sponsored by

Telkom

COMVERSE

STORTECH For Your Information

tellabs

easttel

Bright Ideas Projects 39

THRIP TECHNOLOGY AND HUMAN RESOURCES FOR INDUSTRY PROGRAMME

RHODES UNIVERSITY
Where leaders learn

CONVERGENCE RESEARCH GROUP

A less attack-prone, Internet deployment of iLanga

Researcher: Courage Radu

Email: g11r3764@campus.ru.ac.za

Supervisor : M. Tsietsi

Co-Supervisor : A. Terzoli

Outline

1) Introduction
2) System Architecture
3) Threats
4) Preliminary Phases
5) Asterisk Security
6) AsteriskNOW
7) Way Forward
8) Questions

Introduction

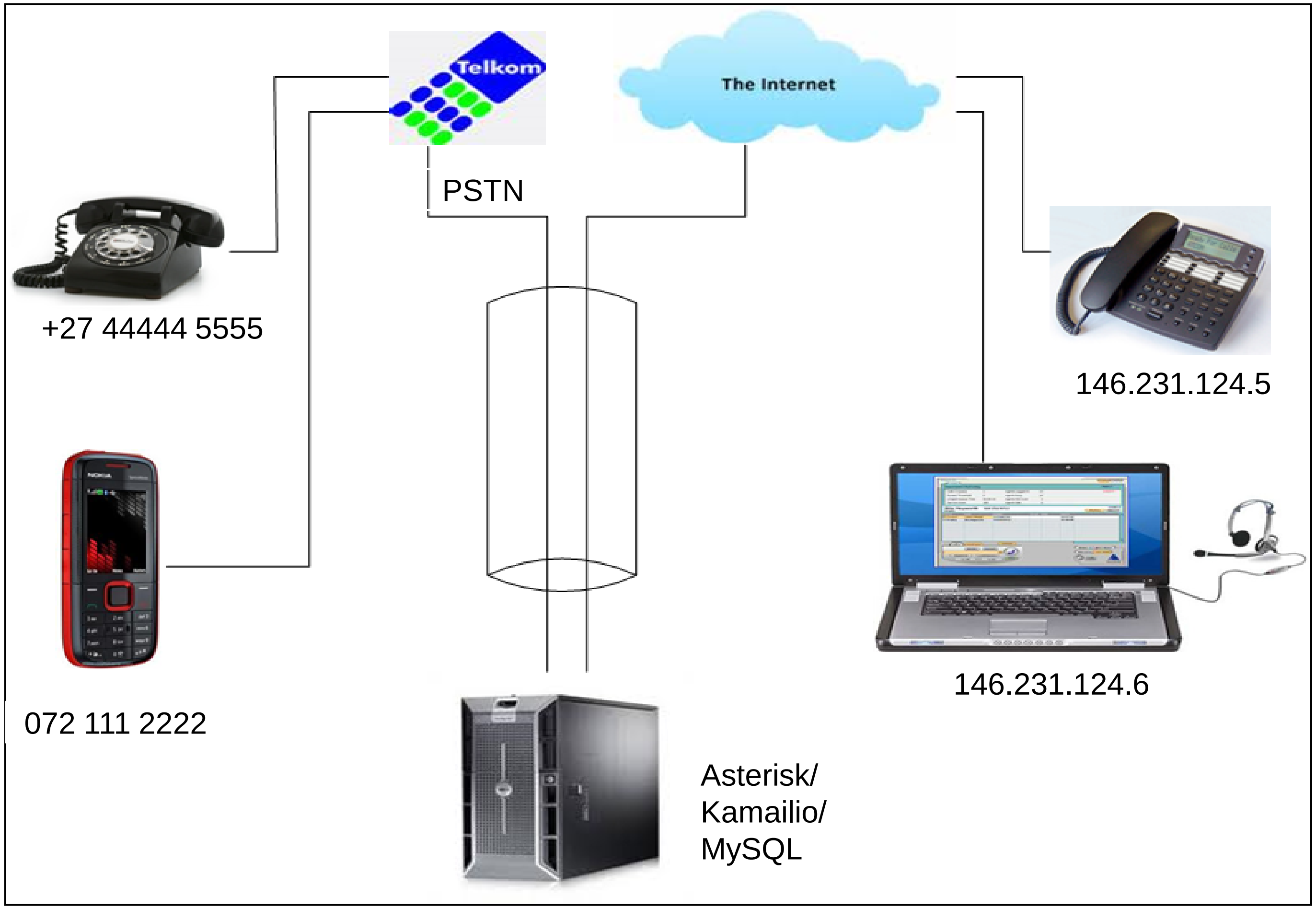
- Objective of project is to have a securely deployed telecommunication system using iLanga as case study.
- A guide with best security practices
- Develop a web based tool that easy up security administration
- Iterative approach

