การ Hardening Linux เบื้องต้น

คมกริช คำสวัสดิ์
วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

การ Hardening Linux เบื้องต้น

ขั้นตอนการ Hardening Linux เบื้องต้น

- การเปลี่ยน Root password
- การ Lock/Unlock users
- การตั้งเวลาของเครื่องเทียบกับ NTP server
- การ Update/Upgrade/Patch ระบบ
- การส่ง System logs ไปยัง Syslog server
- การ Hardening Secure Shell (SSH)
- การ Hardening MySQL server
- การ Hardening HTTPD (Apache)
- Case study: Shellshock

เปลี่ยนรหัสผ่านของ Root

```
[root@Server ~]# passwd root
Changing password for user root.
New password: <NEW PASSWORD>
Retype new password: <NEW PASSWORD>
passwd: all authentication tokens updated successfully.
```

BAD PASSWORD!

```
[root@Server ~]# passwd root
Changing password for user root.
New password: <Password>
BAD PASSWORD: it is based on a dictionary word
Retype new password: <Password>
passwd: all authentication tokens updated successfully.
```

BAD PASSWORD!

BAD PASSWORD: it is based on a dictionary word (e.g. P@$$w0rd)

BAD PASSWORD: it does not contain enough DIFFERENT characters

BAD PASSWORD: is too simple

BAD PASSWORD: it is too short

BAD PASSWORD: it is too simplistic/systematic (e.g. 123456)

BAD PASSWORD: it is WAY too short

BAD PASSWORD: is a palindrome

Lock / Unlock users

```
### วิธีการ Lock User ไม่ให้สามารถ Login ได้

[root@Server ~]# usermod -L username
```

```
### วิธีการปลด Lock User ให้สามารถ Login ได้

[root@Server ~]# usermod -U username
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

```
[root@Server ~]# ntpdate  time.ega.or.th
14 Mar 17:40:09 ntpdate[1225]: step time server
164.115.2.132 offset -25199.971278 sec
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

```
[root@Server ~]# ntpdate  time.ega.or.th
-bash: ntpdate: command not found

[root@Server ~]# yum -y install ntpdate
...
Installed:
  ntpdate.x86_64 0:4.2.6p5-2.el6.centos
Complete!
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

```
### ติดตั้ง ntpd
[root@Server ~]#  yum -y install ntp
...
...
Installed:
  ntp.x86_64 0:4.2.6p5-2.el6.centos

Dependency Installed:
  libedit.x86_64 0:2.11-4.20080712cvs.1.el6

Complete!
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

แก้ไขไฟล์ Configuration ของ ntpd ที่ **/etc/ntp.conf**

```
server time.ega.or.th iburst
server time.navy.mi.th iburst
server time1.nimt.or.th iburst
server time2.nimt.or.th iburst
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

```
### ทำการ Start ntpd
[root@Server ~]# /etc/init.d/ntpd start
Starting ntpd:                                             [  OK  ]
```

```
### กำหนดให้ ntpd ทำงานทุกครั้งที่ restart เครื่อง
[root@Server ~]# chkconfig ntpd on
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

ตรวจสอบการทำงานของ ntpd

```
[root@Server ~]# ntpq -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+164.115.2.132   203.185.67.115   3 u   63   64    1    2.687    1.532   2.017
+113.53.247.3    .PPS.            1 u   60   64    3    4.963    1.854   1.137
*203.185.69.60   .PPS.            1 u   33   64    3    4.008    2.189   1.216
+203.185.69.59   .PPS.            1 u   32   64    7    4.012    1.410   1.344
```

ทำการตั้งนาฬิกาของเครื่องกับ NTP server

ทำการเพิ่มไฟล์ **/etc/cron.d/ntpdate**

```
55 * * * * root /usr/sbin/ntpdate -s -u time.ega.or.th time.navy.mi.th
```

Update/Upgrade/Patch

```
[root@Server ~]# yum upgrade
Loaded plugins: fastestmirror
Setting up Upgrade Process
Loading mirror speeds from cached hostfile
...
================================================================
Install       1 Package(s)
Upgrade      37 Package(s)

Total download size: 77 M
Is this ok [y/N]: y
Downloading Packages:
```

Update/Upgrade/Patch

Updated:

