Penetration Testing

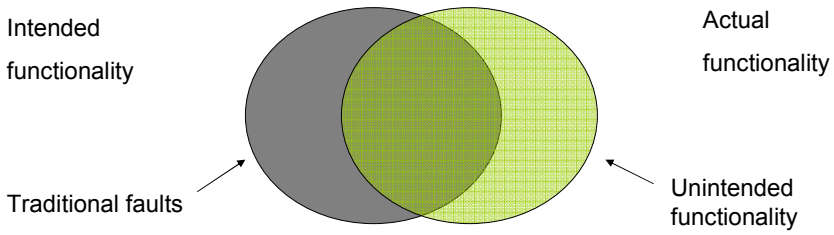
Gleneesha Johnson
Advanced Topics in Software Testing
Fall 2004

Security Testing

- Method of risk evaluation
- Testing security mechanisms to ensure that their functionality is properly implemented
- Identifying risks in a system and creating tests driven by those risks

Security Testing vs. Traditional Testing

- Traditionally test for specification violations
- Security bugs typically manifest as side effects



Why Security Test?

- Any piece of software containing a security flaw can make a secure environment vulnerable to an attack
- Increasing exploits of vulnerabilities in systems show that there are growing needs to develop more secure software

Security Testing Techniques

- Penetration testing ***
  - Focus of this presentation
- Formal Methods
  - Use mathematical description of system and specifications to prove it meets security requirements
- Syntax Testing
  - Feed exceptional input values to the software and observe the security aspects of the resulting behavior
- Fault Injection
  - Insert faults into the environment to determine response
- Gligor's testing method
  - Eliminates redundant test cases

Penetration Testing

- Practice of simulating real-world attacks by discovering and exploiting software, system, and network vulnerabilities
- Normally performed by a specialized team of experts called a *tiger team*

Motivation

- Allow an organization to assess its security posture
- Allow vulnerabilities to be addressed before they are exploited
- Marketing tool
- Can be used to promote awareness amongst non-technical executives
- Can be used to test computer emergency response teams and Intrusion Detection Systems

Testing Models

- Zero-knowledge attack
  - performed by testers who have no real information about the target environment
  - designed to provide the most realistic penetration test possible
- Full-knowledge attack
  - performed with the tester having as much information about the target environment as possible
  - designed to simulate an attacker who has intimate knowledge of the target organization's systems - such as a real employee.

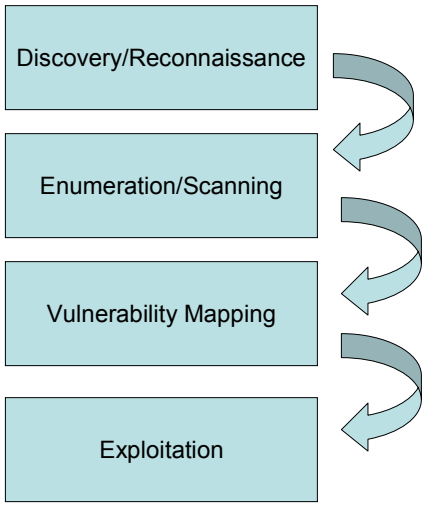
Things To Consider

- What will be done with information after test has been performed
- Methods used to limit unintentional damage to networks and/or systems
- Internal vs. External testing team
- Attack profile of potential threat sources

Potential Threat Sources

- **Script Kiddie**
  - Has limited or no knowledge of how computer systems work. Rely on pre-written exploits and vulnerability scanners to find and exploit vulnerabilities.
- **Master Cracker**
  - Has intimate knowledge of IT technology and system code. They find original vulnerabilities, write customized exploits and spend much of their time learning and finding flaws in new technology.
- **Malicious Insider**
  - Doesn't necessarily know much about IT systems but does know a lot about YOUR system. This enables them to attack a system at its most vulnerable point.
- **Naive employee**
  - Generally damages IT systems through an inability to correctly operate even the most simplest applications.

Methodology



Discovery/Reconnaissance

- Goal is to obtain as much information as possible about the target organization
- Helps to build a picture of the target organizations
- Often considered the most important (yet overlooked) component of zero-knowledge attacks
- If testing performed with initial information, this step is based (not replaced) on that information

Discovery/Reconnaissance Cont.