System Components

iLanga is an open computer based telecommunication system

- Ubuntu Linux – Operating System
- Asterisk – software implementation of a PBX
- Kamailio – proxy server for authentication
- MySQL – database to store user information

High Level System Architecture



PSTN

+27 44444 5555

146.231.124.5

072 111 2222

146.231.124.6

Asterisk/
Kamailio/
MySQL

Threats

Brute force attack – password guessing

Session Initiation Protocol (SIP) brute force

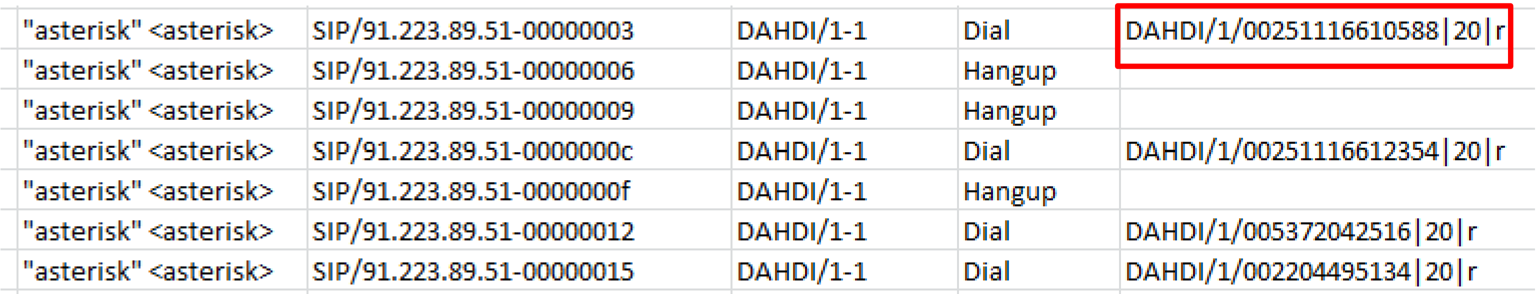
```
[Nov  6 02:57:48] NOTICE[18681]: chan_sip.c:21687 handle_request_register:
Registration from '"9964"<sip:9964@146.231.121.132> failed for
'85.14.178.21' - No matching peer found
[Nov  6 02:57:48] NOTICE[18681]: chan_sip.c:21687 handle_request_register:
Registration from '"9965"<sip:9965@146.231.121.132> failed for
'85.14.178.21' - No matching peer found
```

Root brute force

```
June 16 12:16
Failed password for root from 95.141.193.46 about 40 attempts
Failed password for invalid user test from 95.141.193.46 3 attempts
Failed password for invalid user nagios 2 attempts
Failed password for invalid user postgres  2 attempts
Failed password for invalid user oracle 1 attempt
```

Threats

Toll fraud – unauthorised long distance calls



"asterisk" <asterisk>	SIP/91.223.89.51-00000003	DAHDI/1-1	Dial	DAHDI/1/00251116610588|20|r
"asterisk" <asterisk>	SIP/91.223.89.51-00000006	DAHDI/1-1	Hangup	
"asterisk" <asterisk>	SIP/91.223.89.51-00000009	DAHDI/1-1	Hangup	
"asterisk" <asterisk>	SIP/91.223.89.51-0000000c	DAHDI/1-1	Dial	DAHDI/1/00251116612354|20|r
"asterisk" <asterisk>	SIP/91.223.89.51-0000000f	DAHDI/1-1	Hangup	
"asterisk" <asterisk>	SIP/91.223.89.51-00000012	DAHDI/1-1	Dial	DAHDI/1/005372042516|20|r
"asterisk" <asterisk>	SIP/91.223.89.51-00000015	DAHDI/1-1	Dial	DAHDI/1/002204495134|20|r

