

# Penetration Testing

## Exploitation and Reporting

May 2009

# Overview

## Exploitation

The Goal of the Exploitation Phase

Types of Exploitation

Tools for Executing Exploits

Top Security Vulnerabilities

## Reporting

The Need for Reporting

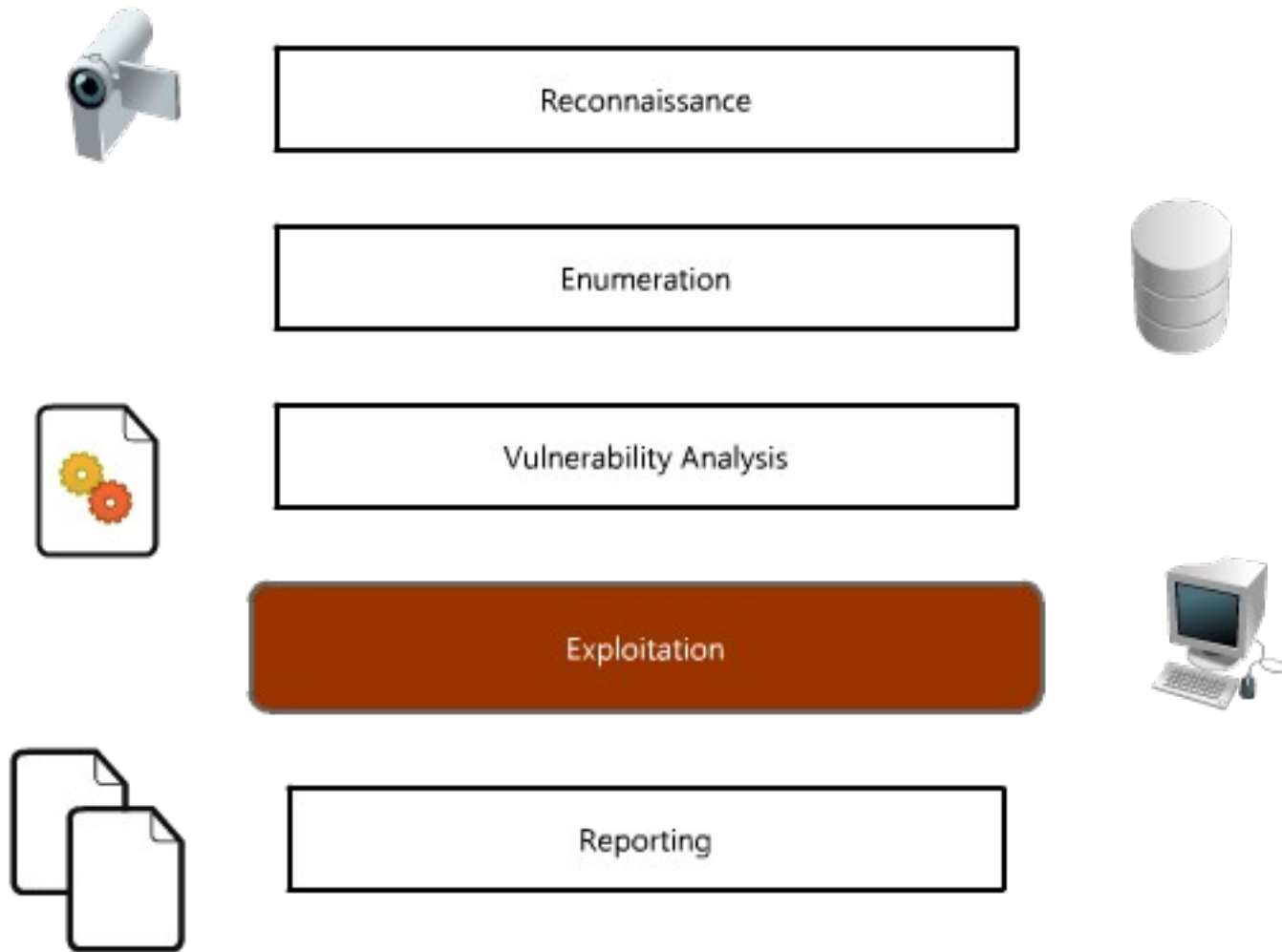
What to Include

Risk Analysis

Compiling the Report

Examples

# Exploitation Phase



# The Goal of Exploitation

To identify points of failure and vulnerabilities which constitute risk to :

