How to secure an Ubuntu 12.04 LTS server

Submitted by The Fan Club on 17 May 2012

Ref: http://www.thefanclub.co.za/how-to/how-secure-ubuntu-1204-lts-server-part-1-basics

This guide is easy step by step following:

1. วิธีการตรวจสอบเครื่องคอมพิวเตอร์ว่า CPU เป็นแบบ 32bits หรือ 64bits
2. วิธีกำหนด Name Server บน Ubuntu 12.04
3. SSH Hardening - disable root login and change port.
4. Force **sudo** to prompt for the root password instead of the password of the invoking user
5. Reset Ubuntu 12.04 password of root or user
6. **Protect su** by limiting access only to admin group
7. Secure shared memory - **fstab**
8. Harden network with **sysctl** settings
9. Prevent **IP Spoofing**
10. Install and configure **Firewall** – **ufw**
11. **Apache2** - Disable Directory Indexing
12. Harden **PHP** for security
13. Install and configure Apache application firewall – **ModSecurity**
14. Protect from DDOS (Denial of Service) attacks with **ModEvasive**
15. Scan logs and ban suspicious hosts - **DenyHosts** and **Fail2Ban**
16. Intrusion Detection - **PSAD**
17. Check for RootKits - **RKHunter** and **CHKRootKit**
18. Scan open Ports - **Nmap**
19. Analyse system LOG files - **LogWatch**
20. SELinux - **Apparmor**
21. Audit your system security - **Tiger**

1. วิธีการตรวจสอบเครื่องคอมพิวเตอร์ว่า CPU เป็นแบบ 32bits หรือ 64bits

- ตรวจสอบได้โดยใช้คำสั่ง ดังนี้

```
cat /proc/cpuinfo
```

หรือ

```
grep flags /proc/cpuinfo
```

- สังเกตจากค่า "flags" จะปรากฏข้อความ "tm (transparent mode)" or "rm (real mode)" or "lm (long mode)"
    - หากปรากฏข้อความ “rm” หมายถึง: 16 bit processor
    - หากปรากฏข้อความ “tm” หมายถึง: 32 bit processor
    - หากปรากฏข้อความ “lm” หมายถึง: 64 bit processor

แล้วรู้ได้อย่างไรระบบปฏิบัติการ Ubuntu ที่ใช้เป็น 32 bits หรือ 64 bits

- ตรวจสอบได้โดยใช้คำสั่ง ดังนี้

```
uname -a
```

- ถ้าผลลัพธ์แสดงผลมาเป็น i686 แสดงว่าเป็น ระบบปฏิบัติการ 32 bit
- ถ้าผลลัพธ์แสดงผลมาเป็น x86_64 แสดงว่าเป็น ระบบปฏิบัติการ 64 bit

2. วิธีกำหนด Name Server บน Ubuntu 12.04

เอกสารอ้างอิง: http://esaikuni.blogspot.com/2012/07/setting-dns-ubuntu-1204.html

---

มีการเปลี่ยนแปลงใน Ubuntu 12.04 ในเรื่องการตั้งค่า DNS หรือ Name Server ที่จะใช้เดิม การตั้งค่า DNS หรือ Name Server จะต้องทำที่ /etc/resolv.conf โดยหากจะระบุ Name Server เช่นต้องการชี้ Name Server เป็น 192.168.99.99 ก็เขียนไปว่า

```
nameserver 192.168.99.99
```

แต่ใน Ubuntu 12.04 มีการติดตั้ง dnsmasq ซึ่งจะทำหน้าที่ Cache Name เอาไว้ โดยผูกกับการทำงานของ NetworkManager ทำให้การ Resolve Name จะไปถาม 127.0.0.1 ซึ่งดีต่อการใช้งานพวก VPN ทำให้การทำงานเร็วขึ้น

หากเราไปแก้ไข /etc/resolve.conf อย่างเดิม จะพบว่าเมื่อ NetworkManager ทำงานก็จะไปเขียนทับข้อมูลที่เขียนไว้