busybox.x86_64 1:1.15.1-21.el6_6
curl.x86_64 0:7.19.7-40.el6_6.4
cyrus-sasl.x86_64 0:2.1.23-15.el6_6.1
cyrus-sasl-lib.x86_64 0:2.1.23-15.el6_6.1
device-mapper.x86_64 0:1.02.90-2.el6_6.1
device-mapper-libs.x86_64 0:1.02.90-2.el6_6.1
dhclient.x86_64 12:4.1.1-43.P1.el6.centos.1
dhcp-common.x86_64 12:4.1.1-43.P1.el6.centos.1
dracut.noarch 0:004-356.el6_6.1
dracut-kernel.noarch 0:004-356.el6_6.1
glibc.x86_64 0:2.12-1.149.el6_6.5
glibc-common.x86_64 0:2.12-1.149.el6_6.5
initscripts.x86_64 0:9.03.46-1.el6.centos.1
iproute.x86_64 0:2.6.32-33.el6_6
kernel-firmware.noarch 0:2.6.32-504.12.2.el6
kpartx.x86_64 0:0.4.9-80.el6_6.3
libcurl.x86_64 0:7.19.7-40.el6_6.4
libssh2.x86_64 0:1.4.2-1.el6_6.1
libxml2.x86_64 0:2.7.6-17.el6_6.1
mdadm.x86_64 0:3.3-6.el6_6.1
nss.x86_64 0:3.16.2.3-3.el6_6
nss-softokn.x86_64 0:3.14.3-22.el6_6
nss-softokn-freebl.x86_64 0:3.14.3-22.el6_6
nss-sysinit.x86_64 0:3.16.2.3-3.el6_6
nss-tools.x86_64 0:3.16.2.3-3.el6_6
nss-util.x86_64 0:3.16.2.3-2.el6_6
openssh.x86_64 0:5.3p1-104.el6_6.1
openssh-server.x86_64 0:5.3p1-104.el6_6.1
openssl.x86_64 0:1.0.1e-30.el6_6.5
policycoreutils.x86_64 0:2.0.83-19.47.el6_6.1
rpm.x86_64 0:4.8.0-38.el6_6
rpm-libs.x86_64 0:4.8.0-38.el6_6
rpm-python.x86_64 0:4.8.0-38.el6_6
rsyslog.x86_64 0:5.8.10-10.el6_6
selinux-policy.noarch 0:3.7.19-260.el6_6.2
selinux-policy-targeted.noarch 0:3.7.19-260.el6_6.2
tzdata.noarch 0:2015a-1.el6

Complete!

[root@Server ~]# **reboot**

Broadcast message from root@Server
        (/dev/pts/0) at 17:58 ...

The system is going down for reboot NOW!

ส่ง System logs ไปเก็บที่ Syslog server

```
### แก้ไขไฟล์  /etc/rsyslog.conf

*.*  @LogServer
หรือ
*.*  @IP-Address
```

```
### ทำการ restart rsyslogd
[root@Server ~]# /etc/init.d/rsyslog restart
Shutting down system logger:                [  OK  ]
Starting system logger:                     [  OK  ]
```

Secure Shell (SSH)

Ref. http://linux-audit.com/auditing-hardening-ssh-configurations/

แก้ไขไฟล์ **/etc/ssh/sshd_config**

```
Protocol 2
X11Forwarding no
IgnoreRhosts yes
PermitEmptyPasswords no
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 4
```

Secure Shell (SSH)

```
[root@Server ~]#  /etc/init.d/sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
```

Secure Shell (SSH)

แก้ไขไฟล์ **/etc/ssh/sshd_config**

ในส่วนนี้ควรกำหนดให้เหมาะสม

```
AllowUsers user1 user2 user3

AllowGroup usergroup1 usergroup2

DenyUsers user1 user2 user3

DenyGroup usergroup1 usergroup2
```

Secure Shell (SSH)

ตัวอย่าง SSH log (/var/log/secure)

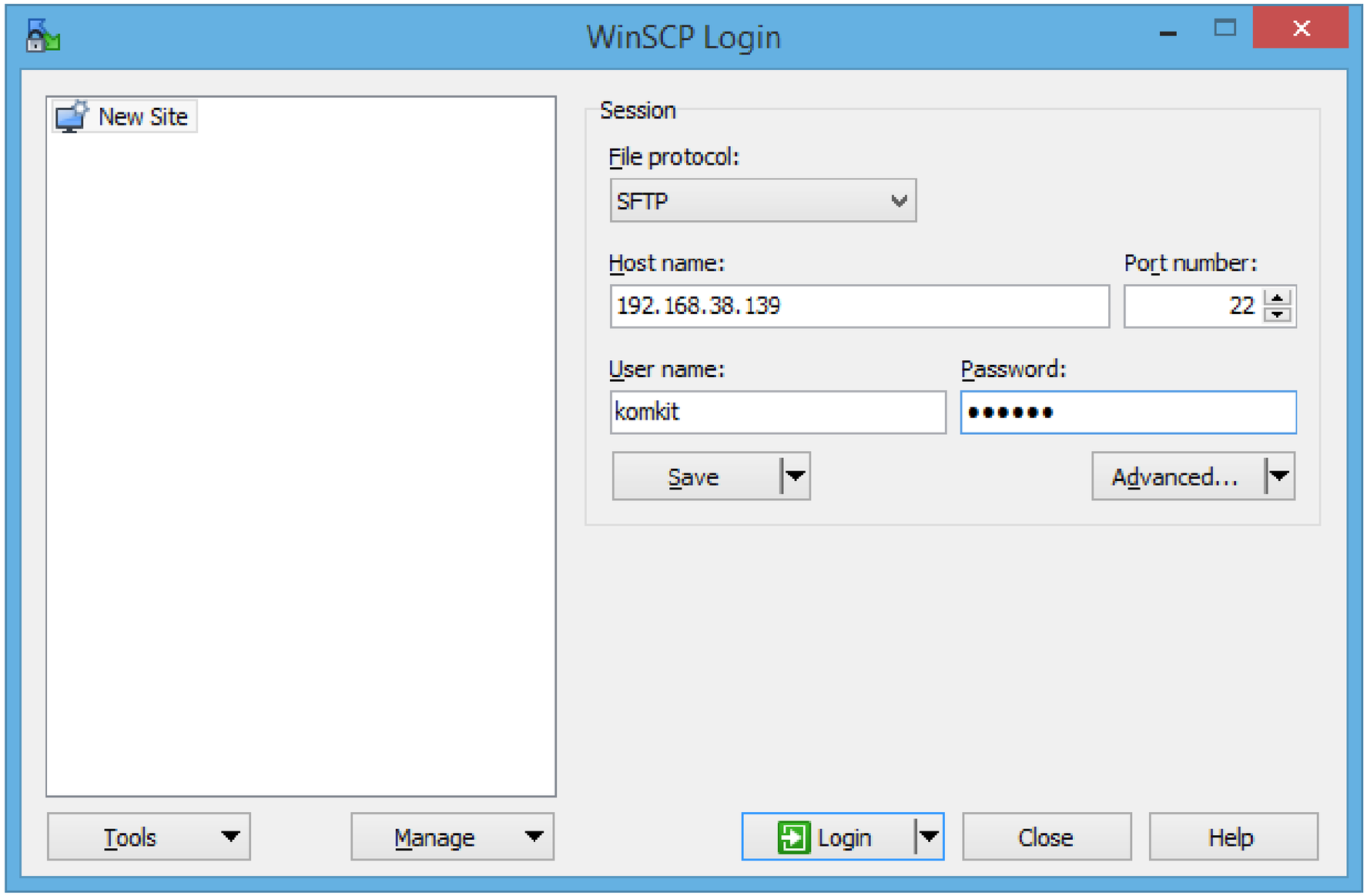
Mar 14 19:02:43 Server sshd[4698]: User cloudadmin01 from 172.17.12.5 not allowed because **not listed in AllowUsers**

