RAPID7

Security !Maturity

October 20, 2010

About me - Joshua “Jabra” Abraham

- Security Consultant/Researcher at Rapid7 LLC.
- Past speaking engagements
  - BlackHat, DefCon, ShmooCon, Infosec World, CSI, OWASP Conferences, LinuxWorld, Comdex and BLUG
- Recently became a Technical Editor for Syngress (Ninja Hacking)
- Contributes to BackTrack LiveCD, BeEF, Nikto, Fierce, and PBNJ
- Twitter: http://twitter.com/jabra
- Blog: http://spl0it.wordpress.com

RAPID7

Rapid7 Overview

- Vulnerability Management

  RAPID7 NEXPOSE

- Open source projects

  metasploit

  w3af
  Web Application Attack and Audit Framework

- Professional Services
  - Network Pentesting
  - Web Application Audits
  - Training
  - Deployment

RAPID7

Understanding the Environment

- People
- Process
- Technologies

- Focus on two points of reference
  - Penetration testing (OPs side)
  - Deploying a secure development lifecycle (non-OPs side)

RAPID7

Breaking through a misconception

How many times during a scoping call have you heard the customer say the goal of the assessment is to “Hack Us?”

RAPID7

“Hack Us” – Is NOT good enough

- “Hack Us” is subjective
- What do you mean by “Hack”?
- How do you know when you are done?
- What is the success criteria for “Hacking” the customer?
- How do you measure the “Hack”?

RAPID7

Agenda

- **The need for a better approach**
- Goal Oriented Overview
- Examples from the Field
- Maturity 101
- Secure Development Lifecycle (SDL)
- Summary/Q&A

RAPID7

Background Information

- The primary objective is to demonstrate risk
- Difference between risk from vulnerability scanner and a business risk (context)
- Vulnerabilities are found by automated tools
- A threat does not have to be demonstrated in order to constitute a risk.

RAPID7

The need for a better approach

- How do you know what is MOST important?
- Achieve Domain Admin access on 1st day
- Access to all data
- Maybe get lucky and guess right
- Should not need to guess
  - Is data X more valuable/important than data Y ?

RAPID7

Which Data or Systems would you go after?

- With Control of
  - The entire network
  - OR .. all windows systems
  - OR .. all *nix systems

- Evil Attacker - Destructive
- Evil Attack – Financially motivated
- Consultant – Penetration tester
- Malicious System Admin
- Malicious Employee
- Malicious Executive

RAPID7

Raising the bar on penetration testing

- There are several technical methodologies
  - Define what and how to test
  - OWASP, OSSTMM and vulnerabilityassessment.co.uk
- Industry lacks a standard process
  - Outline a method to facilitate the testing process
  - Ensure assessment/project completion

RAPID7

Agenda

- The need for a better approach
- **Goal Oriented Overview**
- Examples from the Field
- Benefits of maturity
- Secure Development Lifecycle (SDL)
- Summary/Q&A

RAPID7

Real-World Penetration Testing

- Evil Attackers - Blackhats
  - Financially Motivated
  - Not limited by amount of time and/or resources

- Penetration Testers – Whitehats
  - Context / Goal Focused (experience, 6th sense, etc)
  - Demonstrate real world risks, but limited by the time of the engagement
  - A snapshot of the network/ application at a point in time

RAPID7

Clear Motivation

- Emulate a Blackhat, by using Goals as motivation
- Doesn't decrease the experience / 6th sense elements
- Allows the Testing Team to focus efforts on critical weaknesses

RAPID7

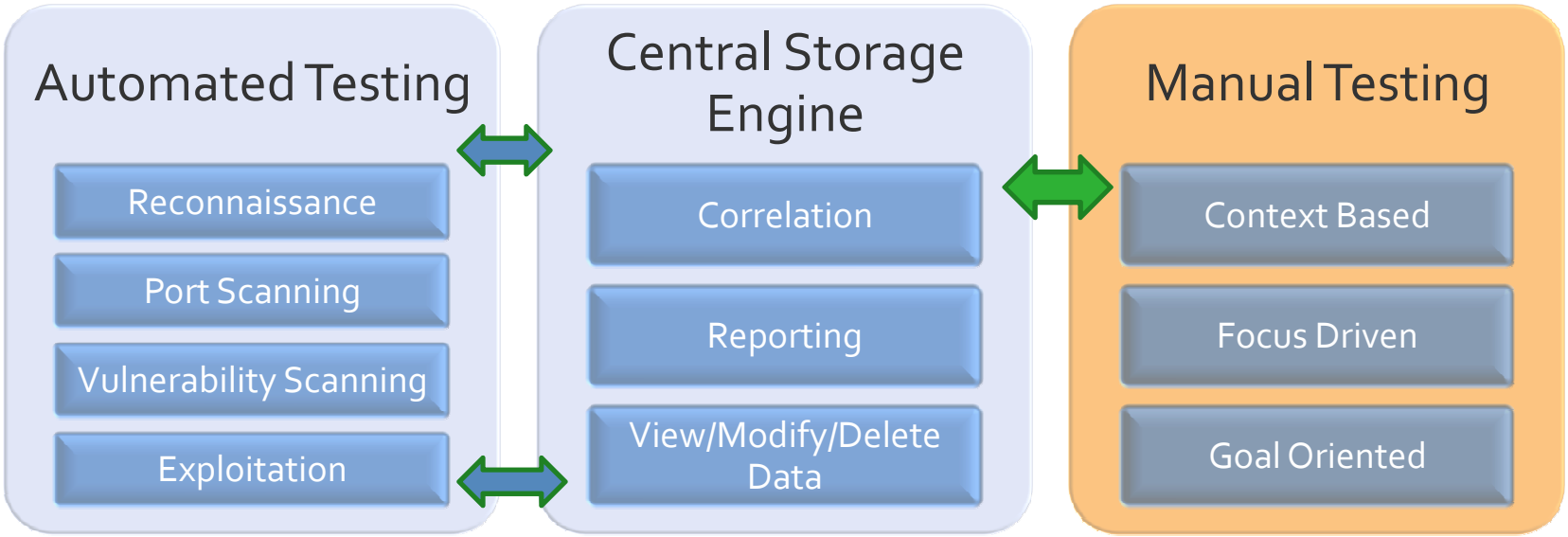
Goal Oriented Penetration Testing

- Non-technical methodology in which the process is the central focus
- Goals are focus points (drivers) for the assessment
- Provides the best (ROI) for organizations when they conduct a penetration assessment

RAPID7

Goals 101

- Goals can be achieved in parallel or a serial process
- Each goal may have a number requirement for unique paths verified
  - Discussed during scoping call