วิธีแก้ไขมี 3 แนวทาง แต่ตามตัวอย่างนี้ขอยกตัวอย่างเพียงวิธีการเดียวให้เห็นดังนี้

1. หากใช้วิธี Fix IP Address ก็ให้ใส่บรรทัด dns-nameservers เข้าเพื่อระบุ Name Server ที่จะใช้ โดยแก้ไขที่ไฟล์ /etc/network/interfaces ดังตัวอย่าง

```
auto eth0
iface eth0 inet static
address 192.168.99.2
netmask 255.255.255.0
gateway 192.168.99.1
dns-nameservers 192.168.99.99   192.168.99.98
dns-search psu.ac.th
```

3. SSH Hardening - disable root login and change port.

- The easiest way to secure SSH is to disable root login and change the SSH port to something different than the standard port 22.
- Before disabling the root login create a new SSH user and make sure the user belongs to the admin group (see *step 4*. below regarding the admin group).
- If you change the SSH port also open the new port you have chosen on the firewall and close port 22.
- Open a Terminal Window and enter :

```
sudo vi /etc/ssh/sshd_config
```

- Change the following and save.

```
Port <ENTER YOUR PORT>
Protocol 2
PermitRootLogin no
```

- Restart SSH server, open a Terminal Window and enter :

```
sudo /etc/init.d/ssh restart
```

Root account access warning

ต้องติดตั้ง appl เพิ่มชื่อ mailutils

```
sudo apt-get install mailutils
```

Add the following to the top of the file /root/.bashrc and you will be informed by email when the root account is being accessed.

```
sudo vi /root/.bashrc

echo -e "Root Shell Access on `tty` \n `w`" | mail -s "Alert: Root Access"
admin@wunca25.in.psu.ac.th
#You are also required to add the captioned line at the sudoers' .bashrc file.
echo -e "Sudoer Shell Access on `tty` \n `w`" | mail -s "Alert: Sudoer Access"
admin@wunca25.in.psu.ac.th
```

4. Force sudo to prompt for the root password instead of the password of the invoking user

Only relevant if you choose to enable the root account, this will require that a user enters the root password instead of their personal password whenever using sudo.

Use the command "visudo" to edit the configuration file /etc/sudoers. Within this file look for the line that begins with "Defaults" and add ",rootpw" at the end. Once you've made your changes, press CTRL+X to exit the editor, followed by Y then ENTER to save the file (/etc/sudoers.tmp). In other words there should be a Defaults entry that appears as follows after you've made your changes:

```
sudo visudo

Defaults    env_reset,rootpw
```

RootSudoTimeout

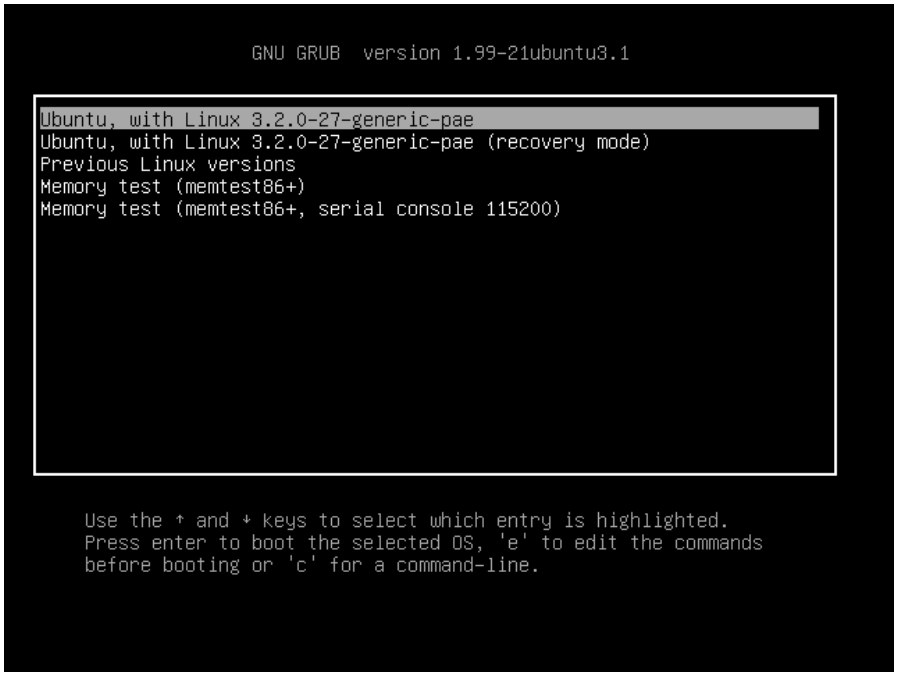
By default sudo remembers your password for 15 minutes. If you want to change that you can do so by

```
sudo visudo

Defaults    env_reset,rootpw,timestamp_timeout=1
```

where X is the timeout expiration in minutes. If you specify 0 you will always be asked the password. If you specify a negative value, the timeout will never expire. E.g. Defaults env_reset,timestamp_timeout=5

