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
7.1 Protocolul HTTP
7.2 Prezentare generala server
7.3 Compilare si instalare
7.4 Structura Apache
7.5 Configurare Apache
7.6 PHP
7.7 Securitate Web
8. Serverul MySql
9. NETFILTER
10. Sistemul de e-Mail
11. Serverul Postfix
12. Serverul POP/IMAP
13. Managementul Logurilor
14. Exemple practice (Ubuntu 14.04 LTS)
15. Webmin

Securitate Web

Securitatea unui sistem informatic este la fel de buna ca cea mai slaba veriga a sa. Este suficient ca un cracker sa compromita serverul web sau sa ruleze un exploit la nivel de aplicatie cum ar fi un Sql Injection pentru ca apoi sa mai aiba un mic pas pana sa devina root pentru intreg sistemul de operare.

Platformele web formate din server http, php, server baze de date si aplicatiile instalate au un istoric plin de vulnerabilitati. De foarte multe ori compromiterea unui sistem de operare a plecat de la configurarea gresita a modulului in care PHP opereaza sau de la serverul MySql ori Apache.

Securitatea informatiei este un proces continuu, o stare de fapt.

Securizarea unui server presupune cunostinte avansate si experienta.

Imi propun enumerarea catorva aspecte minimale care conduc catre o platforma web stabila si sigura.

1. Ascunderea a cat mai multa informatie despre serverul web care ruleaza, versiunea acestuia, versiunea de PHP sau de MySql. Primul pas al oricarui atac informatic este identificarea serviciilor si versiunilor care ruleaza. Ulterior un cracker experimentant sau nu, poate cauta pe Internet exploit-uri pentru anumite versiuni de Apache sau de PHP si le poate rula.
Ascunderea de informatie in vederea cresterii securitatii informatice poarta denumirea de "security through obscurity".
In general acest proces nu imbunatateste securitatea generala a sistemului ci doar evita atacuri din partea persoanelor neexperimentate si care cauta tinte la intamplare.

2. Instalarea ultimei versiuni stabile de server web, php si server MySql
Intre specialistii in securitate si crackeri exista o cursa continua.
Oricat de bun ar fi un produs acesta nu poate fi 'bug-free'. Periodic se descopera erori de programare in majoritatea serverelor care pot fi exploatate de persoane rau intentionate. Singura solutie finala este aplicarea unui patch care 'astupa' respectiva 'gaura de securitate'.

3. Rularea serverului Apache si MySql sub propriul user care sa nu mai fie folosit in alt scop.
Exemplu: apache ruleaza sub wwwuser si wwwgroup, iar MySql sub mysqluser si mysqlgroup

4. Setarea accesului la resursele oferite de server in functie de IP-ul clientilor sau de username si parola.
Directoarele sau fisierele sensibile si confidentiale trebuie protejate impotriva accesului neautorizat. Acces neautorizat poate fi chiar si indexarea paginilor respective de catre motoare de cautare precum Google. In ultima vreme multe tipuri de atacuri se bazeaza pe cautarea pe Google de continut confidential care a fost indexat datorita configurarii necorespunzatoare a serverelor HTTP. Detalii.

5. PHP Session Security.

6. Instalarea si configurarea mod_status pentru a urmarii activitatea si performantele serverului Apache

7. Instalarea Apache in jail (chrooted)

8. Instalarea si configurarea mod_security
mod_security reprezinta cel mai cunoscut si folosit WAF (Web Application Firewall). Acesta este extrem de complex, iar pentru intelegerea aprofundata a modulului in care acesta functioneaza este nevoie de cunostinte avansate.

9. Folosirea protocolului HTTPS in loc de HTTP pentru continut confidential. Oricat de sigur ar fi configurat sistemul si oricat de bun ar fi firewall-ul, informatia poate fi captata si citita pe drumul dintre sursa si destinatie in cel mai simplu mod fiindca aceasta circula in clar. Solutia este criptarea informatiei folosind ssl/tls (HTTPS).

10. MySql Security

- setarea de parola pentru userul root
- stergerea userilor anonimi

Important

Nu exista sistem 100% sigur. Oricat de pregatit este adminul si oricata munca depune in vederea securizarii serverului, tot exista posibilitatea ca acesta sa fie compromis. Sansa ca serverul sa fie compromis trebuie luata in calcul

intotdeauna. De multe ori un backup eficient reprezinta salvarea.

Resurse:

- Apache Security Tips
- Apache Security Book