Ubuntu

8NAB^xd#bkHp5wE2xmrh

1. **Read ALL PARTS of the README.**
2. **Do all of the forensics questions.**
3. Install the scripts:
    a. `$ wget https://github.com/jwinnie/foobar-scripts/archive/master.zip -O scripts.zip && unzip scripts.zip && cd scripts. Sudo bash to run them.`
4. Update
    a. Sudo apt-get update
    b. Sudo apt-get upgrade
    c. In settings, set updates to check daily
    d. Don't do sudo apt-get dist upgrade unless the readme says to
5. Remove bad programs
    a. apt list --installed list of users
    b. $ sudo bash bad_packages.sh
        i. See what a package does `$ apt show [packagename]`
        ii. See why a package is installed `$ aptitude why [packagename] --show-summary`
        iii. Remove package `$ sudo apt purge [packagename]`
    c. $ sudo apt purge ssh ftp telnet openssh-client openssh-server samba telnetd
6. Remove bad processes
    a. $ sudo python bad_processes.py
7.
8. Policies
    a. PAM configuration
        i. $ sudo apt install libpam-cracklib
        ii. $ sudo nano /etc/pam.d/common-password
            1. Pam_unix.cat so remember=5 minlen=8
            2. pam_cracklib.so ucredit=-1 ocredit=-1 lcredit=-1 dcredit=-1
    b. Audit policies
        i. $ sudo apt install auditd
        ii. $ sudo auditctl -e 1
        iii. $ sudo nano /etc/audit/audit.rules
            1. -D
            2. -w / -p rwax -k filesystem_change
            3. -a always,exit -S all
    c. $ sudo nano /etc/login.defs
        i. PASS_MAX_DAYS 90
        ii. PASS_MIN_DAYS 10

iii. `PASS_WARN_AGE 7`

9. Users and groups
    a. `cat /etc/passwd to list all users.`
    b. `$ sudo nano /etc/lightdm/lightdm.conf`
        i. **`sudo gedit /etc/lightdm/lightdm.conf`**
            `allow-guest=false`
        ii. Remove `autologin-user=[username]`
    c. `$ sudo passwd -l root`
    d. `$ sudo less /etc/passwd`
        i. `$ sudo adduser [username]`
        ii. `$ sudo deluser [username]`
    e. `Check /etc/sudoers.d to see if people are admin`
    f. `Check /etc/group to remove non admins from admin groups`
10. Log files var.log
11. Check root files :cd /
12. Gedit to open a text editor
13. Disable ipv6 `sudo echo "net.ipv6.conf.all.disable_ipv6 = 1" >> /etc/sysctl.conf`
14. Prevent ipv spoofing `sudo echo "nospoof on" >> /etc/host.conf`
15. Disable IP Forwarding ;sudo echo 0 > /proc/sys/net/ipv4/ip_forward
16. Enable syn cookie protection: `sysctl -n net.ipv4.tcp_syncookies`
17.

Bad programs/packages

a. $ apt list --installed | grep [packagename]
b. $ sudo apt purge [packagename]
c. Potentially Unwanted Packages
    i. Databases
        1. mysql, postgresql, firebird, mariadb, mongodb
    ii. Insecure Network Protocols
        1. Openssh-client, openssh-server, ssh, ftp, telnet, telnetd, samba, snmp, nis
    iii. HTTP Servers
        1. apache, ngnix, lighttpd, jetty, gunicorn, mongrel, tornado, httpd, yaws, aolserver, boa, uwsgi, hunchentoot, unicorn, tntnet
d. Hacking Tools
    i. aircrack-ng, chkrootkit, hping3, hydra, john, kismet, nessus, netcat, nikto, nmap, ophcrack, owasp, snort, tcpdump, thc, hydra, wireshark, ettercap,

Policies

- PAM configuration
    - `$ sudo apt install libpam-cracklib`
    - `$ sudo nano /etc/pam.d/common-password`