RAPID7

SMARTER Goals

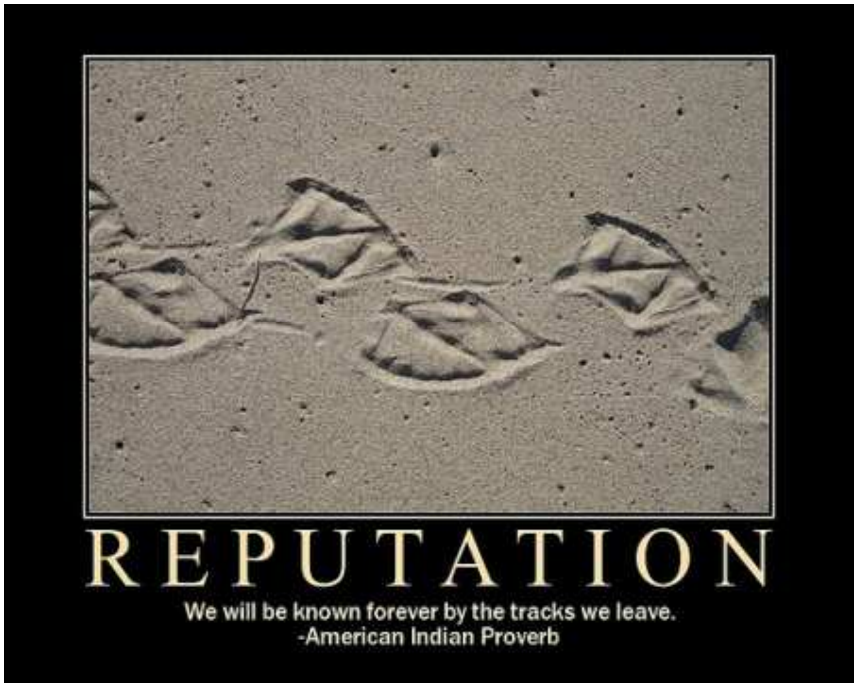
- **S – Specific**
- **M – Measurable**
- **A – Attainable**
- **R – Relevant**
- **T – Time-Bound**
- **E – Evaluate**
- **R – Reevaluate**

- "Hack us" is NOT sufficient!
- S.M.A.R.T.E.R. Goals
  - PM technique
  - Saves Time!
- Customers should demand that consultants use a Goal Oriented Approach

RAPID7

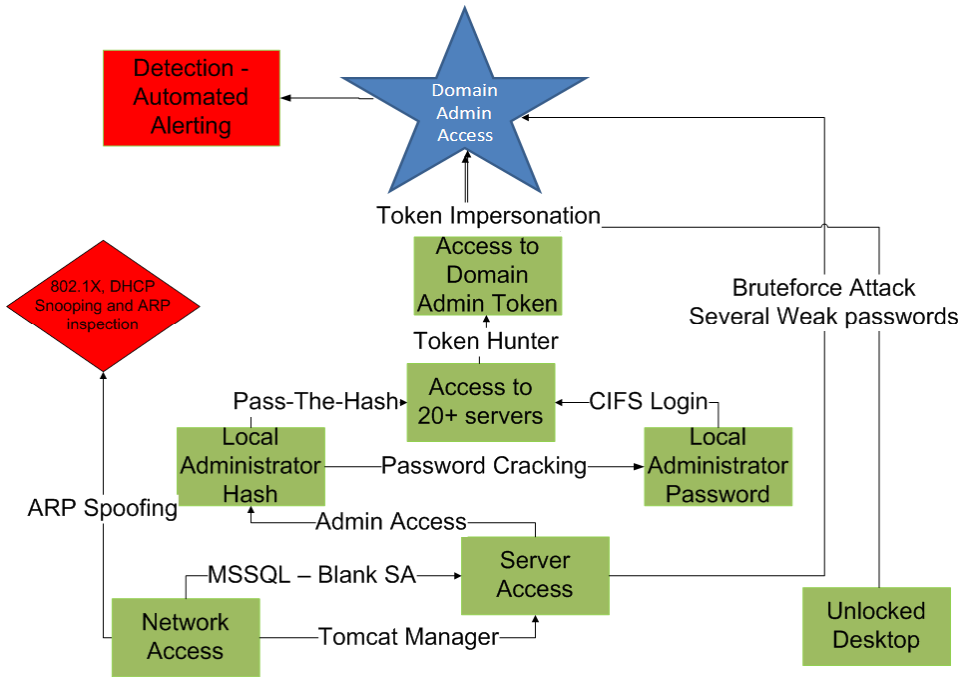
Scoping

- What type of data is most sensitive?
- What data would put the organization on the front-page of the New York Times?
- Data-classifications should be provided to the Testing Team
- Goals can be data-centric (but not always!)



RAPID7

Leveraging Unique Paths



- Success criteria
- Demonstrating a specific number of unique paths
  - Clear-view that weaknesses exist in many areas of environment
- Will a penetration test find all unique paths?
  - Not necessarily
  - Hit a point of diminishing returns

RAPID7

Agenda

- The need for a better approach
- Goal Oriented Overview
- **Examples from the Field**
- Benefits of maturity
- Secure Development Lifecycle (SDL)
- Summary/Q&A

RAPID7

External Network Penetration Assessment – Sample Goals

- Identify all of the externally accessible IPs
- Gain access to
  - Internal network (remotely) –
    - Via network or application based vulnerability
    - Via social engineering
  - Production MSSQL database
- Achieve and maintain undetected access for 24 hours

RAPID7

External Network Penetration Assessment – Customer X

- Found a system external that contained network diagrams (test.company.com)
- Diagram of All internal and external systems!
- Detailed how the network was configured
- Contained several root passwords for the internal network!
- Publicly accessible + No authentication needed
- Used Fierce v2 to find it - Enjoy - http://trac.assembla.com/fierce

RAPID7

Application Assessment – Sample Goals

- Gain access to:
  - A user's account (bypass authentication)
  - An administrator's account (priv escalation)
  - The application's backend database
- Achieve and maintain undetected access for 24 hours to internal network
  - Network/Application based attack
  - Application based attack (social engineering)

