Host-based attacks and defenses
SSH
Common attacks against SSH

- Attempting to login as default users
- Brute-force password guessing
- Protocol attacks against v1

http://www.ciac.org/ciac/bulletins/m-017.shtml
Why worry about SSH in particular?

- The service is commonly used and generally can't be blocked at the border.
- Successful compromises of SSH servers are difficult to detect at a network level.
- Often used to allow remote access to large groups of hosts
- Enabled by default on some servers and often overlooked
Things everybody can do

- Do not allow remote logins from the root user.
- Use a software firewall. Block packets that are not well-behaved. Examples: packets with SYN bit set that aren't part of a session, packets with both SYN-FIN yet, etc. TCP wrappers are better but aren't always available.
- Regularly audit your logs.
What about using different ports?

If you want, but this isn't strong security. Why not?

● SSH banner still identifies SSH server
● Sniffers can still identify traffic going to server/port as SSH traffic
● Scanning is not limited to port 22
You might. . .

- have a small audience of users that need to access your server from a limited set of locations.
- have a large audience of users that need to access your server from anywhere.
Limited list of locations

- Use TCP wrappers or ACL's or fill-in-your-favorite method here to limit SSH connections to authorized hosts.
- Even limiting to just the U campus is an improvement.
- Use TCP wrappers to deny access to hosts where reverse DNS doesn't match, or (more paranoid) hosts without valid DNS. Note: Connectivity depends on reliable DNS.
But I can't limit the list of IP addresses.

• Use SSH keys instead of password authentication and disable password authentication entirely.

• Block hosts who trigger 'Illegal user' alerts in the SSH logs. These are generated when a user attempts to log in with a username that doesn't exist.

• Extra bonus points for blocking IP addresses from all your SSH servers when one is attacked.
Blocking hosts who trigger 'Illegal user' alerts

Several tools available, all of these basically watch the logs for the alert then temporarily or permanently block that IP address.

Swatch, sshdfilter, LogWatch, etc.

Overview of scripts/tools available:

http://www.hexten.net/pam_abl
http://security.linux.com/article.pl?sid=05/09/15/1655234&tid=35
Conclusion

SSH servers are a large target these days. Do everything you can to protect them.
Exercises

- Use Hydra to brute force passwords on your SSH server – what do the logs look like?
- Disable the ability of root user to login via SSH
- Start the SSH server on a different port and scan with nmap
- Set up blocking for IP addresses that trigger 'Illegal user' alerts (swatch)
- Set up and successfully use an SSH key
Apache
Common attacks against web servers

- Denial of service attacks
- Attacks against dynamic pages – perl, asp, python, etc
- Defacements (Zone-h for examples)
Why worry about web servers in particular?

- Web pages are generally supposed to be available to large audiences – limiting access is rarely a viable option.
- Compromised web servers can be used to infect other machines on a large scale.
- Can have a high embarrassment factor.
- May collect sensitive data.
Things everybody can do

- Limit the services run on the web server to the minimum possible.
- Use a software firewall. Block packets that are not well-behaved. Examples: packets with SYN bit set that aren't part of a session, packets with both SYN-FIN yet, etc. TCP wrappers are better but aren't always available.
- Regularly audit your logs.
- Limit the rights of the users that run the scripts to the minimum necessary.
Exercises

- Setup and configure a software firewall.