

Security in Business and Applications

Madison Hajeb
Stefan Hurst
Benjamin Von Slade

Introduction

- Project Concept - Implement security in a small business setting
- Original Plan - Do some security audits for small companies
- Actual Plan - One company need a security review and the other company needed help with user tracking security

Two Different Projects

1. Krames Staywell Access Tracker
2. Wind River Security Review

Krames Staywell Access Tracker (KSAT)

KRAMES
staywell
ACCESS
tracker

TASK

Help them achieve HIPAA compliance by implementing a new applications



Two Initial Projects

Application 1

- Track the access employees have to applications that deal with Electronic Health Patient Information (EPHI)

Application 2

- Collect all the log files in a central location and create an application that can easily present those logs to an end-user for later review
- Dropped because they already have a Splunk server doing what they need

Plan

- Initially wanted to implement with Request Tracker, or RT for short.
 - Even though we looked into this, it seemed as if this may be scope creep.
 - Step Back: What is the end goal of this application?
 - RT is meant to do just that, organize requests.
 - NOT for tracking access to applications
 - They could change some policies and use RT to make application requests, but, in the end, they still need to track who has access to what

KSAT - Requirements Gathering

- CRUD application
- Store all pertinent employee information
- No application specifics, just free form applications
- Ability to edit all information
- Search fields for things
- RT Integration?
- Log usernames, what they did, and timestamps
- Finish by interviewing all employees

