Security Testing:
Step by Step System Audit with Rational Tools

First Presented for:

The Rational User's Conference

Orlando, FL 2002

with:

Chris Walters

Scott Barber
Chief Technology Officer
PerfTestPlus, Inc.

Agenda

Threat Analysis

Security Arenas & Policies

Arsenal of Tools

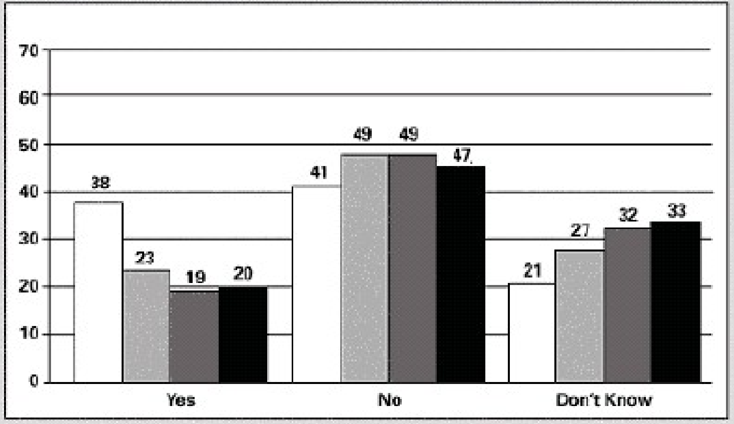
Security Audits

- Security Test Plan
- Systems Lockdown
- Internal Testing
- External Testing
- Reporting

Threat Analysis

Statistics of Breaches

90%	Detected computer security breach
80%	Acknowledged financial loss due to breach
44%	Will or able to quantify losses totaling $455,848,000
55%	Reported denial of service (DOS) attacks



97% of respondents have WWW sites, 47% provide electronic commerce services via their WWW sites; only 43% were doing e-commerce in 2000.

2002: 472 Respondents/94%
2001: 509 Respondents/95%
2000: 603 Respondents/93%
1999: 479 Respondents/92%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

Threat Analysis – Cont.

Examples

- NIMDA Virus
- Code Red
- Remote Denial Of Service
- AOL Instant Messenger Buffer Overflow

