Real Attacks and Threat Models

Steven M. Bellovin
http://www.cs.columbia.edu/~smb
Columbia University

November 6, 2006

Or. . .

Those crazy scenarios the security guys come up with are real!

Disclaimer

I didn't do any of the work tracing or analyzing the attack. Most of the work was done by Darrell Bethea of CRF, with help from many others not including me. I'm speaking about it because I'm here.

The Start

- We were notified by the campus networking folks that a machine of ours — our FTP server — was launching attacks
- We did the obvious: we disconnected the machine from the net
- The campus networking folks informed us that the attack was continuing. . .

Spoofing

- Obviously, someone was spoofing the FTP server's IP address
- We checked the MAC address being used
- It was correct, too. . .

Tracing MACs

- We checked the switches
- The MAC address was being used by a machine — a firewall used for some experiments! — in different building
- Traces showed connections to it (via its spoofed address) every four minutes, from Sweden
- When we disconnected the machine, those connections stopped — and didn't resume

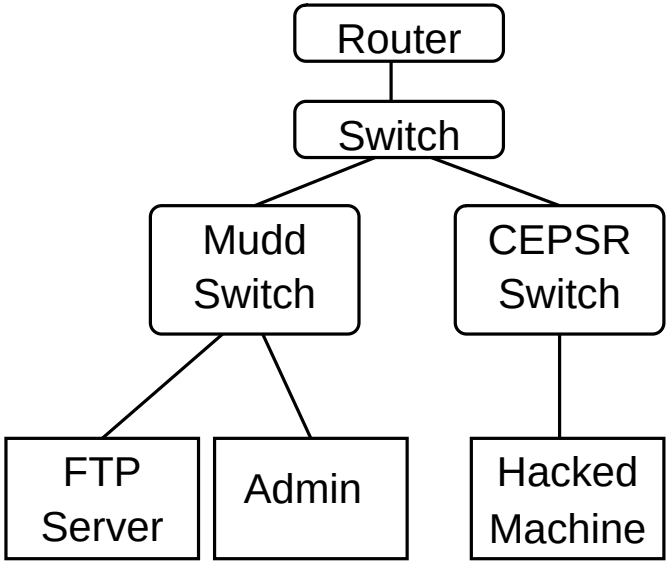
Restarting the Probes

- By temporarily bringing the real FTP server back online, we could get the probes to restart
- We believe that something local was listening for the gratuitous ARP on interface-up, and signaling to Sweden that via some different external machine
- We also found what appear to be deliberately-broken SYN packets used for signaling and/or firewall detection

Why Didn't Our FTP Service Fail?

- It did
- It was even reported, twice
- When tested, though, it worked
- "User on drugs?"

Tests versus Reality



- The testing machine was on the same switch as the real server
- Running the test involved only the Mudd switch
- The path to the outside used different — and confused — switches

The Aftermath

- We pulled the plug on the compromised machine
- Switch logs show that going back to May, it spoofed 225 legitimate local MAC addresses. . .
- We were then hit with two days of intermittent DOS, with spoofed MAC addresses, from within our LAN (great for VoIP. . .)
- Because of accident and inadequate access to the switches — we (and the campus networking folks) really want SNMPv3 — we were not able to track it further
- Things are back to normal — with some unknown number of compromised internal machines

Conclusions

- There are some very sophisticated bad guys out there
- We have reports of at least one other similar incident elsewhere
- This target was low value; its compromise was only detected because the attacker got greedy
- How many more really sophisticated attackers are hiding?
- Let's review our threat models. . .