RAPID7

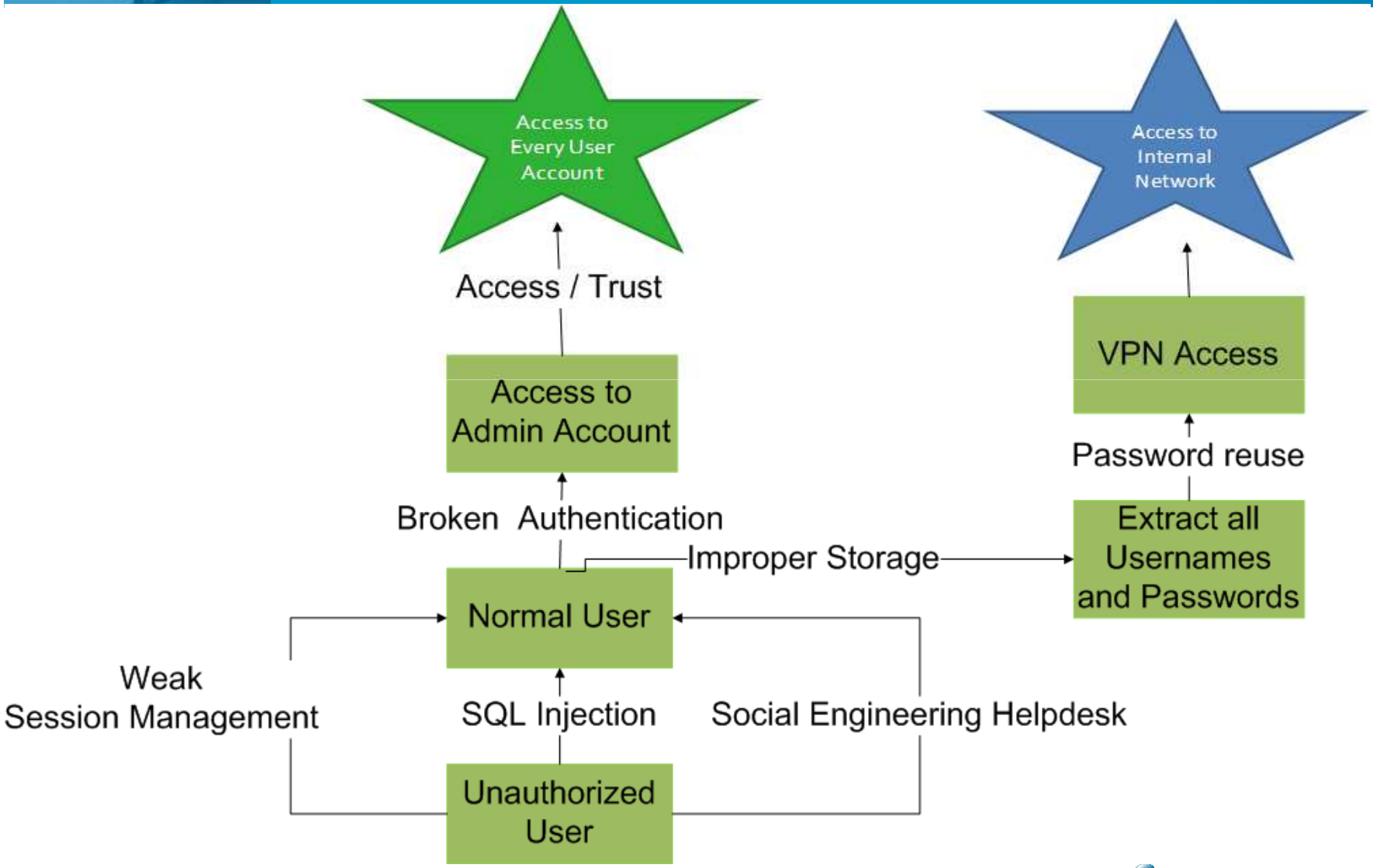
Application Assessment – Customer X

- SQLninja and SQLmap failed me.
  - This is pretty sad!
- How long would it take to develop a PoC to pull data from the database?

- ... Approximately 6 hours.
- Had a working PoC.

RAPID7

Application Assessment – Customer Y



RAPID7

Internal Network Penetration Assessment – Sample Goals

- Gain physical access to the network
- Gain access to the:
  - Corporate wireless
  - Production MSSQL database
  - Domain controller (within the PCI environment) as an administrator
- Achieve and maintain undetected access for 24 hours

RAPID7

How it works!

Recon

- Gather list of employee names
- Social Networking (facebook, linkedin, hoovers, lead411)

Prepare Email

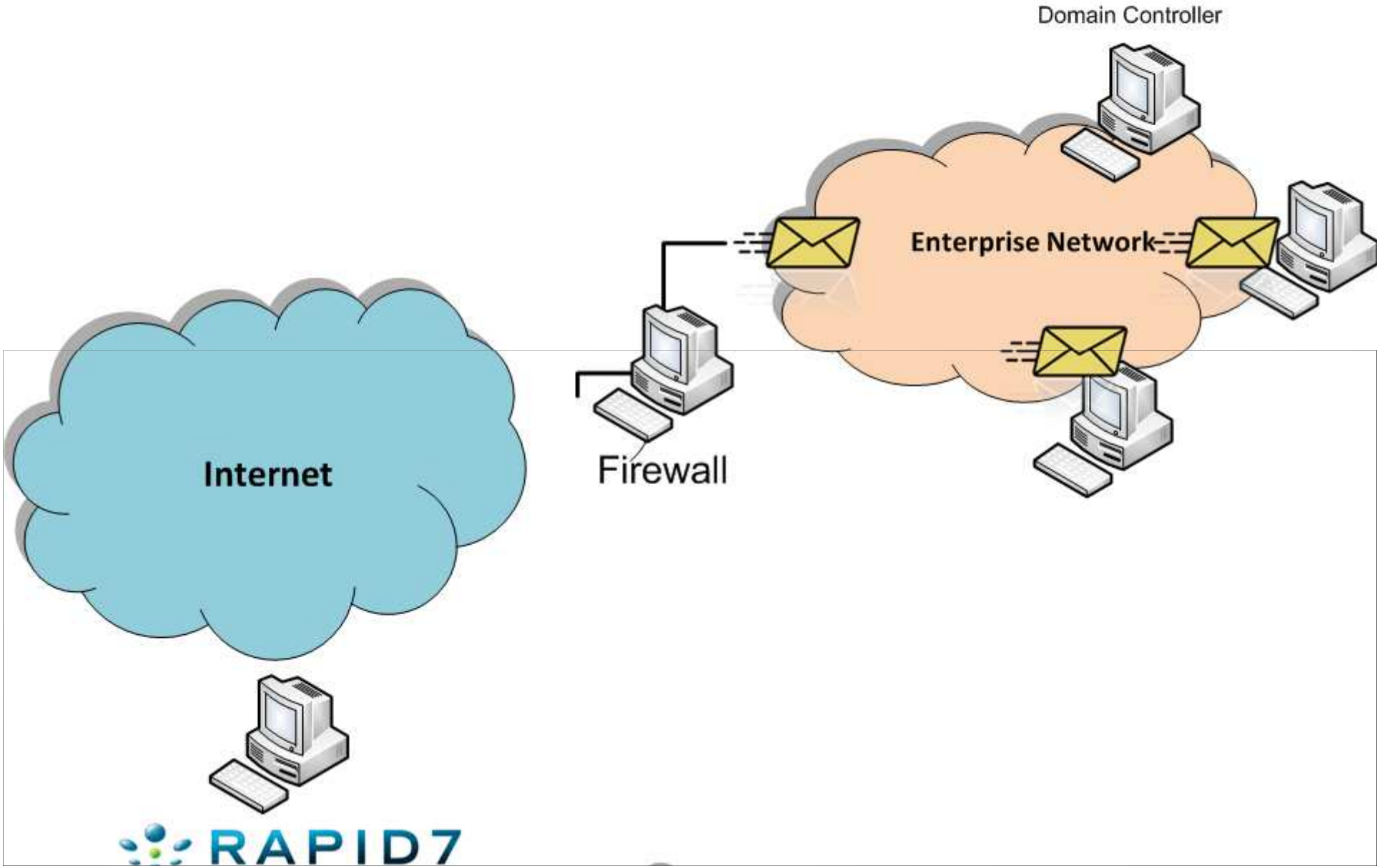
- Construct Email addresses based on email scheme
- Create email for email attack

