1. Give three examples of excellent passwords and explain why each would be a good choice to protect a system from unauthorized users.
Tw1nS3rp3nt12$*(***twinserpent***)
1Like3.1415d0U!%?(***I like pie do you?)***
91nc4N@1l$ (***Nine Inch Nails***)
I personally don't use or know anyone that uses these as passwords, but I do believe they would be good because they are easy for me to remember and are unusual (**A good password is unusual, memorable**). I have a friend that has two pet snakes and is 3 years older than me, I also like pie and NIN. These passwords also have a combination of characters and numbers, is difficult for someone else to guess, has a minimum of eight characters and uses upper- and lowercase characters.

3. System managers can't protect their resources without recognizing all threats and even learning to think like an intruder. Knowing that, and knowing that it's unethical to use a computer system without proper authorization, imagine that you are an unauthorized user who wants to break into your system. Describe how you might begin guessing the password of a legitimate user.
There are a number of ways to accomplish this, some good suggestions were provided in our textbook. I could search the user's desk for a written reminder, try the user's name, try the user birthday, anniversary date, children's birthdates, etc. I could also try the user ID as the password, search log-on scripts and even try names of family members, pets, and hobbies.

5. Imagine that you are the manager of a small business computing center. List at least three reasons that you would use to convince a busy, reluctant staff member to perform regular backups and manage your system's archives appropriately, and elaborate.
Having sufficient backup and recovery policies in place and performing other archiving techniques are standard operating procedure for most computing systems.
Backups become essential when the system becomes unavailable because of a natural disaster or when a computer virus infects your system. If you discover it early, you can run eradication software and reload damaged files from your backup copies.
Any changes made since the files were backed up will have to be regenerated. Most system failures are caused by honest mistakes made by well-intentioned users—not by malicious intruders.

No matter the environment of the company you work for creating a backup of the files you use is always good practice. It not only lessens the burden of the system administrator but also prevents the user from panicking when their system crashes or obtains malicious software. There would be no reason to feel you do not have the time. Once you make a habit of creating backups and your system is in the rhythm of conducting a backup it no longer becomes a burden and is rather simple and fast to do.

9. List 20 viruses discovered in the past 12 months and research three in detail, describing which files they infect, how they spread, and their intended effects.
ALL INFORMATION WAS RETRIEVED FROM THE SYMANTEC WEBSITE (EVEN THOUGH I USE AND PREFER VIPRE ☺)
Trojan.Ransomlock.O was discovered on 05/18/2012
Trojan.Ransomlock.O is a Trojan horse that locks the desktop making the computer unusable. It then asks the user to pay to have it unlocked. When the Trojan is executed, it copies itself to the following location:
%UserProfile%\Application Data\froot\froot.exe. The Trojan then creates the following registry entry so that it executes whenever Windows starts:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Free" = "%UserProfile%\Application Data\froot\froot.exe -b"

W32.Stekct was discovered on 05/17/2012
W32.Stekct is a worm that attempts to spread through instant messaging and social networks. It also opens a back door on the compromised computer. The worm spreads through instant messaging and social networks and arrives as the following file:
%Windir%\MDM.EXE
When the worm is executed, it creates the following registry entries so that it executes every time Windows starts:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Microsoft Firevall Engine" = "%Windir%\MDM.EXE"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Microsoft Firevall Engine" = "%Windir%\MDM.EXE"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run\"Microsoft Firevall Engine" = "%Windir%\MDM.EXE"
The worm then adds itself as a Window's trusted network process:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\"%Windir%\mdm.exe" = "%Windir%\mdm.exe:*:Enabled:MSN Messenger"

Packed.Generic.368 was discovered on 05/17/2012
Packed.Generic.368 is a heuristic detection for files that may have been obfuscated or encrypted in order to conceal themselves from antivirus software. This heuristic detection is used to detect various threat families.

Packed.Generic.367 was discovered on 05/16/2012
Packed.Generic.367 is a heuristic detection for files that may have been obfuscated or encrypted in order to conceal themselves from antivirus software. This heuristic detection is used to detect various threat families.

VirusDoctor!gen12 *(Misleading Application)* was discovered on 05/16/2012
VirusDoctor!gen12 is a heuristic detection used to detect threats associated with VirusDoctor. Files that are detected as VirusDoctor!gen12 are considered malicious.

