Security Triage

How to Secure a Network for a Busy Administrator

About Me

- Jim O'Gorman
  - jameso@elwood.net
  - jogorman@gmail.com
- http://www.elwood.net/

Introduction (1)

- Common Wisdom Says “Security is a compromise between convenience and security.”
  - Security is doing things right. If things are done correctly, security happens.

Introduction (2)

- Sadly, many of us are stuck with systems that are wrong.
  - Organizations have limited resources.
  - Often they chase features, buzzwords, and promises over their true needs.
  - Product correctness and security often do not enter the picture.
- Incorrectly secured products create bad situations for those that have training and experience in security matters.

Introduction (3)

- The situation is even worse for many administrators:
  - Little or no training/experience in dealing with security matters.
  - Security not taken seriously at their facilities by corporate culture.
  - Security a secondary responsibility, if that.
  - Lack of time due to primary responsibilities.

Introduction (4)

- Needing direction, these administrators turn to industry best practices for help.
  - Not written with this category of administrator in mind as a target audience.
  - Lack of experience, understanding documentation and time results in improper implementation.
- This leads to Admins “freezing”.
- The problems are big, but are manageable if broken up into digestible chunks.

Introduction (5)

- We will cover some simple items Admins can do to bootstrap their security.
- As much as matter of mindset than anything else.
- This is not a step by step guide. Instead, this is intended to help “unfreeze” Admins, and give them some direction on where to go next.

Concepts (1)

- Before we start, we need to cover a few concepts.

Concepts (2)

- The only way to improve the situation is through knowledge and work.
  - There is no security silver bullet.
  - Vendors want your money.

http://www.ranum.com/security/computer_security/marketing/hacker-repellant-small.jpg

Concepts (3)

- Just because something is labeled a “Best Practice” does not mean it fits your situation.
  - Every installation is different.
  - Knowledge is all you have to be sure you make the right decisions.
- Decide what your goals are going to be, then focus on them.
  - Bruce Schneier’s “Security Theater”.
  - Make the work you are doing count. Don’t just follow trends or to tick off a box on a form.

Concepts (4)

- Know your enemy.
  - Don't be a lazy attacker's target. Many network attacks are from worms or script kiddies focusing on targets of opportunity.
  - Other attackers are targeting you. What would they target?

First Steps (1)

- Learn as much as you can about what it is you are protecting.
- Understand what the network looks like on a normal basis, not just when there are problems.
- Gather as much existing documentation as possible.
  - May be old, out of date, or just plain wrong.

First Steps (2)

- Perform your own inventory. Gather more than you will likely need.
  - Hardware platform/model number
  - Mac address
  - Switch port number
  - Operating system
  - Patch level
  - Running applications
  - IP address(es)
  - Listening ports
  - Services provided
  - Ps output
  - Df output/Disk usage and mound points
  - Netstat output
  - If there is a package management system, what packages are installed
  - Etc

First Steps (3)

- Review network layout and configuration.
  - Gather configs and logs from router, firewalls, and switches. Read the logs.

First Steps (4)

- Review the backup system.
  - Backups are the most under respected aspects of security. As a final line of defense, they are as big of a part of security as any other measure.
- Talk to your users and co-workers.
- Take a step back and look at the big picture.

Second Steps (1)

- Now it is time to get more active in the information gathering.
  - Watch out before following any of the steps I recommend next. Be sure you have the permission and authority before you start. Don’t get in trouble.

Second Steps (2)

- Port scan all your systems. Log the output.
  - Look into using nmap (http://www.insecure.org/nmap/).
  - Rescan some weeks later, see what changes.
  - Read the docs.

Second Steps (3)

- Look into having a full audit log for your network.
  - Full packet captures are best, but give you a lot of data to manage.
    - Tools make this easier, for example idabench (http://idabench.ists.dartmouth.edu/).
  - Argus (http://www.qosient.com/argus/) can give you a searchable audit log with little hardware requirements.

Second Steps (4)

- Argus is easy to run.
  - Argus startup:

```
/usr/local/sbin/argus -c -d -i $INTERFACE \
-w /usr/netlog/savefile.arg – ip
```

-c - direct argus to create a pid file.

-d - run Argus in daemon mode.

-i – interface to listen on

-w – write to output file

Second Steps (5)

- Now that Argus is running, manage the output.
  - Decide how often to rotate the logs.
  - Retention policy - These logs hold all the IP traffic for the network.
  - Storage requirements - Look to see how much space an average day takes up.