Send out email

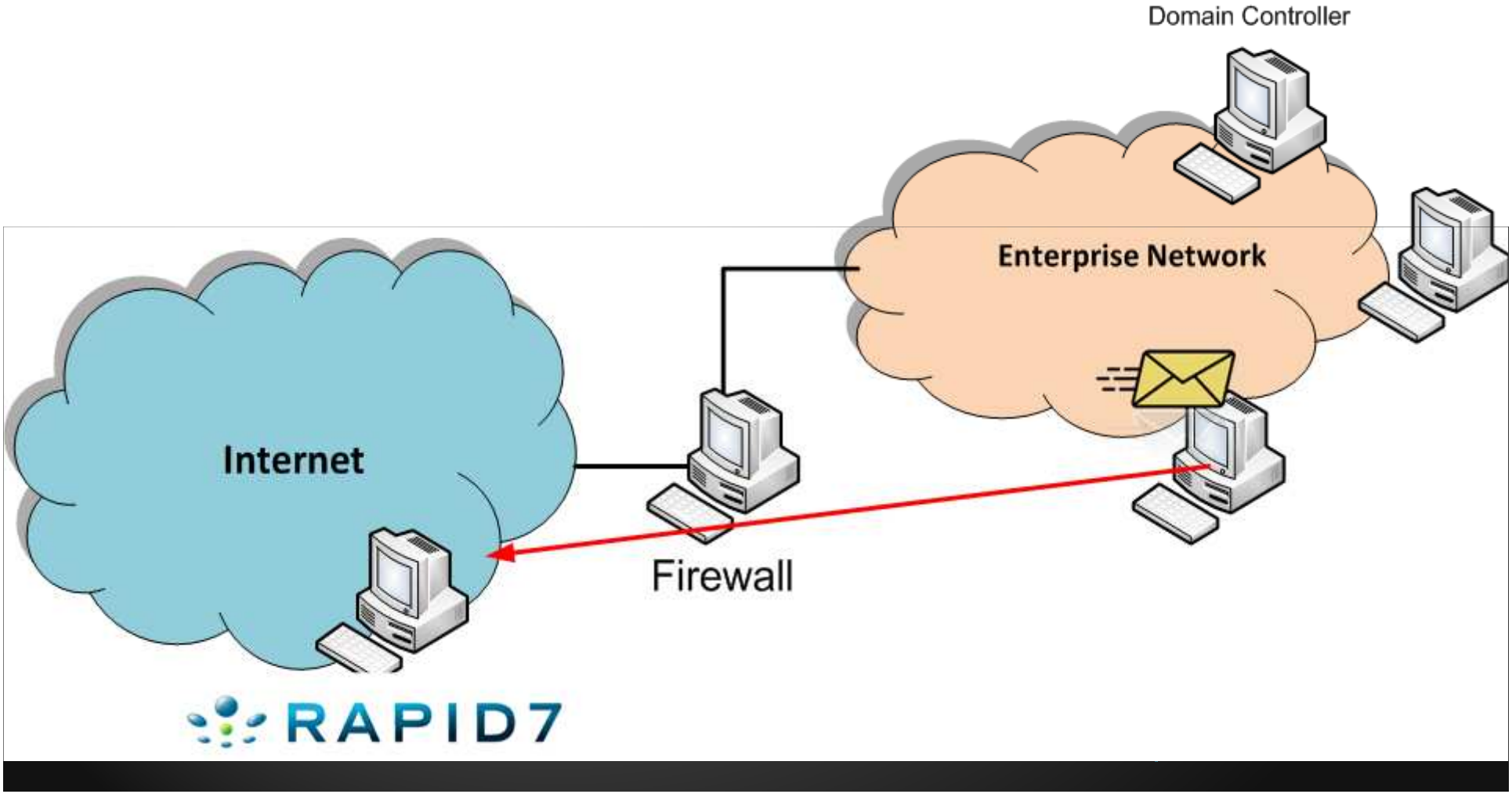
- Setup Metasploit for connections
- Send out Phishing Attacks