Mar 14 19:08:11 Server sshd[4758]: User cloudadmin01 from 172.17.12.5 not allowed because **none of user's groups are listed in AllowGroups**

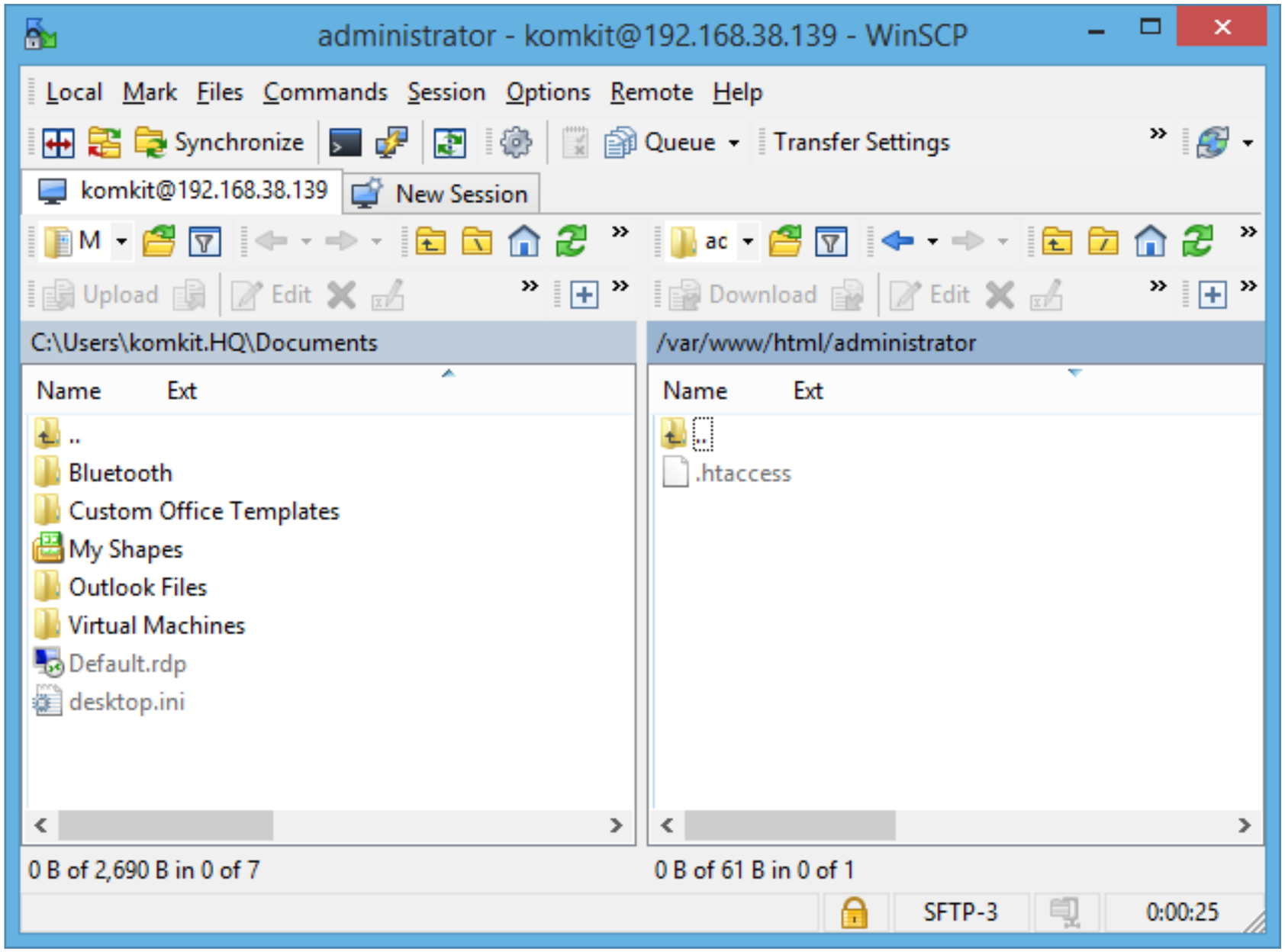
Mar 14 19:18:27 Server sshd[4972]: User cloudadmin01 from 172.17.12.5 not allowed because **listed in DenyUsers**

