

Cyber Security Lab 1 Comments

Most of the design descriptions were fine. A few were a little too detailed or command oriented. One group had a nice table that described features and then implementing commands. I was looking for a few paragraphs that could be returned to Bob Co showing how you formalized their more vague requirements.

Most groups had good examples of what not to do in real life including:

- Don't have the management network directly connected to the internet router.
- Use better passwords.
- Use a more granular mechanism to eliminate bad java/activeX without removing all of it.
- Encourage use of secure POP rather than regular POP
- Don't allow all employees to SSH to DMZ. Only a subset should need to do this.
- Move syslog off box.

A number of the groups also had problems with the Boss' SSH in access. Certainly, this is including the boss' home environment in your domain of protection which is undesirable. Some of you recommended that the boss' machine be put in the DMZ for this reason. This is probably not practical from a human relations perspective. This might not be desirable either because if the boss' machine includes sensitive information (which is likely) we don't want to put it in on the same network link with machines that have more outside exposure (and thus are more likely to be exploited).

Many of the groups suggested using VPN (presumably IPSec) instead of SSH. There are arguments both ways on this, and it is not straightforward to say that tunneling through SSH is superior to tunneling through IPSec or visa versa. One of you did note that with a VPN that terminated at the border other intermediate scanning tools could look for hostile traffic. With end-to-end encryption, you would need to rely on a desktop solution for scanning viruses, etc in the traffic stream.

Everyone had a reasonable answer for the fifth question. The firewall helps, but it does not completely protect Bob Co from malware. You still have the insider threat bringing in malware on physical media, downloading malware through allowable traffic, etc.

Most folks had configurations that looked mostly operational. Some groups were missing some aspects of the requirements like pinning down the management interface or turning off unnecessary application proxies. Most groups used a combination of in and out ACLs. Many groups had some overbroad rules, but with the combination of in and out ACLs, the net effect was safe.