5.Reset Ubuntu 12.04 password of root or user



- เมื่อบูตหน้อจอ Ubuntu ให้กด Shift ค้างไว้ จะปรากฏเมนูให้เลือกเมนูแรก

  Ubuntu, with Linux 3.2.0-23-generic-pae

- กดตัวอักษร "e" เพื่อเข้าโหมดแก้ไข edit the commands

  เลื่อนไปหาบรรทัด

  ```
  linux /boot/vmlinuz-3.2.0-23-generic-pae root=UUID=d690681f-204e-401\f-91f5-6e81b22dcfa2 ro text
  ```

  เปลี่ยนเป็น

  ```
  linux /boot/vmlinuz-3.2.0-23-generic-pae root=UUID=d690681f-204e-401\f-91f5-6e81b22dcfa2 rw init=/bin/bash
  ```

- จากนั้นกดปุ่ม Ctrl + x
- ลองทดสอบด้วยคำสั่ง whoami
- ลองใช้คำสั่ง cat /etc/shadow |grep mama
- ใช้คำสั่ง passwd mama
- หากไม่สามารถเปลี่ยนรหัสผ่านได้ ให้ใช้คำสั่ง
  mount -rw -o remount /
- ลองใช้คำสั่ง cat /etc/shadow |grep mama
- หรือทดสอบใช้คำสั่งเปลี่ยนรหัสผ่าน root ดังนี้ passwd root

6. Protect su by limiting access only to admin group.

- * โดยปกติ Ubuntu ติดตั้งจะไม่มีการตั้งรหัสผ่านของ root ทำให้ su ไม่ได้ใช้ได้แต่ sudo
- To limit the use of **su** by admin users only we need to create an admin group, then add users and limit the use of su to the admin group.
- Add a admin group to the system and add your own admin username to the group by replacing <YOUR ADMIN USERNAME> below with your admin username.
- Open a terminal window and enter:

```
sudo groupadd admin
```

```
sudo visudo
```

- create new user account "yaya"

```
sudo useradd -d /home/yaya -m yaya -G admin
```

- กรณีมีการสร้าง user account ไว้แล้ว ให้เพิ่มเข้ากลุ่ม

```
sudo usermod -a -G admin yaya
```

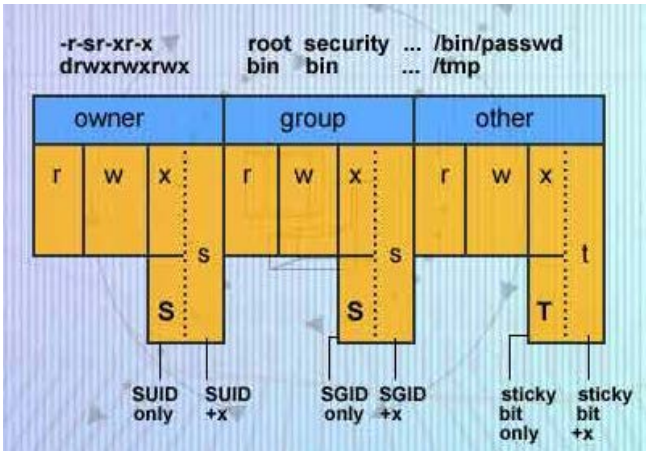
```
sudo dpkg-statoverride --update --add root admin 4750 /bin/su
```

SUID, SGID และ Sticky

ทั้ง SUID, SGID และ Sticky ต่างก็เป็นบิทพิเศษที่เอาไว้กำหนดค่าการนำงานโดยทั้ง 3 บิทนี้จะแสดงในส่วน

