E-banking Security Assessment

HOW TO TRAIN

Your Ninja

K-159 <k-159@echo.or.id>

A Ninja?

23-Nov-09 09:50

The Agenda

#WHOAMI

A FATHER
RESEARCHER
SOCIAL
ENGINEER
GOSSIPER

noose

PROLOG

EVER CHOOSED A BANK 'COZ THEIR SECURE IT SYSTEM?


STETSON
EVER DREAMED TO HACK YOUR OWN BANK?

Selasa, 05/10/2010 18:30 WIB

Akhir Kisah Si 'Pembobol' Bank Rp 67 Triliun

Nurul Qomariyah - detikFinance

Share : Share 65 58 retweet

Jerome Kerviel (Foto: Reuters)

SOMEBODY DOES ..

Kerviel, 33 tahun dinyatakan bersalah melanggar kepercayaan, penyalahgunaan komputer dan pemalsuan dengan vonis 5 tahun penjara.

Pengadilan di Paris juga memerintahkan Kerviel untuk mengembalikan dana yang 'dibobolnya' sebesar 4,9 miliar euro atau sekitar US$ 6,8 miliar kepada bank asal Prancis itu.

Hakim menilai Kerviel tidak menerima otorisasi bahkan yang secara diam-diam dari atasannya untuk melakukan spekulasi secara berlebihan.

Hakim juga menilai Kerviel secara pasti tahu apa yang dilakukan itu melampui izinnya sebagai pialang dan mencoba menyembunyikan posisi trading-nya.

John Dilinger - Public Enemy (2010)

Inside Man (2006)

WARNING

Restricted Area

It is unlawful to enter this area without permission of the Installation Commander.

Sec. 21, Internal Security Act of 1950; 50 U.S.C. 797

While on this Installation all personnel and the property under their control are subject to search.

Use of deadly force authorized.