RAPID7

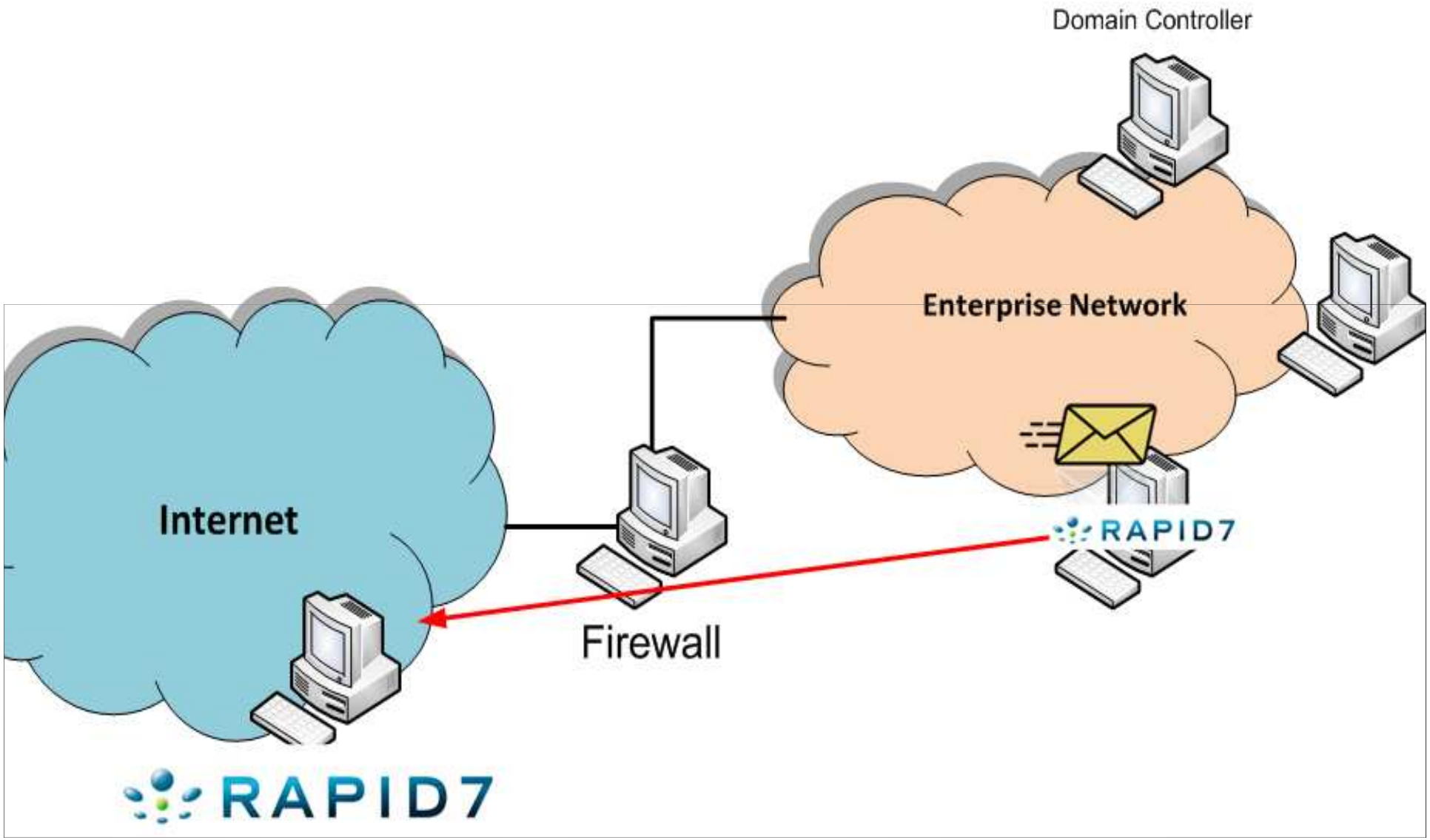
Phishing Attacks



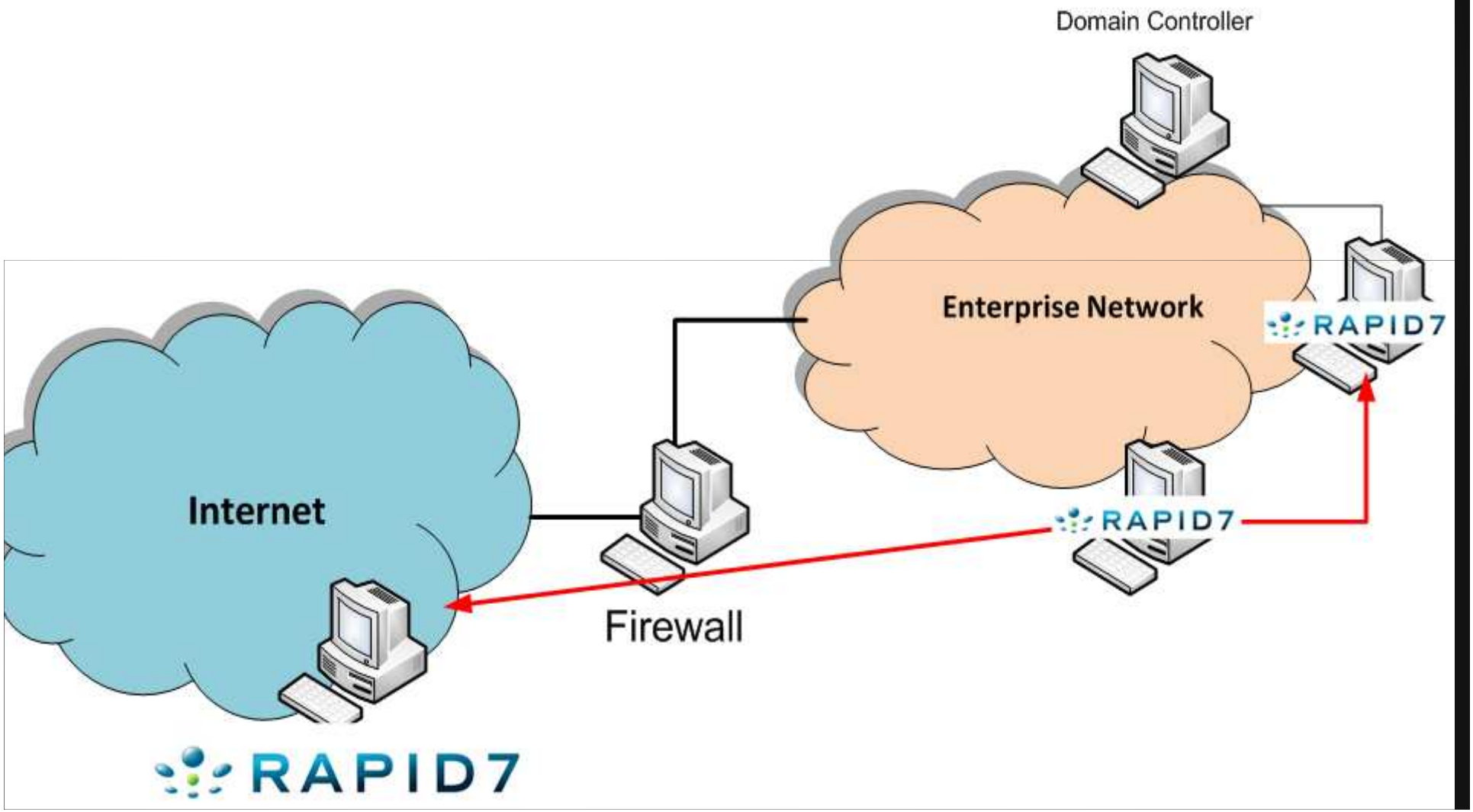
Malicious Executable (Egress Connection)



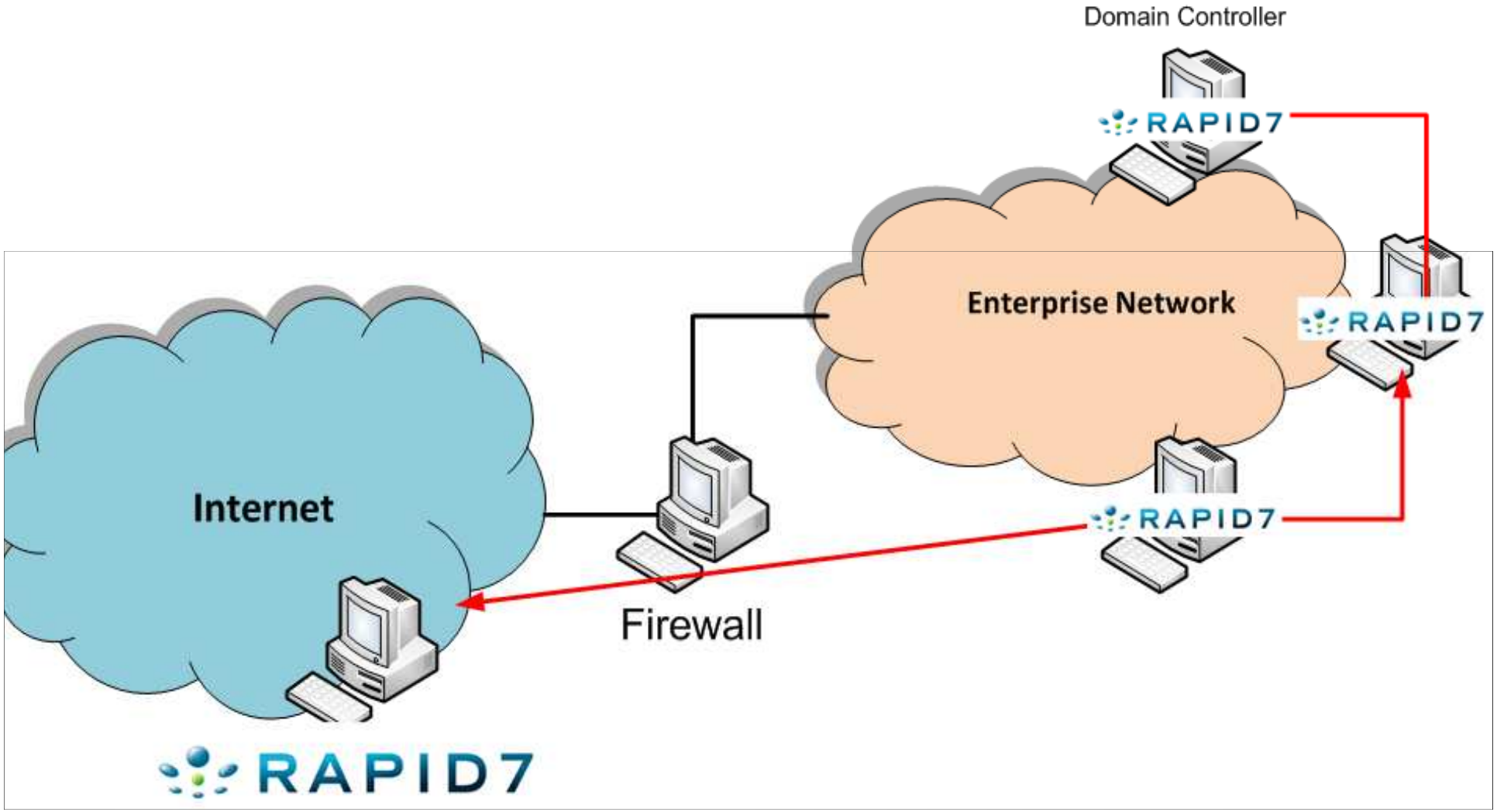
Internal Access



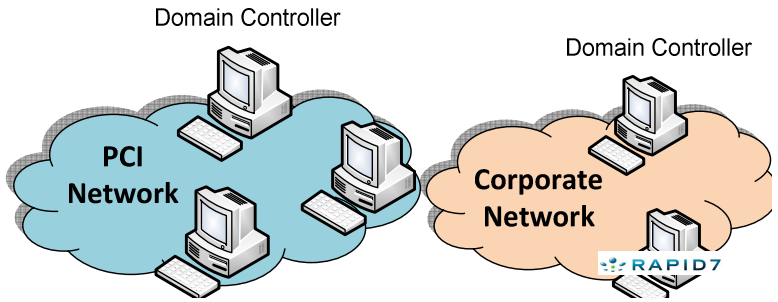
Pass-The-Hash

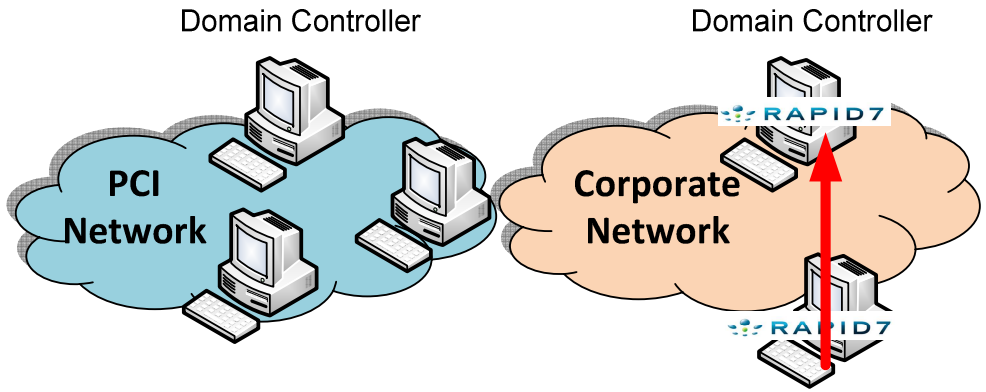


Pass-The-Hash (Domain Admin)