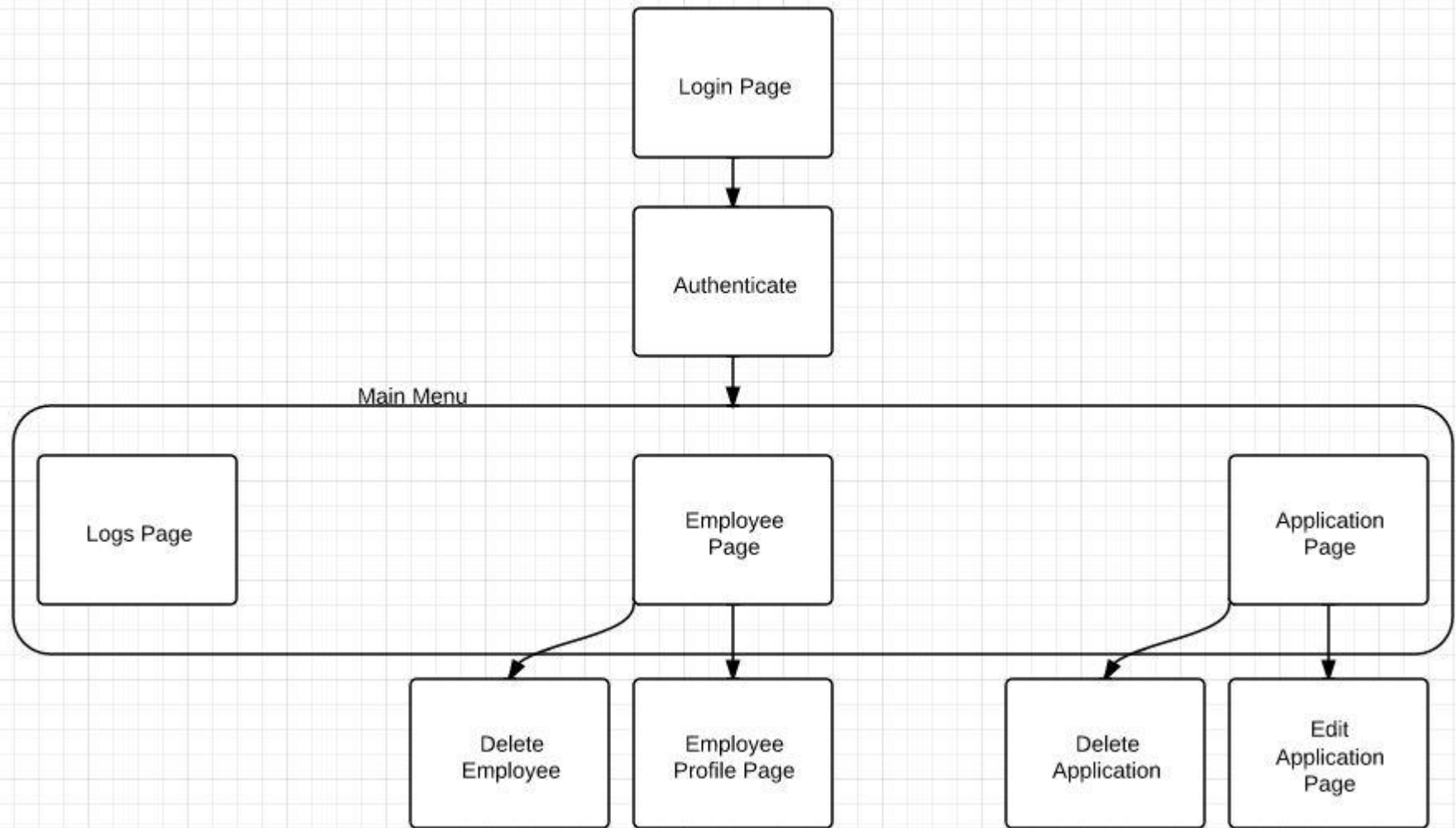
Action

Setting up a testing environment

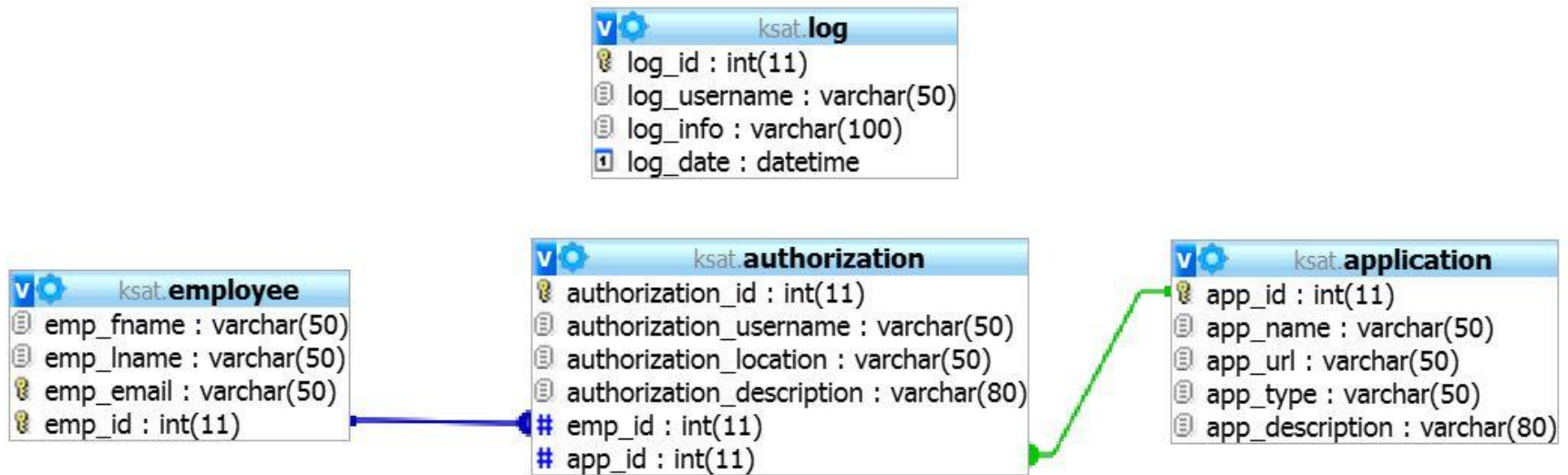
- Windows Server 2008 Standard VM
- XAMPP Server (Apache, PHP, and MySQL)
- Cisco VPN from home
 - If we are on the school's network, VPN is not required

Special thanks to Jon Soldan and Dr. Randy Boyle for helping to get a testing environment up and running

