1. **DISABLE IPV6**

Some of your employees want to be able to access this server remotely. Please install OpenSSH server in order to allow your employees to be as productive as possible.

2) sudo apt-get install openssh-server

Your job is to install OpenSSH server, secure this computer, and disable ipv6. This company's security policies require that all user accounts be password protected.

3) Password on every user: {Choose a hard password}

Employees are required to choose secure passwords, however this policy may not be currently being enforced on this computer.

4) Password requirements

The presence of any non-work related media files and "hacking tools" on any computers is strictly prohibited.

5) Antivirus. Look by hand for tools. Make sure they are deleted, any associated files are deleted, they are not in task scheduler, that they are not in the registry. Media files, use everything. Look in every user directory, not just your own.

This company currently does not use any centralized maintenance or polling tools to manage their IT equipment. This computer is for official business use only by authorized users. It is company policy to use only Ubuntu 12.04 on this computer. It is also company policy to use only the latest, official, stable Ubuntu 12.04 packages available for required software and services on this computer.

6) Update - First thing you do.

Management has decided that the default web browser for all users on this computer should be the latest stable version of Firefox.

7) Hopefully update & upgrade catches firefox. If not, try this command.

```
a) sudo apt-get install firefox
```

Company policy is to never let users log in as root. If administrators need to run commands as root, they are required to use the "sudo" command.

8) Disable root login, in both the OS and ssh

Critical Services This server is configured to run MySQL. It contains data from customers such as credit card information and user feedback for the app. MySQL should be only accessible locally and therefore, no one should have remote access to the server.

9) Force MySQL to listen on localhost, along with other security settings (especially changing the root password)

Critical Services: MySQL Authorized Administrators and Users The root password, and the MySQL root password is "patio" (without quotes).

Authorized Administrators: Joshua (you) Password: L!ght3r Murtah Password: 0ldM4N Riggs Password: $t00ges Authorized Users: Andrew Kevin Scott Martin Rodger Brandon Eric Kyle Kenny John Seth Owen Gary

1) Carefully look at the README

2) DO NOT UPDATE TO UBUNTU 13.04/14.04/15.04

3) Update & Upgrade FIRST
    a) sudo apt-get update
    b) sudo apt-get upgrade

   If updates aren't working
    c) Go to Update Manager
    d) In "Settings" make sure to select important updates and install automatically
    e) Check for updates and "Install Now"
    f) NOTE** THE UPDATE MANAGER WILL KEEP YOU FROM RUNNING ANY APT-GET OPERATIONS UNTIL ALL UPDATES ARE COMPLETED.

4) Automatic Security Updates (Do this with the GUI first and see if you get points)
        i) Use unattended-updates package

(1) sudo apt-get install unattended-upgrades
(2) sudo dpkg-reconfigure -plow unattended-upgrades

5) Change password of current user > passwd <usrname> Note: Check README, this is not always necessary
    a) List of all users
        i) cut -d: -f1 /etc/passwd
    b) List of all groups
        i) cut -d: -f1 /etc/group
    c) Give a user admin permissions
        i) sudo usermod -a -G sudo username
    d) Delete users
        i) sudo userdel -r username
            (1) -r deletes home directory of user
        ii) cd /b
    e) Change info of users
        i) sudo chfn username

6) (ONLY IF YOU NEED TO) Remove folder with permissions denied
    a) sudo rm -rf “path to file”
7) lsof -i -n -P
    a) LOOK FOR PROGRAMS RUNNING THAT SHOULDN’T BE
    b) Examples include nc (netcat)

8) Disable global read/write/execute permissions
    a) Look for files that might have 777 (global read/write permissions)
        i) ls -l /path/to/file
        ii) One way to see permissions in ---rw- format

9) If you forget who you are, type in “whoami” in the terminal
    a) Cycle through users and run commands to find any specific files/permissions

10) When using gedit for the first time, go to Edit → Preferences → Uncheck “Create a backup copy of files” to avoid saving issues

11) Media Files
    a) sudo apt-get install tracker-gui
        i) Doesn’t work too well. Avoid
        ii) locate -i "*.mp3"
        iii) Needs to be tested**
    b) sudo find -iname '*.mp3' -or -iname '*.avi' -or -iname '*.mp4' -or -iname '*.jpg' -or -iname '*.wav' -or -iname '*.mov’ -or -iname '*.mpeg'

i) Confirmed. Make sure to limit search to home folder of all users, not the local filesystem

c) You can go to file explorer
   i) Type in a dot into the search bar
   ii) Use the extra options to search for pictures, videos, and music
   iii) Will take a while so start the search and come back later

0

12) Password Policy
   a) Type sudo gedit /etc/login.defs
      i) Change PASS_MAX_DAYS to 90
      ii) Change PASS_MIN_DAYS to 10
      iii) Change PASS_WARN_AGE to 7
   b) sudo apt-get install libpam-cracklib
   c) sudo gedit /etc/pam.d/common-password
      (1) password requisite pam_cracklib.so retry=3 minlen=8 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
      (2) password requisite pam_pwhistory.so use_authtok remember=5 enforce_for_root
      (3) password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512