Second Steps (6)

- Searching Argus data is easy as well. You can limit the results with syntax similar to tcpdump filters:

```
ra -n  -L0 -c -Z b –r savefile.arg - net 68.142.226
    StartTime         Flgs   Type      SrcAddr     Sport Dir     DstAddr     Dport
    SrcPkt   DstPkt    SrcBytes     DstBytes     Status
01 Jun 05 07:48:39           tcp     10.10.80.66.1053   ->   68.142.226.51.www   9
          11         1253          13450       FSPA_FSPA
01 Jun 05 07:48:47           tcp     10.10.80.66.1059   ->   68.142.226.51.www   5
          4          1073          413         FSPA_FSPA
01 Jun 05 07:48:47           tcp     10.10.80.66.1060   ->   68.142.226.51.www   5
          4          1138          322         FSPA_FSPA
01 Jun 05 08:11:17           tcp    10.10.80.100.1162   ->   68.142.226.34.www   9
          11         974           13444       FSPA_FSPA
01 Jun 05 08:11:21           tcp    10.10.80.100.1170   ->   68.142.226.34.www   5
          4          956           413         FSPA_FSPA
01 Jun 05 08:11:21           tcp    10.10.80.100.1171   ->   68.142.226.34.www   5
          4          1021          322         FSPA_FSPA
01 Jun 05 08:49:02           tcp     10.10.80.48.1139   ->   68.142.226.47.www   9
          11         1177          13707       FSPA_FSPA
```

Second Steps (7)

- Network traffic audit logs can be a great help for many purposes, including security.
  - Track network utilization, who is talking when?
  - A host gets a virus. When it was infected, who did it talk to? Was it being remotely controlled? If so, who was controlling it. Has any other hosts talked to that remote server?

Third Steps (1)

- Next we move into simple clean up. This is the easy stuff, low hanging fruit. Yet, there is a drastic return on these simple efforts.
- Hopefully, you are already doing these things, if so great!

Third Steps (2)

- Anti-Virus
  - One of the oldest security tools, and as such it is very mature.
  - No reason not to have this. Its free! ClamAV (a popular unix anti-virus tool http://www.clamav.net/) has been ported to Windows as well (http://www.clamwin.com/).
  - Ensure that signature files are being kept up to date and periodic scans are occurring.

Third Steps (3)

- Anti-Spyware.
- There are a multitude of risks posed by spyware, including but not limited to:
  - 3rd party tracking all usage on computer. Websites visited, address e-mailed, programs ran, etc.
  - Keystroke loggers capturing all input, logging to a file and uploading it to remote servers.
  - Evil proxies. Proxies that just capture all the web traffic, index it, send results off to 3rd party. High potential for leaking information from internal web applications.

Third Steps (4)

- Patching
  - Patching is a frustrating issue, as applications should be designed correctly from the start, without a need for frequent patching.
    - Marcus Ranum even goes so far as to argue that we should not patch (http://www.ranum.com/security/computer_security/editorials/master-tzu.html).

Third Steps (5)

- “So you put yourself on the patch treadmill and sink all these costs into chasing the latest mostly-works version, and you're still going to get clobbered by the next big worm that comes along and exploits a vulnerability that you and your 1.6million peers currently have installed. If you're a good patch addict, you'll have the patch installed nearly immediately - unlike me - and your window of exposure will be hours instead of days or even years. But the problem is that you'll still be exposed for a while. It might be too long. Me? I'm not exposed to IIS bugs because I don't run IIS. I'm not exposed to IE bugs because I don't run IE. I'm not exposed to Outlook bugs because I don't run Outlook.”

Third Steps (6)

- While what Mr. Ranum says is true, many of us can not deploy systems that don't need patching (and it's a sad commentary on the industry).
- It would be negligent not to patch your systems.
  - This is not getting addressed as it should. If you look at most of the internet worms that have spread in the last few years, many had a patch to protect against it before the worm was released (example: slammer http://www.eweek.com/article2/0,1759,1654585,00.asp).

Third Steps (7)

- Patching
  - Will the patch break existing applications?
  - Can you test the patch?
  - Is there a roll back?
  - How will you track what needs to be patched, when the patches come out, etc.?

Third Steps (8)

- Policy
  - You must have formal policies on what should and shouldn't be done with the systems or you have nothing to enforce.
  - Often this is boring work. Get over it. It has to be done.
  - Involve HR and legal departments (if you have them).

Third Steps (9)

- If you don’t have a policy, don’t start from scratch. Bootstrap yourself. http://www.sans.org/resources/policies/#
- Don’t let the document be static. Change with technology. If you still have the same AUP since 1995, something is wrong.