Internal Network Penetration Assessment – Customer X

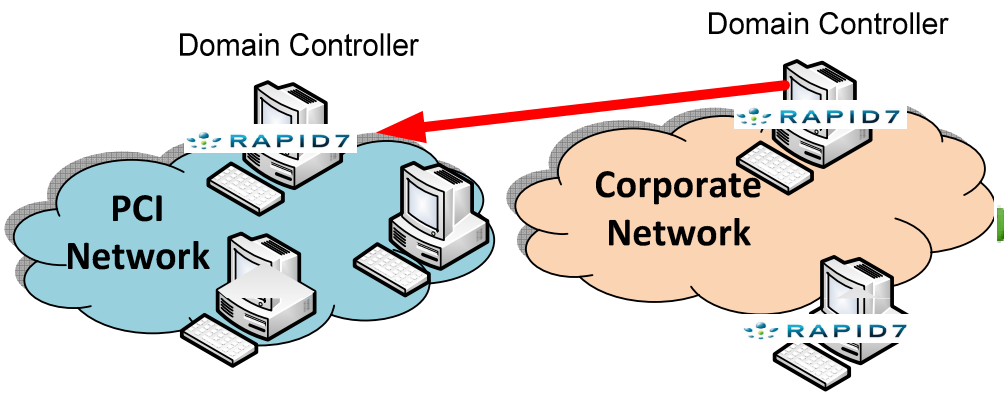




- Pass-The-Hash + Token Impersonation
- ARP Spoofing
  - Unclear-text protocols
- Weak passwords
- Unpatched systems
- Workstation Network was easy
- PCI Network was well protected

RAPID7

Internal Network Penetration Assessment – Customer X



- Added Admin Account onto PCI Network Domain Controller
- Inter-Domain Trust

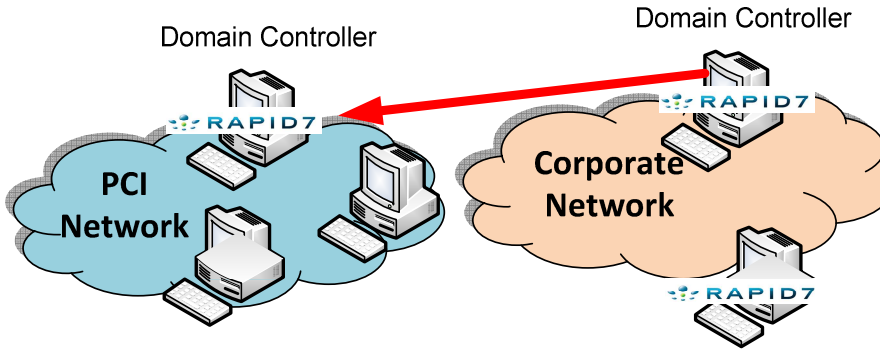
RAPID7

Agenda

- The need for a better approach
- Goal Oriented Overview
- Examples from the Field
- **Maturity 101**
- Secure Development Lifecycle (SDL)
- Summary/Q&A

RAPID7

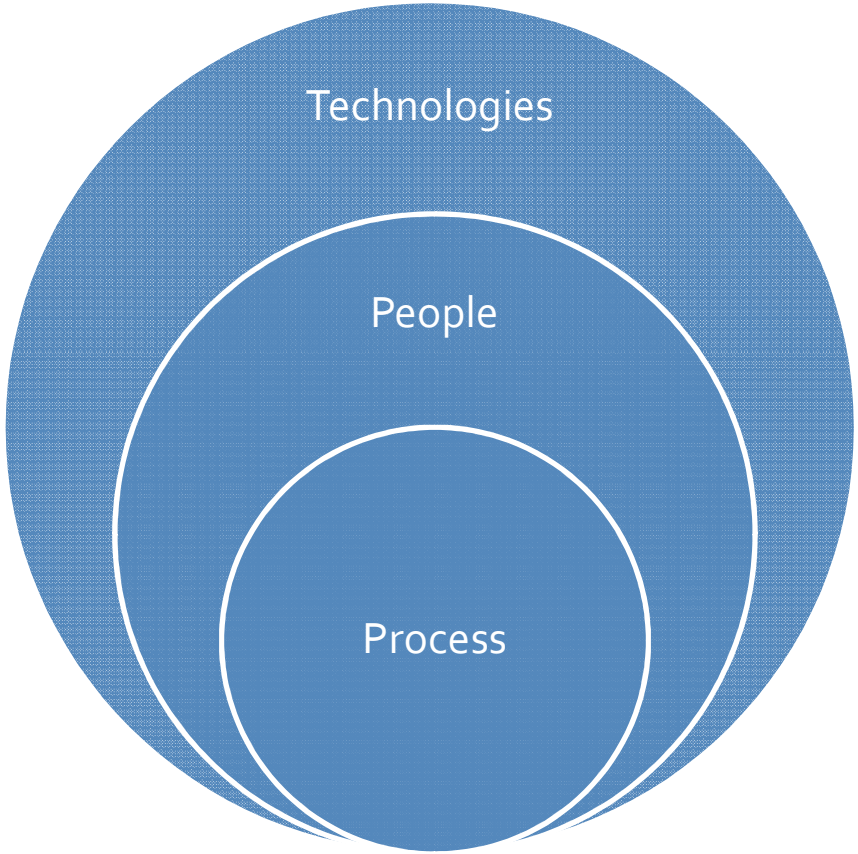
Goal Oriented Pentesting



- Explain the Process (Goal Oriented 101)
- Result of the penetration testing
  - Value security testing
  - Value of internal understanding the environment

RAPID7

Understanding the Environment



RAPID7

Understanding the Environment

If you don't understand the environment,
you probably won't be getting the most value
out of your security assessment

RAPID7

Security Testing

- Demonstrates risk in areas of weaknesses
  - (known areas of focus - critical systems
  - (unknown areas of focus - trust relationships, stepping stones)
- Which is more scary?
  - Known areas of focus
  - Unknown areas of focus

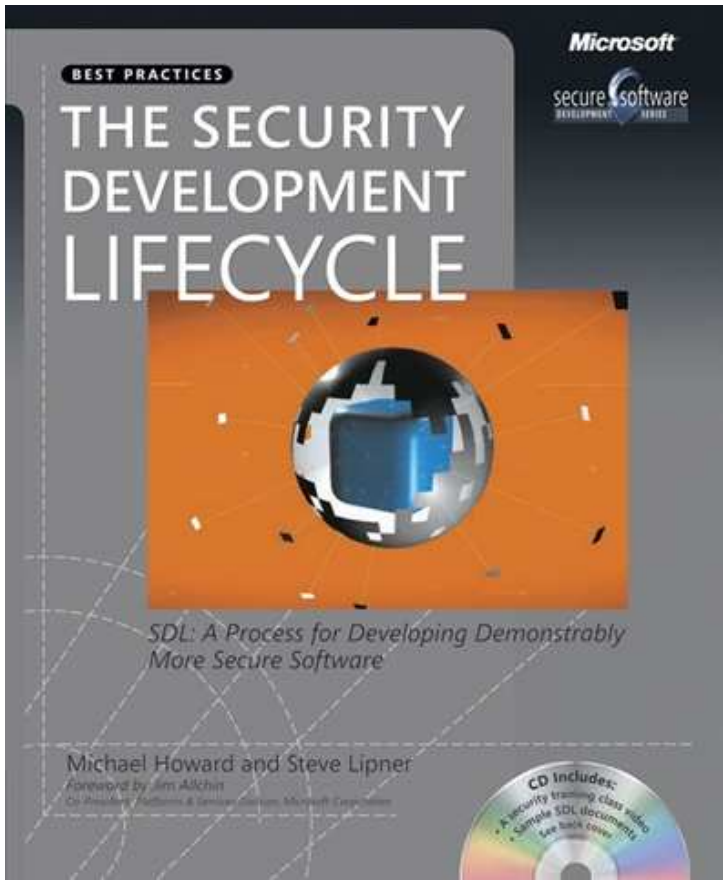
RAPID7

Agenda

- The need for a better approach
- Goal Oriented Overview
- Examples from the Field
- Maturity 101
- **Secure Development Lifecycle (SDL)**
- Summary/Q&A