13) Setup failed login attempts + Password History
   a) Open terminal and type sudo gedit /etc/pam.d/common-auth
   b) ORDER MATTERS
      i) auth optional pam_tally.so deny=5 unlock_tme=300 onerr=fail audit
      ii) auth [success=1 default=ignore] pam_unix.so nullok_secure

14) Disable user accounts after too many failed login attempts
   a) sudo gedit /etc/pam.d/system-auth
   b) auth required /lib/security/$ISA/pam_tally.so onerr=fail no_magic_root
   c) account required /lib/security/$ISA/pam_tally.so per_user deny=5 no_magic_root reset

15) Restrict direct logons **DO AT END IF YOU NEED POINTS
   a) sudo gedit /etc/pam.d/login
      i) account required pam_access.so
   b) GNOME
      i) sudo gedit /etc/pam.d/gdm
      ii) account required pam_access.so
   c) sudo gedit /etc/security/access.conf
      i) Add “-:ALL EXCEPT users :ALL”

16) Change Apache Settings
    a) Navigate to settings: sudo vi /etc/apache2/mods-available/ssl.conf
    b) Add/Edit this line: SSLProtocol all -SSLv2 -SSLv3
    c) Restart service: sudo /etc/init.d/apache2 restart

17) Apache INFO Leak
    a) sudo vi /etc/apache2/conf.d/security
    b) Add/Edit the following:
        i) ServerTokens Prod
           ServerSignature Off
           TraceEnable Off
           Header unset ETag
           FileETag None
        ii) Enable modheaders
            (1) sudo ln -s /etc/apache2/mods-available/headers.load
                /etc/apache2/mods-enabled/headers.load
        iii) sudo /etc/init.d/apache2 restart

18) If commands using sudo fail, one must manually install sudo:
    a) $ su
       # apt-get install -y sudo

19) If an application must be removed
    a) sudo apt-get remove vsftpd
    b) $ sudo apt-get -y purge <application>
    c) sudo find / -iname 'john'
        i) Find all files related to an application so that you can delete them

20) Prevent Source Routing (When attacker specifies a path for a possibly dangerous packet to take) and log bad IPs with sysctl.conf
    a) sudo gedit /etc/sysctl.conf
    b) Add the following lines:
        i) # IP Spoofing protection
           net.ipv4.conf.all.rp_filter = 1
           net.ipv4.conf.default.rp_filter = 1

           # Ignore ICMP broadcast requests
           net.ipv4.icmp_echo_ignore_broadcasts = 1

           # Disable source packet routing
           net.ipv4.conf.all.accept_source_route = 0
           net.ipv6.conf.all.accept_source_route = 0
           net.ipv4.conf.default.accept_source_route = 0

```
net.ipv6.conf.default.accept_source_route = 0

# Ignore send redirects
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Log Martians
net.ipv4.conf.all.log_martians = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1
```

ii) Reload sysctl.conf with: sudo sysctl -p

21) Killing Frozen Processes
    a) top
    b) kill [PID_Number]

22) Killing Frozen Processes

    a) sudo gedit /etc/host.conf
    b) Add/Edit:
        i) order bind,hosts
        ii) nospoof on
    c) Restart Firefox, apache2

23) Check crontab
    a) crontab -l
    b) Edit if needed

24) Time and Date

a) Update time
    i) sudo ntpdate ntp.ubuntu.com
b) Time and Date Preferences
    i) Automatically get time
c) sudo apt-get install ntp
    i) sudo ntpq -p

25) Turn off Internet search
a) Go to search bar
b) Security and Privacy
c) Search tab, turn off online search

26) Samba
a) dpkg --get-selections | grep “samb”
b) apt-cache search samba
c) netstat -tulnp
    i) Ports 137, 138, 139, 445 may be used for Samba
d) server samba status
    i) If nothing samba probably not installed
e) Samba is in the /etc/samba
f) smb.conf
    i) Change workgroup to the domain (NOT NAME) of the company (if given)
    ii) below workgroup
        (1) security = user
    iii) Look at share definitions
        (1) guest ok = no
        (2) read only = yes
        (3) browseable = no
    iv) sudo service samba reload

27) SHOW HIDDEN FILES
a) Click Files
    i) Edit > Preferences> Show Hidden Files

28) Disable printing in Ubuntu
a) Edit /etc/inti/cups.conf and comment out the start line (s).
b) #start on (filesystem
c) # and (started dbus or runlevel [2345])
d) # and stopped udevtrigger)
e) Disable remote printer installation
    i) sudo service cups-browsed stop
    ii) gksudo gedit /etc/init/cups-browsed.override
    iii) Add “manual” in the first and only line
f) Edit `/etc/cups/cupsd.conf`
    i) `Browsing Off`

