

Sysadmins' Round Table

4 November 2004

New faces
Current practices
Old processes

The Intro and the Outro

- ❖ Mark Leininger ...
 - ◆ Joining as CST leader, roughly replacing Dane Skow.

- ❖ Matt Crawford ...
 - ◆ Leaving CST when a replacement is found.

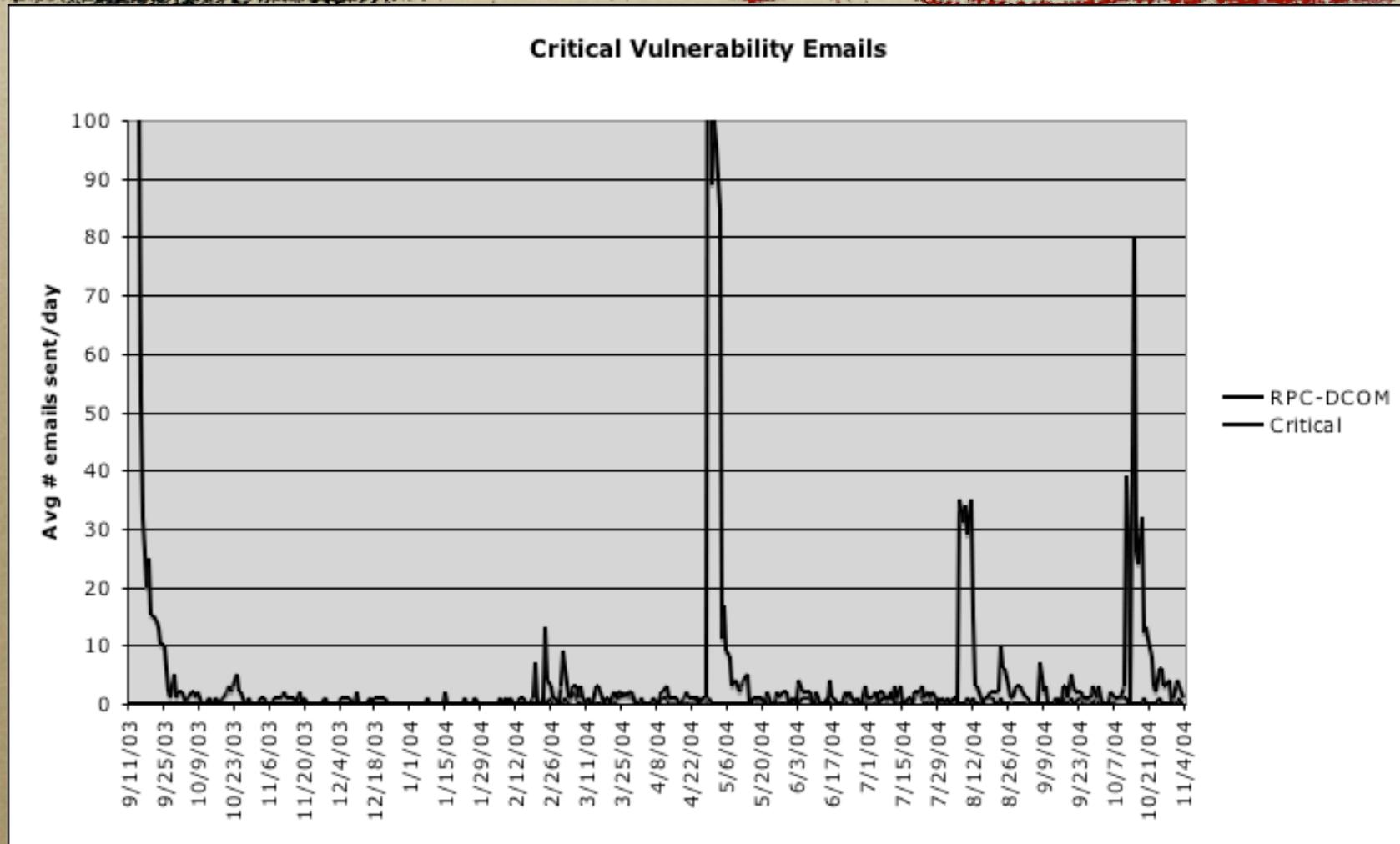
Current practice: incidents

- ❖ #1 now and always: report actual or suspected computer security incidents.
 - ◆ **computer-security@fnal.gov** non-urgent
 - ◆ x2345 for urgent situations
- ❖ Don't let users put compromised machines back into service without FCIRT release!
- ❖ No need to report: spam or bounce messages for mail you never sent.