Sitemap

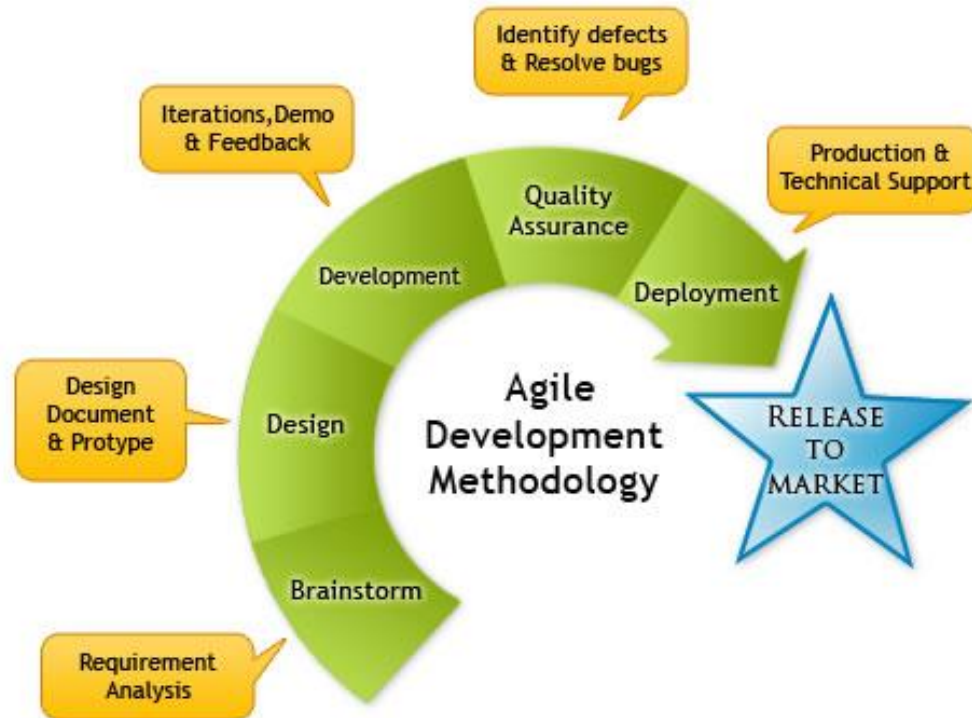


ERD



Process

- Agile process



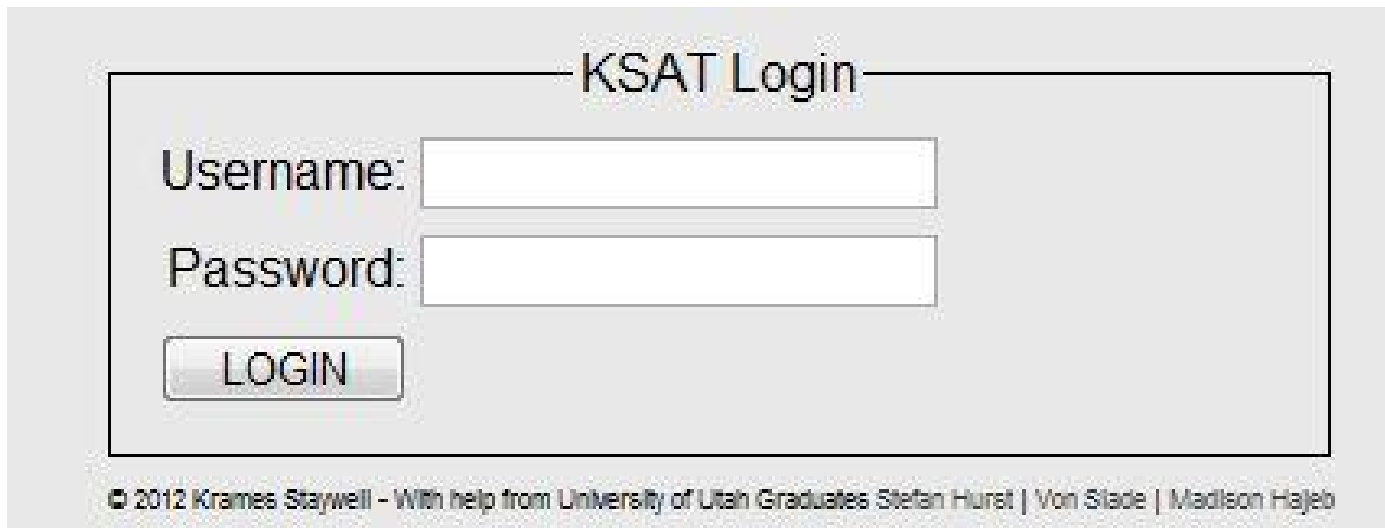
Settings File

- We created a central location for all specific url, database, and user settings.
- This made the transition from our testing environment to their production environment much easier.

```
define('AD_HOST', '155.97.56.231'); // Active Directory Server IP address
define('DN', 'CN=Users, DC=msv, DC=local'); // Common Name Information
define('USER_GROUP', 'KSAT'); // Active Directory Normal User Group
define('MANAGER_GROUP', 'KSAT'); // Active Directory Manager Group (Same as User group if using ONE group)
define('DOMAIN', '@msv.local'); // Domain Name for authenticating username
define('MYSQL_HOST', '155.97.56.231'); // MySQL Server IP address
define('MYSQL_USERNAME', 'ksat_user'); // MySQL Username to access DB
define('MYSQL_PASSWORD', 'TASKp@@$w0rd'); // MySQL Password to authenticate user
define('MYSQL_DB', 'ksat'); // MySQL DB Name
```