29) Screensaver security
    a) Under Settings > Brightness and Lock

30) Settings > Startup Applications
        i) Stop anything that shouldn't be there
    b) bash -i -v >bash-i.out 2>&1
    c) Look for any suspicious startup scripts

31) Look at a list of all packages
    a) dpkg --get-selections
        i) If you can't see all packages, click "Edit" > "Profile Preferences" > Scrolling > Unlimited
    b) sudo apt-get remove
        i) netcat-traditional
        ii) netcat-openbsd
        iii) Ettercap - captures usernames and passwords
        iv) Driftnet
        v) dsniff
        vi) aircrack-ng
        vii) Fsshjohn
        viii) djohn-data
            (1) Could not get lock
                (a) sudo rm /var/lib/dpkg/lock
                (b) sudo rm /var/cache/apt/archives/lock
                (c) sudo dpkg --configure -a
                (d) ps -A | grep apt-get

32) Auditing!
    a) sudo apt-get install auditd
    b) Enable audits by typing: sudo auditctl –e 1
    c) View and modify policies by typing: sudo gedit /etc/audit/auditd.conf
        i) YOU WILL NEED ROOT ACCESS
    d) AUDIT CHANGES TO A FILE
        i) auditctl -w /path/to/file -p wra -k secret-changes
        ii) cd /var/log/audit
        iii) ausearch -k secret-changes
        iv) aureport -f
            (1) SEE ALL CHANGES MADE
            (2) OUID gives uid
            (3) getent passwd <uid>

33) PASSWORD CHANGES
    a) Install cracklib, a tool for checking password strength, via terminal: sudo apt-get install libpam-cracklib
    b) Install expect by sudo apt-get install expect
    c) Either change passwords manually or use script (as of 11/9 not working)

34) Other Users
    a) Navigate to the “home” folder
    b) “**cd ..”** in terminal if you need to go back a folder
    c) Enter another user’s folder and look for files

35) Install Gufw Firewall
    a) Navigate to Gufw website
    b) Install Gufw via Ubuntu Software Center
        i) Alternative: sudo apt-get install -y gufw
        ii) sudo ufw deny 22/tcp && sudo ufw deny 22/udp
        iii) Assistance from Digital Ocean for commands you may need
    c) sudo ufw default deny incoming
    d) sudo ufw default allow outgoing
    e) sudo ufw allow ssh (Won’t work if you change port)
    f) sudo ufw allow http
    g) sudo ufw allow https
    h) FIREWALL STATUS: sudo ufw status verbose

36) Change SSH settings
    a) Update SSH >> sudo apt-get install openssh-server
    b) Change SSH port
        i) SSH as root: ssh root@localhost
            (1) If it needs root password and you don’t know it, then do ‘sudo su’
            (2) Change root password by ‘passwd root’
        ii) OPTIONAL: Backup SSH settings file
            (1) cp /etc/ssh/sshd_config /etc/ssh/sshd_config_backup
        iii) Edit SSH settings file: sudo gedit /etc/ssh/sshd_config
            (1) Use Protocol 2
            (2) Change port from 22 to anywhere between 49152 through 65535
                (a) Block Port 22 using firewall
        iv) If needed, enable Public/Private Key Authentication
    c) vi /etc/ssh/sshd_config
        i) Change PermitRootLogin to No
    d) More Settings
        i) HostbasedAuthentication no
        ii) Limit only specific users to access your machine via SSH:

(1) AllowUsers user1 user2

iii) Disable password-based authentication and allow public key based authentication
   (1) ChallengeResponseAuthentication no
   (2) PasswordAuthentication no
   (3) PubkeyAuthentication yes

iv) Disable X11 Forwarding, TCP Forwarding

v) Privilege Separation yes

vi) Comment out the sftp line

vii) Encrypted Graphic Communication
   (1) Add the following line: ForwardX11 yes
   (2) Now you can connect the server using...
      (a) ssh -X -c user@IP -p 123
         (i) sudo -X option allows use of forwarded XWindow system
         (ii) The -p designates port to connect to if using different port than the default 22

viii) Add line for login message
   (1) Banner /etc/ssh/text.txt
   (2) Create file /etc/ssh/text/txt
   (3) "This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personnel may provide the evidence of such monitoring to law enforcement officials."
   (4) sudo service ssh apt-reload
   (5) sudo service ssh restart

e) Authorized users

i) Remove or rename the directory .ssh/ in the user's home folder to prevent further SSH authentication capabilities
   (1) Kill any open connections
      (a) who |grep username (to get the pts/# terminal)
      (b) sudo pkill -f pts/#

ii) Allow only certain users to use ssh
   (1) Create a group sshalloweduser
      (a) groupadd sshallowedusers or addgroup sshallowedusers
   (2) cat /etc/group
   (3) sudo adduser username sshallowedusers
      sudo service ssh restart
   (4) sudo gedit /etc/ssh/sshd_config

