7

Security Tools

# Linux sXID

## How to do it?

1. apt-get install sxid
2. nano /etc/sxid.conf
3. sxid -c /etc/sxid.conf -k

# Port Sentry

## Getting Ready

apt-get install nmap

## How to do it?

1. apt-get install portsentry
2. grep portsentry /var/log/syslog
3. nmap -sT -v 192.168.1.102
4. nano /etc/portsentry/portsentry.conf
5. nano /etc/default/portsentry
6. nano /etc/portsentry/portsentry.ignore.static
7. /etc/init.d/portsentry restart
8. nmap -sT -v 192.168.1.102
9. ping 192.168.1.102
10. cat /etc/hosts.deny
11. less /var/lib/portsentry/portsentry.history

# Using Squid Proxy

## Getting Ready

apt-get update

apt-get upgrade

## How to do it?

1. apt-get install squid
2. Edit the file /etc/squid3/squid.conf
3. nano /etc/squid3/squid.conf
4. Add line – visible\_hostname ourProxyServer.
5. Next add a line –cache\_mgr email@yourdomainname.
6. Then add – http\_port 3128 888
7. Add rule – acl localnetwork src 192.168.1.0/24
8. Next add the line - “http\_access allow localnetwork”
9. service squid3 restart

# Open SSL Server

## How to do it?

1. apt-get install openssl
2. apt-get install apache2
3. a2enmod ssl
4. service apache2 restart
5. mkdir /etc/apache2/ssl
6. openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.crt
7. Edit file /etc/apache2/sites-available/default
8. Edit the lines –

<VirtualHost \*:443>

ServerAdmin webmaster@localhost

ServerName 192.168.1.103:443

1. Scroll to the end and before the <VirtualHost> block closes, add the lines-

SSLEngine on

SSLCertificateFile /etc/apache2/ssl/server.crt

SSLCertificateKeyFile /etc/apache2/ssl/server.key

</VirtualHost>

# Trip Wire

## How to do it?

1. apt-get install tripwire
2. tripwire --init
3. nano /etc/tripwire/tw.pol
4. touch tripwire\_testing
5. tripwire --check --interactive
6. nano /etc/crontab

00 6 \* \* \* /usr/sbin/tripwire --check

# Shorewall

## How to do it?

1. apt-get install shorewall
2. /etc/init.d/shorewall start
3. nano /etc/default/shorewall

“startup=1”

1. nano /etc/shorewall/shorewall.conf

“IP\_FORWARDING=On”

1. nano /etc/shorewall/interfaces
2. Add the lines

net eth0 detect tcpflags,nosmurfs

local eth1 detect

1. nano /etc/shorewall/zones
2. Add lines

fw firewall

net ipv4

local ipv4

1. nano /etc/shorewall/policy
2. Add lines

local net ACCEPT info

local fw ACCEPT info

fw net ACCEPT info

fw local ACCEPT info

net all DROP info

all all REJECT info

1. nano /etc/shorewall/rules

ACCEPT net fw tcp 80

1. shorewall check
2. service shorewall restart