What Can Go Wrong During a Pen-Test?

Chad Schieken
Manager, Business Risk Services
Grant Thornton LLP

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

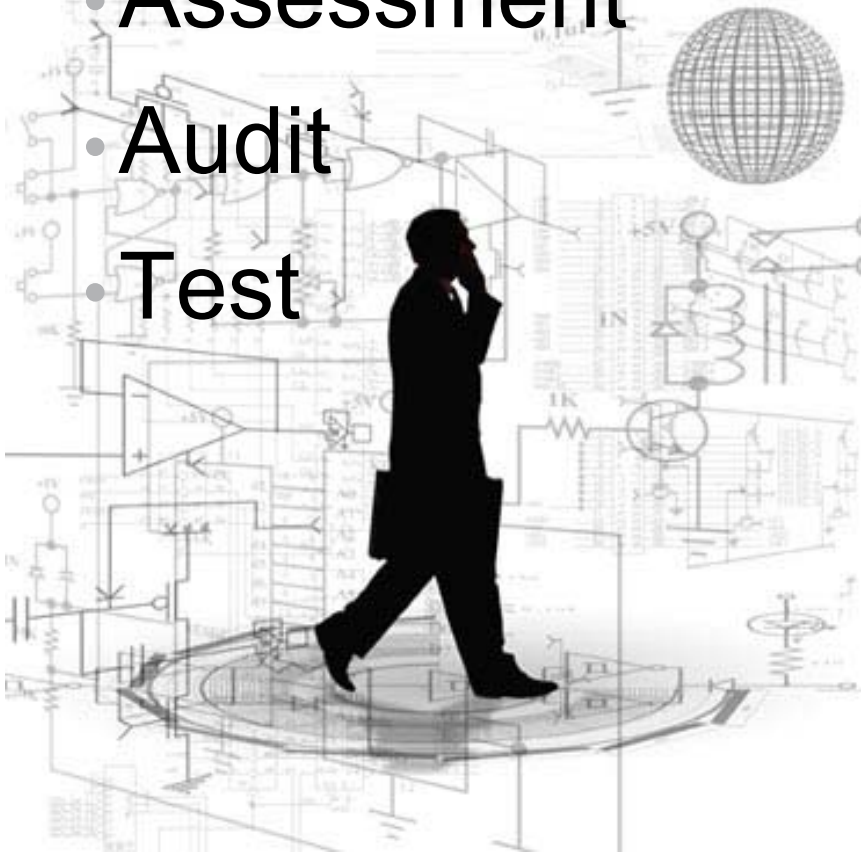
shared knowledge • shared power

encompass

AN HP USER GROUP

Terms

- Zero Knowledge
- Exploit
- 0-Day
- Vulnerability
- Assessment
- Audit
- Test



How Systems Are Compromised??