(5) Add the following line:
(a) -X AllowGroups sshallowedusers

f) Restrict Direct Logons (Do this last if you need more points)
i) sudo gedit /etc/pam.d/sshd
ii) account required pam_access.so

g) Restart Service: sudo /etc/init.d/ssh restart
i) sudo service ssh restart

37) CLAM ANTIVIRUS
a) sudo apt-get install clamav
b) To update:
i) sudo freshclam
c) Scan system
i) sudo clamscan -irv --exclude=/proc --exclude=/sys --exclude=/dev --exclude=/media --exclude=/mnt
d) Or particular directory
i) sudo clamscan -ri /path/to/
e) CLAMTK is a GUI
i) sudo apt-get install clamtk

38) FQDN
a) /etc/hosts
i) 127.0.1.1
ii) cyber.dev.local cyb
iii) In the above line, cyber.dev.local is the FQDN and cyb is hostname
iv) Add hostname to /etc/hostname
v) sudo service hostname restart
vi) hostname
(1) Should show hostname
vii) hostname -f
(1) Should show FQDN
viii) REDIRECT REQUESTS
ix) Under the first 2 lines add
(1) 127.0.0.1 www.something.com hostname

39) Rootkit detection
a) sudo apt-get install chkrootkit << Install two rootkit detect (2 > 1 !!!)
b) sudo chkrootkit -q
i) -q will only show infected
ii) sbin/init may be false positive
c) Copy rkhunter from USB to Desktop

d) tar zxf Rootkit_Hunter.tar.gz
   cd rkhunter-1.4.2
   ./installer.sh --install
e) sudo rkhunter --update
f) sudo rkhunter --propupd
   i) Updates rkhunter's properties database with those of the current system
g) sudo rkhunter --check
h) In case the above command to run didn't work, use: sudo rkhunter -c --sk

40) Use DENYHOSTS to take down SSH attacks
a) sudo apt-get install denyhosts
b) sudo vi /etc/denyhosts.conf
c) ADMIN_EMAIL = root@localhost
   SMTP_HOST = localhost
   SMTP_PORT = 25
   #SMTP_USERNAME=foo
   #SMTP_PASSWORD=bar
   SMTP_FROM = DenyHosts nobody@localhost
   #SYSLOG_REPORT=YES
d) Try the above. Fail2Ban is more comprehensive.
   i) sudo apt-get install fail2ban
   ii) sudo gedit /etc/fail2ban/jail.conf
   iii) [ssh]
   enabled = true
   port = [NEW PORT # YOU SET IN STEP 13]
   filter = sshd
   logpath = /var/log/auth.log
   maxretry = 3
   iv) Restart: sudo /etc/init.d/fail2ban restart
   v) Status: sudo fail2ban-client status
   vi) EXTRA CONFIG INFO

41) Check for unwanted packages
a) Install rpm with sudo apt-get install rpm
b) To get a list of all installed RPMs you can use the following command: rpm -qa
c) rpm -e --test (to test what deleting will do)
d) rpm -e (actually delete the packet)
e) If you want to know more about a particular RPM, run: rpm -qi <package_name>
f) To check for and report potential conflicts and dependencies for deleting a RPM, run: rpm -e --test <package_name>

42) Check computer for open connections
a) sudo netstat -plntu will show all programs and their connection type (TCP/UDP)

i) netstat, or network status shows all programs actively using network communications
ii) netstat -anlp | grep LISTEN
(1) Shows ports and services

b) Install nmap w/ sudo apt-get install nmap (Use nmap -h) for help
i) Do a scan (w/ UDP) on a computer IP with: nmap -sTU <remote_host>
ii) NMAP OPEN PORTS: nmap -v -sT localhost
iii) NMAP SYN FLOODS: sudo nmap -v -sS localhost
iv) Reference the services returned by nmap with the netstat local address
(1) nmap, or network mapper, shows the ports of running programs, allowing you to block ports with unauthorized programs
(a) sudo service cups stop
(b) ^ CUPS is a printing protocol so disable based on README
(c) Port 53 is NOT a threat (it's a dns service)
(2) You can also use lsof
(a) lsof -i -n | egrep 'COMMAND|LISTEN|UDP'

43) Secure Shared Memory (Shared memory is mem. that's shared among several programs)
a) sudo vi /etc/fstab
b) Add at the end:
i) tmpfs /dev/shm tmpfs defaults,noexec,nosuid 0 0
c) sudo mount -a

44) NOTE*** IGNORE THE CHKCONFIG BELOW. WHILE YOU CAN MAKE IT WORK, IT'S A HASSLE AND NO LONGER SUPPORTED BY UBUNTU.