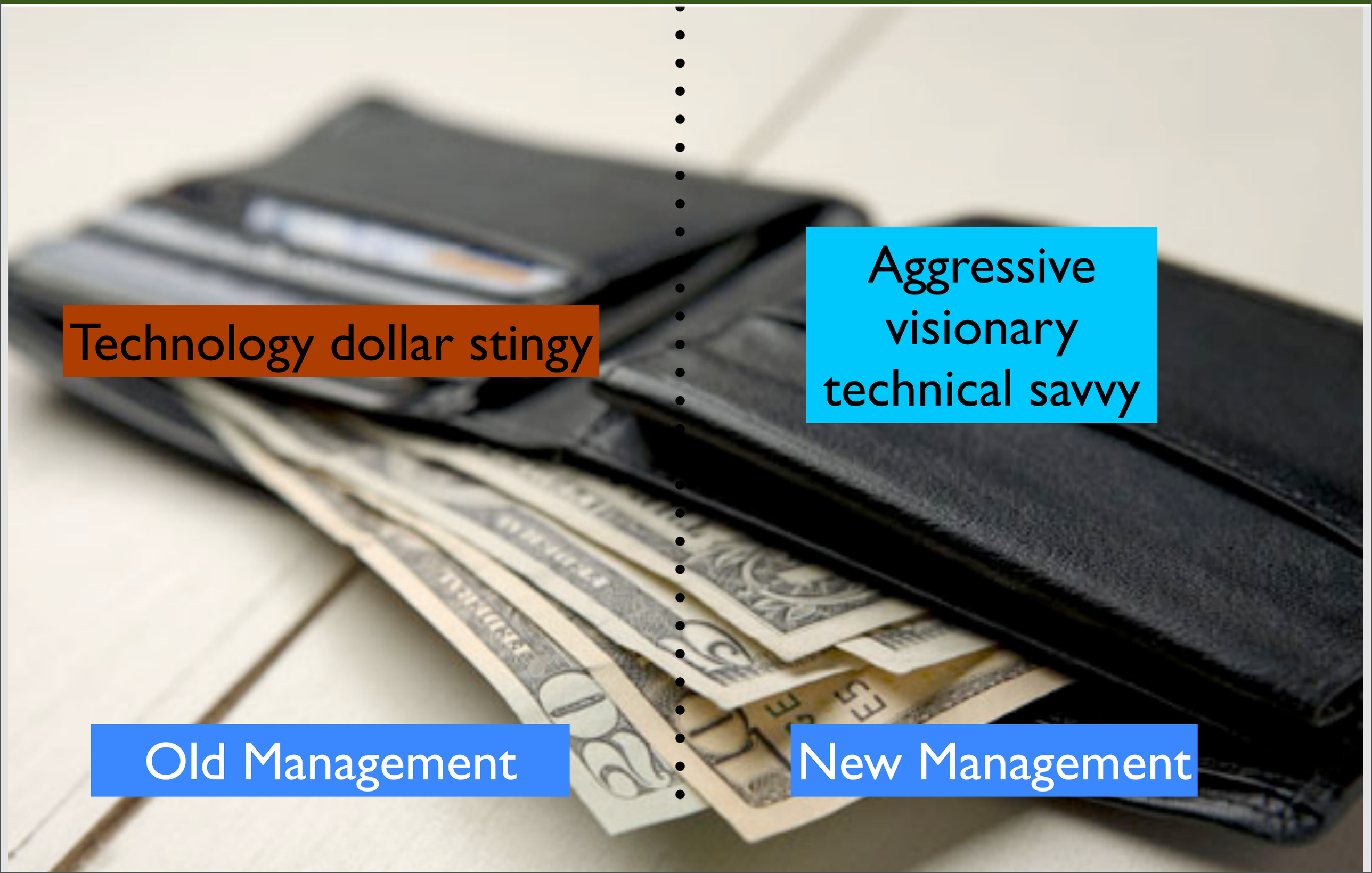
AFVA 207-1
10 October 1986

INSIDE THE BANK

THE BANK IS ..

Deposits,Loan,prosperity

SHIFTING ORG.BEHAVIOUR



COMMON SITUATION

High risk. The IT department is high risk