        - pam_unix.so
            - remember=5 minlen=8
        - pam_cracklib.so
            - ucredit=-1 ocredit=-1 lcredit=-1 dcredit=-1
    - $ sudo nano /etc/pam.d/common-auth
        - auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800
- Audit policies
    - $ sudo apt install auditd
    - $ sudo auditctl -e 1
    - $ sudo nano /etc/audit/auditd.conf
- $ sudo nano /etc/login.defs
    - PASS_MAX_DAYS 90
    - PASS_MIN_DAYS 10
    - PASS_WARN_AGE 7

Users

- $ sudo nano /etc/lightdm/lightdm.conf
- $ sudo nano /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
    - allow-guest=false
    - Remove autologin-user=[username]
- $ cat /etc/passwd
    - $ sudo adduser [username]
    - *$ sudo useradd [username]*
    - $ sudo deluser [username]
    - *$ sudo userdel [username]*
    - $ sudo passwd [username]
- $ sudo passwd [username]
- $ passwd -l [user]
    - Disable user account (ie. root)
- $ usermot -a -G sudo [username]

https://www.digitalocean.com/community/tutorials/how-to-use-passwd-and-adduser-to-manage-passwords-on-a-linux-vps

- $ sudo less /etc/shadow
- $ cat /etc/group
- *Less /etc/group*
- *cut -d : -f 1 /etc/group*
-
    - $addgroup [groupname]
    - $adduser [username] [groupname]
    - $deluser [username] [groupname]
    - $sudo delgroup [username] sudo

[How to view system users in Linux on Ubuntu]

Media files

- $ls -a /home/*/*

Shared memory

Bad programs/packages

- $apt list --installed | grep [package]
- $dpkg -l | less or $apt list --installed
- $less /etc/passwd
- *cut -d : -f 1 /etc/passwd*
- $sudo apt purge [packagename]
    - aircrack, apache, brutus, cain, chkrootkit, crack, ettercap, ftp, hping, hydra, John the Ripper, kismet, maltego, metasploit, nessus, netcat, nikto, mysql, nmap, ophcrack, owasp zed, postgresql, rainbow-crack, samba, snort, tcpdump, telnet, thc hydra, winzapper, wireshark

Updates

- $sudo apt update
- $sudo apt upgrade
- System settings > software and updates > updates

Firewall

- $sudo apt install ufw
- Allow services
    - $sudo ufw allow [ssh, http]
- $sudo ufw enable
- Check status
    - $sudo ufw status verbose
- $sudo apt install gufw

Openssh

- Disable root login
    - $sudo nano /etc/ssh/sshd_config
    - PermitRootLogin [yes or no]
    - Add “ AllowUsers [username]
    - Restart
        - $service ssh restart

https://www.a2hosting.com/kb/getting-started-guide/accessing-your-account/disabling-ssh-logins-for-root

https://wiki.ubuntu.com/UncomplicatedFirewall

Jeremy's notes
https://askubuntu.com/questions/46501/why-can-other-users-see-the-files-in-my-home-folder
https://unix.stackexchange.com/questions/91488/allow-a-user-to-read-some-other-users-home-directories
https://fossbytes.com/best-hacking-tools-of-2016-windows-linux-mac-osx/
http://www.junauza.com/2008/07/10-best-hacking-and-security-software.html

Windows Checklist

Readme/Forensic Questions

Malwarebytes

- Use to search for malware

Security Policies

- Local Security Policy
  - Account Policies > Password Policy
    - History=5
    - Max passwd age=90 or
    - Min passwd age=30
    - Min passwd length=8
    - Complexity requirements=Enabled
    - Store passwords using reversible encryption=Disabled
  - Account policy > Account Lockout Policy
    - Duration=30 min
    - threshold=3 attempts
    - Reset lockout=30 min
  - Audit Policies
    - Local Policies > Audit Policy
  - Security options
    - Accounts:
      - Administrator account status
      - Guest account status
      - Limit local account use of blank passwords to console logon only
      - Rename administrator account
      - Rename guest account
    - Audit:
      - Audit the access of global system objects