Services: A 3-Step Process

1 - Use sysv-rc-conf to turn off
2- Use the echo manual command to disable it
3 - For good measure, remove the service from the init.d folder
**Remember that some services are controlled by xinetd and will follow different procedures

45) Alternative:
a) sudo apt-get install sysv-rc-conf
b) sudo sysv-rc-conf
i) Allows you to select/deselect what services to turn on/off
c) sudo sysv-rc-conf --list
d) Ex. sudo sysv-rc-conf apache2 on
e) Also do a sudo service apache2 stop
i) Check the status - service apache2 status - to make sure it's off
f) sudo rm /etc/init.d/apache2

g) For good measure:
    i) echo manual | sudo tee /etc/init/apache2.override

46) Disable NFS
    a) Install chkconfig, sudo apt-get install chkconfig
    b) sudo ln -s /usr/lib/insserv/insserv /sbin/insserv
    c) chkconfig --list
        i) NFS, or Network File System, allows for possibly insecure connections to a LINUX computer
        ii) IMMEDIATE OFF: /etc/init.d/nfs stop
            (1) chkconfig nfslock off
            (2) chkconfig rpcgssd off
            (3) chkconfig rpcidmapd off
            (4) chkconfig portmap off
            (5) chkconfig nfs off
            (6) Since chkconfig is deprecated, use /etc/ini.d/[Service] stop
        iii) IF NFS IS REQUIRED
            (1) Install the following
                (a) nfsd
                (b) mountd
                (c) statd
                (d) lockd

47) You may want to disable services like telnet, finger and other unwanted services running on your server with xinet
    a) nano /etc/xinetd.d/telnet
       nano /etc/xinetd.d/krb5-telnet
    b) Look for lines disable=no and change to disable=yes
       (http://www.mysql-apache-php.com/basic-linux-security.htm)

48) Disable Services
    a) Check xinetd, which monitors all ports used by network processes
        i) If not installed, sudo apt-get install xinetd
        ii) Navigate to /etc/xinetd.d
        iii) ls to see different services
        iv) Open with nano or vi and set Disable to Yes
        v) Things to disable
            (1) Telnet
                (a) rpm -e telnet-server (remove the package)
            (2) Anonymous FTP
            (3) Remote processes (Rexec.Rlogin,Rsh)
            (4) Rstatd
            (5) Finger

(10) Talk, Ntalk

b) Use chkconfig
   i) chkconfig telnet off (Unless it's a telnet server)
   ii) chkconfig apache2 off (Unless it's a web server)
   iii) CHECK TO SEE IF IT ACTUALLY TURNED OFF
      (1) cat /etc/xinetd.d/telnet | grep disable
   iv) sudo /etc/init.d/apache2 stop
   v) sudo rm /etc/init.d/apache2
c) Yet another alternative in case the above fails to work
   i) Bum's a GUI so it may be easier to navigate
      (1) apt-get install bum
      (2) type: bum
d) NOTE IN FILE - inetd.conf - YOU CAN COMMENT OUT SERVICE DAEMONS

49) Harden PHP
a) nano /usr/local/lib/php.ini
b) OR sudo vi /etc/php5/apache2/php.ini
   i) Look for the lines and make sure you have the lines as below:
   disable_functions = exec,system,shell_exec,passthru
   register_globals = Off
   expose_php = Off
   display_errors = Off
   track_errors = Off
   html_errors = Off
   magic_quotes_gpc = Off
   ii) RESTART
      (1) Depends on web server service, most likely Apache, if not...
      (2) sudo /etc/init.d/apache2 restart

50) Harden DNS Server
a) Figure out DNS IPs: nano /etc/nameserverips
b) nano /etc/named.conf
c) Find options and ***above it*** add the following (where xxxx and yyyy are the 2 IPs):
   i) acl "trusted"
   {x.x.x.x;
   y.y.y.y;
   };
d) Find the line that says *" // query-source address * port 53; "* and ***below it*** add the following (to disable recursion and thus keep it from being accessible to anyone)
   i) version "Bind";
   allow-recursion { trusted; };
   allow-notify { trusted; };
   allow-transfer { trusted; };

e) To prevent spamming of forged IPs to your DNS, add the following in options:
    i) use-id-pool yes;
f) Restart bind: service named restart
g) OPTIONAL: Check namesever for vulnerabilities: http://www.intodns.com/
h) OPTIONAL WAY OF DISABLING RECURSION:
    i) sudo vi /etc/bind/named.conf.options
    ii) Add the following:
        (1) recursion no;
            version "Not Disclosed";
        (2) Restart Bind DNS: sudo /etc/init.d/bind9 restart

51) Setup Snort to serve as an IDS (Intrusion Detection System)
a) Install snort by sudo apt-get -y install snort-mysql
b) Initiate snort by sudo /etc/init.d/snort start
c) Verify if snort has been successfully installed by sudo /etc/init.d/snort status
d) MORE DETAILED TUTORIAL BELOW

52) Set up Tiger for security audits
a) sudo apt-get install tiger
b) sudo tiger
c) sudo less /var/log/tiger/security.report.*

53) Use AppArmor
a) sudo apt-get install apparmor apparmor-profiles
b) sudo apparmor_status

54) Want to actually see all those logs Ubuntu's generating?
a) sudo apt-get install logwatch libdate-manip-perl
b) sudo logwatch | less