- Common Tools
  - Nslookup (Available on Unix and Windows Platforms)
  - Whois (Available via any Internet browser client)
  - ARIN (Available via any Internet browser client)
  - Dig (Available on most Unix platforms and some web sites via a form)
  - Web Based Tools (Hundreds if not thousands of sites offer various recon tools)
  - Target Web Site (The client's web site often reveals too much information)
  - Social Engineering (People are an organizations greatest asset, as well as their greatest risk)

Nslookup

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Gleneesha Johnson>nslookup
Default Server:  VTOT.proxy.aol.com
Address:  205.188.146.146

> www.hotmail.com
Server:  VTOT.proxy.aol.com
Address:  205.188.146.146

Non-authoritative answer:
Name:    www.hotmail.com.nsatc.net
Addresses:  207.68.171.233, 207.68.172.239, 207.68.173.245
Aliases:  www.hotmail.com
```

Whois

Enumeration/Scanning

- Gain as much information as possible about entities found during discovery
- Goal is to identify potential targets for security holes and vulnerabilities of the target host or network.
- Identify live (accessible) systems
- Scan for open ports and services on the target host(s) or network

Enumeration/Scanning Cont.

- Tools
  - Nmap
  - Telnet
  - Hping2
  - Netcat

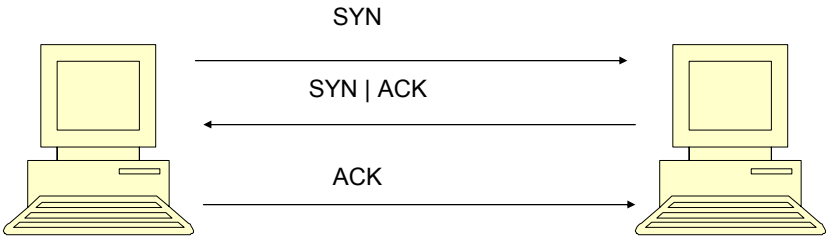
Telnet

```
Connected to www.notarealdomain.org.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Date: Mon, 13 May 2002 21:43:56 GMT
Server: Apache
Location: http://www.notarealdomain.org/newlook/home.php
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>301 Moved Permanently</TITLE>
</HEAD><BODY>
<H1>Moved Permanently</H1>
The document has moved <A
HREF="http://www.notarealdomain.org/home.php">here</A>.<P>
<HR>
<ADDRESS>Apache/1.3.24 Server at www.notarealdomain.org Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
```

TCP Side Note



Scan Types

- SYN
- FIN
- Xmas Tree
- NULL

Nmap

```
-=[toolbox]=- -9:54pm- ~# nmap -sS -v -v -P0 -p 53 ns1.mytestlab.net
 Starting nmap V. 2.54BETA33 ( www.insecure.org/nmap/ )
Host ns1.mytestlab.net (192.168.107.66) appears to be up ... good.
Initiating SYN Stealth Scan against ns1.mytestlab.net (192.168.107.66)
The SYN Stealth Scan took 62 seconds to scan 1 ports.
Interesting ports on ns1.mytestlab.net (192.168.107.66)
Port       State      Service
53/tcp     filtered   domain
 Nmap run completed -- 1 IP address (1 host up) scanned in 62 seconds
```

Vulnerability Mapping/Assessment

- Goal is to identify all potential avenues of attack
- Use information from previous phases to map specific system attributes against publicly available sources of vulnerability information
  - Bugtraq
  - Computer Emergency Response Team (CERT) advisories
  - vendor security alerts

Vulnerability Categories

- High
  - Can jeopardize host or network security if exploited
  - Present threat to organizations integrity
- Medium
  - Usually present a nuisance , but not nearly as serious as high
- Low
  - Usually commonplace
  - Can't be exploited to directly gain access to network resources

Exploitation

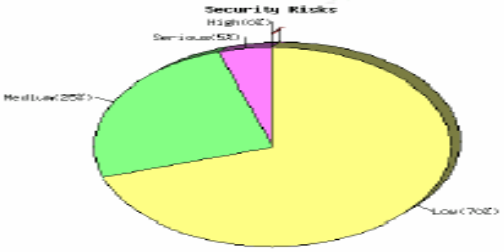
- Goal is to attempt to compromise the network by leveraging the results of the vulnerability analysis, following as many avenues identified as time allows
- Can be done manually
- Can be done using automated tools
  - Nessus

Nessus

The Nessus Security Scanner was used to assess the security of 1 host

- 2 security holes have been found
- 35 security warnings have been found
- 42 security notes have been found

PART I : GRAPHICAL SUMMARY :



Nessus

- unknown (53/tcp) (Security warnings found)
- unknown (135/tcp) (Security warnings found)
- unknown (139/tcp) (Security hole found)
- unknown (443/tcp)
- unknown (445/tcp)

Nessus

Vulnerability found on port unknown (139/tcp)

It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access. To prevent null sessions, see MS KB Article Q143474. Note that thid won't completely disable null sessions, but will prevent them from connecting to IPC$
All the smb tests will be done as "/" in domain

Problems

- Testing is based heavily on the experience of the tester
- The results of a test only provide a snapshot of a system's security at a given time
- No well defined and tested criterion used to decide when to stop penetration testing

Questions?