Confidentiality

Integrity

Availability

# Types of Exploitation

- Software Systems
- Network
- Web
- Social
- Configuration
- Physical

# Software Exploitation

- Takes the output of the Vulnerability Analysis Phase and attempts to exploit the vulnerabilities discovered.
- Relies on bugs and logical oversights within the software systems.
- Examples:
  - Buffer Overflows (jill)
  - Directory Traversal (double decode & unicode)
  - Brute Forcing SMB Password Guessing

# System Exploitation

ENUMERATION

GAINING ACCESS

ESCALATING PRIVILEGE

PILFERING

COVERING TRACKS

CREATING BACK DOORS

DENIAL OF SERVICE

Attempt to access the target

Seek to gain SU access

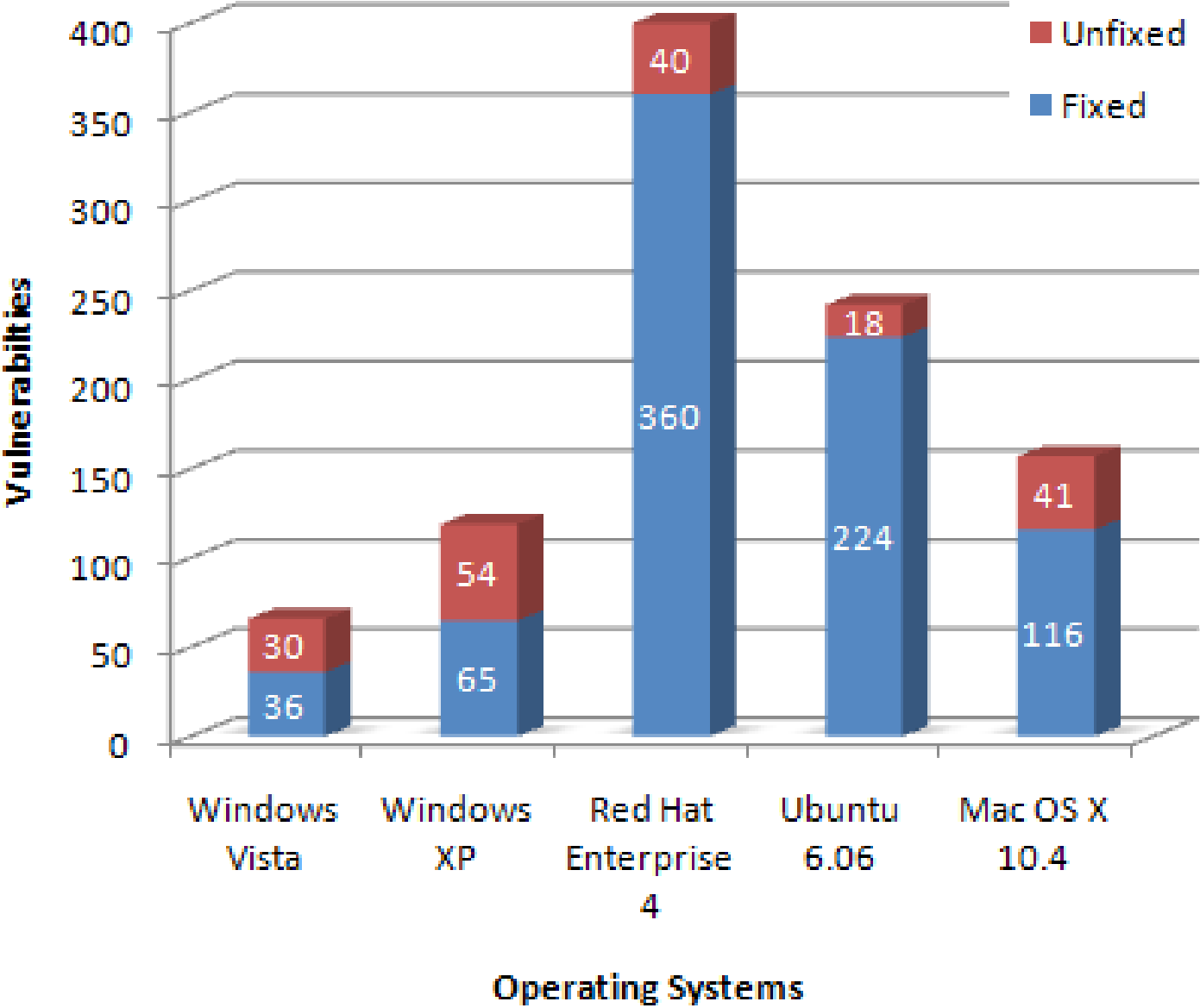
Gather confidential data

Remove audit trail

Ensure future access

Disable target

# OS Vulnerability Report 2008



# Network Exploitation

- Relies on unsecured networks, lack of encryption and/or access to open network cables.
- Eavesdropping | Packet Sniffing | Traffic Analysis
- DNS poisoning, DOS and DDOS
- Protocol Vulnerabilities
  - e.g.: Microsoft PPTP with MS-CHAP relying on weak cryptographic functions.

# Web Exploitation

- SQL Injection
- Script Injection
- Web Directory Browsing
- Web Field Overflow
- XXS
- SSI (Server Side Includes) Injection

# Social Exploitation

- Makes use of data obtained through social engineering from the Active Reconnaissance phase.
- Use employees names to aid in brute force attacks.
- Gauge degree to which policy is adhered to via social engineering during a blind and/or double blind penetration test.
- Often overlooked, yet can be more damaging than an unpatched network service.

# Configuration Exploitation

- Unchanged, default configuration presents a security risk.
- Commonly overlooked.
- Examples:
  - Default MySQL password
  - Default Wireless Router configuration
  - Default Router Password
  - Default OS firewall settings