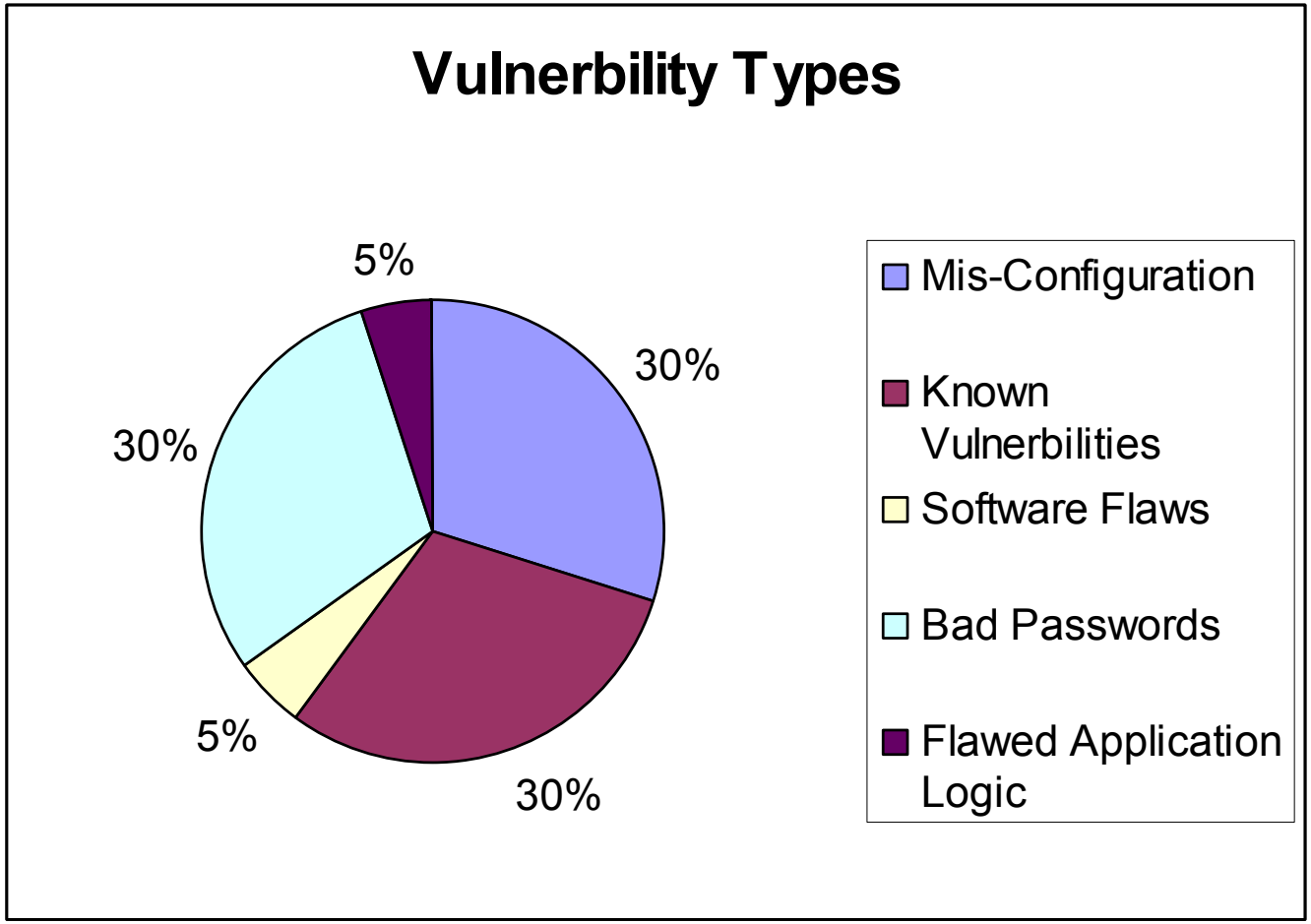


Chart for illustration only, not based on study data

Typical Pen-Testing Methodology

- Footprinting
  - Discovery phase
  - How an attacker learns about a network.
  - Compared to a burglar “casing” a retail establishment. determine active devices and what services are running on those device. "doorknob rattling"
- Reconnaissance
  - Researching the target network and systems using publicly available information.
  - American Registry for Internet Numbers (ARIN), and WHOIS for technical information related to DNS and network addressing.
  - Google search engine
- Enumeration
  - Expanding a folder or a service to obtain more details.
  - For example, after discovering a Windows NT domain, identifying a list of user accounts, shares, groups etc. for a particular device or network.
- Exploitation
  - Can involve “brute force” guessing of passwords
  - Tools and utilities are used to gain control of the system and/or network.

An Example of “Information Leakage”

