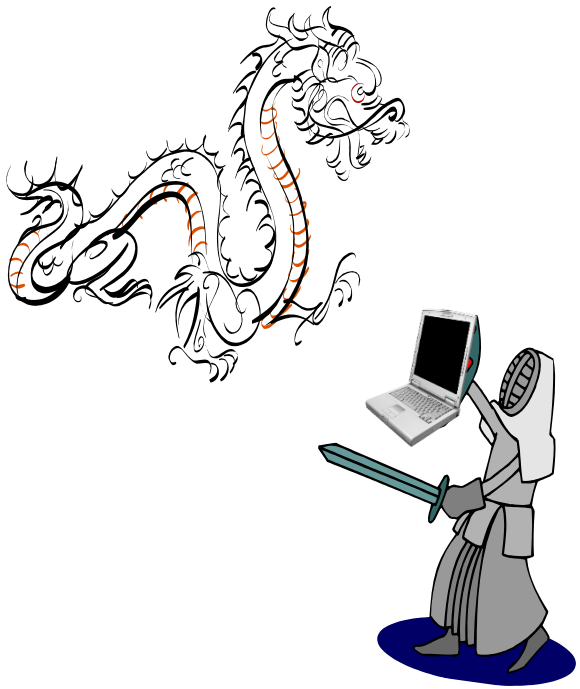
Penetration Testing



Penetration Testing

- Types
  - Black Box
    - Less productive, more difficult
  - White Box
    - Open, team supported, typically internal
    - Source available
  - Gray Box (Grey Box)
    - Mixture of the two
- Methods
  - Automated
  - Manual
  - Hybrid

Penetration Testing

- We are considering White Hat hacking
  - Ethical hacking
- But to do that, we have to act like an attacker
- How security engineers treat the test cycle
- Even if it's your own software
- You are not doing feature testing

What Do You Need?

- A site that is hopefully dedicated to your test
  - Because you are going to work it over
  - Always try to work on a site that is a duplicate of the production environment
  - But not a production system
- Tools at your disposal
- Knowledge
- A plan
- A bad attitude
  - The site is weak and you can prove it
  - You're going to kick bits and take names

Test Parts

- Preparation
  - Goals, scope, tool collection, permissions, documents
- Testing
  - More to come
- Reporting
  - Permanent, possible legal
  - Executive summary, intro, findings, conclusions
  - Criticality, type, scenario, mitigations
- Presentation
  - Optional, educational, potential for confrontation

Document Flow (Ethical Hacking)

- Statement of Work (SOW)
  - Typically details what parts of the app you are going to test
  - What you are to deliver
  - Your responsibilities to the customer
- Scoping document
  - Filled in by the customer
  - Tells you things about the system and the application that will make it easier and faster to get started
- Threat Model - helps you decide what to test
- Test Plan – what you intend to test, not how
- Pen Test Report – what you found out

SOW

- Who you are
- Who we are
- Outline of the work description
  - This implies that we already know something about the app
- Limitations on our work
- Deliverables
- Dates
- Contract completion criteria
- Cost
- Signatures

Scoping Document

- Demographics of the app
  - Known threats
  - Assets to be protected by the app
  - Architectural design
- System Information
  - Components
  - Users and roles
  - Interfaces and entry points
  - Authentication model
  - Authorization model
  - In scope/Out of scope
  - Languages

Scoping Document

- Network information
  - Domain IP
  - Network architecture
  - In scope/Out of scope
- System information
  - IP addresses
  - Operating System
  - Web Server, DNS server, other services
  - File system structure
  - In scope/Out of scope

Threat Model

- Yet to come
- Describes the threats to your system
- A prescriptive process for finding threats
- Almost always done after a preliminary hands-on test of the application

Test Plan

- Given the threats, what are you going to test

Test ID	Test Title	Test Description	Result
1	Login SQL Injection	Test for SQL Injection in the login process	
2	Secure SSL	Check that the SSL crypto algorithms are secure	
3	Cookie HttpOnly	Check that HttpOnly flag is set on all cookies	

- There could be hundreds of these or maybe thousands

Outline of Testing

- Now you are the attacker
  - You may have some privileged information to make life easier, but you need to proceed as though you don't
- Your attack will follow the following process
  - Reconnaissance and mapping
  - Discovery
  - Exploitation

What the Attacker Sees

- Servers and clients
- Operating systems
- Application servers
- Exchanges of data/protocols
  - TCP, SSL/TLS
  - HTML, HTTP
  - Authentication methods
  - Session management schemes
  - Forms data processing
  - Database access
- How much they know depends on the situation

Reconnaissance

- Identify the infrastructure
- Identify servers
- Detect the operating systems
- Profile the servers
- Detect software configurations
- Using external sources

Discovery

- Automated searching
- Vulnerability specific searching
- Manual searching

Exploitation

- Pivoting
  - Gather private data
  - Use it for more discovery
- Bypassing protections
- Injection attacks
- Session attacks

Manual Testing

- Tester processes each part of the app
- Scripts and tools are used
- Slooooooowwwww

Automated Testing

- One or more scanners are used
  - HPWebInspect
  - Paros
  - Burp
  - Cenzic Hailstorm
  - skipfish
- Fast
- Still takes a long time
- Thoroughness still controllable

What Next?

- For each of the tasks, there are methods and tools
- We (you) are going to do a series of labs to get familiar with the process
- The object of your attack will be DVWA
- And the tools will be from Samurai WTF
- These may not be the optimal set of tools, but it's a start.
- You are encouraged to look into other tools and try them