Simple Bash Backdoor

- Bash is a very powerful command language.
- Used in Unix & Uinx-like operating systems, this includes :
  - Linux.
  - Mac OS X.
  - IOS.
  - And Android.
- Bash can be used to send a reverse shell to a remote computer.

-> The result is a one like command that can be used as a backdoor and would work on all of the operating systems mentioned above!

ZLogger

- Remote keylogger for Linux.
- Runs in the background of target system.
- Reports every key pressed on the target machine to email.
- Starts with system boot.
- Does not require root.

LazaGne

- Post exploitation tool to retrieve saved passwords on local computer.
- Recovers saved passwords from lots of programs.
- Recovers passwords from memory.
- Works with Windows and Linux.
- Displays results on screen or store it on local machine.

Execute & Report

- Simple payload.
- Executes a command.
- Waits for result and sends it by email.
- Execute linux commands and get info from computer.
- Download a file, execute it and report its output.
- ....etc.

Creating a Linux Trojan

Problems:

- Executables don’t run by double click.
- User have to manually change file permission to executable.
- Therefore user’s can’t be fooled into running an image or a pdf as an executable.

Solution :

- Embed evil code in an executable package.
- Use a legitimate app to make the rojan less suspicious.
- Runs by double click with root (admin) privileges.

Creating An Android Trojan

- Embed a backdoor in a normal app.
- Everybody makes apps these days.
- Pretend to be a friend and send the app to the target.
- When the app is executed, the user will see a functional app but at the same time our backdoor will run in the background.