CSE 4481
COMPUTER SECURITY LAB

Mark Shtern

Introduction

Security

- Our life depends on computer systems
  - Traffic control
  - Banking
  - Medical equipment
  - Internet
  - Social networks
- Growing number of attacks on computer systems

Security

- Hacker may not be a computer expert
  - Numerous attacking scripts / tools available
  - Hacker training material also available

Security

- Results from malicious attack
  - Financial loss
  - Loss of reputation
  - A drop in the value of a company's stock
  - Legal issues

Statistics (2009)

- 85% of attacks were not considered highly difficult
- 96% of breaches were avoidable through simple or intermediate control
- 48% involved privileges misuse
- 86% of victims had evidence of the breach in their log files

http://www.verizonenterprise.com/DBIR/2009/

Statistics (2013)

- 78% of attacks were not considered highly difficult
- 13% involved privileges misuse
- 75% of attacks were opportunistic

http://www.verizonenterprise.com/DBIR/2013/

Method of Entry (2013)

- 47% → Remote Access
- 26% → SQL Injection
- 18% → Unknown
- 2% → Client-Side Attack
- 2% → Remote File Inclusion
- 3% → Remote Code Execution
- 1% → Authorization Flaw
- 1% → Physical Theft

Trustwave 2013 Global Security Report

Method of Entry (2014)

- 31% → Weak Passwords
- *25% → Unknown*
- *12% → File upload flaw*
- *10% → Vulnerable off-the-shelf software*
- *8% → SQL injection*
- *6% → Phishing*
- *4% → Authorization flaw*
- *4% → Remote file inclusion, physical access or directory traversal*

Trustwave 2014 Global Security Report

Spam (2014)

- 59% of malicious spam included attachments
- 41% of malicious spam included malicious links
- 70% of inbox mail was spam

Trustwave 2014 Global Security Report

Intrusion to Containment (2013)

- 5% → >2Years
- 14% → 2Years
- 25% → 181-365 Days
- 20% → 91-180 Days
- 27% → 31-90 Days
- 4% → 10-30 Days
- 5% → <10 Days

Trustwave 2013 Global Security Report

Statistics (2014)

- 71% of victims did not detect a breach themselves
- 67% of victims were able to contain it within 10 days
- The median number of days between the date of the initial intrusion and detection of the breach was 87 days
- The median number of days between the date of the initial intrusion and containment of the breach was 114 days

Trustwave 2014 Global Security Report

Course Objectives

- Hands on experience in various security topics
  - Execution of popular attacks
  - Attack prevention and risk mitigation

Attack Examples

- Network (sniffing, session hijacking)
- Password Cracking
- Web
- Code injection
- Overflows (Buffer, Number)

Defence Techniques

- Auditing
- Vulnerability scanners
- Firewalls (Network and application)
- Intrusion Preventions and Detections
- Honeypots

Administrivia

Marking Scheme

- The performance of the students will be evaluated as a combination of
  - 7 labs (18%)
  - Term Project (67%)
  - Project presentation (5%)
  - Game (5% + bonus)
  - Participation (5%)
- Labs are worth 3%
  - Lab mark:
  - 1 → at least 50% + lab participation
  - 2 → at least 75% + lab participation
  - 3 → 100% + lab participation

Labs

- Completed task must be demonstrated to the instructor
- Lab reports are optional
- The lab report must be a short, precise and professional document (title, table of contents, page numbering etc)
- The lab report must contain sufficient evidence that you completed the lab exercise
- Code developed during the labs is expected to be **simple**
- Developed applications are **prototypes**

Report antipattern

- Screenshots are attached
  - Figure number? Figure description?
- "I verified DNS configuration using nslookup"
  - How? Evidence?
- "I created a folder named 'xxx' and gave read/write and execute permission ..."
  - How? Evidence?
- "I developed a script ..."
  - Evidence? Script source code?

Term Project

- Project consists of four phases
  - Implementation
  - Security testing
  - Fixing security bugs
  - QA phase
- Developed application is a **final product**
- The project report must be a detailed, precise and professional document (title, table of contents, page numbering etc)

Report Antipattern

- Design is just a list of functions
- Design justification : “The design is flexible”
  - Why is the design flexible?
- Test case : “Run the application”
  - What are the user inputs?
    What are the expected results?

Game

- Developer
  - Project presentation
- QA
  - Review project design
  - Penetrate other projects
- IT Security
  - Secure infrastructure

Lab 1

Lab1

- Bandit game
- Social Engineering