DoS – service disruption

Preliminary Phases

- Current state-of-art of the system

-Documenting versions for each component

- Replicated the system

- Learning the system

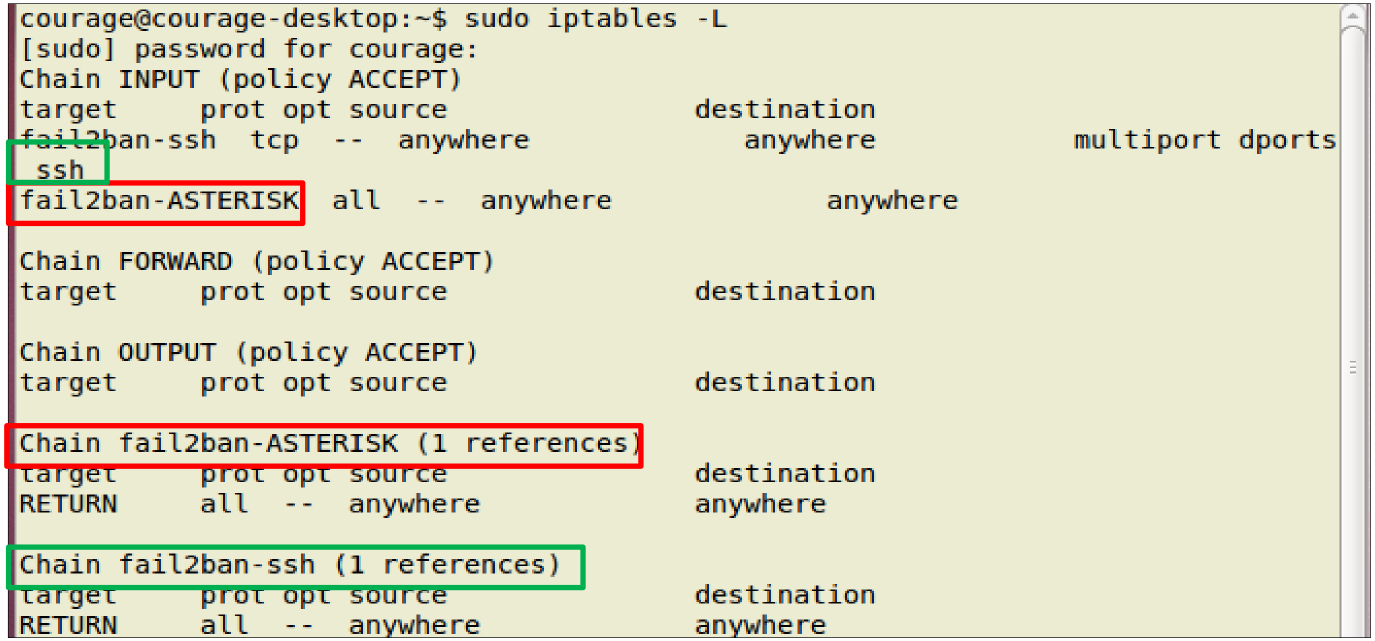
- How asterisk handles phone calls

- How the components are integrated

Asterisk Security

- Fail2ban

  - ban IP address with more than 5 wrong passwords



```
courage@courage-desktop:~$ sudo iptables -L
[sudo] password for courage:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere            multiport dports
 ssh
fail2ban-ASTERISK  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-ASTERISK (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere

Chain fail2ban-ssh (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

Asterisk Security (Cont.)

- Using Secure Shell (SSH) – terminal connection security

  - Disable password authentication

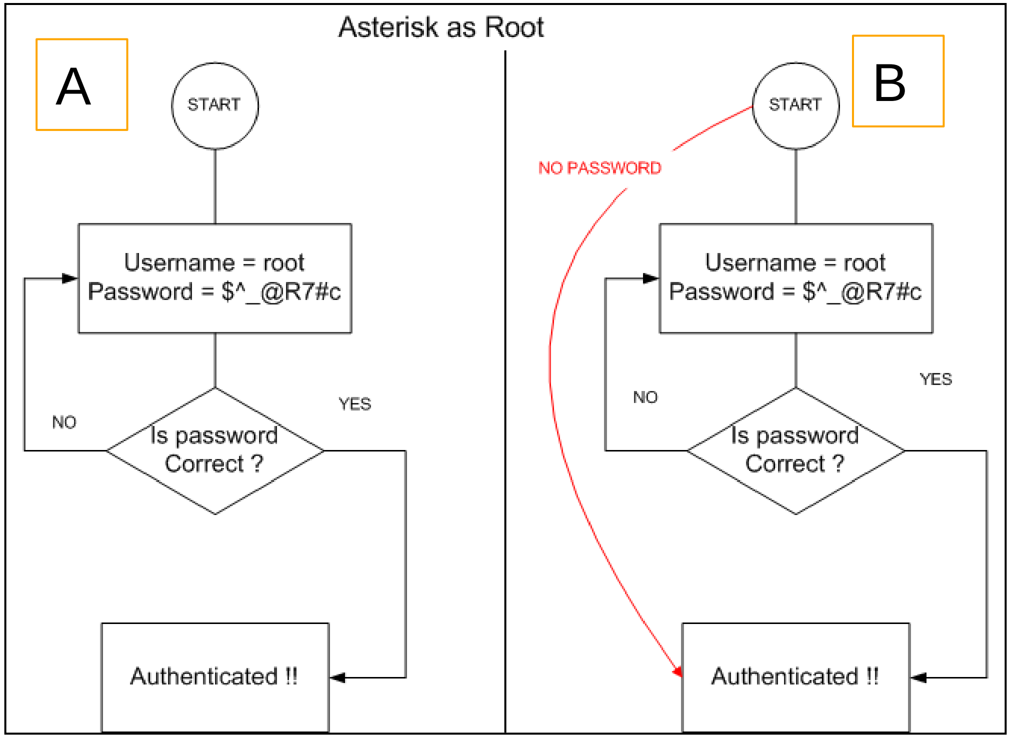
  - SSH - uses public and private keys for authentication.

  - SSH - uses RSA algorithm whose security lies in the factorisation problem.

- A well designed dialplan will prevent toll fraud

- Kamailio has inbuilt anti-flood functionality

Asterisk Security (Cont.)



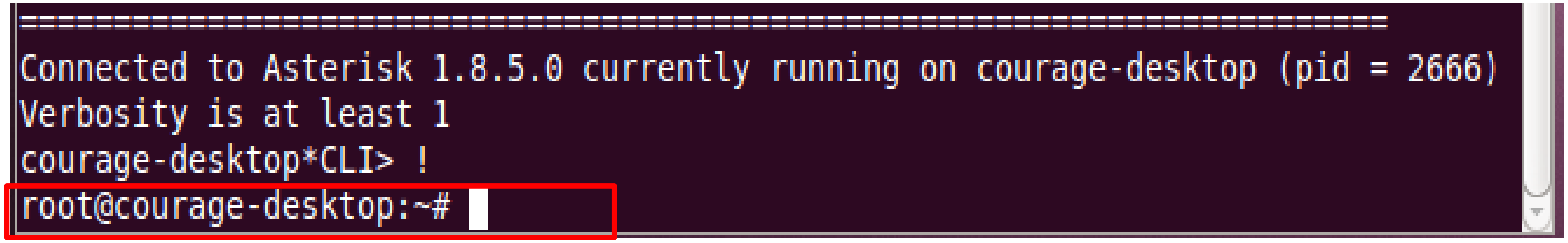
Good practice

- Running Asterisk as User

Asterisk Security (Cont.)

- Unusual for Ubuntu

- (Shift + ! + Enter)

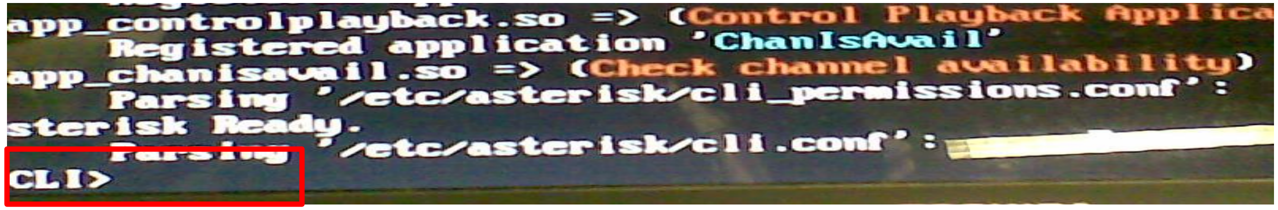