ของ Execute bit โดยแต่ละแบบมีการทำงานดังนี้

- SUID เมื่อมีใครก็ตามรันไฟล์นี้ โปรเซสนั้นจะถูกรันโดยใช้ชื่อของเจ้าของไฟล์
- SGID เมื่อมีใครก็ตามรันไฟล์นี้ โปรเซสนั้นจะถูกรันโดยใช้ชื่อของกลุ่มที่ระบุ
- Sticky ใครก็ตามสามารถอ่านหรือแก้ไขไฟล์นี้ได้ แต่ไฟล์นี้จะไม่สามารถถูกคนอื่นลบได้ นอกจากเจ้าของไฟล์เท่านั้น
- เมื่อมีการกำหนดค่า SUID หรือ SGID แล้ว บิทที่เป็นส่วนของ Execute bit จะแสดงสัญลักษณ์ตัว S เช่น ถ้ากำหนด SUID ให้กับไฟล์ ไฟล์นั้นจะมีสิทธิ์การใช้งานเป็น rwS------
- เมื่อมีการกำหนดค่า Sticky bit ให้กับไฟล์ บิทที่เป็นส่วนของ Execute bit จะแสดงสัญลักษณ์ตัว t



สิทธิ์การใช้งาน	ค่า
SUID	4
SGID	2
Sticky	1
Read	4
Write	2
Execute	1

7. Secure shared memory. /etc/fstab

- **/dev/shm** can be used in an attack against a running service, such as httpd. Modify **/etc/fstab** to make it more secure.
- Open a Terminal Window and enter the following :

```
sudo vi /etc/fstab
```

- Add the following line and save. You will need to reboot for this setting to take effect

```
tmpfs       /dev/shm        tmpfs    defaults,nosuid,noexec,rw    0    0

tmpfs       /tmp            tmpfs    defaults,noatime,mode=1777   0    0
```

- noatime: Linux will update the access time property of a file whenever it is read or written, something that is really only useful on servers or if you use mutt for your email. I add this option to most of my file systems for a small performance boost.
- mode=1777: Sticky bit This will give read and write permissions to everybody.
- dump: If set to 1, dump will make backups of this file system. To not make backups we set to 0.
- pass: This is the order fsck will check each filesystem. 0 is skip, 1 is reserved for /root and 2 should be used for the rest.

- **ทดสอบโดยการใช้โปรแกรม Browser เขียนข้อมูลใน disk cache ตำแหน่ง /tmp**

Speed and security sounds like something I want Chromium to benefit from as well. To move Chromium's cache to our new tmpfs open up/usr/share/applications/chromium-browser.desktop. This is the configuration filefor how Chromium appears in menus and is launched. Near the bottom will be a line starting with Exec similar to:

```
Exec=chromium-browser %U
```

Change this to:

```
Exec=chromium-browser --disk-cache-dir="/tmp" %U
```

8. Harden network with sysctl settings.

การทดสอบก่อน Harden network with sysctl

- ที่เครื่องเซิร์ฟเวอร์ Ubuntu ให้ลองใช้คำสั่งจับ packet ดังนี้

```
$ sudo tcpdump -ni eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
23:40:47.098084 IP 192.168.1.38 > 192.168.1.35: ICMP echo request, id 40710, seq 0, length 8
23:40:47.098150 IP 192.168.1.35 > 192.168.1.38: ICMP echo reply, id 40710, seq 0, length 8
23:40:48.097110 IP 192.168.1.38 > 192.168.1.35: ICMP echo request, id 40710, seq 256,
length 8
23:40:48.097166 IP 192.168.1.35 > 192.168.1.38: ICMP echo reply, id 40710, seq 256, length 8
```

- เครื่องสำหรับ Testing firewall rules ทำการติดตั้งโปรแกรม Hping ดังนี้
  Hping
  โปรแกรมจำพวก Packet Assembly โดยสามารถจะตรวจสอบแพ็กเกตประเภท ICMP, TCP และ UDP แล้วส่งไปยังเครื่องคอมพิวเตอร์เป้าหมายได้โดยไม่ต้องเขียนโปรแกรม ดังนั้นเราสามารถจะใช้โปรแกรม Hping นี้เพื่อทดสอบไฟร์วอลล์ สั่งสแกนพอร์ต และทดสอบระบบเครือข่ายในรูปแบบต่างๆ สามารถส่งได้ทั้งแพ็กเกตแบบปกติ และในแบบที่เป็น Fragment

- ติดตั้งโปรแกรม hping3 เพื่อทดสอบ

```
$ sudo apt-get install hping3
```

- เรียกใช้คำสั่ง hping3 เพื่อทำการส่ง packet testing ICMP

```
$ sudo hping3 -1 192.168.1.35
```

