Welcome to

RPC Hell

Jay Stamps, October 7, 2003
In the Beginning...

- KB823980 RPC/DCOM security patch released
- News reports on expected hacker exploits
- At Stanford, Tina Bird et al urge everyone to install patch
- A few people actually do…
Two weeks later…

- July 31: PCs at Stanford start being hacked
- Directed attacks, installation of backdoors and fileservers (backdoor.hale/padmin)
- August 1-3, 2003: Def Con 11
- Hacked PCs at Stanford are being rebuilt right and left
- The knowledgeable suspect the worst is yet to come…
The 33571 Listener

• August 1 (or so), 2003: a new directed attack on Stanford
• Spooky b/c it could hide itself, b/c Stanford appeared to be specifically targeted, and b/c we still don’t know how it propagated
• Exploit installed KB823980 patch, to shut out future attacks
• Dubbed 33571 listener
The Blaster Worm

• August 11, 2003: first calls to Stanford Help Desk about Blaster infections
• The worm doesn’t get onto SUNet at first, but inevitably it does, probably taking a ride on someone’s laptop
• Copycat variants of Blaster appear
• Man, this thing spread fast!
Welchia – the Worm That Cares

Have a Nice Day!
Welchia

- August 18, 2003: Stanford and the rest of the world hit by Welchia (Nachi)
- Most efficient worm to exploit RPC/DCOM vulnerability
- Unpatched PCs attached to SUNet would be infected w/in a few minutes
- Welchia installed the KB823980 security patch, to prevent other worms from getting in, and would try to remove Blaster infections
Welcome to

RPC Hell
Stanford’s Response

• August 11, 2003: ITSS activates Emergency Operations Center
• August 13, 2003: the regime of 8 am planning meetings begins
• ITSS and security staff from other parts of the university work together to develop a viable approach to an emerging crisis
To clean? Or to rebuild?

• As antivirus vendors were struggling to keep up w/ the virus authors, the standard approach to repairing compromised PCs was to rebuild them
• Rebuilding takes many hours, and is nasty, tedious work
• It was quietly acknowledged that we needed a less labor-intensive approach to a growing problem
The RPC Cleaner!
RPC Cleaner

• ITSS staff began work on a tool that could detect and clean infections and patch Windows 2000 and XP systems (the only OS’s widely affected)
• Great discovery made that the 33571 Listener exploit was detected and removed by Symantec’s WinShell.50/Stealth.B removal tool
• Tool also incorporates Symantec Blaster removal tool, and can remove Welchia on its own
• Tool designed to self-update and to write a log file to AFS space
Secure Computing Web Site

• The Secure Computing @Stanford web site has been growing for over a year now, and has turned into a valuable source of information, documentation and education for end users.
• The RPC Cleaner download and other self-help documents, along w/ more technical information about the RPC/DCOM attacks and Stanford’s response to them, were posted to this site.
DNS Black Hole

- RPC Cleaner worked well for PCs w/out privileged access to sensitive data
- Biggest problem was getting users, who might not know they were infected, to clean and patch
- Security scans of SUNet round the clock
- DNS Black Hole dreamt up and implemented
- The so-called “171.66.66.66” server was set up so that users in the Black Hole could still help themselves to get cleaned and patched
ESS CD and the Students

• ESS CD designed to auto-launch RPC Cleaner
• ResComp network registration system integrated w/ RPC Cleaner
• Students get cleaned and patched before they get onto SUNet
• It worked! (about 98% success rate)
All’s not quiet…

• Unpatched PCs attached to SUNet are still likely to be infected (usu w/ Welchia) w/in a few minutes – but maybe not quite as fast as before
• And on September 10, 2003, Microsoft announced 3 more RPC/DCOM vulnerabilities in MS03-039
• No new exploits (yet!) in the wild for these latter vulnerabilities, but we can’t rest easy…
What’s Next?

• The need to provide a more controlled computing environment at Stanford has become clearer than ever

• And after the past couple of months, that’s what our clients want, too…

• ITSS is working hard to plan for the future, to develop means to avoid crises, and to deal w/ them better when they do arise
HAVE A NICE DAY!