The Data Center is small and crowded

There is no Help Desk system

Most of the communication lines are at speeds of 64 K

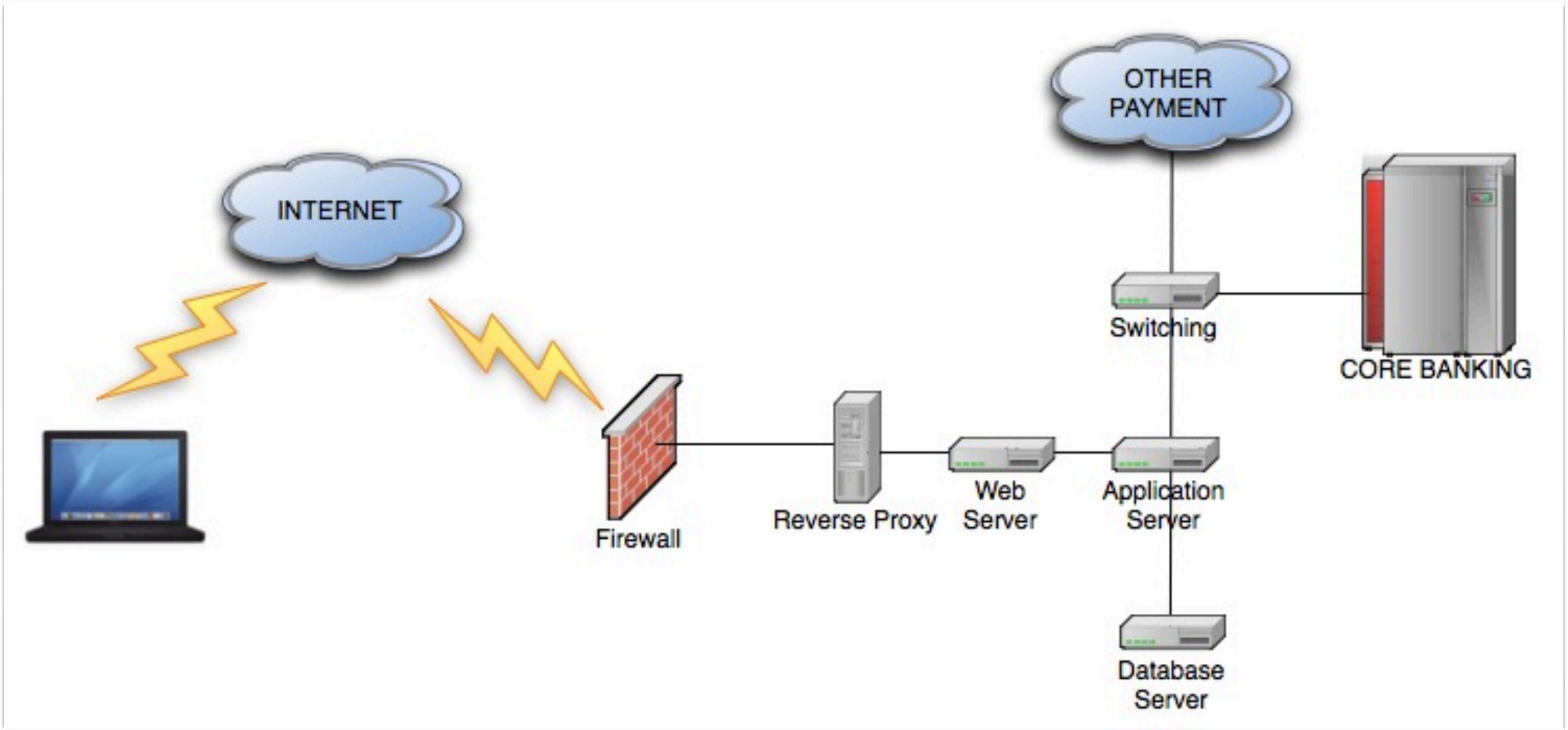
The core banking system is old and obsolete