การทดสอบ Harden network with sysctl settings

- The **/etc/sysctl.conf** file contain all the sysctl settings.
- Prevent source routing of incoming packets and log malformed IP's enter the following in a terminal window:

```
sudo vi /etc/sysctl.conf
```

- Edit the **/etc/sysctl.conf** file and un-comment or add the following lines :

```
# IP Spoofing protection
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Disable source packet routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
```

```
# Ignore send redirects
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Log Martians
net.ipv4.conf.all.log_martians = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1
```

- To **reload sysctl** with the latest changes, enter:

```
sudo sysctl –p
```

9. Prevent IP Spoofing.

- Open a Terminal and enter the following :

```
sudo vi /etc/host.conf
```

- Add or edit the following lines :

```
order bind,hosts
nospoof on
```

10. Firewall - UFW

- A good place to start is to install a Firewall.
- Install UFW and enable, open a terminal window and enter :

```
sudo apt-get install ufw
sudo ufw enable
```

- Check the status of the firewall.

```
sudo ufw ufw status verbose
```

- Allow SSH and Http services.

```
sudo ufw allow ssh
sudo ufw allow http
```

11. Apache2 - Disable Directory Indexing

- ก่อน Disable Directory Indexing ทดสอบเครื่องก่อนโดยการสร้างไดเร็กทอรี
- Create a directory "mama" in /var/www/ directory on command

```
sudo mkdir /var/www/mama
cp /var/www/index.html /var/www/mama/first.html
```

- เรียกโปรแกรม Chromium และเปิดเว็บไซต์ทดสอบ

```
http://localhost/mama/first.html
http://localhost/mama
```

The Directory Indexing feature prints out the contents of directories (this is especially true where there is no index.html or index.php file in the directory). On a Ubuntu server, there are enabled modules in the /etc/apache/mods-enabled directory. The modules to be removed are: autoindex.load and autoindex.conf. You can remove those files with the following commands:

```
sudo rm -rf /etc/apache2/mods-enabled/autoindex.load
sudo rm -rf /etc/apache2/mods-enabled/autoindex.conf
```

For other distributions look for the "index" option in the particular directory container and remove the option. A directory container starts with <Directory> and ends with </Directory>. Within those tags you will find the line: Options index FollowSymLinks... . Just remove the "index" option, save the file, and restart Apache.

12. Harden PHP for security.

- Edit the php.ini file :

```
sudo vi /etc/php5/apache2/php.ini
```

- Add or edit the following lines :

```
disable_functions = exec,system,shell_exec,passthru
register_globals = Off
expose_php = Off
magic_quotes_gpc = On
```

13. Web Application Firewall - ModSecurity.

- Configure ModSecurity rules.

```
sudo mv /etc/modsecurity/modsecurity.conf-recommended
/etc/modsecurity/modsecurity.conf
```

```
sudo vi /etc/modsecurity/modsecurity.conf
SecRuleEngine On
SecRequestBodyLimit 16384000 ( increase the request limit to 16 MB )
SecRequestBodyInMemoryLimit 16384000 ( increase the request limit to 16 MB )
```

-We need to download and install the latest OWASP ModSecurity Core Rule Set from the project website

```
cd /tmp
sudo wget http://downloads.sourceforge.net/project/mod-security/modsecurity-
crs/0-CURRENT/modsecurity-crs_2.2.5.tar.gz
```

```
sudo tar -zxvf modsecurity-crs_2.2.5.tar.gz
sudo cp -R modsecurity-crs_2.2.5/*  /etc/modsecurity/
sudo rm modsecurity-crs_2.2.5.tar.gz
sudo rm -rf modsecurity-crs_2.2.5
sudo mv /etc/modsecurity/modsecurity_crs_10_setup.conf.example  (ต่อ)
/etc/modsecurity/modsecurity_crs_10_config.conf
```

-Now we create symbolic links to all activated base rules. Open a terminal window and enter :

```
ls -l /etc/modsecurity/base_rules
ls -l /etc/modsecurity/activated_rules
cd /etc/modsecurity/base_rules
for f in `ls * ` ; do sudo ln -s /etc/modsecurity/base_rules/$f  (ต่อ)
/etc/modsecurity/activated_rules/$f ; done
ls -l /etc/modsecurity/activated_rules
ls -l /etc/modsecurity/optional_rules
cd /etc/modsecurity/optional_rules
for f in `ls * | grep comment_spam` ; do sudo ln -s
/etc/modsecurity/optional_rules/$f /etc/modsecurity/activated_rules/$f ; done
ls -l /etc/modsecurity/activated_rules
```

