



Performance and Technology

# Audit Logging & Security Monitoring

11<sup>th</sup> June 2010

Advisory

# Overview

- **Auditing Policy and Strategy**
- **Building Alerting Rules**
- **User Monitoring Regulations**
- **The Future**
- **Summary**
- **Questions**

**Me**

## **Mark Johnson CISSP, MSc**

- **IBM**
- **MBNA/Bank of America**
- **KPMG**

# Auditing Policy and Strategy

## Top down...

- **Policy**
  - **What is the objective for the business?**
- **Standards**
  - **How does this translate to systems?**
- **Baselines**
  - **How do I configure it?**

# Timekeeping

## Policy

- **Audit logging must be configured such that event timings are accurate and consistent**

## Standard

- **All systems must synchronise time with a corporate ntp server**
- **System clock changes must not be achieved through time 'drifting'\***
- **All systems must be configured to use Universal Time**

## Baseline

- **The /etc/ntp.conf file must contain the entry "server 10.160.1.12"**
- **The /etc/default/rcS file must contain the entry "UTC=yes"**

# Retention

## Policy

- All audit logs must be kept for a minimum of 6 months

## Standard

- All systems must send log files to a centralised syslog server
- Centralised logs must be configured with a retention period of at least 6 months.

## Baseline

- The /etc/syslog.conf file must contain the entry `"*.alert @10.160.1.13"`
- The 'Minimum Retention' field in the 'Options' dialogue box must be set to '6 Months'

# Protection

## Policy

- **All audit logs must be protected from unauthorised modifications**

## Standard

- **All audit logs must be configured with no write permissions for non-administrative users**
- **Administrative access to the syslog server must be controlled through keystroke monitoring**
- **No individual may have administrative access to both the syslog server and the keystroke log manager**

## Baseline

- **The /var/log/syslog file must have permissions 644**

# Building Alerting Rules

# Audit logging in a nutshell

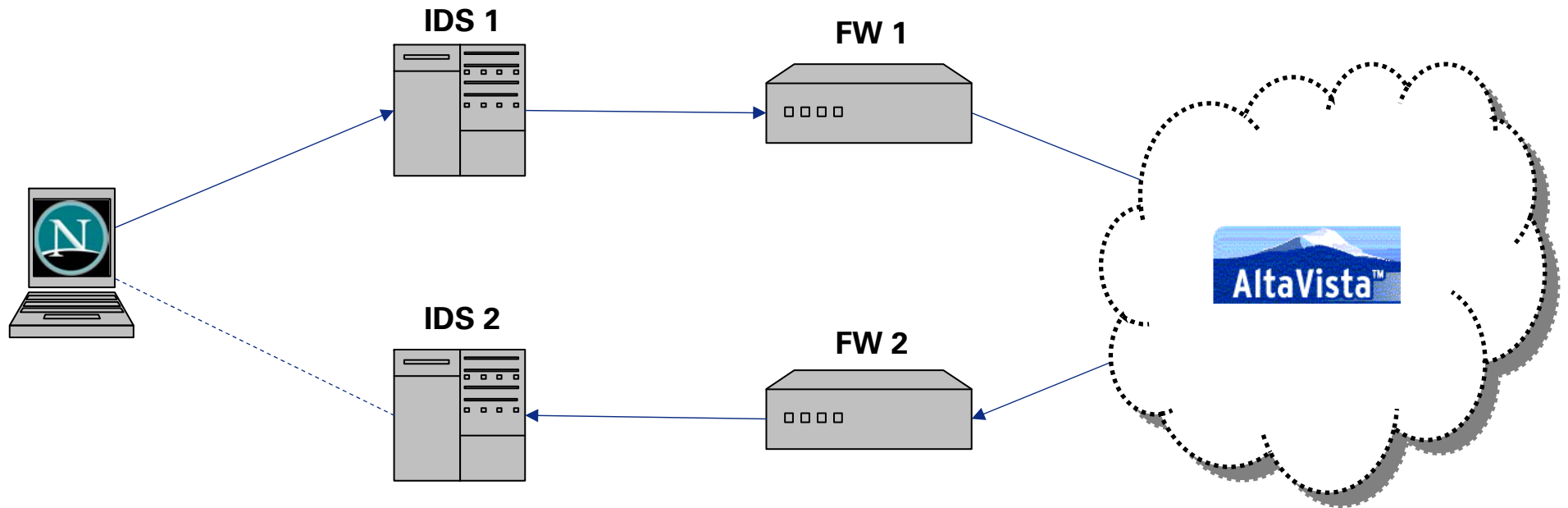
- **Who**
- **What**
- **When**

**It is NOT**

- **Why**

# What do I mean?

## Load balancing IDS



*Images courtesy of Netscape and AltaVista*

# Where is our risk?

## Examples:

- **Malicious network scanning**
- **High risk financial transactions**
- **Inappropriate access to data**
- **Separation of duties violations**