# Physical Exploitation

- Information security is useless if the physical security which protects it is lacking.
- Penetration Testing may include attempts at physical security breach.
  - Examples:
    - Tailgating
    - Unsecured network cables
    - Unattended terminals
    - Poor visitor procedural enforcement
    - Lack of monitoring
    - Lack of fire and gas detection

# Tools for Exploitation

- **Metasploit**
  - <http://www.metasploit.com>
- **List of Common Pentesting Tools**
  - <http://www.webhackingexposed.com/tools.html>
- **AirCrack, Hydra**
- **Penetration Testing Framework**
  - <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
- **Default Password Lists**
  - <http://www.vulnerabilityassessment.co.uk/passwords.htm>

# Top Security Vulnerabilities

## **# 14**

Lack of accepted and well-promulgated security policies, procedures, standards and guidelines.

## **# 13**

Inadequate logging, monitoring, and detection capabilities at the network and host level.

## **# 12**

Unauthenticated services allowing users to capture remote keystrokes.  
E.g. : X Windows

# Top Security Vulnerabilities

## # 11

Excessive trust relationships can provide access to sensitive systems. (NT Domain Trusts, .rhosts, hosts.equiv)

## # 10

Excessive file and directory access controls. (NT shares, UNIX NFS exports)

## # 9

Unpatched, outdated or unconfigured software.

# Top Security Vulnerabilities

**# 8**

Misconfigured firewall or router ACL.

**# 7**

Misconfigured Internet servers, especially CGI scripts, and anonymous FTP with world-writable directories.

**# 6**

User or test accounts with excessive privileges.

# Top Security Vulnerabilities

**# 5**

Weak, easily guessed, and reused passwords.

**# 4**

Hosts running unnecessary services. (E.g.: FTP, DNS, Samba, SMTP, NFS)

**# 3**

Information leakage (application versions, finger, telnet, rusers, etc..)