Login Page

- Connects to a Microsoft Active Directory
- Allows to have a normal user group and an administrator group
 - We only utilized one group, so both settings point the same group. Allows them to add more control later if needed



The image shows a screenshot of a login page titled "KSAT Login". The page contains a form with two input fields: "Username:" and "Password:". Below the "Password:" field is a button labeled "LOGIN". The form is enclosed in a rectangular border. At the bottom of the page, there is a copyright notice: "© 2012 Krames Staywell - With help from University of Utah Graduates Stefan Hurst | Von Slade | Madison Hajeb".

Successful Login Landing Page

- After a successful login, the user is taken to the employee page

KRAMES staywell ACCESS tracker

Shurst (Logout)

Employees | Applications | Logs

Last Name First Name Email Find Add

Name	Email	
Alphonse, Jonelle	jonelle.alphonse@kramestaywell.com	Delete
Bob, Bob	char@gmail.com	Delete
Charley, Ryan	varchar@gmail.com	Delete
Charley, Ryan	rchar@juno.com	Delete
Danny, Sookdeo	dsookdeo@kramestaywell.com	Delete
Dominguez, Jorge	jorge.dominguez@kramestaywell.com	Delete
Foote, Martha	martha.foote@kramestaywell.com	Delete
Fritz, Edward	ed.fritz@kramestaywell.com	Delete
Gardner, Kalli	kgardner@kramestaywell.com	Delete
Hajeb, Madison	madison.hajeb@gmail.com	Delete
Harrinarine, Avinash	avinash.harri@kramestaywell.com	Delete
Hurst, Stefan	stefan.hurst11@gmail.com	Delete
Hurst, Stefan	stefan@stefan.com	Delete
Jones, Ryan	ryan.jones@kramestaywell.com	Delete
Kelly, Brent	bking@kramestaywell.com	Delete
Last, First	flast@gmail.com	Delete
Phelps, Ronnie	rphelps@kramestaywell.com	Delete
Roy, Donald	don.roy@kramestaywell.com	Delete
Ryan, Kobe	von@slade.com	Delete
Sinclair, Cullen	cullen.sinclair@kramestaywell.com	Delete

Export to CSV

© 2012 Kramés Staywell - With help from University of Utah Graduates Stefan Hurst | Von Slade | Madison Hajeb

KSAT Demo

Interviews

- After application completion
- Given company laptops
- Each individual employee
- Query employees about all access they may have to applications dealing with EPHI

KSAT - Complications

- Unforeseen application errors
- Slight miscommunication on how the application functions
 - After KSAT was developed we found out that many of the applications go through a Development, Staging, and Production environment.
 - It would have helped to have an extra table in the DB where we could define "environments"
- Interview Communication
 - Each employee has their own naming conventions for applications, making populating KSAT difficult
- INTERNET EXPLORER!
 - CSS always looked slightly different in IE

KSAT - Lessons Learned

- Planning Planning Planning...
- Understand the business process to the fullest
 - Helps for application building process
 - Helps for interview process to fill database
- Constantly make sure you are on the same page as the company
- Some people are going to be difficult to work with

Wind River Security Review

- Excavation company located in Salt Lake City with job sites throughout Utah
- Have done many jobs here at the University of Utah, including work on the new business buildings



Task

- Security review of the technology and physical space of the office
 - Followed a security checklist for small businesses
- Provide recommendations about security and system upgrades
- Provide recommendations for security policies in the office

Requirements Gathering

- Access files from home
- Monitor employee activity
- Feel confident in computer security
- Change as few habits as possible

Initial Review

- Logged all hardware on the network
- Renamed computers numerically
- Physical security interview