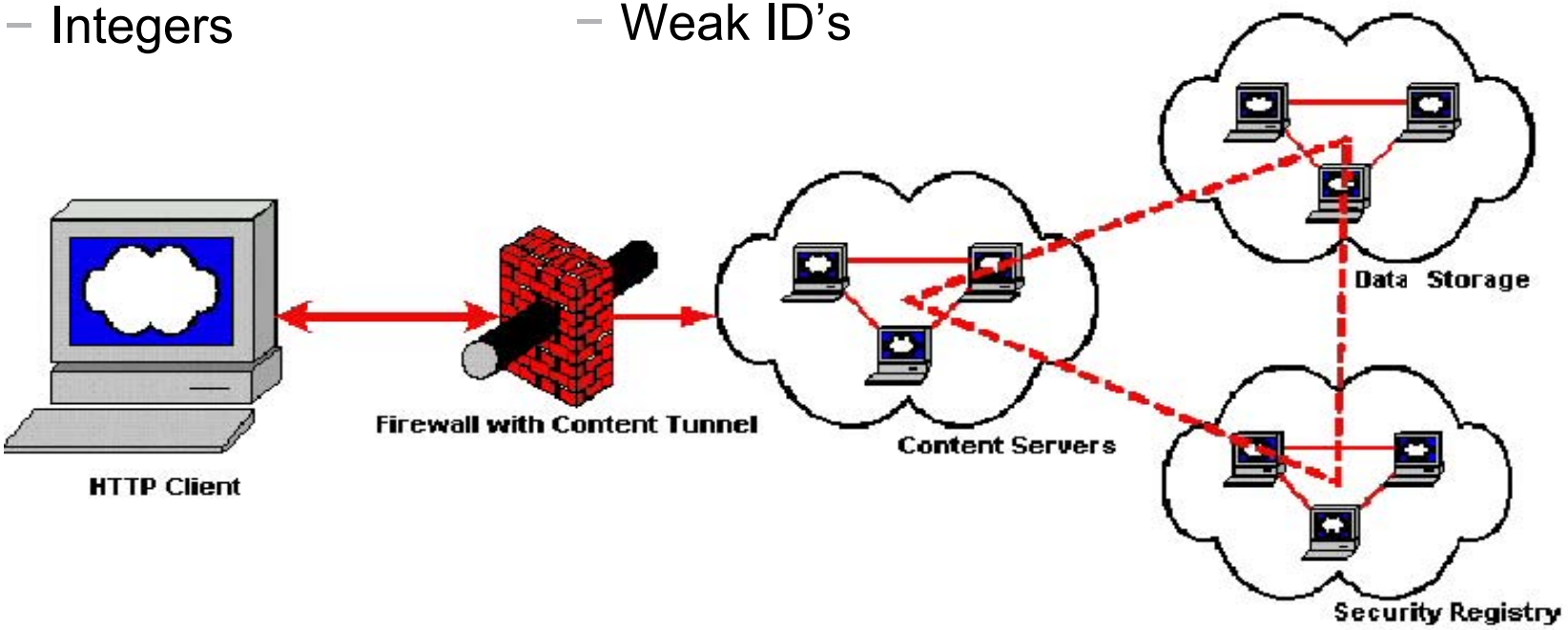
```
cschieke@somehost cschieke]$ telnet  www.BigCo.com 80
Trying www.BigCo.com...
Connected to BigCo.com on Port 80
Escape character is '^]'.

HEAD /

HTTP/1.1 401 Access Denied
Server: Microsoft-IIS/5.0
Date: Thu, 19 Jun 2003 16:00:39 GMT
WWW-Authenticate: Basic realm="10.1.1.6"
Content-Length: 4431
Content-Type: text/html
```

