LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

1. Shell Scripts
2. Linux Kernel
3. Serverul DHCP
4. Serverul FTP
5. NFS - Network File System
6. Serverul DNS
7. Serverul Apache
8. Serverul MySql
9. NETFILTER
9.1 Prezentare generala
9.2 Firewall
9.3 Structura NETFILTER
9.4 Sintaxa iptables
9.5 Scenarii si exemple
10. Sistemul de e-Mail
11. Serverul Postfix
12. Serverul POP/IMAP
13. Managementul Logurilor
14. Exemple practice (Ubuntu 14.04 LTS)
15. Webmin

Firewall

Un Firewall reprezinta o componenta a infrastructurii de securitate care separa retele de calculatoare sau calculatoare care au nivele diferite de securitate.

Un firewall poate fi de 2 feluri:
a) Hardware - echipament dedicat, special creat, care are drept scop filtrarea datelor dintre 2 entitati (Exemplu: Cisco ASA).
b) Software - aplicatie, care ruleaza pe calculator(server) impreuna cu alte programe care are acelasi scop ca si un firewall hardware

Nota

Un firewall hardware foloseste software pentru a realiza filtrarea. Pe langa filtrarea propriu zisa un firewall hardware are si alte functii precum VPN, criptarea datelor etc.

Important

Filtrarea pachetelor se bazeaza pe headerele protocoalelor din stiva TCP/IP. O intelegere foarte buna a acestor protocoale (inclusive structura headerelor) este esentiala pentru crearea/configurarea unui firewall eficient.

Exista 3 generatii de firewall:
1. Packet based
Filtreaza in functie de campurile din headerele de la Layer 3 (Network) si 4 (Transport) ale OSI.
Nu diferentiaza intre pachete.

2. Circuit-based numit si stateful firewall
Filtreaza in functie de campurile din headerele de la Layer 3 (Network/IP) si 4 (Transport/TCP,UDP) OSI.
Suplimentar se tine cont de relatiile dintre pachetul curent si celelalte.
Exemplu: un pachet adresat hostului local este permis daca acesta reprezinta raspuns la un pachet generat din interior (de hostul local).

3. Application Layer Firewall (Proxy Based Firewalls)
Firewall care "citeste" datele de la nivelul aplicatie (FTP/HTTP/DNS etc).

In Linux singura modalitatea de a crea un firewall este reprezentata de arhitectura NETFILTER. Aceasta arhitectura foloseste comanda iptables (user space tool) pentru a filtra pachetele de date.

NETFILTER este o tehnologie foarte avansata care permite crearea unui firewall de la zero extrem de eficient care poate fi folosit cu incredere pe servere din mediul Enterprise.

NETFILTER inglobeaza caracteristicile tuturor celor 3 generatii amintite mai sus (aplication layer firewall cu module speciale).

Resurse

- Firewall Q&A