Tutorial: Lessons From A Real Mainframe Break-In Over the Internet

Stu Henderson
5702 Newington Road
Bethesda, MD 20816
(301) 229-7187
STU@STUHENDERSON.COM

What You'll Hear Today

- Brief comments on why TCP/IP security is important to us (If you don't understand a few of the buzzwords, That's the point)
- Description of a real mainframe break-in over the Internet
- Lessons we can take from this

Chief New Source of Opportunities to Break Into Mainframes:

Mainframe TCP/IP Connections

- Tools are there to secure it
- Lack of knowledge leaves weak configurations
- Organizational issues, not technical, are the weakness
- Internet, FTP, TN3270, httpd, other daemons
- CICS, MQ Series

More Critical Issues

- DB2, TCPALVER, SQL Injection, Distributed Connections
- Weak communication between mainframe and TCP/IP experts
- "Not My Job"

Free Security Tools From IBM for Mainframe TCP/IP Connections

- Basic steps: block all the ports
- Basic steps: ensure all sensitive data encrypted, including passwords
- PAGENT (Policy Agent) Firewall-like functions
- Change control over configuration files, programs, JCL

Firewall-Like Functions You Get With PAGENT

- Packet Filtering
- Encryption (Including SSL and TLS)
- IPSEC and VPN and NAT
- Intrusion Detection

What Would You Pay for This on a Windows LAN?

Quick Self Test You Can Make Today:

- Does Your RACF Administrator Understand These Basic Techniques for Securing TCP/IP?
- Does Your TCP/IP Administrator Know About PAGENT?
- Do They Know Each Other?

Quick Self Tests You Can Make Today

- Is the Started Task Named PAGENT Running?
- Do You Know Who Administers It?
- The Concept of a Baseline Document
- Do You Have a Policy Saying Who Is Responsible for TCP/IP Security on the Mainframe?

SOME COMMON THEMES

All of these weaknesses can be traced to organizational issues:

- Who decides?
- Who approves?
- Who has the knowledge?
- Who is responsible?
- How do we measure?

Take Just a Few Examples: Blocking the Ports, Encryption Over TCP/IP, and SQL Injection

- Does the Person Who Understands It Have the Responsibility?
- Who has the Knowledge?
- Who is Responsible?
- Is It Documented and with Formal Change Control?

Here's the Story of

A Real MAINFRAME BREAK-IN

- This was a deliberate, successful, criminal attack
- On a European service bureau's mainframes
- Over the Internet.

A Real MAINFRAME BREAK-IN

- Not stealing a tape or tricking out passwords.
- RACF, but applies to ACF2 or TopSecret.
- Discovered from high CPU usage. Shades of "The Cuckoo's Egg" by Cliff Stoll

A Real MAINFRAME BREAK-IN

- First used FTP to download the RACF database and crack all the userids and passwords.

- People seem to think that because passwords are encrypted, they can't be read.

A Real MAINFRAME BREAK-IN

- But brute force cracker programs will do the job.

- In a couple of days they cracked the passwords for 30,000 userids.

A Real MAINFRAME BREAK-IN

- "Is this where we process State Police records?" YES

- Hackers broke into front-end distributed computers to get to the mainframes

A Real MAINFRAME BREAK-IN

- Hackers installed outbound programs which called out over the Internet, making it easier for the hackers to bypass firewalls and other protections.

- All of the holes the hackers used resulted from mis-configuration, not weaknesses in mainframe security or RACF.

SOME COMMON THEMES

All of these weaknesses can be traced to organizational issues:

- Who decides?
- Who approves?
- Who has the knowledge?
- Who is responsible?
- How do we measure?

A Real Mainframe Break-In

LESSONS LEARNED

- Mainframes are targets now.
- Internet connections make them more vulnerable
- Most securable platform, but …
- Organizational issues

A Real Mainframe Break-In
LESSONS LEARNED

- Your Mainframe Isn't Secure If It Uses TCP/IP and Someone Doesn't Address This Stuff
- You Can't Believe Those People Who Wave Their Arms Saying "Don't Worry, We Have a Firewall!"
- You Can Conduct The Basic Tests Described Here Today
- By Default, We Assume That the RACF Admin is Responsible for Any Mainframe Breaches

Lessons From A Real Mainframe Break-In

For more information:

- IBM Security Portal at www.ibm.com/systems/z/advantages/security/integrity.html
- The Henderson Group: www.stuhenderson.com