55) Task Manager for Ubuntu
a) htop
b) System Monitor (search for it)

56) MYSQL INI FORCE LOCALHOST
a) Config file may be in any of the following locations
i) /etc/my.cnf
ii) /etc/mysql/my.cnf
iii) $MYSQL_HOME/my.cnf
iv) [datadir]/my.cnf
v) ~/.my.cnf

b) [mysqld] bind-address = localhost

c) MYSQL SECURE SCRIPT

i) sudo mysql_secure_installation

d) CHANGE ROOT PASSWORD

i) sudo dpkg-reconfigure mysql-server-5.5

ii) Goes through installation, prompt to reenter root password

e) Block Port 3306 incoming in gufw

57) Enter "$ sudo -H gedit /etc/lightdm/lightdm.conf
   a) If file exists, simply add the following line:
      i) allow-guest = false
   b) If file is not present, add the following:
      i) [SeatDefaults]
         user-session = ubuntu
         greeter-session = unity greeter
         allow-guest = false

58) CHANGE SU ACCESS TO ADMINS ONLY
   a) sudo groupadd admin (if this doesn't work sudo addgroup admin
   b) sudo usermod -a -G admin <YOUR ADMIN USERNAME>
   c) Repeat command above with other admins
      i) Confirm users for group
         (1) sudo apt-get install members
         (2) members [group name]
   d) sudo dpkg-statoverride --update --add root admin 4750 /bin/su
   e) Disable root password
      i) sudo passwd -l root
      ii) sudo passwd -dl root
         (1) Local lock of root

59) DEV FILES SHOULD BE WORLD-WRITEABLE BUT NEVER EXECUTABLE
   a) /dev/null, /dev/tty & /dev/console
   b) chmod -x /dev/null OR
   c) chmod -rw /dev
   d) chmod +w /dev/null
   e)
   f) toor:x:0:0:root:/root:/bin/bas

60) Disable shortcuts that are not needed
   a) Screenshots
   b) Launchers

c) Sound and Media
d) Universal Access
e) Custom Shortcuts
f) Example
    i) System Settings → Hardware / Keyboard → Shortcuts → Screenshots → Take a screenshot
    ii) Tap on a shortcut, highlighting it so that it says “New Accelerator”
    iii) Hit backspace to disable

61) Disable IPV6 in Ubuntu
a) Add these lines to the bottom of /etc/sysctl.conf
    i) net.ipv6.conf.all.disable_ipv6 = 1
    ii) net.ipv6.conf.default.disable_ipv6 = 1
    iii) net.ipv6.conf.lo.disable_ipv6 = 1
    iv) Then run sudo sysctl -p or reboot
b) Edit /etc/default/bind9 like so:
    i) # run resolvconf? RESOLVCONF=yes
    ii) # startup options for the server OPTIONS="-4 -u bind"
c) Check via
    i) cat /proc/sys/net/ipv6/conf/all/disable_ipv6
    ii) 0 is enabled and 1 is disabled

62) Enable TCP SYN cookie protection
a) Edit the file /etc/sysctl.conf, run:
b) sudo gedit /etc/sysctl.conf
c) net.ipv4.tcp_syncookies = 1
d) Save and close the file. To reload the change, type:
e) sysctl -p

63) Disable rogue aliases
a) ~/.bashrc
b) ~/.bash_profile
c) /etc/bashrc
d) /etc/profile
e) Look for any aliases (user-defined commands) that shouldn’t be there

64) Lynis auditing <<<< AWESOME tool
a) njq
b) sudo lynis audit system

65) Setup a GRUB password
a) Edit /etc/grub.d/40_custom file

b) password <<username>> <<password>>
c) Example:
    i) password john johnP123
d) If you want to add a hashed password, use the *grub-mkpasswd-pbkdf2 utility to generate a hashed password. Add this hashed password to the /etc/grub.d/40_custom file like this:
    i) password_pbkdf2 <<username>> <<hashed-passwd>>
e) Save the file and run sudo update-grub.

66) Bootup Manager
    a) Install from Ubuntu Software Center
    b) Very extensive, very helpful
67) Still stuck after 66 steps? Here's a 50 page doc on Linux security!

Interesting tools

PSAD (Network Intrusion Detection)

Good Links & Resources

Comprehensive Linux Security
http://askubuntu.com/questions/146775/what-can-be-done-to-secure-ubuntu-server

CyberPatriot-specific Linux (and Windows)
https://mhs-la.haikulearning.com/khuynh/cyberpatriotclub/cms_page/view/15379677

Advanced Audit Policy Configuration

https://technet.microsoft.com/en-us/library/dn452415.aspx

Modify Security Policies in Default Domain Controllers Policy
https://technet.microsoft.com/en-us/library/cc731654(v=ws.10).aspx

Advanced tutorial on NFS Hardening
http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Hosts.allow and Hosts.deny files
https://jamalahmed.wordpress.com/2010/03/19/using-etchosts-allow-and-etchosts-deny-to-secure-unix/

