Goal Oriented Pentesting

Getting the most value out of Penetration Testing

June 15, 2010
About me

- **Joshua “Jabra” Abraham**
  - Joined Rapid7 in 2006 as a Security Consultant
  - Extensive IT Security and Auditing experience
  - Worked as an enterprise risk assessment analyst for Hasbro Corporation

- **Specializes in...**
  - Network Pentesting, Web Application Audits and Custom Code Development

- **Open-source code development projects**
  - Contributes to BackTrack LiveCD, BeEF, Nikto, Fierce, and PBNJ

- **Past speaking engagements**
  - BlackHat, DefCon, ShmooCon, Infosec World, CSI, OWASP Conferences, LinuxWorld, Comdex and BLUG

- **Twitter**: [http://twitter.com/jabra](http://twitter.com/jabra)
- **Blog**: [http://spl0it.wordpress.com](http://spl0it.wordpress.com)
How many times during a scoping call have you heard the customer say the goal of the assessment is to “Hack Us?”
“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”?
Agenda

- The need for a better approach
- Goal Oriented Overview
- Defining SMARTER Goals
- Methods for Success
- Examples from the Field
- Summary/Q&A
The primary objective of all assessments is to demonstrate risk.

Difference between a risk rating from a vulnerability scanner and a business risk is that a business risk takes into account the value of each asset.

Vulnerabilities are found by automated tools.

A threat does not have to be demonstrated in order to constitute a risk.
Vulnerability Management
- Identify vulnerabilities (False positives / False negatives)
- Risk of 10 Vulnerabilities compared to 1000
- Assign value to assets and data

Penetration Testing
- Demonstrating Risk

Methodology
- OSSTMM, OWASP etc
The need for a better approach

- How do you know what is MOST important?
- Achieve Domain Admin access on 1\textsuperscript{st} day
- Access to all data
- Maybe get lucky and guess right
- Shouldn’t need to guess
  - data X more valuable/important than data Y ?
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 - Pentester
- Malicious System Admin
- Malicious Employee
- Malicious Executive
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 common process
  - Outline a method to facilitate the testing process
  - Ensure assessment/project completion
Agenda

- The need for a better approach
- Goal Oriented Overview
- Defining SMARTER Goals
- Methods for Success
- Examples from the Field
- Summary/Q&A
Real-World Pentesting

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

- Pentesters – 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
Clear Motivation

- Emulate a Blackhat, by using Goals as motivation
- Doesn’t decrease the experience / 6th sense elements
- Allows the pentesting team to focus efforts on critical weaknesses
Goal Oriented Pentesting

- 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
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

Automated Testing
- Reconnaissance
- Port Scanning
- Vulnerability Scanning
- Exploitation

Central Storage Engine
- Correlation
- Reporting
- View/Modify/Delete Data

Manual Testing
- Context Based
- Focus Driven
- Goal Oriented
Agenda

- The need for a better approach
- Goal Oriented Overview
- Defining SMARTER Goals
- Methods for Success
- Examples from the Field
- Summary/Q&A
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
SMARTER Goals (S – Specific)

- What is involved?
  - Sharing of Data (customer and pentest team)
  - Completeness w/ Recon

- Internal Pentest
  - Access to Oracle database

- External Pentest
  - Access to the internal network via social engineering
How do you know when a goal is achieved?
Focus on systems that can lead to achieving the goal
Gain RW privileges
  - AAA table
  - BBB database
Gain access to 1+ domain admin accounts
Define goals based on the perspective of the assessment
- Limit goals to the most important areas

Example of a goal that is NOT attainable:
- Identify all risks within an application
SMARTER Goals (R – Relevant)

- Every goal in a penetration assessment should be focused on either:
  - Achieving access to sensitive data for the business
  - Demonstrating real world risks

- Example:
  - Gain access to the corporate ERP database containing sensitive information

- Keep in mind, that not all goals are data-centric
  - Create a DoS condition against the IPS or WAF
  - Deface a website
SMARTER Goals (T – Time-Bound)

- Nearly all assessments are time-bound
  - 1 day, 1 week, 1 month etc
- Limit the amount of time spent to achieve a goal
- Example:
  - Gain access to the internal network via wireless (limited 1 day).
- Time constraints may need to be adjusted
  - Goal is achieved sooner
  - Constraints are limiting progress
Discuss the status after amount of time.

- Time bound (x days or x weeks)
- Nothing is preventing progress (modify goals as needed)

Unique methods

- Sometimes there is a requirement for specific number of unique paths
- Demonstrate ease of exploitation and attacker’s flexibility
Discuss the status after goal completion
- Event bound

Access to the database was achieved, but SQLmap and SQLninja failed.

How long would it take to create a tool script kiddies could use?
Agenda

- The need for a better approach
- Goal Oriented Overview
- Defining SMARTRER Goals
- Methods for Success
- Examples from the field
- Summary/Q&A
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 Pentesting team
- Goals can be data-centric (but not always!)
Leveraging Unique Paths

- Success criteria for goals is to achieve them
- Demonstrating a specific number of unique paths
  - Provides a clear-view that weaknesses exist in many areas
- Will a pentest find all unique paths?
  - Not necessarily
  - Hit a point of diminishing returns
- Number of unique paths should be agreed upon with the scope
Agenda

- The need for a better approach
- Goal Oriented Overview
- Defining SMARTER Goals
- Methods for Success
- Examples from the field
- Summary/Q&A
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
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
Application Assessment – Sample Goals

- Gain access to:
  - A user’s account
  - An administrator’s account
    - Elevate the privileges of a user’s account
  - The application’s backend database

- Achieve and maintain undetected access for 24 hours
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.
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
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
Internal Network Penetration Assessment – Customer X

- Added Admin Account onto PCI Network Domain Controller
- Inter-Domain Trust
Internal Network Penetration Assessment – Customer Y

Detection - Automated Alerting

Domain Admin Access

Token Impersonation

Access to Domain Admin Token

Token Hunter

Pass-The-Hash

Local Administrator Hash

Password Cracking

Local Administrator Password

Access to 20+ servers

CIFS Login

BruteForce Attack

Several Weak passwords

Local Admin Access

MSSQL – Blank SA

Network Access

Server Access

Admin Access

Tomcat Manager

Unlocked Desktop
Agenda

- The need for a better approach
- Goal Oriented Overview
- Defining SMARTER Goals
- Methods for Success
- Examples from the field
- Summary / Q&A
Summary

- 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
- Whitepaper still in the works...
  - It will be released at Rapid7.com
References

Acknowledgements/Special Thanks!

- Rafal Los
- Chris Eng
- Zach Lanier
- Mike Bailey
- Marcus J. Carry
- Jack Mannino
- Will Vandevanter
- Rob Fuller
- Marcella Carby-Samuels
 Comments/Questions?

▶ Joshua “Jabra” Abraham

- Company: [http://www.rapid7.com](http://www.rapid7.com)
- Blog: [http://spl0it.wordpress.com](http://spl0it.wordpress.com)
- Twitter: [http://twitter.com/jabra](http://twitter.com/jabra)

- Jabra_aT_spl0it_d0t_org
- Jabra_aT_rapid7_d0t_com