RAPID7

Implementing Secure Development Lifecycle (SDL)



- Proactive Approach
- Reduce and limit the impact of vulns
- Incorporate security into the development process

RAPID7

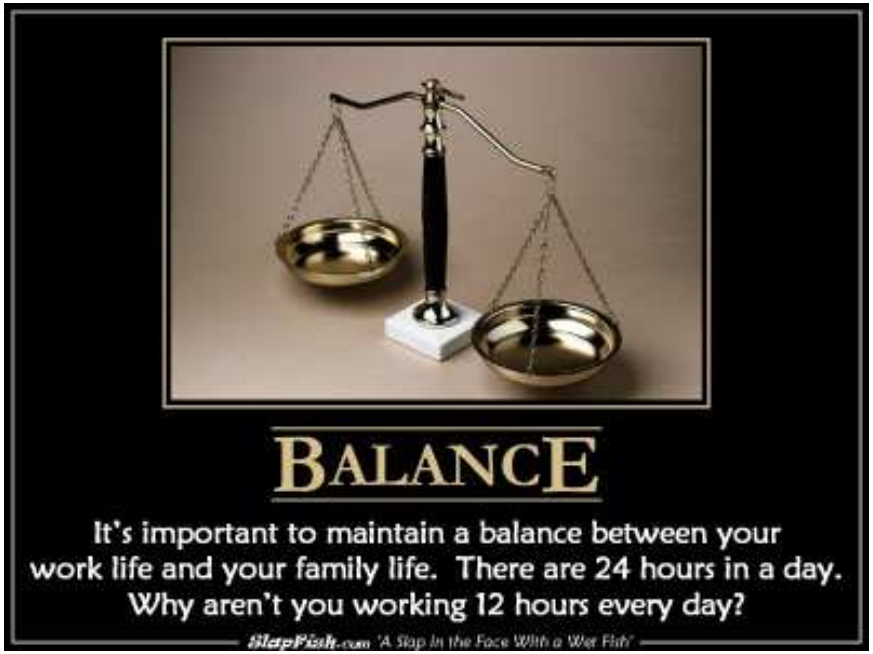
Effect of SDL

- Development process
- Resources Requirement
  - Process changes
  - Training
  - New policies/standards/guidelines
  - Third-party review

RAPID7

Is it worth doing?

- Rate of application development
  - Lines of code ? # new web apps over next 6-12 months?
- What type of data (stored, processed or transmitted)?
- Importance of the application(s) to the business?



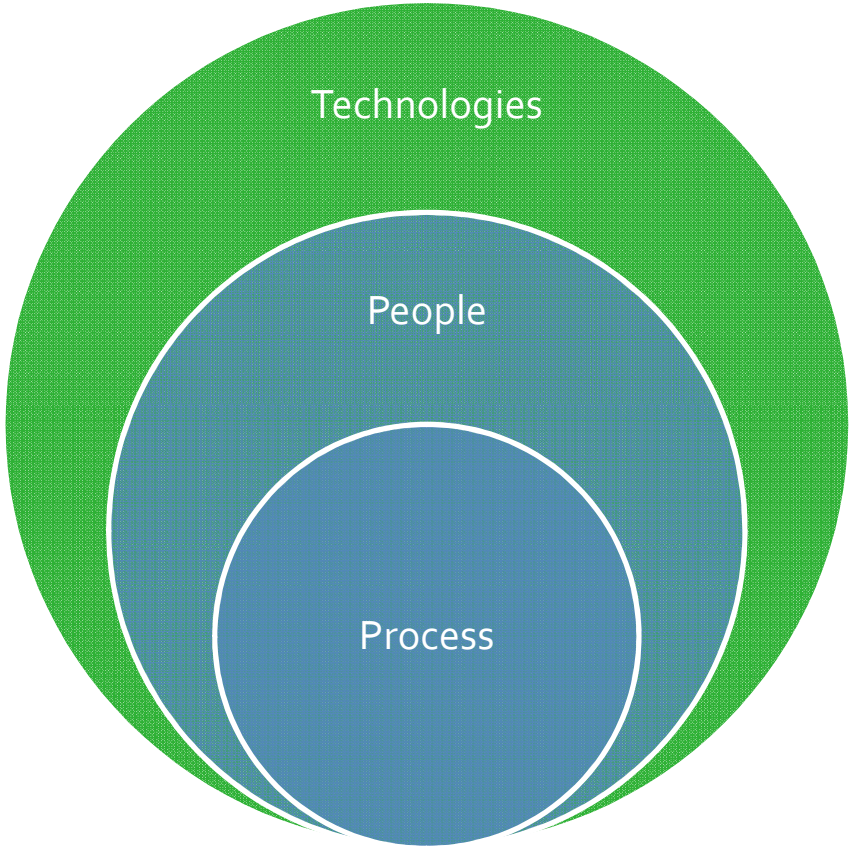
RAPID7

SDL Requirements

- Understanding
- Buy-in
- Requirements and Motivations
- Training

RAPID7

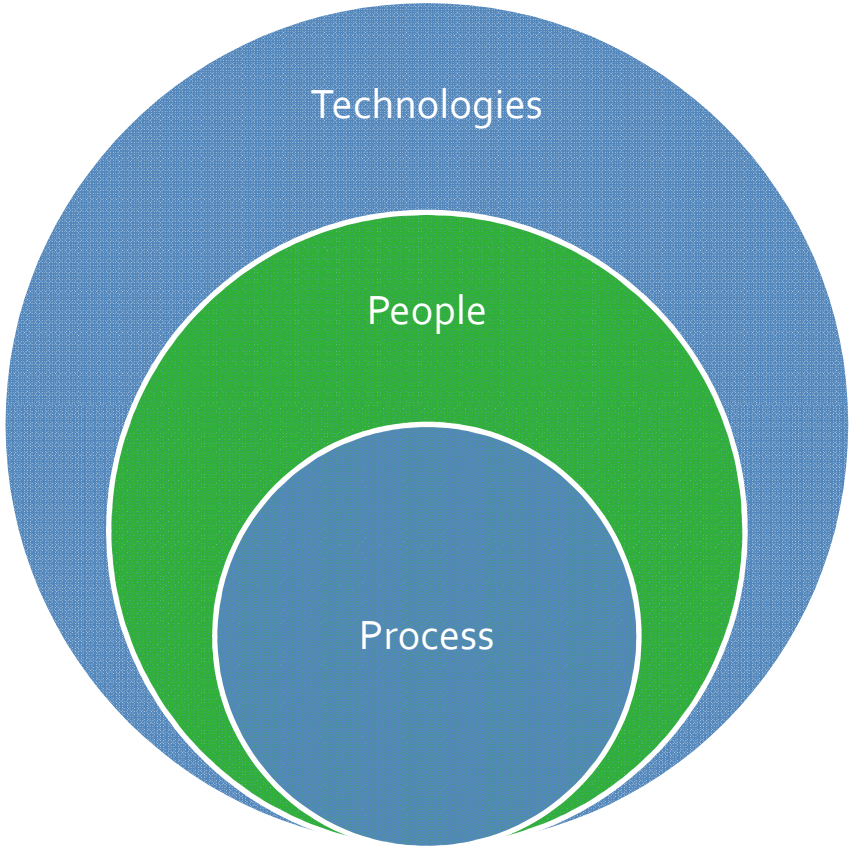
SDL – Technologies



- What types of applications are being developed ? (web apps, mobile etc.)
- What types of data do they store, process and transmit?
- What languages/frameworks are being used?

