# LINUX AND SECURITY

# OBJECTIVES

- Understand what threats Linux faces
- Discuss what items administrators need to be concerned with
- Understand there is no such thing as a secure computer

# IS LINUX SECURE?

- Linux can be configured in a way that it is as secure as every other OS out there
- NO COMPUTER OR OS IS COMPLETELY SECURE!
- Linux can be configured nearly any which way you want it to be configured
- This also provides pitfalls if we provide secure measures incorrectly

# BENEFITS OF LINUX FOR SECURITY

- Most software on Linux is open source – so you have communities of developers helping to secure it
- The Linux kernel itself is relatively secure
- Software usually has less privileges
- Size is smaller, so software, not kernel is sought after

# HOW LINUX MAY BE COMPROMISED

- Software vulnerabilities
- Configurations errors
- Social Engineering or Users in general
- Rootkits, Viruses, and Trojans

# SOFTWARE VULNERABILITIES

- Buffer overflows are still the number one software vulnerability
- Linux software is not infallible
- “Linus Law” states – “given enough eyeballs, all bugs are shallow” – meaning the more people you have looking at software the more it is secure and bugs are patched, however some bugs still make it through
- Developers of custom software may not have luxury of testing software
- Software may not be patched

# CONFIGURATION ERRORS

- Since software needs to be installed in a certain, typically, in Linux, configuration pages may have enhanced privildges
- It's very easy to do something in Linux
- It's very hard to undo something in Linux
- Forgetting to close ports or remove configuration pages is a common issue

# SOCIAL ENGINEERING AND USERS

- Even though it is the job of the system administrator to make sure systems are secure, humans are not 100% infallible
- Users may make mistakes
- Amazon and other larger corporations have been taken down because of a simple, inadvertant command

# ROOTKITS, VIRUSES, AND TROJANS

- There are still rootkits, viruses and Trojans that are developed for Linux, but not in the same ballpark as other OS's
- Moris Worm in 1988 was the first Linux worm
- Linux has open source AV however
  - chrootkit
  - Rkhunter
  - ClamAV

# CONCLUSION

- Administrators need to be diligent in securing Linux systems
- While Linux does not contract viruses in a traditional sense typically, they are a target for hackers who wish to exploit software vulnerabilities