# Malicious Network Scanning

System	Log File	Message Count
Apache	error.log	554
	access.log	639
Linux	syslog	132
	daemon.log	139
	auth.log	157
MySQL	mysql.log	1595

May 17 08:06:14 ubuntu telnetd[1288]: tloop: read: Connection reset by peer

May 17 08:04:13 ubuntu in.ftpd[1241]: connect from unknown (unknown)

May 17 08:02:21 ubuntu telnetd[1167]: tloop: peer died: EOF

May 17 08:04:48 ubuntu ftpd[1243]: pam\_unix(ftp:auth): authentication failure; logname=  
uid=0 euid=0 tty= ruser= rhost=192.168.236.131  
#####

# Building Rules

## Warning Messages in syslog

\*in.ftpd[\*]: connect from unknown (unknown) (8)

\*ftpd[\*]: getpeername (in.ftpd): Transport endpoint is not connected (4)

\*telnetd[\*]: ttloop: read: Connection reset by peer (3)

\*telnetd[\*]: ttloop: peer died: EOF (2)

Example Rule: any 5 events in 1 minute on any system

Example Rule: any 50 events in 5 minutes across all systems

# Building Rules

## Warning Messages in error.log

\*[error] [client \*] File does not exist: \* (456)

\*[error] [client \*] script\*not found or unable to stat\* (47)

\*[error] [client \*] Invalid URI in request GET \* (30)

\*[error] [client \*] Invalid method in request \* (4)

Example Rule: any 100 “File does not exist” in 1 minute on any system

Example Rule: all of the above seen in 1 minute on any system

Example Rule: both Rule 1 and Rule 2 seen in 1 minute on any system



# Building Rules

## General Messages in mysql.log

59 Query SELECT \* FROM wp\_users WHERE user\_login = 'dummy'

57 Query INSERT INTO `wp\_usermeta` (`user\_id`,`meta\_key`,`meta\_value`) VALUES ('2','nickname','hackme')

60 Query UPDATE `wp\_options` SET `option\_value` = '1' WHERE `option\_name` = 'users\_can\_register'

Example Rule: User login does not exist

Example Rule: New user being added

Example Rule: Security settings changed

# Continual Improvement

## Ongoing opportunities:

- **False Positives**
- **Incident Management**
- **Vulnerability Assessments/Penetration Tests**
- **Management Information**
- **Validate other Monitoring Systems**

# User Monitoring Regulations

# Legal/Regulatory Issues

## **April 2007, UK gov coughs up £3,000 damages and costs**

The monitoring of an employee's email, phone and internet use by a Welsh college was a breach of her human rights, the European Court of Human Rights has ruled. The UK Government must pay £3,000 damages and legal costs in the case.

*Source: [theregister.co.uk/OUT-LAW.COM](http://theregister.co.uk/OUT-LAW.COM)*

# Legal/Regulatory Issues

## Privacy Rights Clearinghouse, California

In most cases, employees find out about computer monitoring during a performance evaluation when the information collected is used to evaluate the employee's work.

*Source: <http://www.privacyrights.org>*

# Legal/Regulatory Issues

## **German rail firm pays €1.1m fine over employee snooping**

Germany's national rail company has agreed to pay a €1.1 million fine for spying on its employees for more than a decade.