-Now add these rules to Apache2. Open a terminal window and enter:

```
sudo vi /etc/apache2/mods-available/mod-security.conf
```

-Add the following to towards the end of the file with other includes and save the file :

```
Include "/etc/modsecurity/activated_rules/*.conf"
```

-Check if ModSecurity is enabled and restart Apache.

-Before restarting Apache2 check if the module has been loaded.

```
sudo a2enmod mod-security
```

-restart the Apache2 webserver

```
sudo service apache2 restart
```

14. Protect from DDOS (Denial of Service) attacks - ModEvasive

- Install ModEvasive.

Open the Terminal Window and enter :

```
sudo apt-get install libapache2-mod-evasive
```

- Create log file directory for mod_evasive.

  Open the Terminal Window and enter :

```
sudo mkdir /var/log/mod_evasive
```

  Change the log folder permissions :

```
sudo chown www-data:www-data /var/log/mod_evasive/
```

- Create mod-evasive.conf file and configure ModEvasive.

  Open the Terminal Window and enter :

```
sudo vi /etc/apache2/mods-available/mod-evasive.conf
```

and add the following, changing the email value, and other options below as required :

```
<ifmodule mod_evasive20.c>
  DOSHashTableSize 3097
  DOSPageCount  2
  DOSSiteCount  50
  DOSPageInterval 1
  DOSSiteInterval  1
  DOSBlockingPeriod  10
  DOSLogDir   /var/log/mod_evasive
  DOSEmailNotify  EMAIL@DOMAIN.com
  DOSWhitelist   127.0.0.1
</ifmodule>
```

7. Check if ModEvasive is enabled and restart Apache.

Before restarting Apache2 check if the module has been loaded.

Open the Terminal Window and enter :

```
sudo a2enmod mod-evasive
```

Then restart the Apache2 webserver :

```
sudo /etc/init.d/apache2 restart
        OR
service apache2 restart
```

15. Scan logs and ban suspicious hosts - DenyHosts and Fail2Ban.

- DenyHosts is a python program that automatically **blocks SSH attacks** by adding entries to /etc/hosts.deny. DenyHosts will also inform Linux administrators about offending hosts, attacked users and suspicious logins.
- Open a Terminal and enter the following :

```
sudo apt-get install denyhosts
```

- After installation edit the configuration file **/etc/denyhosts.conf** and change the email, and other settings as required.
- To edit the admin email settings open a terminal window and enter:

```
sudo vi /etc/denyhosts.conf
```

- Change the following values as required on your server :

```
ADMIN_EMAIL = root@localhost
SMTP_HOST = localhost
SMTP_PORT = 25
#SMTP_USERNAME=foo
#SMTP_PASSWORD=bar
SMTP_FROM = DenyHosts nobody@localhost
#SYSLOGREPORT=YES
```

- Fail2ban is more advanced than DenyHosts as it extends the log monitoring to other services including **SSH, Apache, Courier, FTP, and more**.
- **Fail2ban scans log files and bans IPs that show the malicious signs** -- too many password failures, seeking for exploits, etc.
- Generally Fail2Ban then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action could also be configured.
- Out of the box Fail2Ban comes with filters for various services (apache, courier, ftp, ssh, etc).
- Open a Terminal and enter the following :

```
sudo apt-get install fail2ban
```

- After installation edit the configuration file **/etc/fail2ban/jail.local** and create the filter rules as required.
- To edit the settings open a terminal window and enter:

```
sudo vi /etc/fail2ban/jail.conf
        [ssh]
        enabled  = true
        port     = ssh
        filter   = sshd
        logpath  = /var/log/auth.log
        maxretry = 3
```

- If you would like to receive **emails from Fail2Ban** if hosts are banned change the following line to your email address.

```
destemail = root@localhost
```

- and change the following line **to** :

```
action = %(action_mwl)s
```

- You can also **create rule filters** for the various services that you would like fail2ban to monitor that is not supplied by default.

```
sudo vi /etc/fail2ban/jail.local
```

