Check List: Linux Machines

High Level

- **Install and maintain malware protection software**
    - **Install MalWare (Defender)**
    - **Install AntiVirus (Microsoft Security Essentials)**
- **Account Management**
    - **Remove guest user**
    - **Remove old accounts**
    - **Ensure all accounts use strong passwords**
- **Delete Suspicious Files**
    - **Write down file names and locations that were deleted**
- **Delete Unauthorized Files**
    - **Write down file names and locations that were deleted**
- **Enabling the Firewall**
- **Services (Also called a daemon) Disable unnecessary services**
- **Attach Detection**
    - **Monitor your processes**
    - **Port Checks**
    - **System Logs (syslog)**
- **Network**
- **Installing and Automating Updates**
- **Setting Audit Policies**
- **PAM Files**

Low Level

- Install and maintain malware protection software
    - Install Malware (Linux Malware Detect (LMD))
    - Install Anti-Virus (AVG Anti-Virus)
    - Adding and Removing Software
        - Linux software is bundled into packages
        - Packages are managed by packagemanagers
            - In Ubuntu, the package manager is called “Ubuntu Software Center.”
            - It looks and functions a lot like Mac’s App Store
        - To access Ubuntu Software Center, click the shopping bag on your Ubuntu menu bar
            - Use to manage or uninstall software you have already installed
            - Use to view a log of all the recent software installs, removals, and updates on your system
        - Users must enact root permissions to install, uninstall, or modify software.
- Account Management
    - **Click User Accounts in the System Settings window**
    - Write Down Accounts you delete
    - Account types: User and Root
    - Root–the Linux Administrator account
        - For Ubuntu, the root account must be enabled by giving it a password using the **sudo** command
        - **Sudo** allows an authorized user to temporarily elevate their privileges using their own password instead of having to know the password belonging to the root account
        - Root users are authorized to do many different tasks, but they must first authenticate their identity by entering their password
    - Groups
        - To list all groups: cat /etc/group
        - To add a group: addgroup [groupname]
        - To add a user to a group: adduser [username] [groupname
    - Defaults Users and Groups
        - Permissions and privilege tips
            - Disable login for well known accounts (bin,sys,uucp)
            - Disable all account(s) with no password and lock them down
            - passwd -l {user-name}
    - Turn off guest account
        - Like in Windows, the Ubuntu guest account is turned on by default
            - You should disable it so people can’t access the computer anonymously
        - The guest account is controlled by LightDM, the display manager controlling the Ubuntu login screen
        - To turn off the guest account, edit the LightDMfile:
            - After root authenticating, type gedit/etc/lightdm/lightdm.conf
            - Add the line allow-guest=falseto the end of the Light DM file that pops up and click Save
            - Restart your system and click your username button in the top-right corner of your desktop. The guest account should be disabled.
    - User Accounts
        - Locking a user account may not prevent a user access. They may still be able to gain shell access, without the need for any password.
        - As in Windows, it is important to restrict root (Admin) privileges and password protect all accounts
            - A. To make account management changes, you must enact root permissions by clicking Unlock and authenticate yourself by entering your password
            - B. Switch users from Administrator to Standard User by clicking next to Account Type
            - C. Change passwords by clicking the asterisks next to the Password option
- Delete Suspicious Files
    - Write down file names and locations that were deleted
- Delete Unauthorized Files
    - Write down file names and locations that were deleted