RAPID7

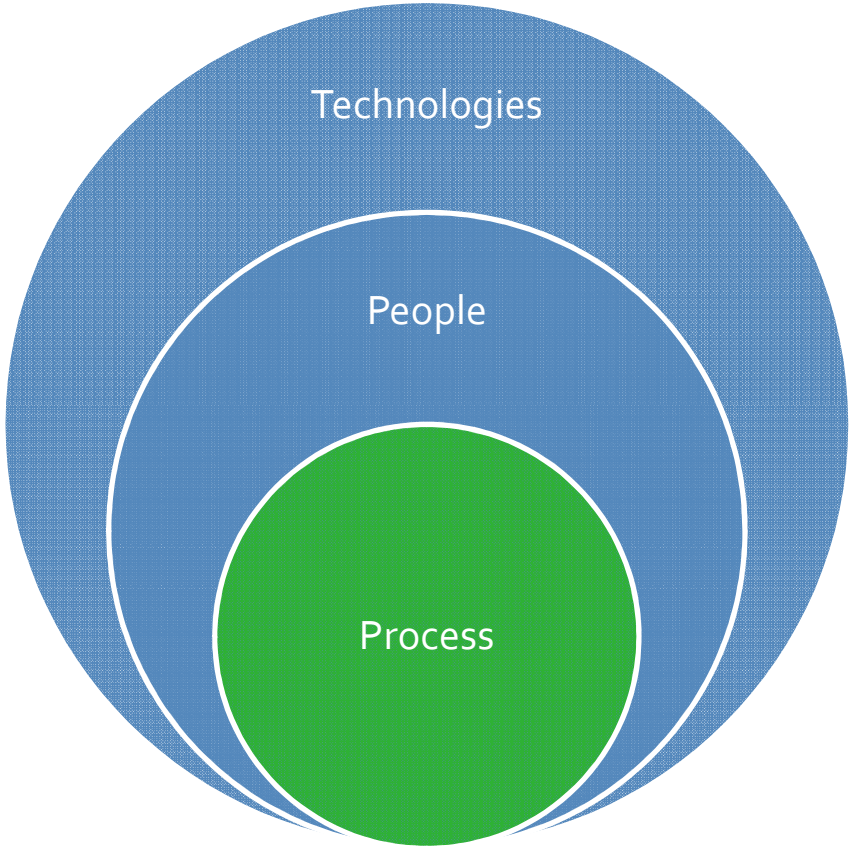
SDL – People



- Who/Where are the developers?
- How many Dev/QA/Release teams are there?
- Who is involved during development, testing, production?
- Who is involved in the transition between dev stages?

RAPID7

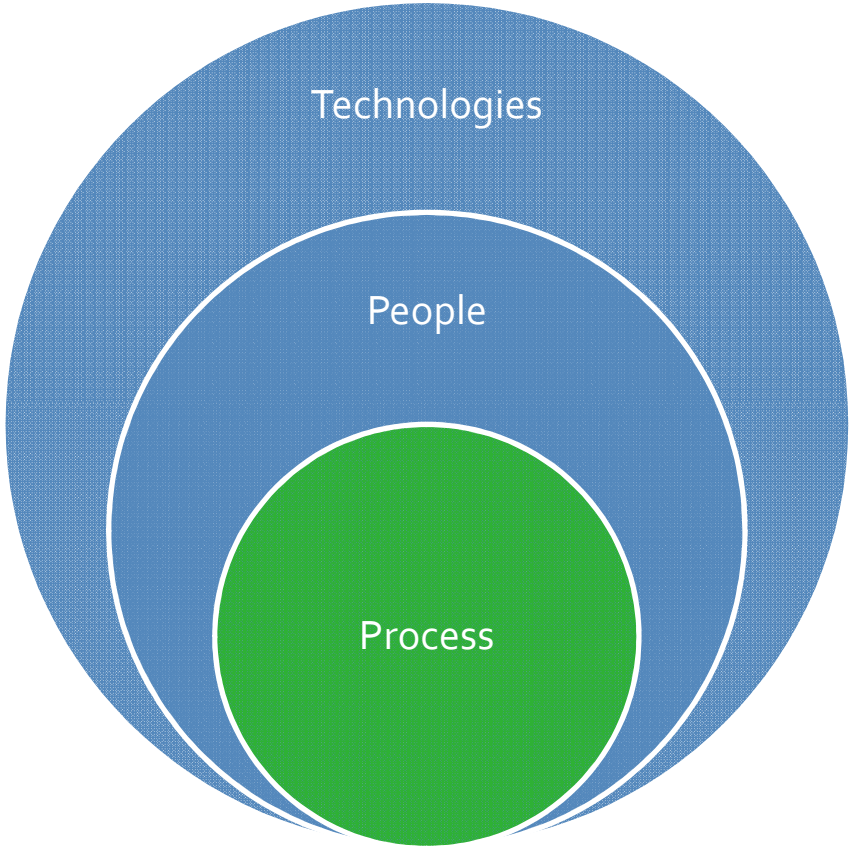
SDL – Process



- What is the process for building new custom apps?
- What development method is used?(Agile/Scrum, Waterfall, etc.)
- What are the stages of development?

RAPID7

SDL – Process



- What are the requirements before a product is ready to move from one stage to the next?
- Formal review occur before moving into production?

RAPID7

Agenda

- The need for a better approach
- Goal Oriented Overview
- Examples from the Field
- Maturity 101
- Secure Development Lifecycle (SDL)
- **Summary/Q&A**

RAPID7

Summary

- Understanding the Environment is very important to a creating a successful security program!
- Goal Oriented Penetration Testing - Strategic and Practical Methodology for Improving the ROI of any security assessment
  - Leverages project management ideals
  - Goals are not the only element of testing, only a place to start
- Slides will be posted online!

  http://spl0it.org/files/talks/rss10/Security_Immaturity.pdf

RAPID7

Discussion/QA

- How are you handling these problems from a (client or consultant) perspective ?
- Questions/Comments/Rants/Feedback

RAPID7

References

- http://spl0it.wordpress.com/2009/11/16/goal-oriented-pentesting-the-new-process-for-penetration-testing/
- http://spl0it.wordpress.com/2009/11/17/goal-oriented-pentesting-%E2%80%93-the-new-process-for-penetration-testing-part-2/
- M. Howard and D. LeBlanc. *Writing Secure Code*. Microsoft Press, 2nd edition, 2002.
- http://en.wikipedia.org/wiki/SMART_criteria

RAPID7

Comments/Questions?

- Joshua “Jabra” Abraham
  - Company: http://www.rapid7.com
  - Blog: http://spl0it.wordpress.com
  - Twitter: http://twitter.com/jabra
  - Jabra_aT_spl0it_d0t_org
  - Jabra_aT_rapid7_d0t_com

RAPID7