A Security Sampler

Kevin Fenzi, tummy.com, ltd.

kevin@tummy.com

2004-10-12

Outline

- updates
- firewalls
- secure shell
- security enhanced Linux
- virus scanning
- wireless security
- virtual private networks
- email security

Updates

- keep up with your distribution!
- Easy to do with most major distributions
- Lots of tools to check for updates
- CD's available if you can't download

Updates (continued)

- yum, apt, emerge
- Be careful of totally automated updates
- check signatures
- remove packages you don't use/need

Firewalls

- most installs setup simple firewall
- everything denied unless specifically allowed
- clients need very little allowed
- iptables/netfilter
- ipfwadm, ipchains going away.

Firewalls (continued)

- logging can be useful
- rate limit with logging: -m limit --limit 1/sec --limit-burst 20
- firewall even internal machines

Secure Shell

- never ever use telnetd
- prefer version 2
- use keys where possible
- keep keys on secure machine/drive
- use for remote X applications
- use even on private networks

selinux

- written by NSA
- all GPLed
- modifies kernel to use MAC (mandatory access control)

selinux (continued)

- extended attributes
- files are labeled according to a policy
- security context
  - roles
  - objects
  - type
  - user

selinux (continued)

- roles and users are checked against objects and types
- very fine grained control
- permissive vs enforcing
- will ship “somewhat” enabled in FC3

Virus Scanning

- useful for windows clients
- ClamAV
- scan samba shares
- scan emails as they arrive

Wireless Security

- “closed” network
- restrict to MAC address
- WEP (old)
  - easily broken
  - performance hit
- WPA (new)
  - not as easily broken
  - performance hit
- Use a VPN

VPNs

- virtual private network
- avoid IPSEC if possible
- avoid binary only
- openvpn
  - works on Linux, windows, macosX
  - easy to setup
  - uses SSL as back end
  - No kernel mods needed

VPNs (continued)

- openvpn (continued)
  - can send all traffic except vpn/local over vpn
  - can use SSL certificates
  - can be setup as a bridge instead of a router

Email Security

- gnupg encryption
- gnupg signing
- integration with many MUA's now
- kgpg, gpgme
- key servers to distribute keys
- use SSL/TLS for pop/IMAP/SMTP where available

Email Security (Continued)

- Can filter at the MTA level attachments, etc

References

- these slides: http://www.tummy.com/Presentations/SecuritySampler
- yum: http://linux.duke.edu/projects/yum/
- netfilter: http://www.netfilter.org
- Openssh: http://www.openssh.com/

References (continued)

- selinux:
  - http://www-106.ibm.com/developerworks/library/s-selinux/
  - http://www.crypt.gen.nz/selinux/faq.html
  - http://www.nsa.gov/selinux/info/faq.cfm
- clamav: http://clamav.net/

References (continued)

- openvpn: http://openvpn.sf.net/
- gnupg: http://www.gnupg.org/
- kgpg: http://devel-home.kde.org/~kgpg/