Mar 14 19:26:36 Server unix_chkpwd[9920]: password check failed for user (root)

การใช้งาน SSH ในการ SFTP



การใช้งาน SSH ในการ SFTP



MySQL server

แก้ไข LISTEN address หากไม่มีการติดต่อมาจากเครื่องอื่น (e.g. LAMP)

```
[root@Server ~]# netstat –ant
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
```

แก้ไขไฟล์ /etc/my.cnf

```
[mysqld]
bind-address=127.0.0.1
```

MySQL server

ทำการ restart mysqld

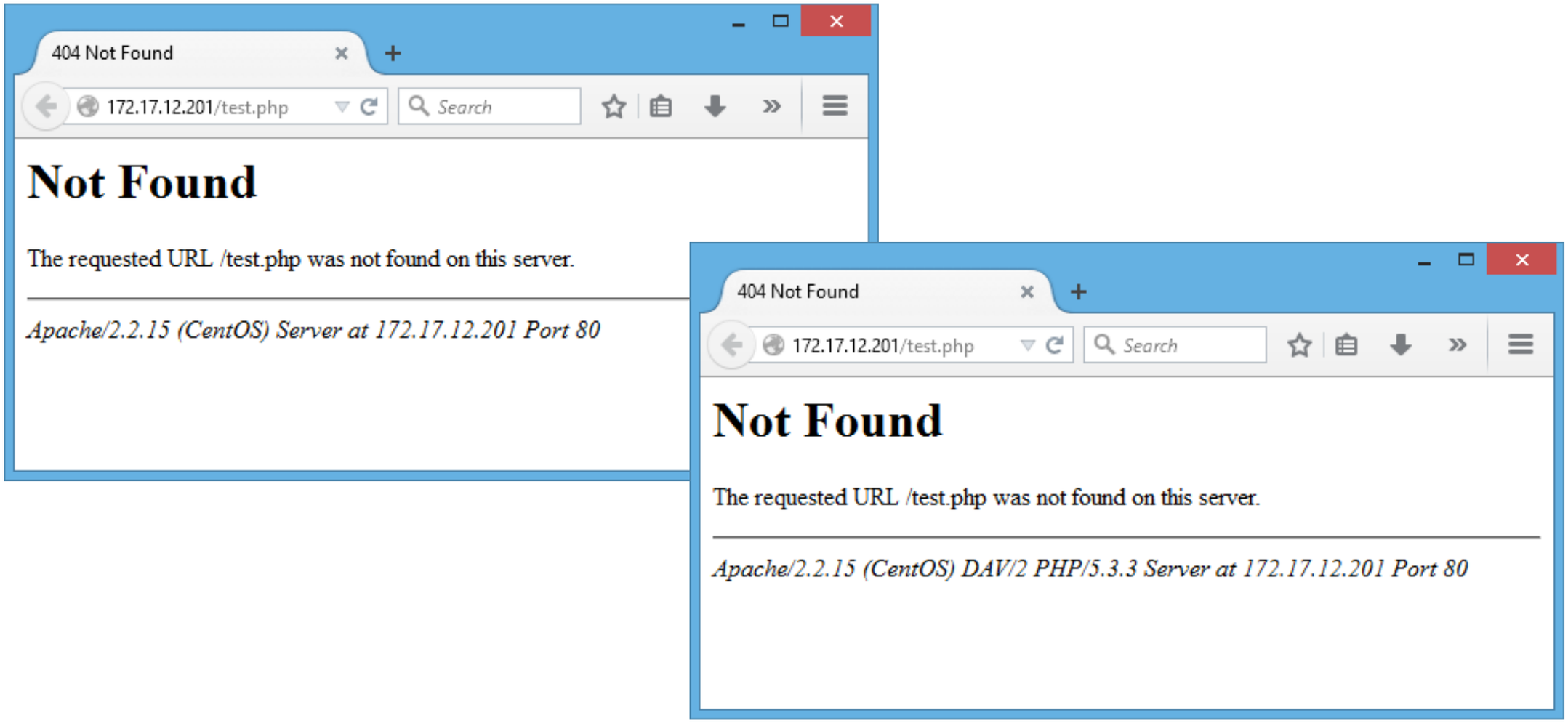
```
[root@Server ~]# /etc/init.d/mysqld restart
Stopping mysqld:                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

ตรวจสอบ MySQL LISTEN address

