

Homework 9

Review 6.1

- Social engineering attacks - that convince users to install trojans or get phished,
- Infect existing exe's
- exploit software vulnerabilities through worms

Review 6.11

- Backdoor - passes through normal authentication procedures to get access to the system
 - can be presented as either a worm or trojan
- Bot - remotely controlled and is installed secretly. Can take over computer entirely
 - usually wants to stay discrete
- Keylogger - captures keystrokes to monitor sensitive information of a user. Gains virtually all text information
- Rootkit - programs installed to gain admin privileges while being hidden. Has complete control of the system
- Spyware - gathers info and transmits it to another system.
- They are all separate packages

Problem 6.3 All the commands in the metamorphic code end up reversing itself, resulting in the same program as the Original Code

Problem 6.5 - This is a Logic Bomb. They are used to perform some malicious function when a condition is met

Problem 6.6 Backdoor, program allows secret access to the login '1337 H4ck0r' to giving higher privileges compared to the common user

Problem 6.10 The malware could collect info of contacts in the user's phone through a Trojan Horse. Should be suspicious if the app has nothing to do with messaging.
• Could also send messages to people

Problem 6.11 Selecting the "Open" button means it's either a Trojan or a Worm. User can check suspicions if they scroll through the image and read the code without opening or launching. This is a phishing attack. This can be sent to one or a group of people in hope someone clicks it.