```
=========================================================================
Connected to Asterisk 1.8.5.0 currently running on courage-desktop (pid = 2666)
Verbosity is at least 1
courage-desktop*CLI> !
root@courage-desktop:~#
```

Asterisk Security (Cont.)

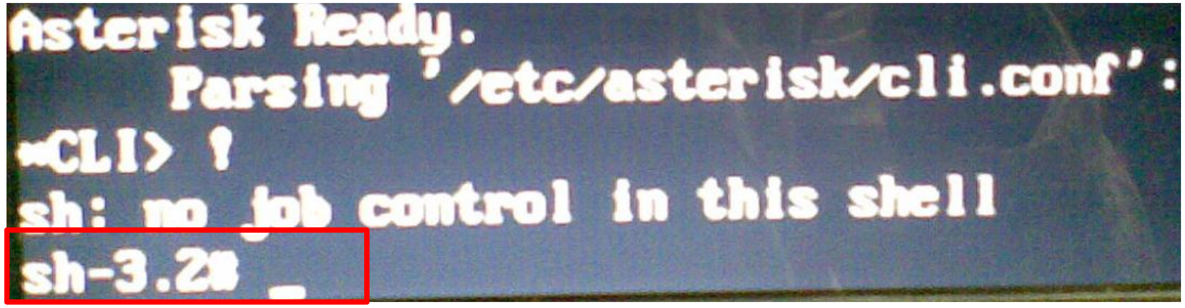
- Unusual for CentOS

- (Alt + F9)



