Web Programming -- 5

Web Security
( Chapter 4 )

Basic Security Measures

• Limit the number of users on server machine
• Good password
• System’s logging facilities to detect break-in
• Do not run Internet daemons that are not needed
• Periodically check system files

Turning Off Insecure Web Features

• Automatic directory listing
• Symbolic link
• User-Supported directories (use of buggy scripts)
• Executable scripts
• Sharing document root with FTP
• Use file system permission
• Running in chroot environment

Access Control

Restricting access to certain IP addresses

Server check that the client is connecting from one of the allowed addresses.

HTTP/1.0 403 Forbidden
Date: Monday, 27-Jan-97 14:23:10 GMT
Server: Apache/1.1.1
Mime-Version: 1.0
Content-type: text/html
Access Control

Restricting access to unauthorized users

Server check that the client is an authorized user.

HTTP/1.0 401 Unauthorized
Date: Monday, 27-Jan-97  15:11:17 GMT
Server: Apache/1.1.1
Mime-Version: 1.0
Content-type: text/html
WWW-Authenticate: Basic realm="Designers"

Configuring Access Control

Begin an access restriction section
<Limit GET POST>
End an access restriction section
</Limit>

Order in which to evaluate other directives
order  deny,allow

deny from . cracker.ltd phreaks.com
allow from . capricorn. org

Deny/Allow access to some domains
deny from . cracker.ltd phreaks.com
allow from . capricorn. org
Configuring Access Control
(Restrict all except few)

<Limit GET POST>
  order mutual-failure
deny from all
  allow from .capricorn.org
  allow from 18.157.0.5 18.157.0.22
</Limit>

Adjusting Directories

user fred or any member of designer or web-admin

<Directory /local/web/fall_colors/>
  AuthName Designers
  AuthType Basic
  AuthUserFile /usr/local/etc/htpd/htpasswd
  AuthGroupFile /usr/local/etc/htpd/htgroup
  <Limit GET POST>
    require user fred
    require group designers web-admin
  </Limit>
</Directory>
Firewall - Dual Homed Gateway
Proxies run on Gateway

Firewall -- Screened-Host Gateway
Router act as the filter -- One way mirror

Web Browsing From Inside the Firewall

SOCKS
Proxy program on gateway
Routines to replace the standard network calls

TIS Firewall Toolkit
Use browsers proxy-aware feature

Web Server-Based Proxies
Server two purpose: Web server for outside
Web proxy for inside.

Security and Web Server
Security and Web Server

(B) The Sacrificial Lamb

Security risk -- Bastion and server on same machine

Router is configured to pass through any incoming packet for port 80 to the Web server host

Security and Web Server

(C) HTTP Server Running on the Gateway

Security and Web Server

(D) HTTP Server Running Alongside the Gateway

Inner and Outer Web Servers Connected by a Chaining Proxy
Use of Encryption --- Public/Private key

A encodes with B’s public key
B decodes with her private key

A encodes signature with his private key
B decodes with A’s public key