- Good instructions on how to configure fail2ban and create the various filters can be found on HowtoForge
- When done with the configuration of Fail2Ban restart the service with :

```
sudo /etc/init.d/fail2ban restart
```

- You can also check the status with.

```
sudo fail2ban-client status
```

16. Intrusion Detection - PSAD.

- Cipherdyne PSAD is a collection of three lightweight system daemons that run on Linux machines and analyze iptables log messages to detect port scans and other suspicious traffic.
- Currently version 2.1 causes errors during install on Ubuntu 12.04, but apparently does work. Version 2.2 resolves these issues but is not yet available on the Ubuntu software repositories. It is recommended to manually compile and install version 2.2 from the source files available on the Ciperdyne website.
- To install the latest version from the source files follow these instruction : How to install PSAD Intrusion Detection on Ubuntu 12.04 LTS server
- OR install the older version from the Ubuntu software repositories, open a Terminal and enter the following :

```
sudo apt-get install psad
```

Edit the PSAD configuration file.

```
vi /etc/psad/psad.conf
```

EMAIL_ADDRESSES - change this to your email address.
HOSTNAME - this is set during install - but double check and change to a FQDN if needed.
ENABLE_AUTO_IDS - set this to Y if you could like PSAD to take action - read configuration instructions before setting this to Y.
ENABLE_AUTO_IDS_EMAILS - set this to Y if you would like to receive email notifications of intrusions that are detected.

- Add iptables LOG rules for both IPv4 and IPv6.
  For an explanation of this step click here. Add the following iptables policies :

```
iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG
ip6tables -A INPUT -j LOG
ip6tables -A FORWARD -j LOG
```

Reload and update PSAD.

- To restart, update the signature file and reload PSAD to complete the install open a Terminal Window and enter :

```
psad -R
psad --sig-update
psad -H
psad --Status
```

- To check the status of PSAD, open a Terminal Window and enter :

```
psad --Status
```

17. Check for rootkits - RKHunter and CHKRootKit.

- Both RKHunter and CHKRootkit basically do the same thing - check your system for rootkits. No harm in using both.
- Open a Terminal and enter the following :

```
sudo apt-get install rkhunter chkrootkit
```

- To run chkrootkit open a terminal window and enter :

```
sudo chkrootkit
```

- To update and run RKHunter. Open a Terminal and enter the following :

```
sudo rkhunter --update
sudo rkhunter --propupd
sudo rkhunter --check
```

18. Scan open ports - Nmap.

- Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.
- Open a Terminal and enter the following :

```
sudo apt-get install nmap
```

- Scan your system for open ports with :

```
nmap -v -sT localhost
```

- SYN scanning with the following :

```
sudo nmap -v -sS localhost
```

19. Analyse system LOG files - LogWatch.

- Logwatch is a customizable log analysis system. Logwatch parses through your system's logs and creates a report analyzing areas that you specify. Logwatch is easy to use and will work right out of the package on most systems.
- Open a Terminal and enter the following :

```
sudo apt-get install logwatch libdate-manip-perl
```

- To view **logwatch output** use less :

```
sudo logwatch | less
```

- To **email a logwatch report for the past 7 days** to an email address, enter the following and **replace** yourmail@domain.com with the required email. :

```
sudo logwatch --mailto mail@domain.com --output mail --format html --range 'between -7 days and today'
```

20. SELinux - Apparmor.

- National Security Agency (NSA) has taken Linux to the next level with the introduction of Security-Enhanced Linux (SELinux). SELinux takes the existing GNU/Linux operating system and extends it with kernel and user-space modifications to make it bullet-proof.
- More information can be found here. Ubuntu Server Guide - Apparmor
- It is installed by default since Ubuntu 7.04.
- Open a Terminal and enter the following :

```
sudo apt-get install apparmor apparmor-profiles
```

- Check to see if things are running :

```
sudo apparmor_status
```

21. Audit your system security - Tiger.

- Tiger is a security tool that can be use both as a security audit and intrusion detection system.
- Open a Terminal and enter the following :

```
sudo apt-get install tiger
```

- To run tiger enter :

```
sudo tiger
```

- All Tiger output can be found in the **/var/log/tiger**
- To view the tiger security reports, open a Terminal and enter the following :

```
sudo less /var/log/tiger/security.report.*
```