*Source: OUT-LAW News, 27/10/2009*

# The Future

## Monitoring of Desktop Actions

- **Direct monitoring of user behaviour**
  - **Data Loss Prevention**
  - **Copy & Paste**
  - **Email**
  - **Upload to Internet**
- **Less reliance on system logs**
  - **Ineffective in comparison**

## Mixing of Security and Information Security

- **CCTV**
- **Badge Access**

## Broader Correlation of Technology

- **VOIP**
- **Mobile Devices**
- **Corporate Card Transactions**
- **Instant Messaging**

# The Future

## Lower Expectation of Privacy

“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”

*Eric Schmidt, Chairman & CEO of Google Inc*



*Images  
courtesy of  
Wikimedia  
Commons  
and Google*

## Lower Expectation of Privacy

“My problem (...*is*...) the premise that privacy is about hiding a wrong. It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect.”

*Bruce Schneier, CTO of BT Counterpane*



*Images  
courtesy of  
Wikimedia  
Commons*

## Lower Expectation of Privacy

"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people."

"We view it as our role in the system to constantly (...) reflect what the current social norms are."

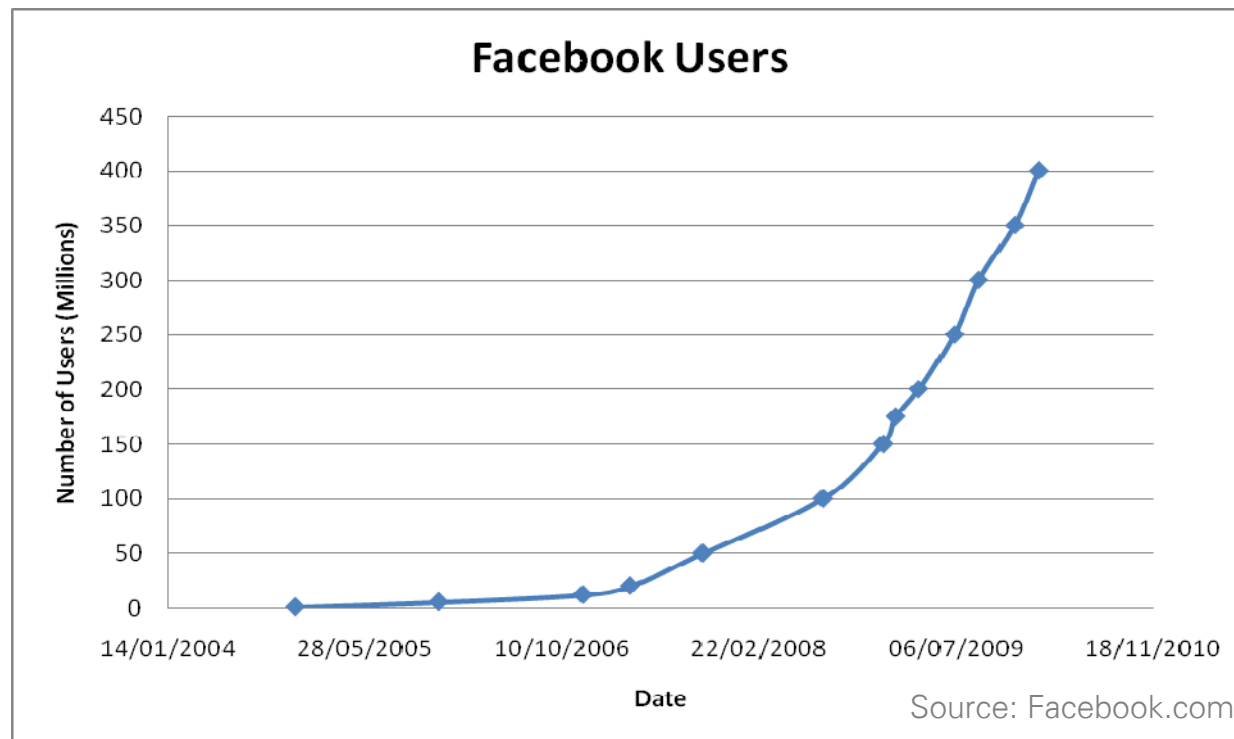
*Mark Zuckerberg, CEO & President of Facebook*



*Images courtesy of Wikimedia Commons and Facebook*

# The Future

## Lower Expectation of Privacy



**Q: How many people quit Facebook on 'Quit Facebook Day' (31<sup>st</sup> May 2010)?**

**A: 36,000 (0.01%)**

# Summary

- **Auditing Policy and Strategy**
- **Building Alerting Rules**
- **User Monitoring Regulations**
- **The Future**

# Questions?