A Little bit of Network Security

INFO 341

Why is security important?

Some Common Threats

- Password/Authentication
- Trojan Horse
- Worm
- Virus
- Macro Virus
- Email Attacks
- Network Attacks
- Code Attacks
- Social Engineering

What is a password-authentication attack?

Preventing password-authentication attack?

- Require 7-8 character or longer passwords
- Don't use "real" words, instead use a combination of letters, numbers or special characters – consider using a phrase like stb&^av "Squash tomatoes beans and carrots are vegetables"
- Change the administrator or root password periodically
- Consider asking users to change their passwords regularly – but be careful about forcing people to change too often
- Educate users not to share their passwords with others

What is a Trojan Horse?

What is a Trojan Horse?

- A malicious program that masquerades as a legitimate program.
- People who 'share' software were often at more risk.
- These seem to be less common these days.

What is a Worm?

What is a Worm?

- Worms are stand-alone programs that are designed to search for known vulnerabilities and exploit them.
- Once they find a hole, they propagate by copying themselves to that new host and start executing.
- They are typically able to propagate very quickly and are the source of most of the serious outbreaks

What is a Virus?

What is a Virus?

- A piece of executable code attached to (inserted in) a legitimate program.
- Can only execute when the legitimate program runs
- Spreads by infecting un-infected copies of the legitimate or other programs.

What is a network attack?

What is a network attack?

- Packet Sniffing
  - Find interesting data
- Port Scanning
  - Find, well-known, insecure services

What is a code attack?

What is a code attack?

- An attack that takes advantage of a software flaw or deeper understanding of a protocol
- Buffer Overruns
- Denial of Service (DoS), Distributed Denial of Service (DDoS)
  - Rely on external compromised machines (botnet)
  - SYN Flood
  - ICMP Flood

What is 'social engineering'?

What is 'social engineering'?

- An exploit that plays on an individuals' notions of proper authority or an individuals' naiveté.
  - "Hi, I'm Jake Smith, I work in the IT group. I need to fix your roaming profile. If you give me your password I'll have it fixed in just a second."
  - "Hi, my name is Darrin, I'm with your ISP …"

What can be done?

A useful resource

- Computer Emergency Response Team (CERT) provides a central coordination point for many security issues
- http://www.cert.org/