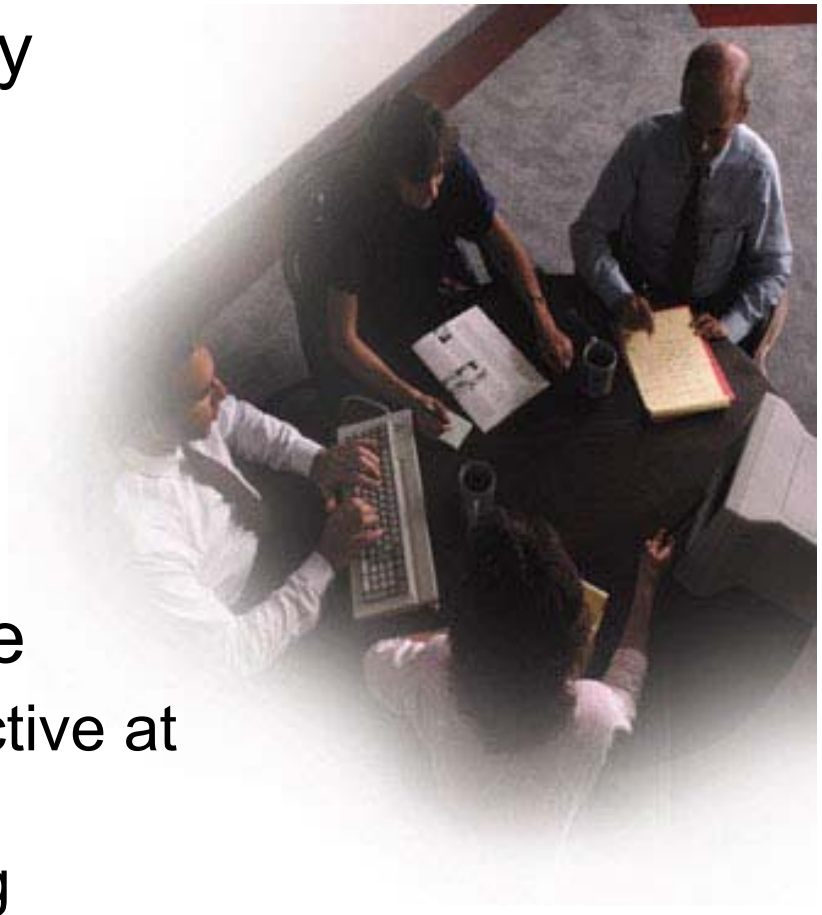
Application Security

- Input Validation
  - SQL Injection
  - Off-by-one
  - Integers
- Session
  - Session Fixation
  - Timeout
  - Weak ID's
- Access Control
  - Weak Enforcement
  - Privilege Leaks
  - Implemented?



Measuring Business Value

- Inadequate ways to quantify results:
  - We exploited 100 Systems
  - We compromised 500 Gig of Critical Business Data
  - We found 1000 High Risk Vulnerabilities
- Qualifying more appropriate
  - Security Infrastructure ineffective at stopping attacks
  - Business data obtained using commonly available tools
  - Avoid: “It was easy”



Return on Investment

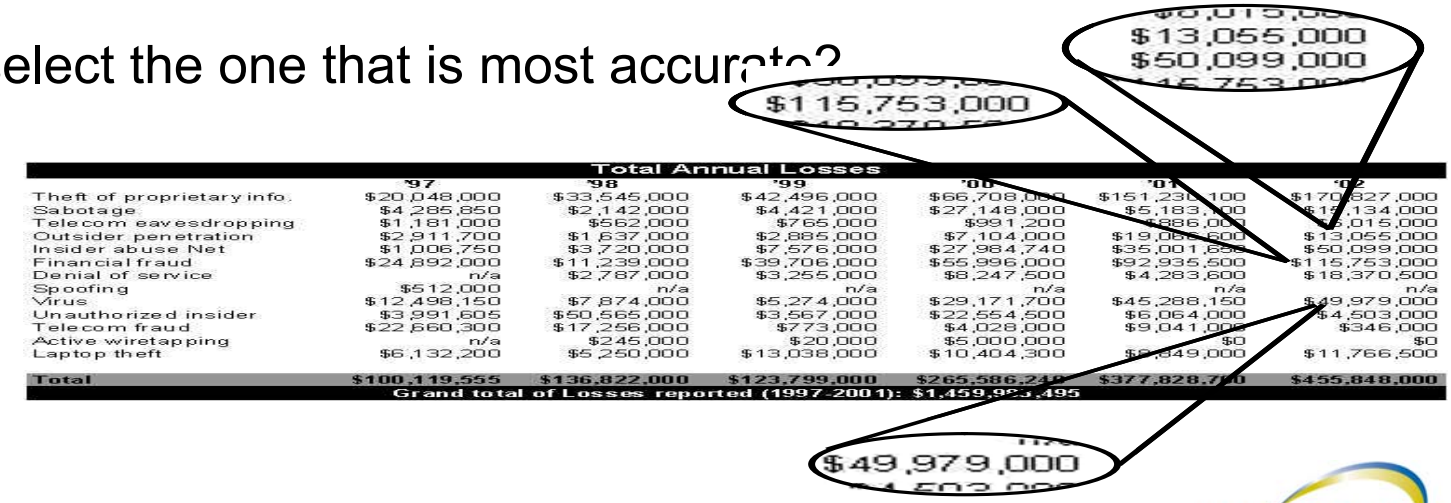
- Classic ROI doesn't work
- Does the Classic Definition Apply?

  A. "We saved over $100,000 in carrier costs by switching to IPsec VPN"

  B. "We saved over $100,000,000.00 by finding and fixing vulnerabilities in the transaction processing system"

  C. "We saved our business by having a penetration test"

  Please select the one that is most accurate?