- Enabling the Firewall
  - Enable UFW (Uncomplicated Firewall)
    - Default Ubuntu firewall; but not activated by default
    - Command line interface (frontend for iptables)
    - Configure and enable
      - Set default policies such as drop all connections (deny), then add (allow) rules for specific services
      - Enable logging
    - https://wiki.ubuntu.com/UncomplicatedFirewall?action=show&redirect=UbuntuFirewall
  - Using Gufw
    - You can download Gufw, a graphical firewall interface, from the Software Center and use it to make changes to the UFW in the GUI
      - Type “sudo apt-get install gufw” at the command line
      - Screenshots for Gufw at https://help.ubuntu.com/community/Gufw
    - You might need to install Ubuntu updates before installing Gufw
    - After downloading Gufw from the Software Center, click the Ubuntu button in your menu bar → Search → Firewall Configuration
    - Click the Unlock button on the Gufwwindow → Enact root permissions by authenticating → Turn Firewall Status On
    - The default (and recommended rules) governing traffic are to Deny all incoming traffic and Allow all outgoing traffic
    - The Reject option is the same as Deny, but also sends a notification to the sender that connection has been blocked
    - The Preconfigured rule panel allows incoming and/or outgoing traffic to be controlled for certain applications or services
      - Similar to the Windows Firewall Exceptions list
      - Open entire ports by clicking the Simple or Advanced tabs
- Services (Also called a daemon)
  - Process that runs in the background
  - Can be viewed and managed in the GUI
  - To install, type apt-get install bum in Terminal
  - After installing, type bum to run
    - To enable a service, check the box next to it
    - To start a service, right-click it and select “Start”
    - When a service is started, the light bulb will light up. When stopped, the light bulb will be dark.
  - Disable unnecessary services (daemons)
    - If your system is configured with inetd, look at /etc/inetd.conf and prefix a line with a "#" character to make it a comment; then restart the inetd service or reboot
    - If you are using xinetd, its configuration will be in the directory /etc/xinetd.d.
    - Each file in the directory defines a service, and add disable = yes to any that you want to disable
    - Disable daemons not normally used such as
      - Telnet
      - Anonymous FTP
      - Remote processes (Rexec.Rlogin,Rsh)
      - Rstatd
      - Finger
      - Talk, Ntalk
- Attach Detection
  - Monitor your processes
    - Use tools such as Snort, Nessus
    - Monitor syslog
    - Monitor run levels (0 to 6)
      - Runlevels define what services or processes should be running on the system
        - http://www.unixtools.com/Linux-Runlevels.html
      - Make sure all processes are operating on the appropriate runlevel

        - Check running proceses (approx. 203 processes)
            - ps -ef
    - Port Checks
        - netstat -tulpn
    - System Logs (syslog)
        - Similar to Windows Event Viewer
        - From the Search field in the Ubuntu menu on the left of the desktop, type System Log to view available logs
        - Four types of logs
            - **auth.log**: Tracks authentication events that prompt for user passwords (e.g., uses of PAM files and sudo)
            - **dpkg.log:** Tracks software events (e.g., installations and updates)
            - **syslog**: Tracks operating system events (e.g. error messages)
            - **Xorg.0.log:** Tracks desktop events (e.g., service changes and graphic card errors.
        - Can add different types of logs
        - Configure the Syslog daemon to log messages and events
        - Located at the /etc/syslog.conf
- Network
    - Encrypt network traffic
        - Install ssh
    - Utilize access control
        - Configure *hosts.allow* and *hosts.deny* files for tcpd and sshd
- Installing and Automating Updates
    - The open-source community regularly develops improvements and patches for Ubuntu
    - You should install these updates regularly
        1. Click the Ubuntu button in the menu bar and search for Update Manager
        2. Click Settings on the Update Manager Screen
        3. To set automatic updates, go to the Updates Tab and make sure "Automatically check for updates" is set to "Daily"
        4. After applying the changes, install any available updates from the main Update Manager window
- Setting Audit Policies
    - Unlike Windows, auditing is not set up by default in Ubuntu
    - Three step process to setting up audits:
        1. Install the auditing program by typing apt-get install auditd
        2. .Enable audits by typing auditctl –e 1
        3. View and modify policies by typing gedit/etc/audit/auditd.conf
- PAM Files
    - Pluggable Authentication Modules (PAM) are used for logon and applications
    - They simplify user authentication
        - They *do not* govern authorization (i.e. grant privileges to users)
    - 4 types of PAM files:
        - Account –control account conditions (e.g. not expired, etc.)
        - Authentication –verify user identities
        - Password –control some password policies
        - Session –define actions performed at the beginning and end of user sessions.
    - Editing the PAM Password File
        - Type gedit /etc/pam.d/common-password
        - Lines in the file starting with "#" are comments to help the user understand the file. They do not enforce any policies.
        - After making changes, save the file and close it.
            - To enforce password history of : Add **"**remember=5" to the end of the line that has "pam_unix.so" in it.
            - To enforce password complexity with one of each type of character:* Add **"**ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1" to the end of the line with "pam_cracklib.so" in it.**
              *ucredit= upper case, lcredit=lower case, dcredit= number and ocredit= symbol
              **cracklibmay need to be installed before enforcing password complexity