Android.Acnetsteal was discovered on 05/16/2012
Android.Acnetsteal is a detection for Trojan horses on the Android platform that steals information from the compromised device. The Trojan may arrive as an APK package.

Android.Acnetdoor was discovered on 05/16/2012
Android.Acnetdoor is a detection for Trojan horses on the Android platform that open a back door on the compromised device. The Trojan may arrive as an APK package.

W32.Wergimog.B was discovered on 05/17/2012
W32.Wergimog.B is a worm that attempts to spread through removable drives. It also opens a back door and may steal information from the compromised computer. When the worm is executed, it copies itself as one of the following file:
%UserProfile%/Application Data/Microsoft/services[THREE RANDOM NUMBERS].exe
Next, the worm may create the following registry entries, so that it executes whenever Windows starts:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Adobe Reader Speed Launcher" = "%UserProfile%/Application Data/Microsoft/services[THREE RANDOM NUMBERS].exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Adobe Reader Speed Launcher" = "%UserProfile%/Application Data/Microsoft/services[THREE RANDOM NUMBERS].exe"
Next, it creates the following mutexes so that only one instance of the threat executes on the computer:
skkd)*u32hqiajnzja
(asdj2j3e)*oqwjkz
It starts the Explorer.exe process and injects its code into it. It may also inject itself into other processes as well. It won't inject itself into the following system related processes:
System
System Idle Process
csrss.exe
It then attempts to open a back door by connecting to the following remote locations on port 5786:
ns2.kasprsky.org
ns2.lksadxniuszkla.org

Backdoor.Linfo was discovered on 05/16/2012
Backdoor.Linfo is a Trojan horse that opens a back door on the compromised computer. When the Trojan is executed, it creates the following files:
%ProgramFiles%\Internet Explorer\lg.dat
%Windir%\tp.ds
%Windir%\tp.dat
%Windir%\linkinfo.dll
It then creates the following mutex so that only one instance is running on the compromised computer:
ExplorerIsShellMutex

Next, it opens a back door by connecting to the following locations and awaits commands from the remote attacker:
[http://]www.ancold.org.au/mycfg/mycmd/[ENCODED HO[REMOVED]
[http://]www.ancold.org.au/mycfg/myscr/Myup[REMOVED]
The remote attacker is able to perform the following actions:
Upload system information
Download, upload, execute, delete, move, and copy files
Start a remote shell
List running processes
List contents of local drive
Search for local files
Create and remove directories
Download an updated configuration file
Change the frequency of the intervals in which the computer contacts the remote server
Execute shellcode
Change command and control servers
Shut down or reboot the compromised computer
Log off the current user

Backdoor.Wiarp was discovered on 05/16/2012
Backdoor.Wiarp is a Trojan horse that opens a back door on the compromised computer. When the Trojan is executed, it creates the following files:
%SystemDrive%\Documents and Settings\All Users\Application Data \MicroTemp\werport.dll
%SystemDrive%\Documents and Settings\All Users\Application Data \MicroTemp\wiarpc.dll
Next, it opens a back door by connecting to the following location and awaits commands from the remote attacker:
[http://]update.yahoo-upgrade.com/ch[REMOVED]
The remote attacker is able to perform the following actions:
Inject files into running processes
End running processes
Create a service
Download a remote file
Open a command line

Backdoor.Vasport was discovered on 05/16/2012
Backdoor.Vasport is a Trojan horse that opens a back door on the compromised computer. When the Trojan is executed, it copies itself as the following file:
%UserProfile%\Application Data\conime.exe
It then creates the following registry entry so that it runs every time Windows starts:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"ServiceEXE" = "%UserProfile%\Application Data\conime.exe"
Next, it opens a back door by making a HTTP POST connection to the following location:
svr01.passport.serveuser.com
The Trojan is capable of tunneling through a proxy. It may also download and execute a potentially malicious file.

Packed.Dromedan!gen3 was discovered on 05/15/2012
Packed.Dromedan!gen3 is a heuristic detection used to detect threats associated with the Downloader.Dromedan family of threats. Files that are detected as Packed.Dromedan!gen3 are considered malicious.

Backdoor.Briba was discovered on 05/15/2012
Backdoor.Briba is a Trojan horse that opens a back door on the compromised computer.

Backdoor.Nerex was discovered on 05/15/2012
Backdoor.Nerex is a Trojan horse that opens a back door on the compromised computer.