Fourth Steps (1)

- What goes over the wire? What is happening on the network?
  - The Internet works off of stimulus and response.

Fourth Steps (2)

- Routers
  - For some small installations the ISP may be handling the configuration for you.
    - Know how to contact them in case of emergency. If you need to, print out the contact information on a label and slap it on the router.

Fourth Steps (3)

- If you are responsible for the router, review the config.
  - Print the config out and review it line by line.
  - If you have to, go ahead and google each config line to know what it is doing.
  - Notate what OS and version the router is running.
  - Review any maintenance contracts you may have or need.

Fourth Steps (4)

- Firewall
  - Pay special attention to what filtering software it is running (Cisco PIX, OpenBSD pf, Checkpoint, etc).
  - Get a copy of the rule set, and review it line by line to completely understand how it works.
  - Understand the path through the rule set the packet will take when it enters the network.
  - Have a default deny policy. Don’t be a Bilano.

Fourth Steps (5)

- Each pass statement is a hole into your network.
- Review this list of pass statements against your earlier list of what servers are listening on what ports.
- Be sure everything is still needed.
- Make sure the firewall itself is adequate for your needs.
  - Application Proxies are not dead.

Fourth Steps (6)

- Be aware of how the firewall logs, and what it is logging.
  - Many people will log dropped packets. I find what is being passed to be more interesting. Consider logging on that instead of dropped packets that did not enter your network.
  - That is not to say drop logs are worthless, they can be a great source of information in correlating possible attacks.

Fourth Steps (7)

- Review your network audit logs.
- Correlate your audit logs to your firewall pass logs.
  - Are they seeing the same traffic?
  - If not, what is going on?

Fifth Steps (1)

- Detail each host.
  - This can take a while, but is worth the time. It gives you great documentation for each server on your network.
- Review the running process list you had from before.
  - Go through each process, and figure out why it is there.
  - If something is not needed, be sure to turn it off, or uninstall it if you can.

Fifth Steps (2)

- Review periodic process.
  - It is important to know what runs and when for much more than security reasons.
- Review all user accounts.
- Delete any old user accounts that are not needed.
- Be sure password policies are correct and passwords are being changed on a regular basis.

Fifth Steps (3)

- Logs.
  - Review how they are being processed, rotated, and read.
  - Be sure you understand what sort of retention you need for this information.
  - If possible, see about logging to a central location.

Fifth Steps (4)

- Investigate the possibility of a file integrity checker such as tripwire (http://www.tripwire.com/) or samhain (http://la-samhna.de/samhain/index.html).

Sixth Steps (1)

- Time to look at the bigger picture, moving away from specific configurations.

Sixth Steps (2)

- Backups
  - Backups are the most disrespected aspect of security infrastructure.
  - If all else fails, backups are all you have.
  - Take the time to review your backup systems, and see if there is anything you can do better. Test restores.
  - And yes, I have this twice in this presentation to make sure no one misses it.

Sixth Steps (3)

- Review mail filtering.
  - Spam is an annoyance, but mail born viruses are much more.
  - A good spam filter will often stop virus as well.
  - Investigate greylisting (http://projects.puremagic.com/greylisting/) to see if it may be right for your networks, greylisting has a great record of stopping viruses as well as spam.

Sixth Steps (4)

- Look into Google hacking.
  - Google is a popular hacking tool
  - Use it to see what information you are leaking to the world.
  - Review http://johnny.ihackstuff.com/index.php?module=prodreviews.
- Look into running a scanner against your network.
  - Nessus is a free tool (http://www.nessus.org/) you may want to use to do this.

Sixth Steps (5)

- Look into dropping products that simply cannot be secured.
  - There are simply some systems that no amount of effort can secure, they are just flawed.
  - Drop the products that there is no hope for, don’t just throw good money after bad.

Sixth Steps (6)

