The Blunderdome: An Offensive Exercise for Building Network, Systems, and Web Security Awareness

George Louthan, Warren Roberts,
Matthew Butler and John Hale

iSec™
The University of Tulsa
Institute for Information Security

Pre-Introduction: The Blunderdome

- Framework of vulnerable services and systems
- Educational, linear, goal-oriented offensive exercise using the framework
- Deployed twice: graduate course, high school interns
- Note: This is an education talk, not a testbed talk

Overview

- Cyber Security Exercises
- The Blunderdome exercise
  - Architecture / Framework
  - Network attack
  - Systems attack
  - Web attack
- Deployments
  - Graduate course
  - High school interns
- Lessons Learned
- Perspective on Offensive Exercises
- Conclusions

Background: Cyber Security Exercises

- Simulated activity involving cyber attack or defense
- Quick and dirty taxonomy:
  - Offensive vs. Defensive
  - Symmetric (both attack and defend) vs. Asymmetric (only one)
- Some examples
  - DEFCON CTF (Symmetric)
  - Collegiate Cyber Defense Competition; Service Academies' Cyber Defense Exercise (Asymmetric, Defensive)
  - OWASP WebGoat; Blunderdome (Asymmetric, Offensive)
- Frequently built for adaptability, flexibility, and exploration

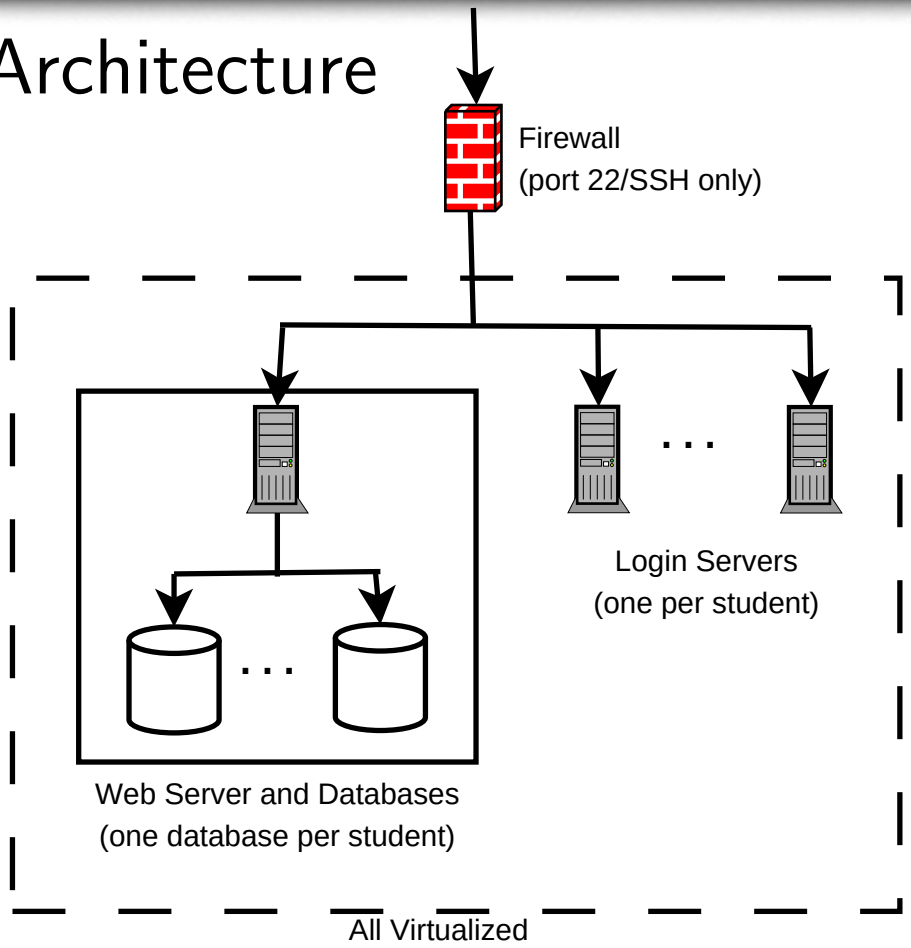
Blunderdome: Overview

- Obstacle course, not a sandbox
- Design goals:
  - Linearity
  - Goal-oriented design
  - Realism of services and vulnerabilities
  - Clear criteria for completion of stages
  - "Off-the-shelf" components
- Simulates an academic network and grades management system
- Scenario: change your grade