Total Annual Losses						
	'97	'98	'99	'00	'01	'02
Theft of proprietary info.	$20,048,000	$33,545,000	$42,496,000	$66,708,000	$151,230,100	$170,827,000
Sabotage	$4,285,850	$2,142,000	$4,421,000	$27,148,000	$5,183,000	$15,134,000
Telecom eavesdropping	$1,181,000	$562,000	$765,000	$991,200	$6,886,000	$6,015,000
Outsider penetration	$2,911,700	$1,637,000	$2,885,000	$7,104,000	$19,068,500	$13,055,000
Insider abuse Net	$1,006,750	$3,720,000	$7,576,000	$27,984,740	$35,001,856	$50,099,000
Financial fraud	$24,892,000	$11,239,000	$39,706,000	$55,996,000	$92,935,500	$115,753,000
Denial of service	n/a	$2,787,000	$3,255,000	$8,247,500	$4,283,600	$18,370,500
Spoofing	$512,000	n/a	n/a	n/a	n/a	n/a
Virus	$12,498,150	$7,874,000	$5,274,000	$29,171,700	$45,288,150	$49,979,000
Unauthorized insider	$3,991,605	$50,565,000	$3,567,000	$22,554,500	$6,064,000	$4,503,000
Telecom fraud	$22,660,300	$17,256,000	$773,000	$4,028,000	$9,041,005	$346,000
Active wiretapping	n/a	$245,000	$20,000	$5,000,000	$0	$0
Laptop theft	$6,132,200	$5,250,000	$13,038,000	$10,404,300	$6,849,000	$11,766,500
Total	$100,119,555	$136,822,000	$123,799,000	$265,586,240	$377,828,700	$455,848,000
Grand total of Losses reported (1997-2001): $1,459,995,495						

Managing Risk

- Some Facts We Can All Agree on:
  - All businesses can expect some “loss” also known as “the cost of doing business”
  - Some businesses are not tolerant of loss in certain areas

Wise businesses choose which losses are acceptable!

My Life as a Fortune Teller!

- Perception
  - This system may be vulnerable, based on the software version number being displayed
  - No known exploits
- Conclusion
  - I'm safe

- Reality:
  - This system has a vulnerability
  - There are tools available on the Internet to exploit this vulnerability
- Conclusion
  - You are not safe

What is being tested?

- Are trying to prove a negative?

"I tried to compromise your systems and was able to do so. "

Your systems are not secure

"I tried to compromise your systems and was unable to do so."

Your systems are secure

Risks in Penetration Testing

- Your systems could **crash**
- You could **lose** business data
- You could miss a **real** penetration

- Someone could follow your incident response procedures (and **call law enforcement**)
- You could remain **unaware** about real vulnerabilities in your environment

When is Ethical Hacking Needed?

- Periodic Checkups
  - Quarterly vulnerability scans
  - After significant change
  - Legacy systems that are not closely monitored
- Investigation of critical applications and systems
  - Where is the most risk?
  - Who has reviewed the effectiveness of controls? (from the technical perspective)
- 3rd Party Vendors/Suppliers
  - Do they connect to your network?
  - Do they handle YOUR DATA?

Questions to ask a Pen-test team

- Do they hire former hackers?
- How do they store engagement data?
- How do they dispose of engagement data?
- Do they perform background checks?
- How do they collect exploits?
- How do they train their staff?
- Do they test exploits in a lab?

Steps to Managing a Pen Test

- Clearly **define** objectives
- Schedule **frequent** status updates
- **Supervise** closely
- Request **raw** data
- Inform internal security **monitoring** group*
- **Review** results with team (**before end of test**)

will leak info in a zero-knowledge effort,

but worth it!

HP WORLD 2004
Solutions and Technology Conference & Expo

Examples of what can go wrong!

- Please don't call the Cops!!
- Yes sir, that was me that caused 450 calls to the help desk.
- Ooops – that's not **your** system?
- Here you go, here's your hard-drive back.
- "Hello, yes, Do You Speak English"?

Questions?

Contact info:

Chad Schieken, CISSP

Manager Business Risk Services

Chad.Schieken@gt.com

609-254-0242