```
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:3306              0.0.0.0:*                   LISTEN
```

HTTPD (Apache)

ปิดการแสดง Apache version และ OS version



HTTPD (Apache)

แก้ไขไฟล์ **/etc/httpd/conf/httpd.conf**

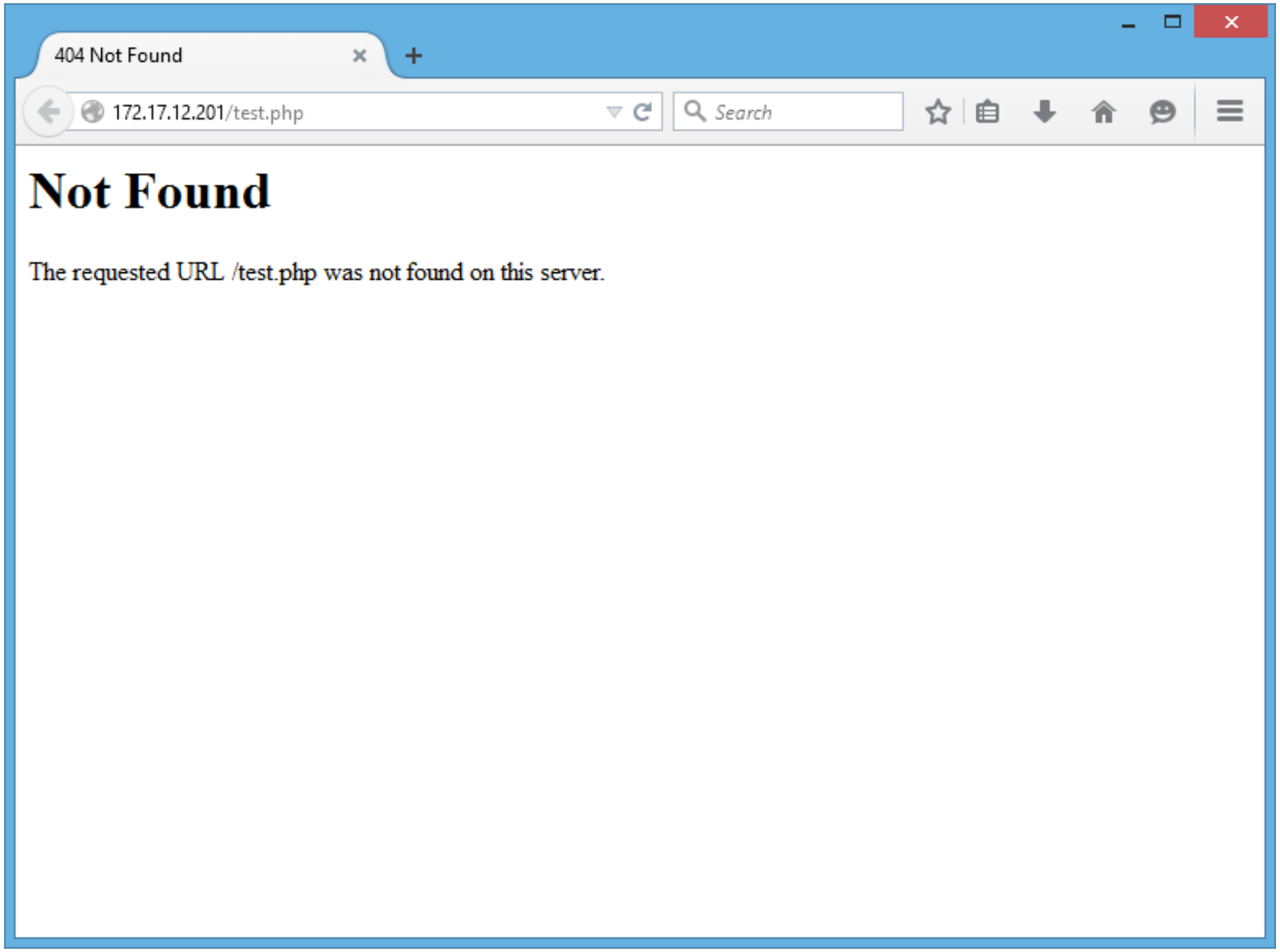
ServerTokens Prod

ServerSignature Off

ทำการ restart httpd