Blunderdome: Architecture

- Simulates a small, firewalled "academic network"
- Web Service (Grades management)
  - Username/password protected (not intentionally vulnerable)
  - SQL injection vulnerability for the grades table
- Login Server
  - Entry point to network
  - SSH key authentication only
  - Unpatched Ubuntu 7.10
  - Pre-configured with weak keys (CVE-2008-0166)
  - Root exploit vulnerability in kernel (CVE-2008-0600)
- Firewall (only permit SSH)

Blunderdome: Architecture



The Blunderdome architecture

Step 0: Set up

- Participants start with:
  - IP address
  - User name
  - SSH public key
- Instructed to:
  - Find the associated public key and log into the machine
  - Gain root, read a root-owned, root-readable file containing grades server credentials and address
  - Change your grade (an A is suggested)

Step 1: Network attack

- IP address and public key to login server are given
- Login server runs Ubuntu 7.10 - Debian OpenSSL bug caused weak keys (CVE-2008-0166)
- Keyspace was only 32,767 possibilities.
- Intended to require coding, but Googling worked as well
- Result: user-level access to login server on "internal" network
- All further actions staged from the login server (SSH tunneling)

Step 2: Systems attack

- Vulnerability (CVE-2008-0600) in vmsplice shipped with Ubuntu 7.10
- Local root privilege escalation exploit available
- Credentials and address for web service read from root-owned, non-public file

Step 3: Web attack

- Very simple homegrown web service
- Internal access only (users tunnel via login server)
- "Check Grades" button that submits a hidden field that is concatenated into an SQL query

Summary of Stages

Stage	Precondition	Attack	Proof
Gain remote user access	SSH public key available (given)	Break weak public key	Create a user-owned text file
Gain root access	User-level access	Execute `vmsplice` privilege escalation	Create root-owned text file
Change grade	Address and credentials for web service	Execute SQL injection	Altered grade in database

Deployment: Graduate Course

- Developed originally for *Information Systems Security Engineering*
  - Course on security engineering and secure software development
  - Vulnerability-related topics on buffer overflows, weak cryptographic protocols, and web vulnerabilities
- Some objectives:
  - Illustrate examples of classes of attacks described theoretically
  - Drive discussion regarding engineering causes of vulnerabilities
  - Reinforce potential for flaws on multiple levels of the stack
- Assigned as a week-long project at end of term

Lessons: Graduate Course

- First issue: problem with student *buy-in*
- Term-end project: limited opportunities for discussion
- Needed tighter lecture integration
- Security is easy. SSH is hard.

Deployment: Interns

- Deployed again to summer interns from high schools (juniors and seniors)
- Some goals:
  - Crash-course introduction to security
  - Assess interns' general technical knowledge
  - Use as a motivator to teach general systems and network knowledge
  - Disillisionment
- Assigned to about 6 students with a graduate student supervising

Lessons: Interns

- Interns learned:
  - Linux command line
  - Asymmetric key cryptography
  - Secure shell and tunneling
  - Network fundamentals
  - GNU toolchain and compiling other people's code from source
  - Vocabulary and exploit/vulnerability taxonomy
  - ...

Lessons: Interns

- Total non-issue: buy-in
- In fact, buy-in was a huge advantage
- Big issue: hand-holding required

Offensive Exercises

- Offensive exercises are controversial in academia
  - Ethics concerns (We don't want to be a "hacker school".)
  - Perception concerns (We don't want people to *think* we're a "hacker school".)
- Nevertheless, we advocate targeted, educational offensive exercises (as well as ethics), particularly for:
  - Penetration testing
  - Security engineering
  - Network operations
- Drives enthusiasm

Conclusion

- Blunderdome: offensive, asymmetric, linear, cross-sectional exercise
- We still believe in all of those properties
- Useful to drive enthusiasm for building general knowledge (intro or survey course) - catch them young
- Needs tight lecture integration
- Overall, demonstrated the usefulness of offensive exercises in coursework

Future Work

- Focus on curriculum integration
- Future expansion to:
  - Interns
  - Information Systems Security Engineering
  - Secure Electronic Commerce
  - Using a real testbed?

Q & A

Acknowledgment.
This material is based on research sponsored by DARPA under agreement number FA8750-09-1-0208. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, or DARPA or the U.S. Government.