Backdoor.Ritsol was discovered on 05/15/2012
Backdoor.Ritsol is a Trojan horse that opens a back door on the compromised computer.

Trojan.Smoaler!gen3 was discovered on 05/15/2012
Trojan.Smoaler!gen3 is a heuristic detection used to detect threats associated with Trojan.Smoaler. Files that are detected as Trojan.Smoaler!gen3 are considered malicious.

Trojan.Festi was discovered on 05/13/2012
Trojan.Festi is a Trojan horse that downloads files on to the compromised computer. When the Trojan is executed, it drops the following kernel driver file:
%System%\drivers\[RANDOM FILE NAME].sys
Next, the Trojan creates the following registry subkey to register itself as a service so that it executes whenever Windows starts:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[RANDOM FILE NAME]
Next, the Trojan attempts to connect to the following remote location in order to download and execute more files on the compromised computer:
muduck.ru

Packed.Generic.366 was discovered on 05/11/2012
Packed.Generic.366 is a heuristic detection for files that may have been obfuscated or encrypted in order to conceal themselves from antivirus software. This heuristic detection is used to detect various threat families. Files that are detected as Packed.Generic.366 are considered malicious.

Android.Gamex was discovered on 05/10/2012
Android.Gamex is a Trojan horse for Android devices that downloads further threats. The Trojan may arrive as a package with the following details:
Version: 1.5.2 **Name:** de.mehrmannd.sdbooster
Permission: When the Trojan is being installed, it requests permissions to write to external storage devices.
Installation: Once installed, the application will register the following service:
com.android.md5.Settings
The threat will then attempt to gain root access on the device. If it is successful it will attempt to get the following embedded packages form /assets/logos.png:
com.android.setting

com.android.update
It will also copy com.android.setting to /system/app/ComAndroidSetting.apk.
System monitoring: The Trojan will then gather the IMEI and IMSI numbers and send them to a remote server.
Downloading: The Trojan also downloads other threats on to the device.
Functionality: The Trojan also monitors SCREEN_ON and SCREEN_OFF status on the phone. If in the SCREEN_OFF status is active, it will launch the downloaded apps. If the SCREEN_ON status is active, the Trojan launches the device's home screen.

Trojan.Tatanarg.B was discovered on 05/10/2012
Trojan.Tatanarg.B is a Trojan horse that attempts to steal information from the compromised computer. The Trojan injects its code into the explorer.exe process. The Trojan connects to the following locations on port 31439:
www.[DOMAIN NAME]/g.php
***Note**: [DOMAIN NAME] is variable and subject to change.*
The Trojan drops the following file:
%UserProfile%\Application Data\Identities\[RANDOM CLSID]\LicenseValidator.exe
The Trojan creates the following registry subkeys:
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\StartCurrId
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\StartMainId
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\PersistFolder
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\PersistFile
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\StartProcIrq
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\StartMainMask
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\StartCurrMask
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\ReserveProgram
The Trojan creates the following registry entry so that it runs every time Windows starts:
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Run\"LicenseValidator" = "%UserProfile%\Application Data\Identities\[RANDOM CLSID]\LicenseValidator.exe"
The Trojan creates the following registry entries:
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\"StartUrlId" = "0"
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\"Browse Files" = "[RANDOM CLSID]"
HKEY_CURRENT_USER\Software\Software\Microsoft\Windows\CurrentVersion\Explorer\"Browse Folders" = "[RANDOM CLSID]"
The Trojan then drops modules in bzip+xor form to the following location:

%UserProfile%\Application Data\TeamViewer\[RANDOM CLSID]\[RANDOM CHARACTERS].dat
The Trojan may monitor activity on the following Web browsers in order to capture details of accessed Web pages:
Sol
Chrome
Firefox
Internet Explorer
Opera
Maxthon
Netscape Navigator
The Trojan captures sensitive information such as data on all processes running, website browsing history, and details of accessed Internet banking sites, and sends it to the following remote locations:
[http://]qualitymayorista.com/swf/[REMOVED]
[http://]klthk.cz/pgm/[REMOVED]
[http://]www.willowbendfitnessclub.com/com/[REMOVED]
[http://]www.go-cube.ch/[REMOVED]
The Trojan may use a fake certificate for man-in-the-middle attacks on banking websites.