  - To enforce Password length of 8: Add **“**minlen=8” to the end of the line that has “pam_unix.so” in it
- Account Lockout
  - Set to a high enough number that authorized users are not locked out of their user accounts simply because they mistype a password
    - Usually set to 5
  - Add the following two lines highlighted in blue to the /etc/pam.d/system-auth file
    - auth required /lib/security/$ISA/pam_tally.so onerr=fail no_magic_root
    - account required /lib/security/$ISA/pam_tally.so per_user deny=5 no_magic_root reset
  - The first added line counts failed login and failed su attempts for each user. The default location for attempted accesses is recorded in /var/log/faillog
  - The second added line specifies to lock accounts automatically after 5 failed login or su attempts (deny=5)
- User profile
  - The adduser utility creates a brand new home directory named /home/username
  - /etc/default/useradd
  - By default, user home directories in Ubuntu are created with world read/execute permissions
- Password Files
  - Located at /etc/passwd and /etc/shadow
  - Passwords are usually not stored in the /etc/passwd file, but rather in the /etc/shadow file
  - Passwords are encrypted in the /etc/shadow file
  - File permissions
    - /etc/passwd
      - Owned by Root
      - Read only to users
    - /etc/shadow
      - Owned by Root
      - Users should not have access to this file
  - To crack Linux passwords you need the shadow file and sometimes have to merge the passwd and shadow file

- Password Policy
  - Minimum Password Length
    - Add the ‘minlen = <x>’ parameter to the pam_unix configuration in the /etc/pam.d/common-password file – Set to 8
      - password required pam_cracklib.so retry=3 minlen=8 difok=3
    - By default, Ubuntu requires a minimum password length of 4 characters
  - Password Expiration
    - Needs a minimum and maximum password age forcing users to change their passwords when they expire
      - PASS_MIN_DAYS – Set to 7 days
        - Minimum number of days allowed between password changes
      - PASS_MAX_DAYS – Set from 30 to 90 days
        - Maximum number of days a password may be used
      - PASS_WARN_AGE – Set to 14 days
        - Number of days warning given before a password expires
  - Parameters can be set in */etc/login.defs*
- Password History (reuse)
  - Create an empty /etc/security/opasswd file for storing old user passwords
  - Set permissions to opasswd to the same as the /etc/shawdow file

- Enable password history by adding the “remember=<x>” to the pam_unix configuration in the /etc/pam.d/common-password file
  - password required pam_unix.so md5 remember=12 use_authtok
  - The value of the "remember" parameter is the number of old passwords to store for a user
- Edit Password History
  - Type gedit /etc/login.defs
  - This is a much longer file. To easily find the section to edit, type Ctrl+Fand then “PASS_MAX_AGE”
  - Modify the following variables to the same recommended settings used in Windows:
    - Maximum Password Duration:
      - PASS_MAX_DAYS 90
    - Minimum Password Duration:
      - PASS_MIN_DAYS 10
    - Days Before Expiration to Warn Users to Change Their Password:
      - PASS_WARN_AGE 7
  - Save the file and close it
- More explanation can be found at
  - http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html

- Edit Set Account Policy
  - Type gedit /etc/pam.d/common-auth
  - This file allows you to set an account lockout policy
  - Add this line to the end of the file: auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800
    - Sets the number of allowed failed login attempts (in this case 5)
    - Sets the account lockout duration in seconds (in this case, 30 minutes)
  - Save the file and close it