The Trade Finance System is old and obsolete

The ATM switch is old and cannot support many of the new ATM functions required

The Call Center is obsolete and supports only 8 agents

E-Banking Is ..


INTERNET
OTHER PAYMENT
Switching
CORE BANKING
Firewall
Reverse Proxy
Web Server
Application Server
Database Server


CENTAVOS

Bank Central Regulation

Peraturan BI No. 5/8/PBI/2003

Surat Edaran BI No. 6/18/DPNP, tanggal 20 April 2004

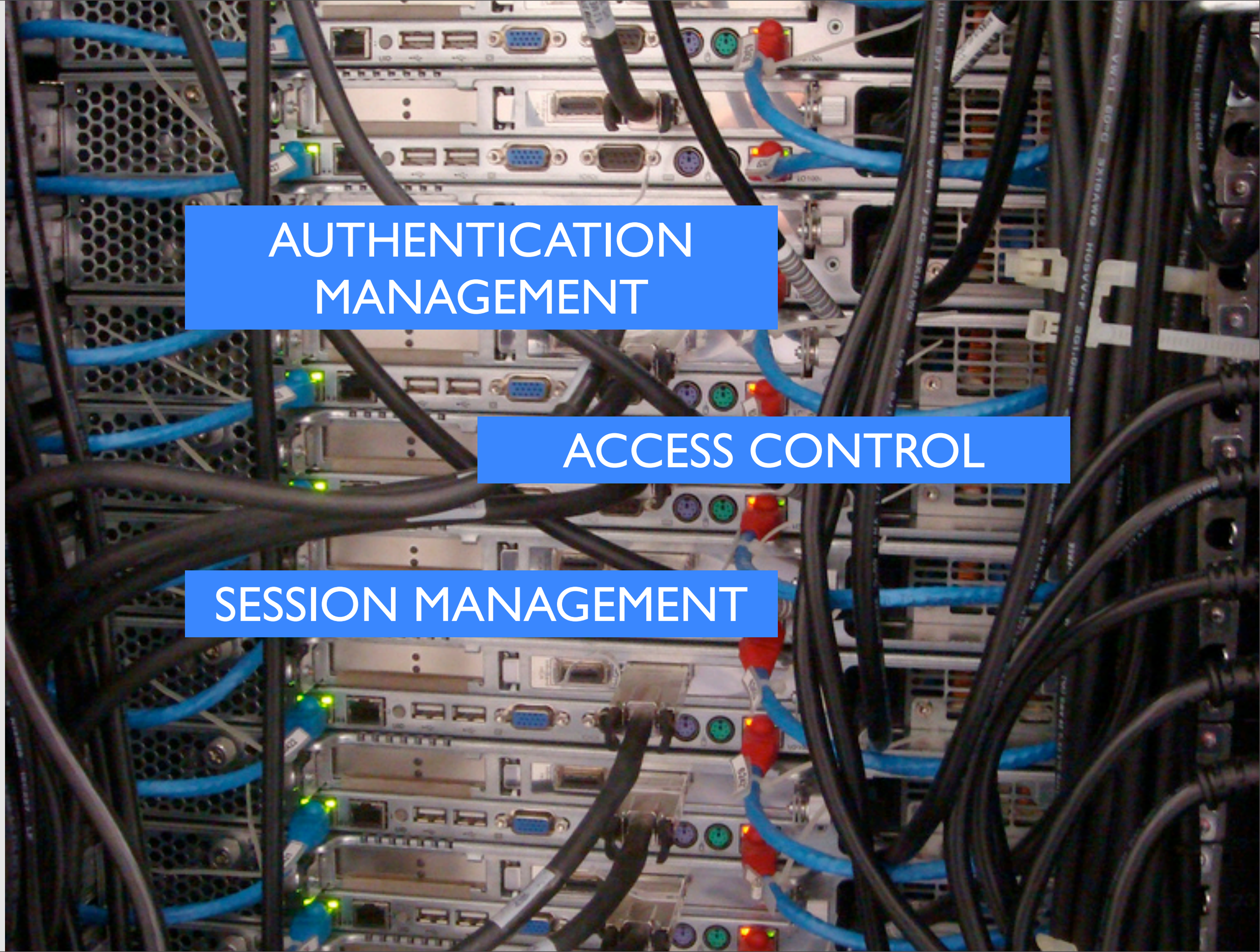
THREAD INCRESE EACH HOUR

PENTESTER ETHICS

Ethics

NON -DISCLOSURE AGREEMENT

Ebanking Assessment Activity


AUTHENTICATION MANAGEMENT
ACCESS CONTROL
SESSION MANAGEMENT

Deliverable ..

MANAGEMENT REPORT

RISK + ASSET + VALUES

TECHNICAL REPORT

TECHNICAL DETAIL+PATCHING+CODING

WELL KNOWN PENTESTER

JIM GEOVEDI

Conclusion..

Please Be Safe!

Q&A

Thanks

Twitter.com/159k

Credits

Page1: http://www.ninjaonline.co.uk/media/gbu0/prodlg/ninjasuit.jpg
Page2: http://alformer259.files.wordpress.com/2009/11/dsc001511.jpg
Page3: http://www.flickr.com/photos/wienwardana/3165753895/
Page4: Kendi Demonic Photograph
Page5: http://www.flickr.com/photos/anonymouscollective/2291139919
Page6: http://www.flickr.com/photos/anonymouscollective/2291896028/sizes/l/in/photostream/
Page7: http://www.flickr.com/photos/cverdier/4837773532/sizes/l/in/photostream/
Page8: http://www.detikfinance.com/read/2010/10/05/183003/1456367/68/akhir-kisah-si-pembobol-bank-rp-67-triliun
Page9: http://www.flickr.com/photos/37021726@N07/3595094343/sizes/l/in/photostream/
Page10: http://cdn-images.hollywood.com/site/insideman_dc.jpg
Page11: http://www.familieharmsen.nl/vakanties/Zomer2001/TikabooValley/MVC-288F.JPG
Page12: http://www.primaironline.com/images_content/20100525BankIndonesia%20bankir-indonesia.org.jpg
Page14:http://www.flickr.com/photos/sutje/1315711528
Page15: http://www.flickr.com/photos/seier/3463984860/sizes/z/in/photostream/
Page16: http://www.flickr.com/photos/fabiano/2783656239/sizes/l/in/photostream/
Page18: http://www.flickr.com/photos/felixtito/334828049
Page19: http://www.files.chem.vt.edu/chem-dept/tissue/images/ethics180x120.png
Page20 : http://2.bp.blogspot.com/_VbdMFZn0qEM/TAHiacMpj9I/AAAAAAAAAmQ/OBKaqC0SN9g/s320/ethics_header.jpgs
Page21: http://www.flickr.com/photos/dcdead/4527722719
Page22: http://www.flickr.com/photos/sugree/3024642081
Page23: http://www.flickr.com/photos/tatraskoda/2057210204/sizes/o/in/photostream/
Page24: http://www.flickr.com/photos/meetings/2073768553/sizes/o/in/photostream/
Page25: http://www.flickr.com/photos/thecrimsonbat/4627770158
Page26: http://www.flickr.com/photos/ingythewingy/4660595849/sizes/l/in/photostream/
Page27: http://www.flickr.com/photos/gvd06a/408242761/
page28: http://sphotos.ak.fbcdn.net/hphotos-ak-ash1/hs062.ash1/6926_149011886357_693241357_2571740_7209947_n.jpg
Page29: http://www.flickr.com/photos/shadphotos/207233715/sizes/m/in/photostream/
Page30: http://www.flickr.com/photos/rundstedt/4412545871/sizes/l/in/photostream/