Activity 2.1.1 - Seven Steps of Hacking

Instructions: (1) instructor cuts sections into slips of paper, (2) mixes the slips, (3) gives the pile of slips to student groups. (Each group gets one set).

Task - The groups must work together to put slips into proper order for a hack. They paste it onto a sheet of paper and hand it in with names of students in their group.

Installing Backdoors - Most hackers will also install a backdoor to allow them access in the future. A backdoor is a hole deliberately left in place to allow access from an uncommon path.

Escalating Privileges - When a hacker gains access to the system, he will only have the privileges granted to the user or account that is running the process that has been exploited. Gaining access to root or administrator will allow the hacker more access or greater power throughout the network. An exploited application that is running under a root user will give the hacker immediate root access. However, if the application that is exploited is not running under a root, the hacker must perform additional actions to earn it. This usually entails trying to crack the passwords.

Covering Tracks - The hacker will usually take the time and effort to modify system logs to hide their actions and try to mislead forensic investigators that a crime has been committed.

Recon/Foot Printing - includes a combination of tools and techniques used to create a full profile of the organization's security posture. These include its domain names, Internet Protocol (IP) addresses, and network blocks.

Gaining Access - Because each device and operating system in your network has a unique security posture, the information provided during system scanning and probing can give hackers insight as to the easiest path into your system.

Exploiting - Exploiting the system can take many forms. Hackers who do it for fun or a challenge will change a web page or leave a "calling card" to let their peers know they were successful. Many hackers are breaking into systems for financial rewards. They will generally download valuable information that can be sold to other parties later. Sometimes, you may even come across a disgruntled employee who may gain access to sabotage the organization.

Scanning/Probing - A hacker will typically perform a series of scans or probes to gather more information about individual machines to gain unauthorized access to the system later. These scans may include ping sweeps, TCP/UDP scans, and operating system identification.