A university's perspective on last spring's security incident

Daryl Herzmann
Department of Agronomy
Iowa State University

Who am I? Why am I here?

Vice Admiral James **Bond** Stockdale pictured in the center.

Who am I?

Second hit on Google Images for 'firefighter and computers'.

- 'Data Monkey' for Iowa State University.
- Bachelor's in Meteorology (ISU 2001)
- Hired in 2001 to work on the Iowa Environmental Mesonet.
- 2002 got the department's SysAdmin role 'added' to my job description after budget cuts.

Why am I here?

Troublemakers

- #1. NCAR asked me!
- During spring 2004, various ISU computers and user accounts were used as attack vectors to NCAR.
- Perhaps we learned something during this adventure.
- My story is not unique, hopefully not boring, and contains a twist.

ISU's use of NCAR

- Access and store data on MSS
- Run models (MM5, WRF, WRF 3dvar, CCM3, CAM3, RegCM, Eta)
- Write models (Cloud Resolving Model, Adaptive Grid)
- Use of support software (NCAR Graphics)

Once upon a time (23 Mar 2004)

- SSH login from somewhere.
- Then runs the nfsshell exploit against vulnerable IRIX and Linux NFS servers.
- Installs the suckit rootkit to hide the system changes and monitoring programs.
- Trojans the SSH client.
- I did not catch this activity at the time.

Wierd things happen in April

- One of the comprimised machines had bad memory and liked to kernel panic, but something would block the kernel debugger and dump explitives to the screen.
- Noticed lots of these, (harmless right?)

  Apr 13 08:21:14 xxx sshd[30042]: refused connect from nerva.ucc.ie (143.239.130.82)
- Noticed some odd hour logins, but never followed up with checking it out.

5 May 2004

- ISU Security Lead gets a call from SDSC, traffic from Ireland is coming through me to U of Minnesota.
- I was asked to leave the main comprised machine alone. The FBI and others were monitoring the connections and wanted to track his movements.
- Started to poke around and found all sorts of nasty setuid files, .bash_history files, and empty syslogs (save remote sysloging).

An Aside: The FBI Court Order

- First time ISU had been served with such a document mandating the network monitoring of a machine.
- Specifically asked for netflow statistics, no packet captures (somewhat disappointing).
- My understanding is that it did NOT mandate the comprimised state of the computer, but ISU administration decided it was wise not to challenge this order.
- Meanwhile, I have a mess. The court ordered system was central to departmental NFS services, compiler licenses, and the frontend to our cluster. (Worried that `rm -rf *` was coming if I tried to isolate the machine from our network.)

May, June, July ...

- We continue to be used as attack vectors and password collector continues to run on our machine.
- Nasty attacks continue to NCAR (detailed in previous talk).
- Very frustrating time.

Local Users Frustrated

- Tough time. The same accounts they needed to use to get to the super-computers were being used to break in to them from ISU.
- I was being really tight lipped with what was going on. Didn't want the users to talk about it via email.
- Labs were frustrated with us for not cleaning up the mess.

Did we learn anything?

Lessons Learned

- Don't run custom kernels unless you are diligent to keep them up to date. Goodbye XFS :(
- Infinitely store syslogs
- National Labs didn't know me and I didn't know them. Need to communicate better.

Computing Changes

- Eliminated old SGIs.
- Installed Red Hat Enterprise Linux on all boxes. (XFS systems running ScientificLinux kernel.)
- Only anonymous FTP (chroot) allowed.
- NFS configured for iptables (firewall).
- Save and archive syslogs

'Policy' Changes

- Absolutely no account sharing. I will report to the lab security contact before supervisor.
- New passwords must not be easily guessed (pass the passwd command logic).
- Off campus SSH pubkey authentication not allowed.

Work in progress

- Fully implement/understand SELinux (Uffffff!)
- Ditch NIS
- Automated penetration testing. By me? If not, who?

Questions?

Daryl Herzmann

3010 Agronomy Hall

Ames, IA 50010

515.294.5978

Cell: 515.451.9249

akrherz@iastate.edu