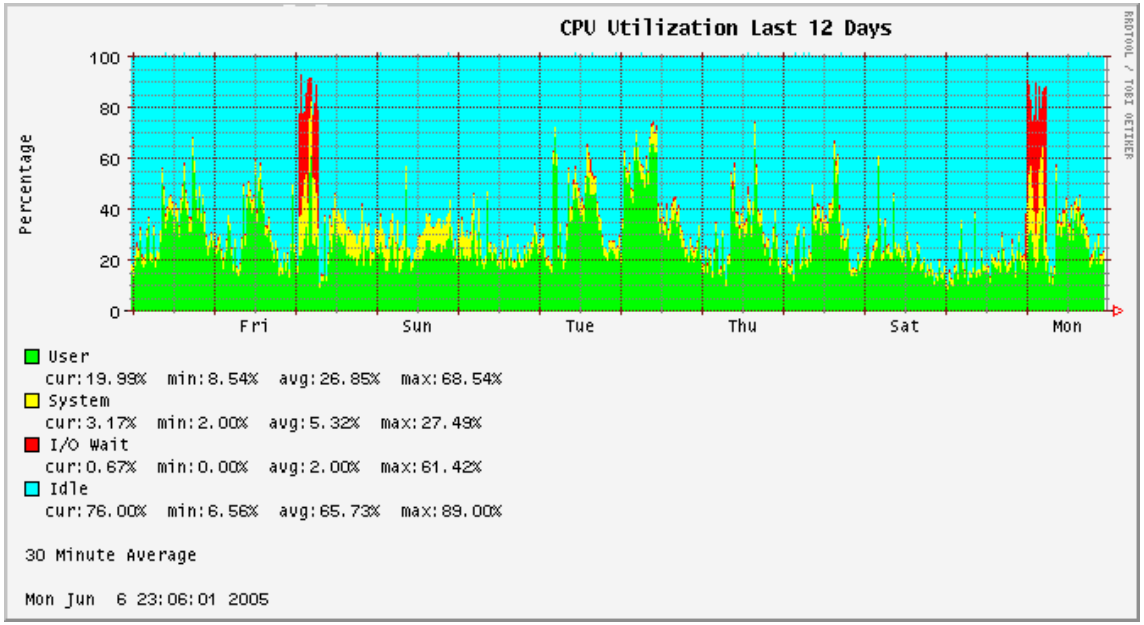
- Consider an IDS.
  - A true IDS can be very time intensive to do correct. If you can't do this right, don't attempt it.
  - If you can't do a true IDS, consider deploying one set to just trigger on traffic that should be blocked by your firewall.
- Get involved with Dsheild. http://www.dshield.org/

Sixth Steps (7)

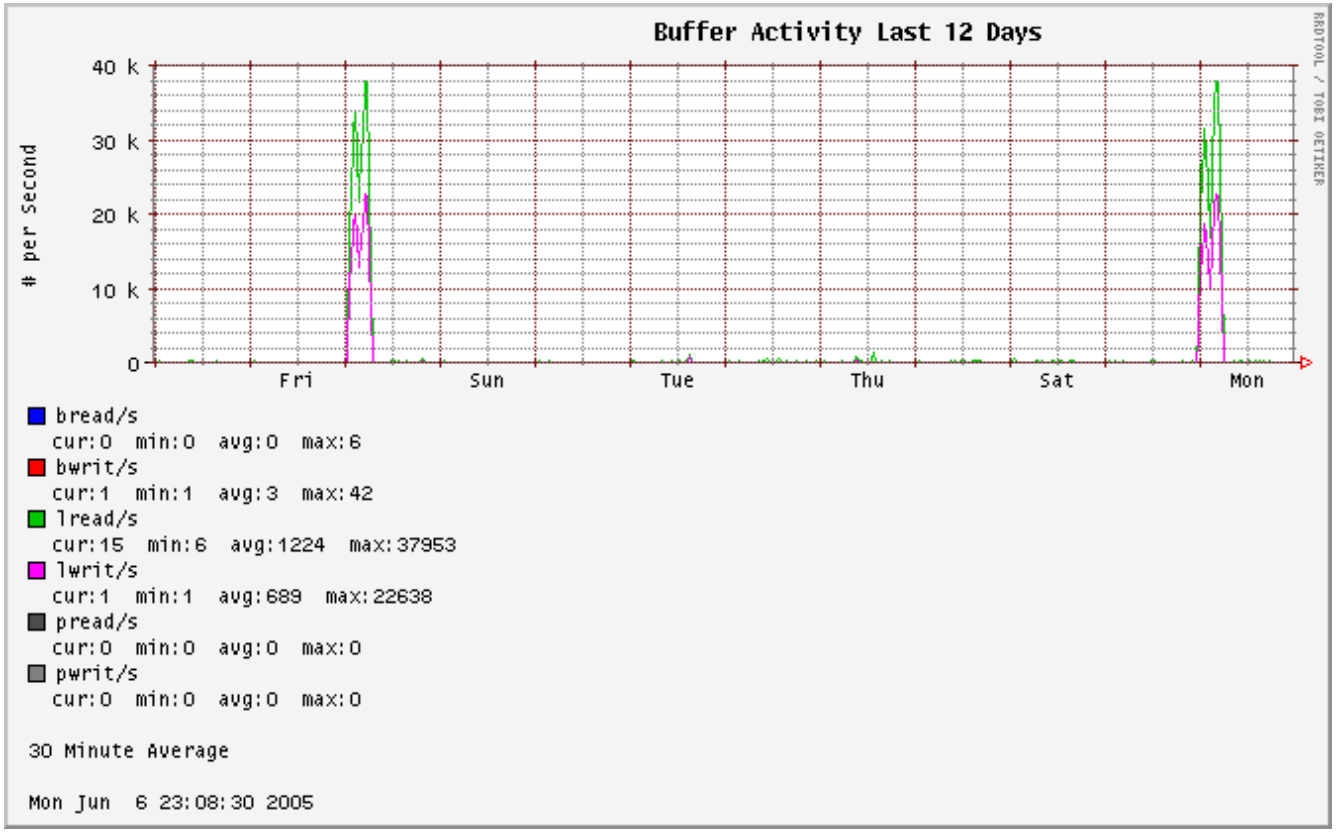
- Trend everything you can!
- Graphing out trends for various systems will make items stand out that would otherwise be hidden.
- Consider trending:
  - Network traffic.
  - CPU usage.
  - RAM usage.
  - Disk usage.
  - On Unix, anything sar will output.

