



# Intermediate Linux

Hal Corcoran

Technical and Operational

Services

Office of Information

Services





# Intermediate Linux

- Documentation/Resources
- Password/ Privileges and Super User.
- Updates
- Security
  - Threats
  - Countermeasures/tools





# Help!

- Linux is generally very well documented (if you know where to look)
- Local Linux Documentation
  - *man* pages
    - *man -k*
    - *apropos*
  - *info* command
  - KDE help
  - `/usr/share/doc` directory



• Next -> Online resources  
University of Rhode Island





# Online Linux Help Resources

- mailing lists and newsgroups
  - The Linux Documentation Project
    - [www.tldp.org](http://www.tldp.org)
  - google
    - [www.dejanews.com](http://www.dejanews.com)
  - [www.redhat.com/docs](http://www.redhat.com/docs)
  - [www.gnu.org/manual](http://www.gnu.org/manual)





# Security Resources

- Platform-independent sites
  - [www.sans.org](http://www.sans.org)
    - System Admin Network Security
  - [www.cert.org](http://www.cert.org)
    - Computer Emergency Response Team
  - [www.securityfocus.org](http://www.securityfocus.org)
    - Info on a wide variety of security-related topics.





# Passwords

- No dictionary words
- No common names
- 6+ characters
- The best passwords combine alphabetic, numeric, and special characters.
  - Avoid control characters which may have special meanings in Linux.





# Good Practices

- Choose good for passwords for administrative accounts.
- Check root's mailbox regularly, or forward root's mail to yourself at another account.
- Monitor system logs frequently.
  - logwatch
- **Principle of Least Privilege:**
  - Never do as **root** what you can do as a less-privileged user.





# up2date

- Up2date is Red Hat's package updating facility
- Red Hat Network
  - Very well-supported for Advanced and Enterprise customers.
  - Free support for Fedora is overworked.
  - URI TOPS runs a mirror site for Fedora updates





# URI Fedora Update Mirror

- In order to use URI's mirror for getting updates for Fedora distributions, make the following changes to the file `/etc/sysconfig/rhn/sources`.
- Comment out the lines beginning with “yum” by putting a “#” character at the beginning of the line.
- Add the following 2 lines:
- yum URI-FC2-Base <ftp://rsync.uri.edu/fedora/2/i386/os/>
- yum URI-FC2-Updates <ftp://rsync.uri.edu/fedora/updates/2/i386>





# Security, security, security!

- The biggest mistake new Linux admins make is usually failing to properly secure, manage, and monitor their Linux systems.
- The current Linux administrative tool set makes these tasks easier than ever before.
- A Linux system is NOT something you can just set up and then leave alone!
- Linux systems are high-value targets for hackers.





# Sniffing

- TCP/IP traffic on the network consists of packets transmitted between devices on the network.
- Sniffing is the act of monitoring network traffic by capturing packets that are not meant to be received by your system.
- System and Network administrators may sniff for legitimate reasons, such as troubleshooting.
- A malicious sniffer may capture a wide range of information about systems and the network, including user and password information, etc.





# Sniffing (Cont'd)

- The “Switched Network” argument only goes so far.
  - Under overload conditions, a switch may behave like a shared medium, broadcasting packets to all ports.
  - How secure is your switch?
    - Is it accessible remotely? How secure is the password? Has it been transmitted in plain text?
  - How secure is the remote network, and everything in between?
- Encryption of sensitive information is the answer to sniffing.





# Logging in Remotely

- Telnet is deprecated except on **extremely secure** networks
- Secure shell (ssh) is the preferred method of remote login access
  - Connections are encrypted
  - *scp* utility (secure version of rcp)
  - X-11 forwarding
  - compatibility with other remote-access programs

(e.g. rsync)

University of Rhode Island





# Web Servers

- If authentication is used or sensitive information is collected by your web pages or forms, consider investing in a certificate and setting up SSL.
- Linux (openssl) also allows you to create your own self-signed certificates.
  - User must verify and accept the self-signed certificate the first time the browser connects.