# Top Security Vulnerabilities

## # 2

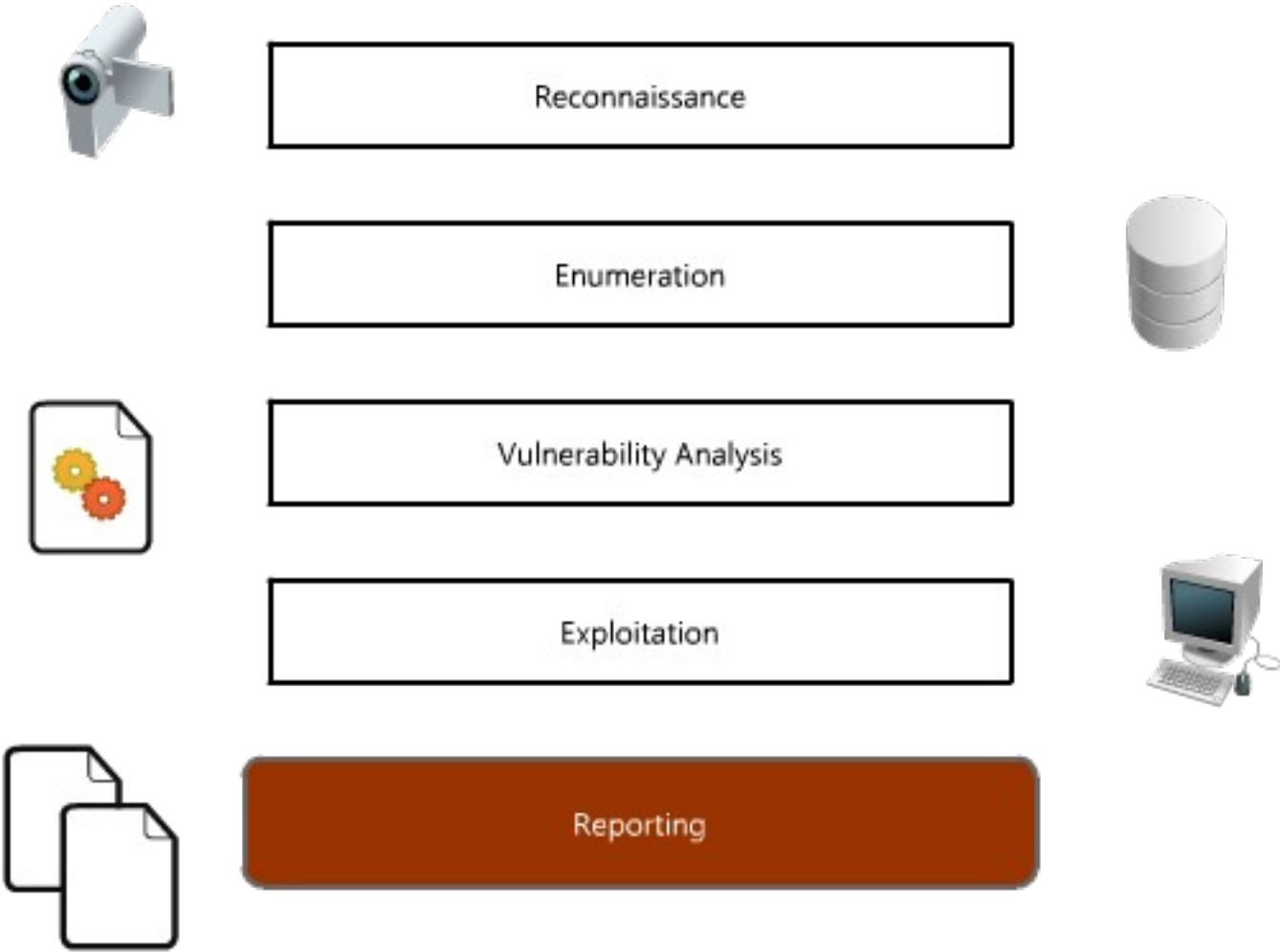
Unsecured and unmonitored remote access points provide one of the easiest means of access to the network.

## # 1

Inadequate router access control:

- Misconfigured router ACLs can allow information leakage through ICMP, IP, NetBIOS etc...

# Reporting Phase



# Reasons For Reporting

- Share Findings
- Provide awareness and promote understanding of the state of the security environment.
- Findings are used to draw conclusions, from which security practices can be refined and improved.
- Historical audit trail of the security environment.
- Guiding document for upper management.

# What to Include

- Vulnerabilities of the system
- Gaps in security measures
- IDS and Intrusion Response Capability
- Whether anyone is monitoring audit logs
- How suspicious activity is reported
- Suggested countermeasures

# Risk Analysis

## **Vulnerability**

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or violation of the system's security policy.

## **Threat**

The potential for a particular threat-source to successfully exercise a particular vulnerability.

# Risk Analysis

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

As the risk calculations are completed, they can be prioritized for attention, as required.

From this, appropriately selected countermeasures can be identified and applied.

