mai multe primitive. Primitivele reprezintă unul sau mai mulţi calificatori urmaţi de un identifi­cator. Există trei tipuri de calificatori :

1. Tip - poate lua una dintre valorile: host (primitiva se va referi la un nume de maşină), net (reţea) şi port.
2. Direcţie - poate lua una dintre valorile: src,dst,src or dst sau src and dst.
3. Protocol - poate lua una dintre valorile: ip, arp, tcp sau udp.

Principalele primitive care pot fi utilizate sunt următoarele :

• dst host maşină - adevărat dacă maşina destinaţie este cea specificată.

• src host maşină - adevărat dacă maşina sursă este cea specificată.

• dst net mask mască - adevărat dacă adresa destinaţie are masca de reţea specificată.

• src net mask mască - adevărat dacă adresa sursă are masca de reţea spe ficată.

• dst port port - adevărat dacă portul destinaţie este cel specificat.

• src port port - adevărat dacă portul sursă este cel specificat.

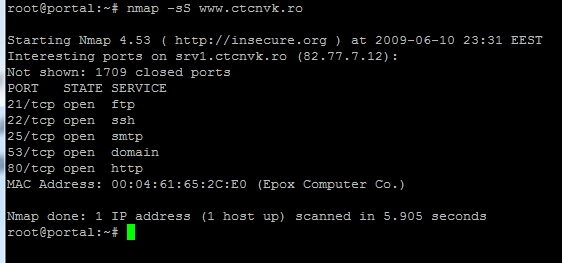
• ip proto protocol - adevărat dacă pachetul are protocolul specificat. Poate icmp, udp sau tcp.

Spre exemplu:

comanda tcpdump dst port 22 va afişa, pachetele care sunt îndreptate către portul 22

**Utilitarul NMAP**

Un scaner (scanner) este un program care accesează porturile şi serviciile TCP/IP şi înregistrează răspunsul, venit de la ţintă. Utilizarea unui asemenea program este folositoare pentru a evidenţia serviciile expuse exteriorului de către o anumită maşină; precum şi pentru a testa configuraţia firewalurilor. Recomandăm folosirea periodică a unui program de scanare, pentru a depista eventualele puncte vulnerabile ale sistemului, cum ar fi serviciile expuse conectivităţii din exteriorul reţelei, sau pentru a testa funcţionarea firewalului

Programul NMAP este unul dintre cele mai răspândite scanere.

nmap [ mod\_scanare ] [ opţiuni ] maşină

**Utilitarul systat**

Utilitarul systat afişează în timp real o serie de statistici privind utilizarea sistemului. Este alcătuit din două ferestre: prima, în partea de sus a ecranului, afişează încărcarea curentă a sistemului. Cea aflată în partea de jos a ecranului afişează informaţii în funcţie de tipul statisticilor. Pe ultima linie de ecran sunt afişate mesaje de eroare.

Programul systat poate primi ca argument tipul statisticilor, astfel:

1. - pids —afişează procesele care consumă procesor cel mai mult timp.
2. - icmp - afişează statistici privind pachetele ICMP care tranzitează interfeţele de reţea.
3. - ip - afişează traficul cu pachete IP şi UDP
4. - tcp - afişează statistici privind traficul de pachete TCP.
5. - iostat - afişează statistici privind utilizarea timpului procesor şi a discurilor instalate în sistem.
6. - swap - informaţii privind utilizarea swap-ului.

**Sugestii metodologice**

Unde predăm ? Conţinutul poate fi predat în cabinetul de specialitate, laboratorul de informatică sau într-o sală dotată cu videoproiector. Locaţiile vor fi dotate cu calculator.

Cum predăm ? Ca metode de predare –învăţare se recomandă utilizarea combinată a explicaţiei cu dialogul dirijat, exemplificarea şi exemplul practic.

Mijloace utilizate: Materiale suport ce conţin noţiunile de bază, fişe de lucru, prezentări media,

personsOrganizarea clasei: Pregătirea practică se va realiza cu clasa împărţită în grupe de 2-3 elevi.

Evaluarea: Teste de evaluare cu itemi, chestionare frontală.

# Fişa rezumat

**Numele elevului**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Numele profesorului:** *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Competenţe care trebuie dobândite** | **Activităţi efectuate şi comentarii** | **Data activitatii** | **Evaluare** | | |
| **Bine** | **Satis-făcător** | **Refacere** |
| Identifică dispozitive şi circuite electronice analogice şi digitale utilizate în realizarea echipamentelor de telecomunicaţii | Activitate 1 |  |  |  |  |
| Activitate2 |  |  |  |  |
| Interpretează parametrii ce caracterizează funcţionarea circuitelor electronice din echipamentele de telecomunicaţii |  |  |  |  |  |
| Citeşte scheme cu circuite electronice din echipamentele de telecomunicaţii |  |  |  |  |  |
| Depanează subansamble electronice din echipamentele de telecomunicaţii |  |  |  |  |  |
| **Comentarii** | | **Priorităţi de dezvoltare** | | | |
| **Competenţe care urmează să fie**  **dobândite (pentru fişa următoare)** | | **Resurse necesare** | | | |

* **Competenţe care trebuie dobândite**

Această fişă de înregistrare este făcută pentru a evalua, în mod separat, evoluţia legată de diferite competenţe. Acest lucru înseamnă specificarea competenţelor tehnice generale şi competenţelor pentru abilităţi cheie, care trebuie dezvoltate şi evaluate. Profesorul poate utiliza fişele de lucru prezentate în auxiliar şi/sau poate elabora alte lucrări în conformitate cu criteriile de performanţă ale competenţei vizate şi de specializarea clasei.

* **Activităţi efectuate şi comentarii**

Aici ar trebui să se poată înregistra tipurile de activităţi efectuate de elev, materialele utilizate şi orice alte comentarii suplimentare care ar putea fi relevante pentru planificare sau feed-back.

* **Priorităţi pentru dezvoltare**

Partea inferioară a fişei este concepută pentru a menţiona activităţile pe care elevul trebuie să le efectueze în perioada următoare ca parte a viitoarelor module. Aceste informaţii ar trebui să permită profesorilor implicaţi să pregătească elevul pentru ceea ce va urma.

* **Competenţele care urmează să fie dobândite**

În această căsuţă, profesorii trebuie să înscrie competenţele care urmează a fi dobândite. Acest lucru poate implica continuarea lucrului pentru aceleaşi competenţe sau identificarea altora care trebuie avute in vedere.

* **Resurse necesare**

Aici se pot înscrie orice fel de resurse speciale solicitate:manuale tehnice, reţete, seturi de instrucţiuni şi orice fel de fişe de lucru care ar putea reprezenta o sursă de informare suplimentară pentru un elev care nu a dobândit competenţele cerute.

***Notă: acest format de fişă este un instrument detaliat de înregistrare a progresului elevilor. Pentru fiecare elev se pot realiza mai multe astfel de fişe pe durata derulării modulului, aceasta permiţând evaluarea precisă a evoluţiei elevului, în acelaşi timp furnizând informaţii relevante pentru analiză.***

# Bibliografie

Dragoș Acostăchioaie - FreeBSD Utilizare, Administrare, Configurare

Adrian Munteanu – Rețele locale de calculatoare proiectare și administrare

Adrian Munteanu – Rețele windows Servere și clienți. Exemple practice

Damir Bersinic – Windows 2000 Directory Services Infrastructure

Michael Turner – Administrarea RedHat Linux, Cunoștințe esențiale

Radu Mârșanu – Calculatoare personale elemente arhitecturale