# WWW/CGI Scripting

- CGI, PHP, ASP etc. scripts may introduce vulnerabilities into your web server.
- Be restrictive about who can execute scripts on your server.
- Execute scripts as the least-privileged user possible.
- When developing your own scripts, be careful to sanitize input data and check bounds.
- When installing 3rd-party scripts, be sure to stay abreast of patches and updates, etc.





# LAMP Platform

- LAMP = Linux Apache MySQL PHP
- Flexible and powerful platform for integrating web servers and databases.
- SQL Injection
  - Injecting SQL code into scripts in such a way as to read or modify database contents not normally accessible to the user.
  - Also a problem with ASP, etc.
  - No silver bullet, mitigated by input bound checking and sanitizing, especially of quotes.





# Insecure Services

- rsh, rlogin, rexec
- finger, talk
- NFS, Portmapper
- Telnet
- It's a good idea not to run these services, or any service, if it's not necessary, and to restrict access to necessary services as much as possible.





# Brute Force Attack

- Brute force is an attempt to guess a valid user/password combination.
- Automated tools can try a large number of combinations in a relatively short time
- Not a very effective method of attack unless a system is found with weak or default passwords set.
- Strong passwords and prompt changing of default application password foil Brute Force attacks.





# Scanning

- Scanning tools may be used to discover hosts and services on the network.
- URI systems and networks are scanned on a daily basis in a search for vulnerable hosts and services.
- Disabling unnecessary services and restricting access to necessary ones will help protect your system against most attacks.
- Scan your systems yourself to see what kind of profile you system presenting to the rest of the Net.  
“See yourself as hackers see you.”





# Buffer Overflows

- Buffer overflows are generally programming errors which can allow an attacker to write into system memory and execute arbitrary instructions.
- If a program accepts data without checking or limiting the size of the data, a buffer overflow may result.
- The best protection against software containing buffer overflows is keeping your software up to date and minimizing the number of applications available on your system from the Internet.





# Root Kits

- If a system is compromised, the attacker may install a software package called a root kit.
- A root kit replaces key system utility programs, often creating back doors and masking the presence of the intruder.
- Once a system has been root-kitted, the system utilities can no longer be trusted.
- The only comprehensive solution to a root kit is to reformat and reinstall!





# Key Secure Practices

- Know what services are running on your system, enable only necessary services, and limit access to services to the extent possible.
- Stay up to date on patches and updates.
- Run closed system whenever possible.
- Always change default passwords, choose strong passwords, avoid unencrypted transmission.
- Monitor system logs frequently (logwatch).





# Tools

- Nmap
- Tripwire
- Encryption (Secure Shell, Secure FTP, SSL, etc.)
- Port Sentry
- Packet filter (iptables)





# nmap

- nmap is a scanning tool which can identify hosts and services on the network.
- Powerful Tool for System Admins and hackers too.
- nmap can show you how your system looks to other on the Internet.





# Tripwire

- Tripwire is a host-level intrusion detection system
- Tripwire takes a snapshot of system files.
  - MD5 hash values
  - Modification and creation times
  - file size
  - inode, etc.
- Tripwire reports filesystem changes since the last snapshot was made.





# Encryption

- ssh
- sftp
- SSL
  - Tunneling





# Packet Filters

- iptables, etc.
  - Stateful inspection packet filtering and decision making
  - Network Address Translation (Masquerading)
- iptables is a highly-configurable packet filter
  - Coarse-control via “Security Level” GUI interface
  - Fine-granular control via command-line interface
    - SYN, etc.





# Port Sentry

- Port Sentry listens on network ports for scanning activity.
- Port Sentry can block access from a scanner's IP address at the TCP/IP (iptables) or application (/etc/hosts.deny) level.
- A sophisticated attacker might be able to create a Denial-of-Service by using packet spoofing.





# Thank You!