# Risk Rating Schemes

## Likelihood and Consequences rating

Likelihood		<u>Consequence</u>	
Rare (very low)	<b>E</b>	<u>Insignificant</u> (low – no business impact)	<b>1</b>
<u>Unlikely</u> (low)	<b>D</b>	Minor (low – minor business impact, some loss of confidence)	<b>2</b>
Moderate (medium)	<b>C</b>	Moderate (Medium – business is interrupted, loss of confidence)	<b>3</b>
Likely (high)	<b>B</b>	Major (High – business is disrupted, major loss of confidence)	<b>4</b>
Almost Certain (very high)	<b>A</b>	<u>Catastrophic</u> (High – business cannot continue)	<b>5</b>

# Risk Rating Schemes

## ANZ 4360 Risk Levels

	<u>Consequence:</u>				
	<u>Insignificant</u>	Minor	Moderate	Major	<u>Catastrophic</u>
Likelihood:	1	2	3	4	5
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D ( <u>unlikely</u> )	L	L	M	H	E
E (rare)	L	L	M	H	H
E	Extreme Risk: <u>Immediate action required</u> to mitigate the risk or decide to not proceed				
H	High Risk: Action should be taken to compensate for the risk				
M	Moderate Risk: Action should be taken to monitor the risk				
L	Low Risk: Routine acceptance of the risk				

# Compiling the Report

## **Executive Summary**

A high-level overview of the findings and recommendations of produced by the penetration test.

## **Categorise Threats by:**

- Physical Security
- Network Security
- Application Security
- Operations Security
- Legal Compliance

## Executive Summary

Briefly describe the activities of the assessment.

Talk about the importance of information security at the client organization.

Discuss security efforts that the organization has under taken.

Highlight three major security issues discovered that could significantly impact the operations of the organization.

### *Top-Ten List*

A top-ten list is used to highlight the ten most urgent issues discovered during an assessment. Clients unfamiliar with security may be overwhelmed by a long list of problems. Putting the major issues together may allow the client to easily focus efforts on these problems first.

The list below contains the “top ten” findings, weaknesses, or vulnerabilities discovered during the site security assessment. Some of the issues listed here are coalesced from more than one section of the assessment report findings. Additional information about each is provided elsewhere in the report.

It is recommended that these be evaluated and addressed as soon as possible. These should be considered significant and may impact the operations of the [CLIENT ORGANIZATION].

#### **1. Information Security Policy**

An information security policy is the primary guide for the implementation of all security measures. There is no formal policy specific to the [CLIENT ORGANIZATION].

**Recommendation:** Develop an information security policy that specifically addresses the needs of the [CLIENT ORGANIZATION] and its mission. Use that policy as a basis for an effective security program.

#### **2. {Security Issue #2}**

[Brief description of Security Issue #2]

**Recommendation:** [Brief list of recommendations for Security Issue #2]

#### **3. {Security Issue #3}**

[Brief description of Security Issue #3]

**Recommendation:** [Brief list of recommendations for Security Issue #3]

#### **4. {Security Issue #4}**

[Brief description of Security Issue #4]

**Recommendation:** [Brief list of recommendations for Security Issue #4]

## **{State the Vulnerability}**

### **Explanation**

[Explain the vulnerability.]

### **Risk**

There are several risks in not having [this vulnerability].

- [Provide a list of risks.]

### **Recommendations**

- [Provide a list of recommendations].

## **Network Security**

Describe the state of network security at the client organization.

List public network resources and sites.

List partner connections and extranets.

### ***Vulnerabilities***

Listed below are the network security vulnerabilities discovered during the assessment. These are considered significant and steps should be taken to address them.

### **The {CLIENT ORGANIZATION} systems are not protected by a network firewall**

#### **Explanation**

A firewall is a network gatekeeper. Based on a configurable set of rules, the firewall determines which network connections to allow or deny. There are generally three types of attacks that can be prevented (or at least slowed) using properly configured firewalls: intrusion, denial-of-service, and information theft.

There are two types of firewalls. One type is incorporated into operating systems (software-based). The other type consists of a networking hardware platform that protects a group of networked systems (hardware-based).

The {CLIENT ORGANIZATION} systems are inconsistently protected by software-based firewalls. Most of the workstations have firewall software installed and configured. Some do not.

#### **Risk**

There are several risks in running network services without a firewall.

- Incoming network-based scans and attacks are not easily detected or prevented.
- Attackers target vulnerable network services.

**Confidential and Proprietary Information: Need to Know**

The End