Additional Information

- Terminal
  - Command line is accessed through a program called Terminal
  - Click the Ubuntu Button on the Ubuntu menu bar→ Search "Terminal" → Open Terminal
  - typing commands in Terminal, it is very important to pay attention to capitalization and spaces
  - Hitting Enter will execute your command and hitting Ctrl+D will close any commands you have running or exit the Terminal
- File System
  - The file system can be accessed by clicking the orange folder on your Ubuntu menu bar
  - Important folders:
    - home: stores each user's documents, media files, etc. Users can only access their own folders, unless they have enacted root permissions
    - etc: system configuration files.
    - boot: contains startup files and kernel files. Should not be modified unless you are an expert user.
  - Network File System (NFS) Security
    - Method of sharing access to a filesystem between Unix systems
    - Only run NFS as needed, apply latest patches (including nfsd, mountd, statd, lockd)
    - Careful use of /etc/exports
    - Read-only if possible
    - No suid if possible
    - Fully qualified hostnames
    - Device Security
    - Device files /dev/null, /dev/tty & /dev/console should be world writeable but NEVER executable
    - Most other device files should be unreadable and unwriteable by regular users
- Editor
  - VI is a text editor used on most Unix operating systems
  - gedit
    - geditis one of many text editor commands in Ubuntu
      - Syntax: gedit [filepath]
      - Unlike with other text editors, using geditwill cause a second window to pop-up where you can easily change the text of a file
      - This command will allow you to edit security policy files
    - You need to enact root permissions before using gedit to edit files that cannot be accessed by standard users (e.g. system and security files)
    - When using gedit for the first time, go to Edit → Preferences → Uncheck "Create a backup copy of files" to avoid saving issues
    - Try using gedit by opening Terminal and entering gedithello2.txt
      - You will not be prompted to authenticate because this is a public file
- sudo command
  - Allows an authorized user (one with root permissions) to temporarily elevate their privileges using their own password instead of having to know the password belonging to the built-in root account
  - This command must be used to perform administrative tasks (e.g. adding a user account)
    - Example: To add "archimedes" as a user on your system, type adduser archimedes and hit Enter
    - You will get the error message below because you have not authenticated yourself
    - Note: user names must be lower case
  - Now try adding "archimedes" as a user by entering the sudo command first:
    - Type sudo adduser archimedes
    - Hi tEnter
    - When prompted, type in your password and hit Enter
      - Note: Your password will not be visible when you type. This is an Ubuntu security feature.
      - Remember, the sudocommand will only work if your are using an account with root permissions
    - When prompted, type a passwordand any other details you wish to add to the user account

        - Hit Enter
    - The sudosucommand is a variation of the sudocommand
        - It tells the command line that you want to run all of the subsequent commands in your current session as root, so that you do not have to enter the sudocommand and your password each time
- Firestarter
    - Shows active connections and who they belong to
    - Controls inbound and outbound traffic
    - Displays intrusion attempts as they occur
    - Configure firewall to behave in a specific manner for certain types of connections
    - Create security policies
    - Screenshots can be found at http://www.fs-security.com/screenshots.php
    - Download at http://www.fs-security.com/
    - Installation directions can be found at http://www.howtogeek.com/howto/ubuntu/install-the-firestarter-firewall-on-ubuntu-linux/
- Packages
    - A compressed program or piece of software
    - Package Managers
        - All software on a linux system is divided into RPM packages, which can be installed, upgraded, or uninstalled
        - Contain a list of software repositories
        - You will be prompted to enter the superuser (root) password before changes are made to the system
        - RPM Package Manager
            - .rpm is the file format for the software package files
            - System administrators must manually install with dependencies
            - Instead, a front end can be used to automate this process
        - Common Package Managers (front end)
            - YUM – automatic update and package installer
                - http://yum.baseurl.org/
            - PackageKit (GUI)
                - Open **Software Updates** by clicking **Applications** → **System Tools** → **Software Update** from the **Activities** menu within the GNOME desktop
            - apt-get
                - Command line tool
            - Aptitude
                - Menu driven text based tool (https://help.ubuntu.com/11.04/serverguide/C/aptitude.html)
            - Synaptic Package Manager (GUI)
                - http://www.nongnu.org/synaptic/