- Audit the use o backup and restore privileges
- Force audit policy subcategory settings to override audi policy category settings
- Shut down system immediately if unable to log security audits

- DCOM:
  - Machine access restriction in security descriptor definition language (SDDL) syntax
  - Machine access restriction in security descriptor definition language (SDDL) syntax
  - Machine launch restrictions in security descriptor definition language (SDDL) syntax
- Devices:
  - Allow undock without having to log onn bn
  - Allowed to format and eject removable media
  - Prevent users from installing printer drives
  - Restrict CD-ROM access to locally logged-on user only
  - Restrict flopyy access to locally logged on user only
- Domain Controller:
  - Allow server operators to schedule tasks
  - LDAP server signing requirements
  - Refuse machine account password changes
- Domain Member:
  - Digitally encrypt of sign secure Channel Data (always)
  - Digitally encrypt secure channel data (when possible)
  - Digitally sign secure channel data (when possible)
  - Disable machine account password changes
  - Maximum machine account password age
  - Require strong (windows 2000 or later) session key
- Interactive logon:
  - Display user information when the session is locked
  - Do not display the last users name
  - Do not require CTRL+ALT+DEL
  - Message text for users attempting to log on
  - Message title for users attempting to log on
  - Number of previous logons to cache (in case domain controller is not available)
  - Prompt user to change password before expiration
  - Require Domain controller authentication to unlock workstation
  - Require smark card
  - Smart card removal behavior
- Microsoft network client

- Digitally sign communications (always)
- Digitally sign communications (if server agrees)
- Send unencrypted password to third-party SMB servers
- Amount of idle time required before suspending sessionDigitally sign communication (always)
- Digitally sign communications (if client agrees)
- Disconnect clients when logon hours expire
- Server SPN Target name validation level

- Network access
  -

Bad Programs/Features

- Programs and Features
  - Delete unwanted features
    - aircrack, apache, brutus, cain and abel hacking tool, chkrootkit, ftp, hping, hydra, iis, John the Ripper, kismet, maltego, metasploit, mysql, nessus, netcat, nikto website vulnerability scanner, nmap, ophcrack, owasp zed, postgresql, samba, snort, tcpdump, telnet, thc hydra, winzapper, wireshark

Bad files

- Home: .jpg, .jpeg, .gif, .png
- Entire thing: .mp3, .mp4, .mov, .avi, .mpg, .mpeg, .flac, .m4a, .flv, .ogg

Services

- View task manager
- Check services

Firewall

- Control panel > system and security > action center > turn on now
- Control panel > system and security > windows firewall
- Control panel > system and security > action center
  - “Windows Security Essentials”
-

Users

- Computer Management > System Tools > Local Users and Groups > Users

Groups

- Computer Management > System Tools > Local Users and Groups > Groups

Updates

- Settings > Update and Security > Windows Update
- Control panel > system and security > windows update
- Windows updates > Change settingsMiscellaneous/Last resort
- Encrypt drive
    - Control panel > system and security > BitLocker Drive Encryption
        - Turn on
- Check host file

```
Click System and Security → Administrative Tools → Local Security Policy
```

Websites

[Basic Windows Security]

Cisco Checklist

Basic Stuff

- #show run
- #show start
- Change hostname
    - #enable (en)
    - #configure terminal (conf t)
    - #hostname [hostname]
- Disable DNS lookup
    - #enable
    - #configure terminal
    - #no ip domain-lookup
- Configure console port
    - #line con 0
    - #password [password]
    - #login
    - #logging synchronous
- Configure vty