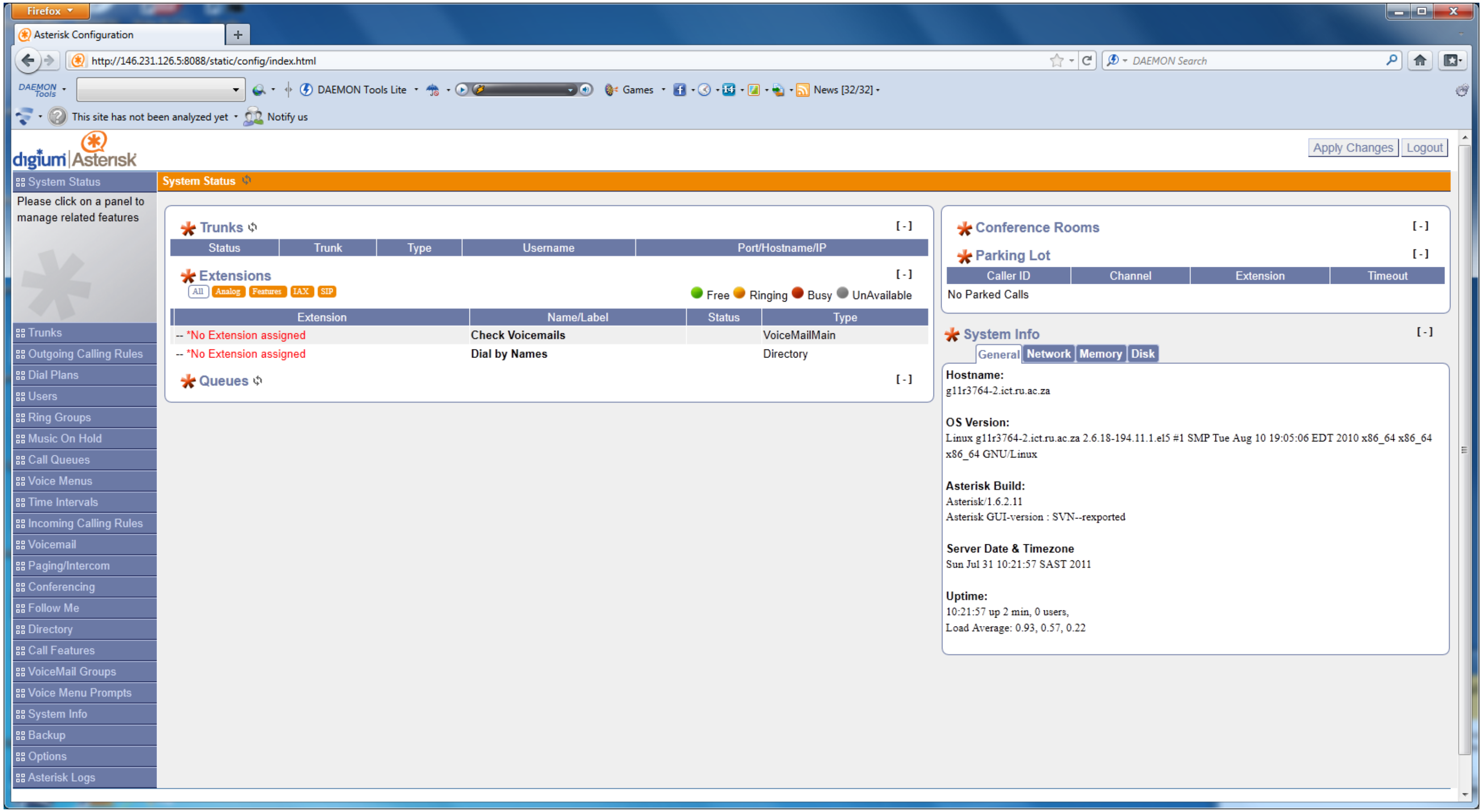
```
app_controlplayback.so => (Control Playback Applica
    Registered application 'ChanIsAvail'
app_chanisavail.so => (Check channel availability)
    Parsing '/etc/asterisk/cli_permissions.conf':
sterisk Ready.
    Parsing '/etc/asterisk/cli.conf':
CLI>
```

- (Shift + ! + Enter)