Security Arenas

Access Control Systems

Telecommunications & Networks

Security Management

Application & System Development

Cryptography

Architecture & Models

Operations Security

Law, Investigation, & Ethics

Business Continuity & Disaster Recovery

Physical Security

Security Policy

Risk Management

- Incident Response
- Point of Contact

Disaster Recovery

- Personal Data Backup

Security Training

- Social Engineering
- Best Practices

The Site Security Policies Procedure Handbook

http://www.ietf.org/rfc/rfc2196.txt?Number=2196

The SANS Security Policy Project

http://www.sans.org/newlook/resources/policies/policies.htm

Arsenal of Tools

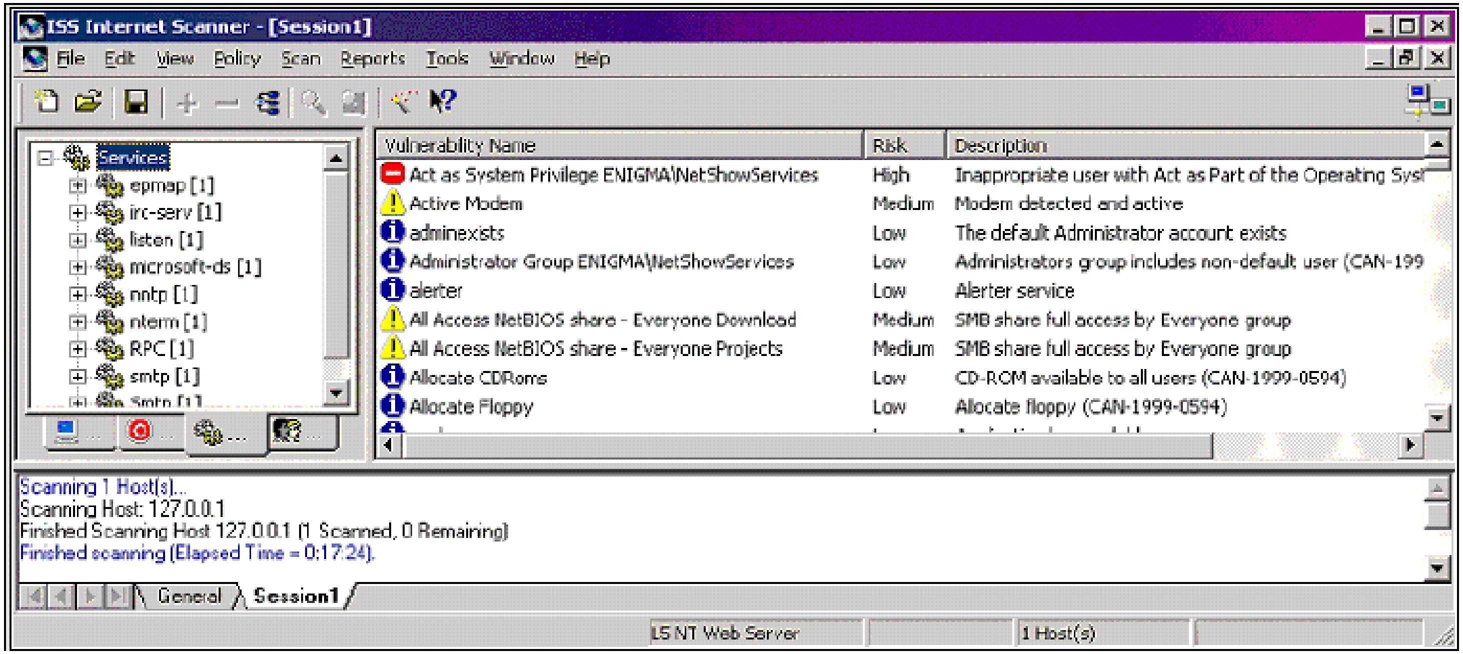
Tools that assist in providing security

- Firewalls
- AntiVirus
- Network Topology

Arsenal of Tools – Cont.

Tools that assist in auditing security

- Rational TestStudio
- Nessus
- Internet Security Scanner



Vulnerability Name	Risk	Description
Act as System Privilege ENIGMA\NetShowServices	High	Inappropriate user with Act as Part of the Operating Syst
Active Modem	Medium	Modem detected and active
adminexists	Low	The default Administrator account exists
Administrator Group ENIGMA\NetShowServices	Low	Administrators group includes non-default user (CAN-199
alerter	Low	Alerter service
All Access NetBIOS share - Everyone Download	Medium	SMB share full access by Everyone group
All Access NetBIOS share - Everyone Projects	Medium	SMB share full access by Everyone group
Allocate CDRoms	Low	CD-ROM available to all users (CAN-1999-0594)
Allocate Floppy	Low	Allocate floppy (CAN-1999-0594)

```
Scanning 1 Host(s)...
Scanning Host: 127.0.0.1
Finished Scanning Host 127.0.0.1 (1 Scanned, 0 Remaining)
Finished scanning (Elapsed Time = 0:17:24).
```