Current practice: warnings

- ❖ Notification of vulnerabilities comes from **nightwatch@fnal.gov**, and replies should go to the same address.
 - ◆ Identify the system(s) concerned.
 - ◆ Include the stated reason for the block.
- ❖ We still plan to move the unblock procedures out of email and reduce the human effort for all.

Critical Vulnerability Email



Sine qua non!

- ❖ Everything hinges on up-to-date system administrator information!



- ❖ `http://fncdug1:7777/pls/miscomp/sysadmin.html`

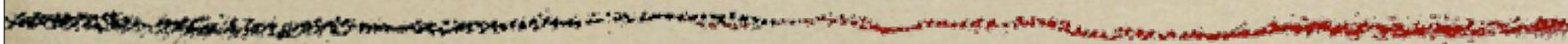
Current practice: scanning

- ❖ Strong Authentication scanner
 - ◆ Checks for compliance with Kerberos rules.
 - ◆ Checks for known vulnerable versions of http and ssh servers.
 - ◆ Does not (in general) lead to network blocks.
 - ◆ GCSC may request a block for recurrent offenders.
- ❖ Runs every two hours.

Current practice: scanning

- ❖ Critical Vulnerability scanner
 - ◆ Nessus, with a small set of tests activated.
 - ◆ Machines with recently-declared vulnerabilities blocked after a grace period of approximately a day. (No admin, no email, no grace period!)
 - ◆ Machines with old or multiple vulnerabilities get no grace period – they are often TWD.
- ❖ Runs continuously.

Current practice: scanning



- ❖ RPC-DCOM scanner
 - ◆ Special tool from MS, more effective than Nessus for this test.
 - ◆ Tests lack of MS04-026/-029 patch (KB824146).
 - ◆ Vulnerable systems blocked when found.
- ❖ Runs 2x/day.

Current practice: scanning

- ❖ Inventory scanner
 - ◆ Collects inventory of network devices.
 - ◆ Gross statistics direct other scanning.
- ❖ Runs only as needed.

Current practice: autoblocker

- ❖ Analyzes network flows summarized by border router.
 - ◆ Triggers if one address sends to 64 hosts or 64 ports on the other side within a minute.
 - ◆ Incoming: 1 trigger gets a block for 6 hours.
 - ◆ Outgoing: 3 successive triggers gets a block for 30 minutes.
 - ◆ Block is removed in the stated time after the scanning behavior stops.

Resources

- ❖ Critical Vulnerabilities
 - ◆ <http://computing/security/CriticalVuln/>

- ❖ Lists of blocked and unblocked addresses
 - ◆ <http://www-dcn/~netadmin/blocked/>
 - ◆ (“ACL” means static IP addresses.)

Exceptions

- ❖ Exceptions to any requirement are possible.
 - ◆ Some are less likely to be granted than others.
- ❖ Exception requests never should go to computer-security...

Exceptions - forms

- ❖ Strong authentication waiver
 - ◆ <http://www.fnal.gov/docs/strongauth/misc/exemption.html>
- ❖ Web server off-site access request
 - ◆ http://computing.fnal.gov/security/Security_Exemption/web_server.html
- ❖ NetBIOS access through the border
 - ◆ No such thing – use a VPN tunnel!

Exceptions - email

- ❖ Send email to **nightwatch** (not computer-security) to request
 - ◆ Possession or use of “security tools” (those which probe or break security weaknesses).
 - ◆ Implementation of restricted services (see FPOC for list).