```
Asterisk Ready.
    Parsing '/etc/asterisk/cli.conf':
*CLI> !
sh: no job control in this shell
sh-3.2# _
```

Administrator Interface for AsteriskNOW



Please click on a panel to manage related features

System Status

Trunks

Status	Trunk	Type	Username	Port/Hostname/IP

Extensions

● Free ● Ringing ● Busy ● UnAvailable

Extension	Name/Label	Status	Type
-- *No Extension assigned	**Check Voicemails**		VoiceMailMain
-- *No Extension assigned	**Dial by Names**		Directory

Queues

Conference Rooms

Parking Lot

Caller ID	Channel	Extension	Timeout

No Parked Calls

System Info

Hostname:
g11r3764-2.ict.ru.ac.za

OS Version:
Linux g11r3764-2.ict.ru.ac.za 2.6.18-194.11.1.el5 #1 SMP Tue Aug 10 19:05:06 EDT 2010 x86_64 x86_64 x86_64 GNU/Linux

Asterisk Build:
Asterisk/1.6.2.11
Asterisk GUI-version : SVN--rexported

Server Date & Timezone
Sun Jul 31 10:21:57 SAST 2011

Uptime:
10:21:57 up 2 min, 0 users,
Load Average: 0.93, 0.57, 0.22

Way Forward…

- Creating a simple web based tool that monitors the system internal security files and give feedback to the administrator.

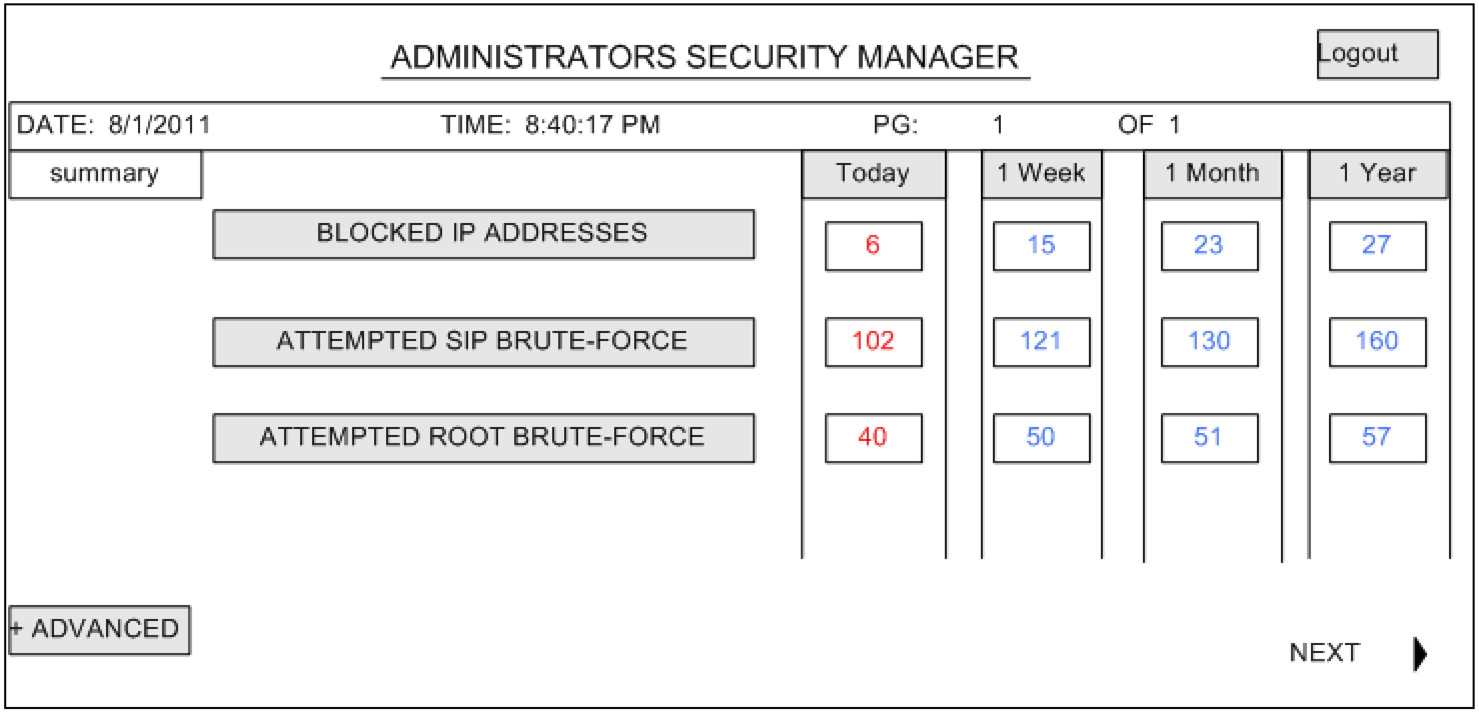
- Combines information from /var/log/auth.log.1log file e.g

```
From the /var/log/auth.log.1log file
June 12 13:17
Failed password for root from 109.237.214. 6 attempts

June 12 22:59
Failed password for root from 122.225.96.156 6 attempts

June 16 12:16
Failed password for root from 95.141.193.46 about 40 attempts
```

Way Forward… (Cont.)



ADMINISTRATORS SECURITY MANAGER

DATE: 8/1/2011   TIME: 8:40:17 PM   PG: 1   OF 1

summary	Today	1 Week	1 Month	1 Year
BLOCKED IP ADDRESSES	6	15	23	27
ATTEMPTED SIP BRUTE-FORCE	102	121	130	160
ATTEMPTED ROOT BRUTE-FORCE	40	50	51	57

Questions and Answers