Security Audits

Security Test Plan

Systems Lockdown

Internal Testing

External Testing

Reporting

Security Test Plan – Gathering Data

Hardware Architecture

-Firewalls, Routers, Gateways, Switches

-Web Servers

-Database Servers

Software Architecture

-Client/Server

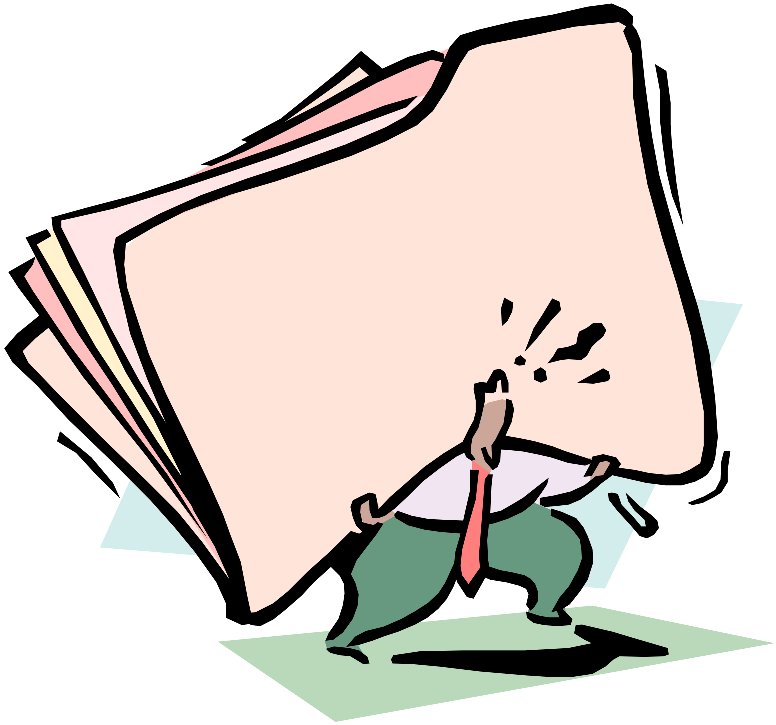
-Web Based

User Model

-SysAdmin

-DBA

-General User



Security Lockdown

Hardening Systems

- Windows
- Solaris
- Linux

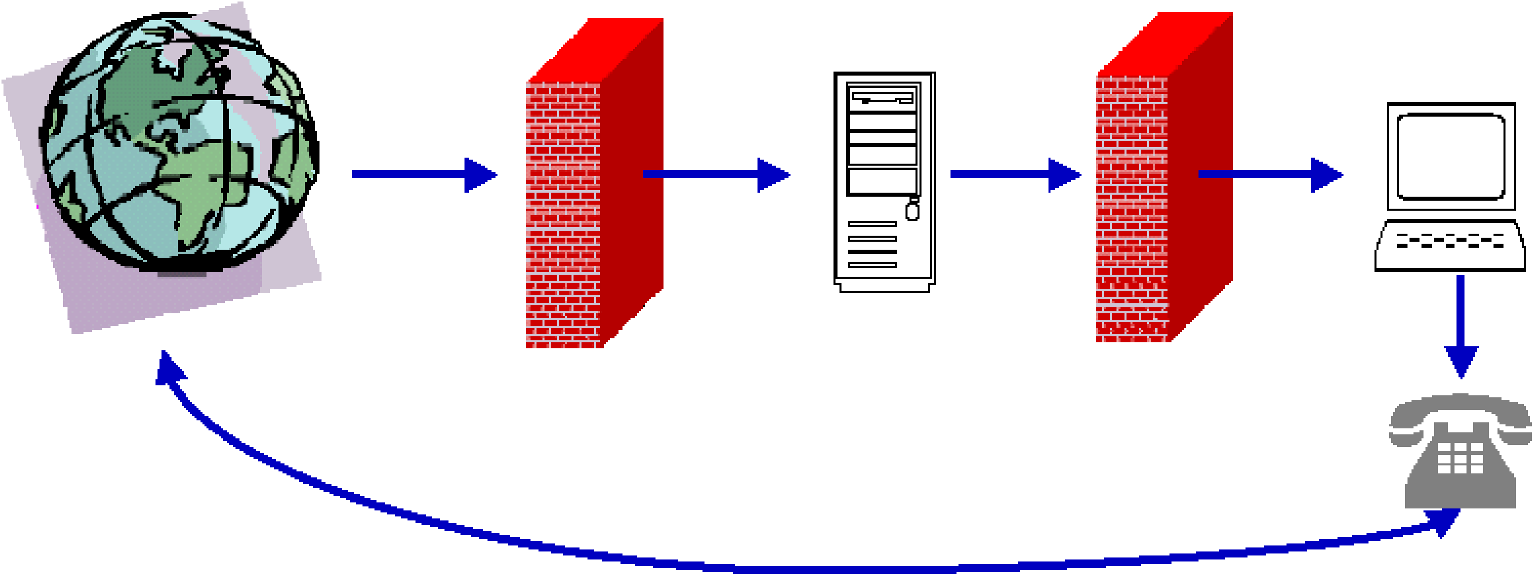
Viruses etc.

- Trojan Horses
- Worms
- Macros
- Viruses

System Lockdown

Firewalls

- DMZ
- Open Ports
- Bypassing



Internal Penetration Test

Port Sniffing

```
#include <VU.h>

string host = "www.rational.com";
int port, bytes;
{
push [Timeout_val=10, Think_avg=0,
Connect_retries=0];

for (port=20; port < 81; port++) {
        display (itoa(port));
        sut = sock_connect("sut", host + ":" +
itoa(port));

        if (sut > 0) {
               set Server_connection = sut;
               sock_send "";
               bytes = sock_isinput();
               sock_nrecv ["sut~" + itoa(port)]
bytes;
        }
}
}
```

IP Aliasing in TestStudio

DEMO – Hacking from the Inside

	Groups		Script	Command	State	Time	Source		Cmd Count	Streak
	Suite	Computer					File	Line		
1	User Group1[1]	Local computer[1]			Not Started			0	0	None

External Penetration Test

Packet Sniffing

- Network Recording between servers

ClearText Transmissions

- Record possible unencrypted data traffic

(Distributed) Denial Of Service Attack

- Simulate using Virtual Testers with no delays in multiple locations

Buffer Overflow

- Playback with larger that allowed fields for POST data submissions

External Penetration Test – Cont.