```
[root@Server ~]# /etc/init.d/httpd restart
Stopping httpd:                                    [  OK  ]
Starting httpd: httpd: apr_sockaddr_info_get() failed for Server
httpd: Could not reliably determine the server's fully qualified
domain name, using 127.0.0.1 for ServerName
                                                   [  OK  ]
```

HTTPD (Apache)



HTTPD (Apache)

ตัวอย่างเพิ่มเติมเกี่ยวกับ ServerTokens

ServerTokens Prod[uctOnly]

Server sends (*e.g.*): `Server: Apache`

ServerTokens Major

Server sends (*e.g.*): `Server: Apache/2`

ServerTokens Minor

Server sends (*e.g.*): `Server: Apache/2.0`

ServerTokens Min[imal]

Server sends (*e.g.*): `Server: Apache/2.0.41`

ServerTokens OS

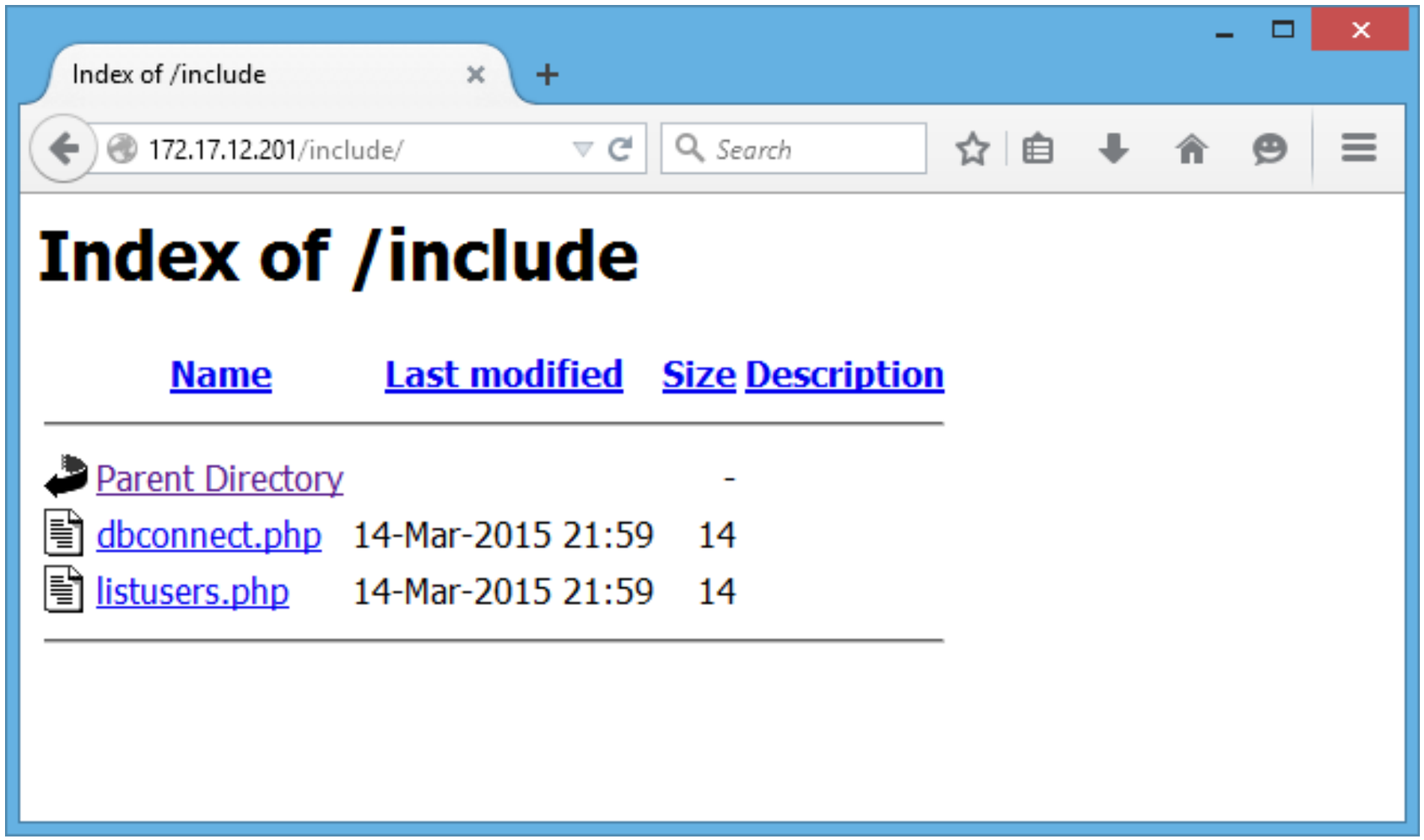
Server sends (*e.g.*): `Server: Apache/2.0.41 (Unix)`

ServerTokens Full (or not specified)

Server sends (*e.g.*): `Server: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2`

HTTPD (Apache)

ปิดการใช้งาน Directory Listing



HTTPD (Apache)

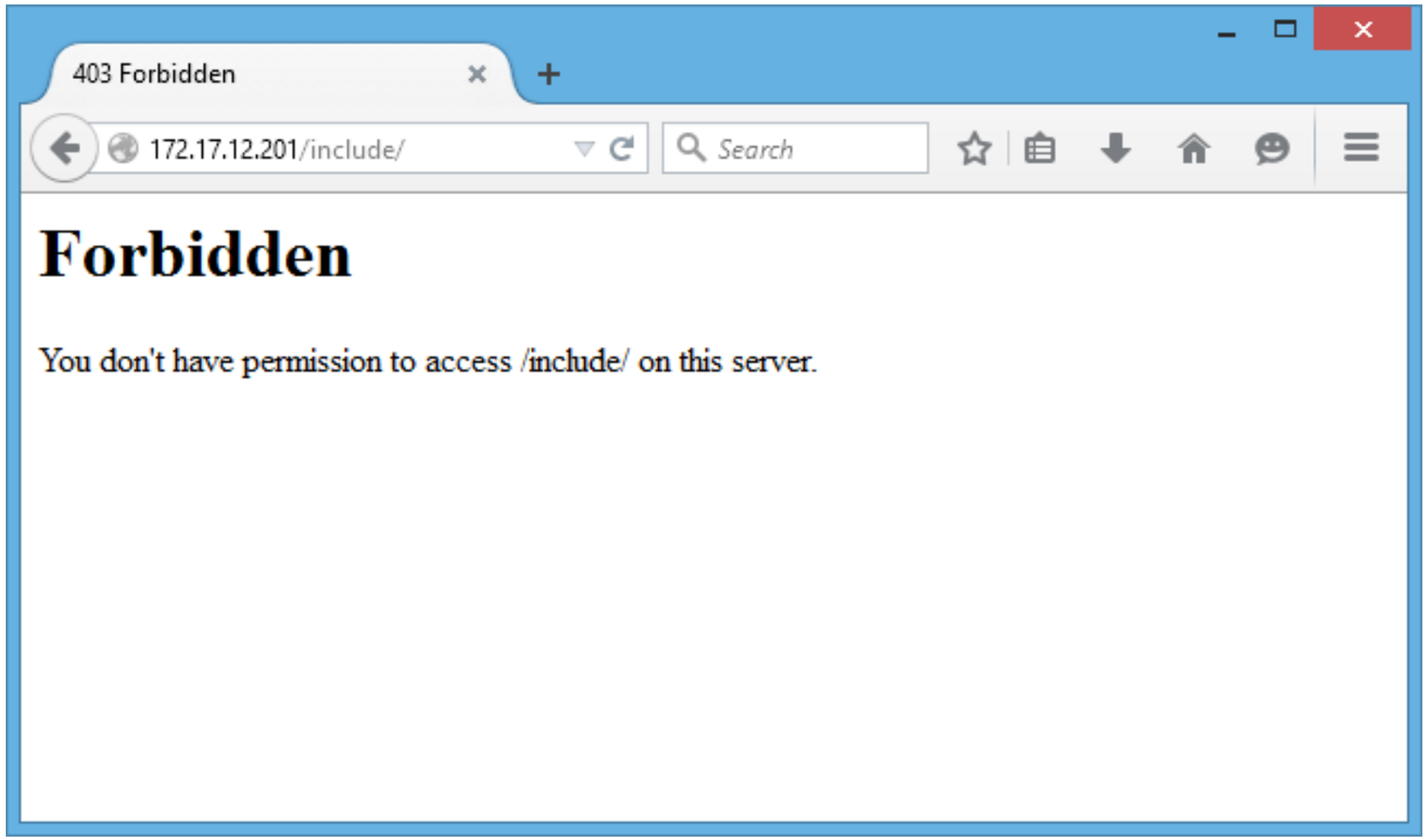
แก้ไขไฟล์ **/etc/httpd/conf/httpd.conf แล้วค้นหา**