Device Information								
IP	Device	Network Name	Type	Brand	Model	Version	Location	Operating System
192.168.1.151	sr-user-06	sr-user-06	AIO	HP	TouchSmart 610		Chaf's Desk	Windows 7 Home Premium 64 bit
192.168.1.153	sr-user-04	sr-user-04	Desktop	HP	p7-1167c		Rachel's Desk	Windows 7 Home Premium
			Monitor	HP				
			Monitor	Dell				
	HP LaserJet 4050 Series		Printer	HP	N911g		Rachel's Desk	
192.168.1.152	HP Officejet Pro 8600	wireless	Printer	HP				
192.168.1.157	sr-user-02	sr-user-02	Desktop	Custom	V1C26			
	ASUS VHQ36		Monitor	ASUS				
192.168.1.21	HP LaserJet 4050 Series	NP17351D	Printer	HP	LaserJet 4050			
	HP LaserJet 4050 Series	NP10E3E74	Printer	HP	LaserJet 4050 N			
192.168.1.160	sr-user-03	sr-user-03	Desktop	Custom				
192.168.1.150	HP Officejet Pro 8500 A910 Series	HP33718F	Printer	HP	Officejet Pro 8500			
	Emission EN9410s		Monitor	Emission	EN9410s			HP 2511 Series Wide LCD Monitor (25")
192.168.1.8	sr-user-01	sr-user-01	Desktop	Custom				
					8830 (510 Series			Dell SH 2220L (22")
					Wide Format)			
192.168.1.90	Xerox 8830		Printer (Plotter)	Xerox	8830			
192.168.1.2	Windriver123	windriver123	Server	SuperMicro?	777			
			Monitor	Asus				ASUS VHQ36 (23")
	CTL 170Lx		Monitor	CTL	170Lx			
192.168.1.1	Netgear N600	WNDR3700-v3	Wireless Router	Netgear	N600 (WNDR3700)	v3		
	Trendnet TEG-S168TX		Switch	Trendnet	TEG-S168TX			

	CPU Information	RAM Information	Hard Drive Information	Monitor Information				
	CPU Type	CPU Model	CPU Socket	CPU Speed	Memory Amount	Memory Type	Hard Drive Space	Monitor Size
C	Intel	i3 550	1156 (LGA)	3.20GHz	2 X 2GB	PC3-10700	390GB	25"
O	Intel	i5 2400	1155 (LGA)	3.1 GHz	2 X 4GB	PC3-10700	1 TB	
O								
K								
K								
K								
K								
Ss	Intel	i5 2400	1155 (LGA)	3.1 GHz	2 X 4GB	PC3-10700	232 GB	
Ss								
Ss	Intel	Pentium 4	775 (LGA)	3 GHz	2 X 1GB	PC2-6300	71 GB	
Ss								
Ss	Intel	i6 750	1156 (LGA)	2.67 GHz	2 X 4GB	DDR3	600 GB	19"
Ss								
Ss	Intel	Xeon E5410	771 (LGA)	2.33 GHz	4 x 1GB	PC2-6300	700GB	ASUS VHQ36H (23") 17"

Access	Main Entrance	Front Door	Back Door	Side Door	Server Room	Filing Cabinets	Cameras
	Everyone	Rachel Chaf Kelly Cameron Kyle Mark (building mgr) Brian	Kelly Rachel Mark	Kelly Rachel Mark	Brian Rachel Mark	Fonz desk - unlocked	None in office

Action

- Set up SSL on email
- VPN
- Nessus scan for vulnerabilities
 - Fixed all critical and important errors
- User accounts and folder access on server
 - Active Directory Workaround
- Trained employees
 - Keyloggers
 - Browser Security
 - Monitoring Systems
 - Backup

Key Learning Points

- Small companies are less receptive to monetary solutions
- Money was a large stalling point
- Security policies are difficult to enforce in a small casual office (without AD)
- People are resistant to change and new habits/software/policies

Comparison

Wind River

- Concern: General Security
- Medium Risk: They are not dealing with health information, but they are dealing with many clients and financial bids
- Legally bound to protect client financial data housed on the server

Krames Staywell

- Concern: HIPAA Compliance
- Higher Risk: Dealing with Patient information and employee login information
- Legally required to provide a log sheet of employee access according to HIPAA, so pressed for time before the next audit

Conclusion

- Security practices can be applied in many different business applications and scenarios
 - Two completely different businesses need security, but they need very different things
 - The umbrella of "security" is large and disparate at times

Questions?