Brute Force Cracking

- Playback with DataPools of usernames and passwords

```
#include <VU.h>
string host = "www.rational.com";{
push [Timeout_val=10, Think_avg=0, Connect_retries=0];
do {
   rational_com = http_request [Brute F~001]
   "www.rational.com:80",
       HTTP_CONN_DIRECT,
       "POST /login/loginprocess.jsp HTTP/1.1\r\n"
       "Accept: image/gif, image/x-xbitmap, image/jpeg,
   image/pjpeg, applicat"
       "ion/vnd.ms-powerpoint, application/vnd.ms-excel,
   application/msword, */*\r\n"
       "Accept-Language: en-us\r\n"
       "Accept-Encoding: gzip, deflate\r\n"
       "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
   NT 5.0)\r\n"
       "Host: www.rational.com\r\n"
       "Connection: Keep-Alive\r\n\r\n";
```

DEMO – Breaking in with Robot

5 Minute Demo
development - Rational TestManager
File View Monitor Tools Window Help
Testers Active Suspended Terminated Normal Abnormal Time in Run
1 0 0 0 0 00:00:44
0%
FULL COM RES SRC MSG
STD GUI SQL HTTP IISP ROOM CUS
Iteration Users Inside
100 %
0 %
1.0
0.0
Init Connect Send Recv Linespeed Quiet GUI Other Exit
User View - Full
Ready
admin

	Groups		Script	Command	State	Time	Source		Cmd Count	Streak
	Suite	Computer					File	Line		
1	User Group1[1]	Local computer[1]			Not Started			0	0	None

Wireless Security

WAP & ECC

- Audit security at the gateway and beyond with TestStudio

Emulators & TestStudio

- Audit security between device and gateway

802.11 & WEP

- Audit security using TestStudio just like on a wired network

Reporting the Results

Defect reporting

- Incorporate ClearQuest

Coverage reporting

- Incorporate RequisitePro

Custom reporting using TestStudio

- Incorporate Manual test
- Created using Crystal Reports and SoDA

Common Security Holes

Vulnerable CGI Programs

Global File Shares

Weak Passwords

Default SNMP Settings

Microsoft IIS Holes

Social Engineering

Other Resources

Websites

- www.sans.org
- www.happyhacker.org
- www.antionline.com
- www.securityfocus.com
- csrc.nist.gov
- www.antionline.com
- And many more!

RFC Documents

- www.ietf.org/rfc.html

Training

Periodicals

Books

- Maximum Security
- Practical UNIX & Internet Security
- Web Security & Commerce
- Building Internet Firewalls
- And many more!

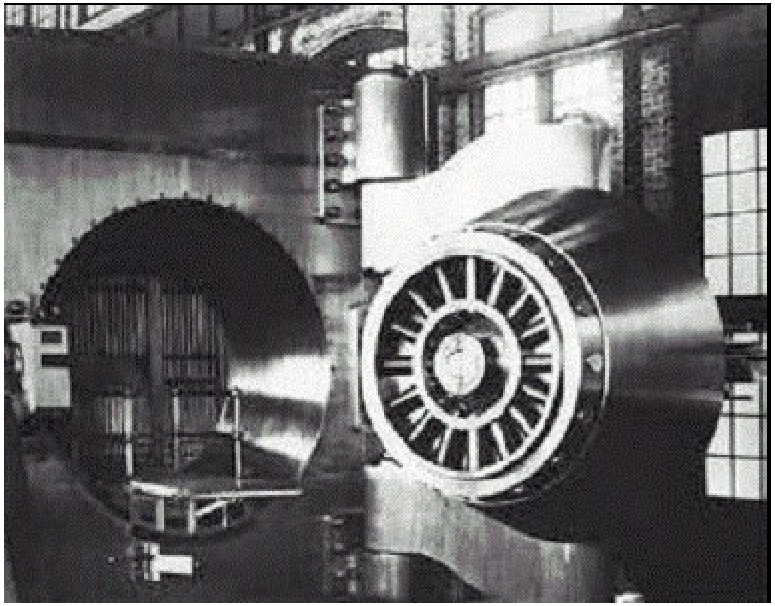
Conclusion

If you are connected, you are at risk

Security policies are required

Incident response forms are a must

Security audits are the only way to test your security



Questions?

Contact Info

Scott Barber

Chief Technology Officer

PerfTestPlus, Inc

E-mail:

sbarber@perftestplus.com

Web Site:

www.PerfTestPlus.com