```
<Directory "/var/www/html">
        --- ตัด Output ---
        Options Indexes FollowSymLinks
        --- ตัด Output ---
</Directory>
```

แก้ไขเป็น

```
<Directory "/var/www/html">
        --- ตัด Output ---
        Options FollowSymLinks
        --- ตัด Output ---
</Directory>
```

HTTPD (Apache)



HTTPD (Apache)

การจำกัดให้เฉพาะบาง IP เข้าถึง Directory โดย .htaccess

การเปิดการใช้งาน .htaccess

แก้ไขไฟล์ **/etc/httpd/conf/httpd.conf แล้วค้นหา**

```
<Directory "/var/www/html">
        --- ตัด Output ---
      AllowOverride None
        --- ตัด Output ---
<Directory>
```

HTTPD (Apache)

แก้ไขเป็น

```
<Directory "/var/www/html">
        --- ตัด Output ---
      AllowOverride All
        --- ตัด Output ---
<Directory>
```

จากนั้น Restart httpd service

HTTPD (Apache)

ตัวอย่างการใช้งาน .htaccess เพื่อจำกัดให้เฉพาะ IP 192.168.0.0/24 เท่านั้นที่สามารถเข้าใช้งาน http://IP-Address/administrator ได้

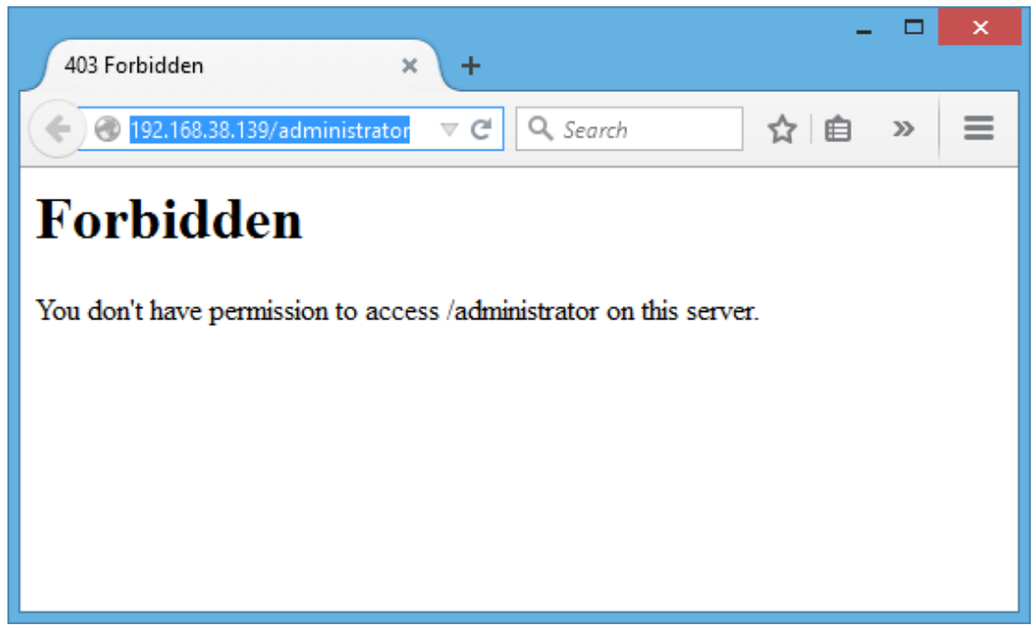
สามารถทำได้โดย สร้างไฟล์ .htaccess ภายใน Directory administrator แล้วใส่ค่า Configuration ดังนี้

```
order deny,allow
deny from all
allow from 192.168.0.0/24
```

จากนั้นทำการบันทึกไฟล์

HTTPD (Apache)

ทดสอบการใช้งานจาก IP **ที่ไม่ใช่ 192.168.0.0/24**



Log การ Deny IP ที่เข้าถึง (/var/log/httpd/error_log)

[Tue Mar 17 19:26:15 2015] [error] [client 192.168.38.1] client denied by server configuration: /var/www/html/administrator

Case study: Shellshock

Original OS installation: CentOS 6.5

GNU bash: version 4.1.2(1)-release

Services: HTTPD (Apache)

Case study: Shellshock