LESS LIKELY TO BE ON THE IMAGES:

1) Heartbleed Bug
    a) Check OpenSSL version
        i) openssl version -v
           openssl version -b
        ii) IF ANY OF THE FOLLOWING
            (1) 1.0.1
            (2) 1.0.1a
            (3) 1.0.1b
            (4) 1.0.1c
            (5) 1.0.1d
            (6) 1.0.1e
            (7) 1.0.1f
        iii) Update OpenSSL
            (1) sudo apt-get upgrade openssl libssl-dev
                apt-cache policy openssl libssl-dev
2) Access Control Lists

a) sudo apt-get install acl
b) In /etc/fstab
    i) UUID=07aebd28-24e3-cf19-e37d-1af9a23a45d4 /home ext4 defaults,acl 0 2
    ii) Where ext4 is name of partition
    iii) Follow tutorial here for adding groups to ACL

3) To terminate non-responsive programs
    a) Go on dash home and click on the launcher.
    b) Type keyboard in the search bar and press enter.
    c) Under the shortcuts tab, select custom shortcuts, and click the "+" sign to create a shortcut.
    d) Enter xkill in the command and name box, hit apply. Then click disabled at the xkill row in the keyboard shortcuts.

4) Clean up crash reports: Go to terminal and type sudo rm /var/crash/*

5) Minimize software: terminal, # yum list installed, # yum list packageName, # yum remove packageName

6) How to verify which accounts have empty passwords: # awk -F: ' ($3 == "0") {print) etc/passwd in terminal

7) Lock all empty password accounts: terminal, # passwd -1 accountName

8) Delete noowner files: Files without an owner are a security problem. Find them by:
    a) find/ dir -xdev \(-nouser -o -nogroup \) -print
    b) Find any world-writable files
        i) find / -path /proc -prune -o -perm -2 ! -type l -ls

9) Postfix security
    a) http://techarena51.com/index.php/configure-secure-postfix-email-server/

10) SSH Key Pairs
    a) https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-key-based-authentication-on-a-freebsd-server
11) Install ModSecurity and ModEvasive
    a) Concise tutorial
    b) Longer Tutorial
12) Process Accounting
    a) apt-get install acct
    touch /var/log/wtmp

13) Enable Universe Repository
    a) http://askubuntu.com/questions/148638/how-do-i-enable-the-universe-repository
    b) If Ubuntu update repositories are disabled
        i) http://ubuntuguide.org/wiki/Ubuntu_Precise_Repositories
14) VERY unlikely - Disable USB drivers
    a) http://askubuntu.com/questions/79043/disable-usb-mass-storage

I do not believe this will be necessary this upcoming round, but will definitely come in handy in future rounds.

Snort Guide (Courtesy of Gabriel)

How to use Snort (Intrusion Detection System)

A. Install the prerequisites for installing and compiling Snort

1) Open the terminal and execute the following command: sudo apt-get install flex bison build-essential checkinstall libpcap-devlibnet1-dev libpcre3-dev libmysqlclient15-dev libnetfilter-queue-deviptables-dev
2) Build and install libdnet from its source code by typing: wget https://libdnet.ogoglecode.com/files/libdnet-1.12.tgz
3) If you type in “ls” (without quotations), you will see that the file has been installed to the directory.

4) Now type in the command: tar xvfvz libdnet-1.12.tgz and hit Enter. (This unpacks all the files that were in the libdnet-1-12.tgz file and creates a libdnet-1-12 directory)
5) Change into the libdnet-1-12 directory by executing: cd libdnet-1.12/
6) Type: ./configure "CFLAGS=-fPIC" (the -fPic C flag is necessary if you compile it on a 64-bit platform)
7) Now you should see something like this:

Type: “make” (without quotations) and hit Enter.

8) After that, type in: sudo checkinstall (the command will create a .deb package and ask questions about settings. Accept the given and default values.

9) Install the .deb package and create a link where snort looks for the libdnet directory. Do this by executing these two commands: “sudo dpkg -i libdnet_1.12-1_amd64.deb” and “sudo ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1”

10) Now we will install another vital piece of software necessary for snort to function known as DAQ(Data Acquisition Library)

11) Download DAQ from snort’s website at http://www.snort.org/snort-downloads (Be sure to download the latest and most stable version. Also, downloads will be placed in the Downloads directory of Ubuntu)

12) First execute: “ls” then “cd Download/”

13) We will follow basically the same steps we did for libdnet.