Sixth Steps (8)

- I like to use Big Brother (http://www.bb4.org/) with various plugins (bb-sar) for hosts.

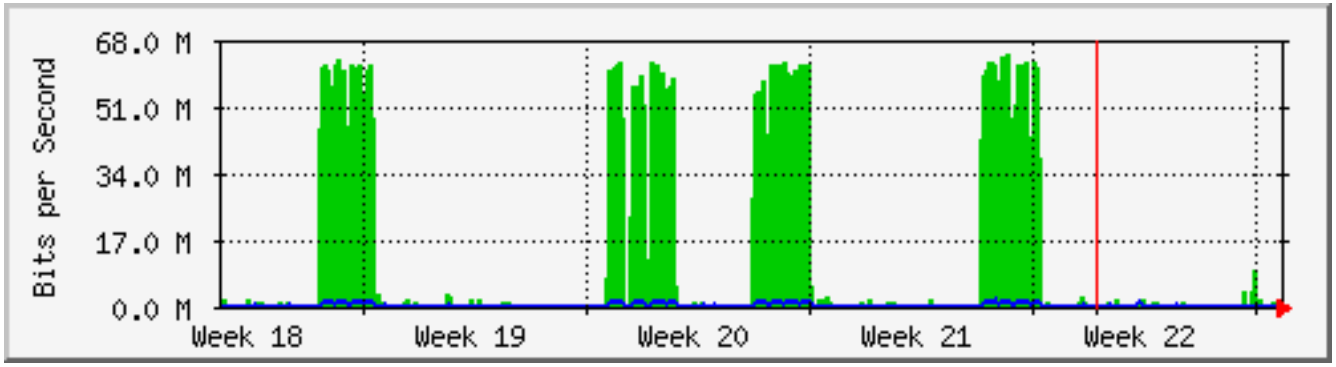


Sixth Steps (9)



Sixth Steps (10)

- MRTG (http://people.ee.ethz.ch/~oetiker/webtools/mrtg) is the old standby for SNMP data.



Wrap Up (1)

- All that was pretty basic!
- After going through these steps, what have you accomplished?
- The biggest thing you have accomplished is you have given your self tools to enable you to know what is happening on a wider scale.
- Knowing your network is the only way to protect your network.

Wrap Up (2)

- The single most important part of securing your network is you.
- Tools are only as good as the person using them.
- Invest in yourself.

Wrap Up (3)

- Subscribe to mailing lists.
  - http://seclists.org/
- Spot check your systems on a regular basis. Compare to your previous documentation, and see what has changed.
- If you don’t know what normal looks like, you won’t know what abnormal looks like.

Wrap Up (4)

- Security is more mindset and point of view than tools and software.
- Don’t compromise.
- For years we have used “Default Deny” as the basis for our firewalls. That policy needs to be applied to all aspects of our networks.
  - If something is not **needed**, don’t have it there.

Wrap Up (5)

- Don’t be scared of the size of the work. Just take it section by section, and each step will improve your situation.
- Security can be fun!
- Hopefully if you were frozen, you now know where to start.
  - Every step helps the situation.
- There is no shame in being busy.
  - There is only shame in doing nothing.