```
### Self test

env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

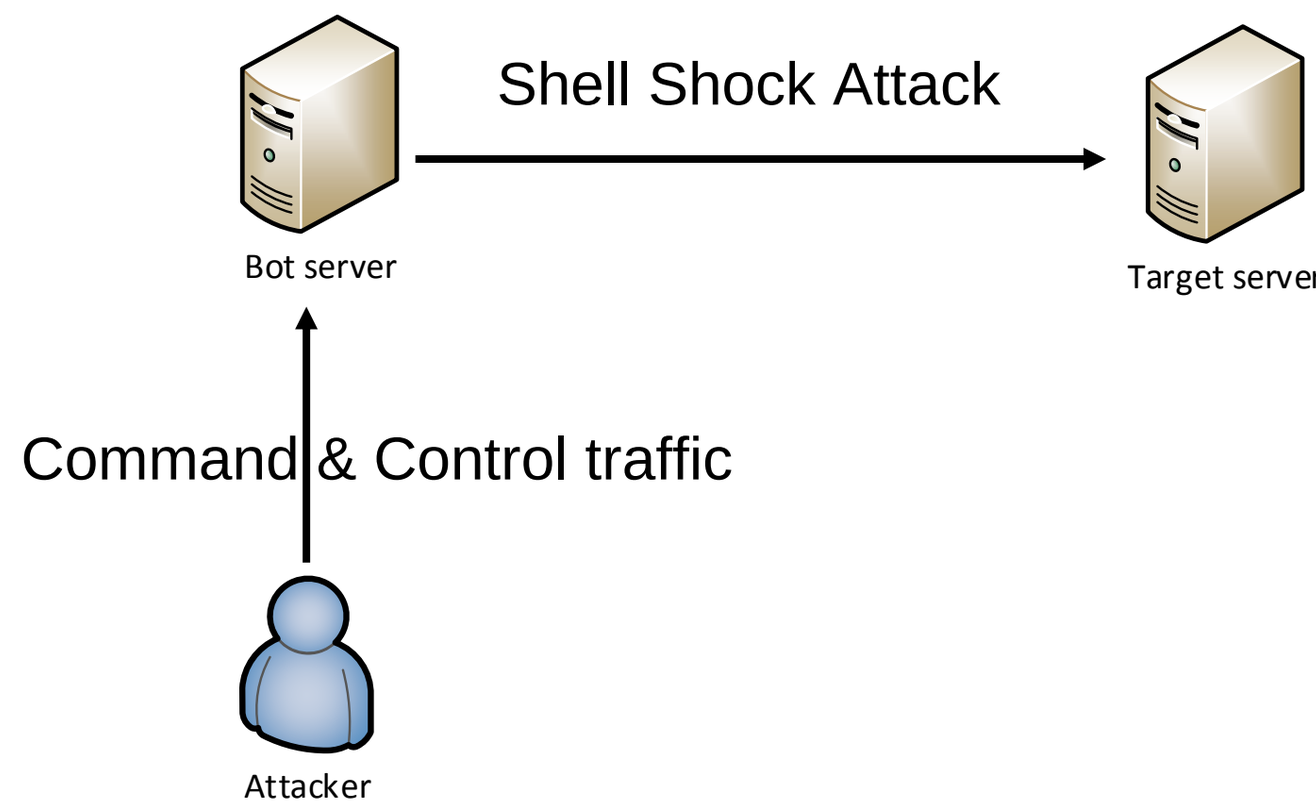
Case study: Shellshock

```
### Self test by Script

[root@Server ~]# bash shellshock_test.sh
CVE-2014-6271 (original shellshock): VULNERABLE
shellshock_test.sh: line 17:  1282 Segmentation fault
shellshocker="() { x() { _;}; x() { _;} <<a; }" bash -c date 2> /dev/null
CVE-2014-6277 (segfault): VULNERABLE
CVE-2014-6278 (Florian's patch): VULNERABLE
CVE-2014-7169 (taviso bug): VULNERABLE
shellshock_test.sh: line 50:  1299 Segmentation fault      bash -c 'true
<<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF
<<EOF <<EOF' 2> /dev/null
CVE-2014-7186 (redir_stack bug): VULNERABLE
bash: line 129: syntax error near `x129'
bash: line 129: `for x129 in ; do :'
CVE-2014-7187 (nested loops off by one): VULNERABLE
CVE-2014-//// (exploit 3 on http://shellshocker.net/): not vulnerable
```

Case study: Shellshock

Live DEMO.



Case study: Shellshock

ตัวอย่างการแก้ไข

- ทำการ Patch BASH ให้เป็น Version ปัจจุบัน
- แก้ไข Configuration ของ Apache หรือ Service อื่นๆ เพื่อป้องกันการโจมตี

Case study: Shellshock

```
### ตัวอย่างการ Configure Apache เพื่อป้องกัน Shell Shock

SetEnvIfNoCase User-Agent "() { " Blocked
<Limit GET POST HEAD>
        order allow,deny
        allow from all
        deny from env=Blocked
</Limit>
```

Case study: Shellshock

ตัวอย่าง Log จาก Apache (/var/log/httpd/error_log)

[Sun Mar 15 00:32:08 2015] [error] [client 172.17.12.201] client denied by server configuration: /var/www/html/test.cgi

Q & A