        - #line vty 0 4
        - #password [password]
        - #login
        - #transport input ssh
        - #login local
    - Encrypt all text passwords
        - #service password-encryption
    - Create a banner
        - #banner motd “[message]”
    - Account lock out policy
        - #login block-for [number of seconds] attempts [attempts] within [how many seconds]
        - #line con 0
        - #exec-timeout [number of minutes till lock] [number of seconds till lock]
        - #exit
        - #line vty 0 4
        - #exec-timeout [number of minutes till lock] [number of seconds till lock]
    - Configure g0/0 interface
        - Configure IP address
            - #int g0/0
            - #ip address [ip] 255.255.255.0
            - #no shutdown
    - Configure g0/1
        - Configure IP address
            - #int g0/1
            - #ip address [ip] 2555.255.255.0
            - #no shutdown
        - Transfer the IOS from flash to the TFTP server
            - R1#show flash
            - 27
        -

Password Strength

- Configure router to restrict all passwords to a minimum number of characters
    - #security passwords min-length [wanted length]
- Change the timeout period
    - #exec-timeout
- #login on-success
- #login on-failure log
- #security authentication failure rate
- #show logn

#(line-desc)

SSH

- Enable SSH
    - Assign [wanted domain] as the domain name
        - #ip domain-name [wanted domain]
    - Create user, assign privilege, and assign password
        - #username [username] privilege [privilege] password [password]
    - Generate a RSA crypto key using a modulus
        - #crypto key generate rsa (general-keys modulus
        - [wanted one]
    - Update SSH
        - (config)# ip ssh version 2
    - Ssh timeout
        - #ip ssh time-out
    - #ip ssh authentication-retries
    - #show ip ssh
    - Enable vty inbound SSH sessions using line vty commands
        - #login local
        - #transport input ssh

Port security

- Disable unused ports
    - Find unused ports
    - (config)# int range f0/[port-port]
    - (config-if-range)# shutdown
- Set the interface to [what is told]
    - (config)# int range f0/[port-port]
    - (config-if-range)# switchport mode [what is told]
- Enable port security to allow only two hosts per port
    - (config-if-range)# switchport port-security maximum [2]
- Record the MAC address in the running configuration
    - (config-if-range)# switchport port-security mac-address sticky
- Ensure that port violation disable ports
    - (config-if-range)# switchport port-security violation shutdown
- Enable port security
    - (config-if-range)# switchport port-security
- #copy run start

Vlan

- Create a VLAN
    - (config)# vlan [number you want to create]
    - (config-vlan)# name [name of vlan]

- Configure a port for access and associate to a VLAN
    - (config)# int f0/[desirable port]
    - (config-if)# switchport mode access
    - (config-if)# switchport access vlan [desirable port]

Port Stuff

- Set a port for trunking
    - (config)# int f0/[diesierable port]
    - (config-if)# switchport mode trunk
- Create a subinterface
    - (config)# int g0/[subinterface]
    - (config-subif)# encapsulation dot1q [number of interface]

6. Configure console port so that it never times out (“exec-time 0 0”).6. Configure console port so that it never times out (“exec-time 0 0”).
show ip int brief
copy run start
ip default-gateway
20
Campus layer 3switch 1 needs banner
Remot site switch 1 ping
Remote site router 1 ping

List of all allowed system users in linux

Root,daemon,bin,sys,sync,games,man,lp,news,uucp,proxy,www-data,backup,list,irc,gnats,nobody,systemd-timesync,systemd-network,systemd-resolve,systemd-bus-proxy,syslog,messagebus,uuidd,lightdm,whoopsie,avahi-autoipd,avahi,dnsmasq,colord,
Speech-dispatcher,hplip,kernoops,pulse,rtkit,saned,usbmux,

rsyslogd
```bash
# apt install rsyslog
# systemctl enable rsyslog
# $EDITOR /etc/rsyslog.conf => remove anything that sends logs to a domain

-e 2
# $EDITOR /etc/audit/auditd.conf
max_log_file_action=keep_log
```
-