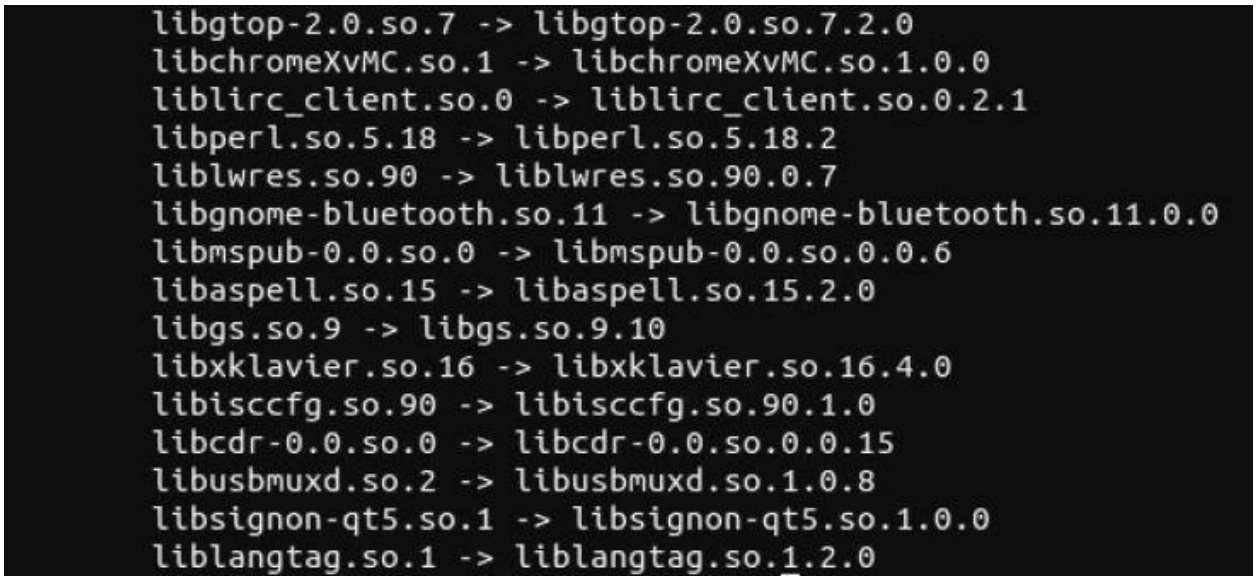
Execute these four commands:
“tar xvfvz daq-2.0.2.tar.gz”,
“cd daq-2.0.2”,
“./configure”
“make”

14) Execute “sudo checkinstall”

15) Now install the package by running “sudo dpkg -i daq_2.0.2-1_amd64.deb”

B. Installing Snort

1) Snort can be installed from its website at http://www.snort.org/snort-downloads
2) Again, we will repeat the steps for installing libdnet and DAQ by unpacking, configuring, making, and then installing
3) Enter these four commands following the same procedures as before
   "tar xvfvz snort-2.9.6.1.tar.gz"
   "cd snort-2.9.6.1"
   "./configure"
   "make"
4) Now do "sudo checkinstall"
5) Install the package by running "sudo dpkg -i snort_2.9.6.1-1_amd64.deb"
6) Now create a symbolic link for snort by executing : "sudo ln -s /usr/local/bin/snort /usr/sbin/snort"
7) After that, execute "sudo ldconfig -v" (This properly sets up the dynamic linker run time bindings for libnet and DAQ. After running the command, something like this should show up)



8) Verify if snort is properly installed by running "snort -V"

C. Configuring Snort

1) Create a separate Linux user that Snort will run as by running these two commands: "sudo groupadd snort" and "sudo useradd snort -d /var/log/snort -s /sbin/nologin -c SNORT_IDS -gsnort"
2) Create a log directory for Snort and give it ownership of that directory by running these two commands: "sudo mkdir /var/log/snort" and "sudo chown snort:snort /var/log/snort"
3) Download snort rules, which can be found at http://www.snort.org/snort-rules/

4) Note which directory the snort rules were downloaded to
5) Create a directory at the /etc directory to which you will unpack the tar files to (execute: “sudo mkdir /etc/snort” and “sudo tar xvfvz snort-rules-snapshot-2960.tar.gz -C /etc/snort *NOTE: the snort rules file may have a different name, be sure to type in the correct file name)
6) Create a white_list.rules file and a black_list.rules file by using “touch”. Execute these commands: “sudo touch /etc/snort/rules/white_list.rules” and “sudo touch /etc/snort/rules/black_list.rules”
7) Create a directory for dynamic rules by running: “sudo mkdir /usr/local/lib/snort_dynamicrules”
8) Change ownership of /etc/snort and move directory and files from the unpacked snort rules by running “sudo chown -R snort:snort /etc/snort/*” and “sudo mv /etc/snort/etc/* /etc/snort

TIP (not part of the official checklist):

- If you forget the Ubuntu password for any user after restarting the VM and you are locked out of the machine, watch this video on resetting passwords:
- https://www.youtube.com/watch?time_continue=275&v=m3rbpR9uuHA
- The process summed up:

1. Reboot your computer
2. Hold shift during boot to start GRUB menu
3. Select advanced options for ubuntu
4. Select the option with recovery mode
5. Select root and press enter
6. Give command: mount -n -o remount,rw /
7. Press enter
8. Give command: passwd [yourUsername]
9. Give new password
10. Reboot