**USMA CCDC 2018 Security Checklist**

****

**Index**

[**Security Priorities**](#_m0oide3pz27) **03**

[Security Priorities](#_oog8cdglgfh) 03

[**System**](#_g5kpnty9pgyc) **07**

[Specific Linux Checklists](#_3arczgca7xif) 07

[End-user UNIX](#_y614g6ho5b2f) 12

[End-User Windows](#_vy6nbta0o7vj) 23

[**Network**](#_ff73fokqoheu) **30**

[Router](#_3xpgd8rrqvb2) 30

[Switch](#_bv8ai426drh0) 33

[Linux Firewall](#_vrvwaj7en8ai) 36

[Windows Server 2008/2012/2016 GUI Firewall Checklist](#_hpfic1b4vu7f) 38

[Windows XP/Vista/7/8/10 Firewall Checklist](#_hy8x55s42hyt) 40

[**Services**](#_rnite8tcdzgr) **41**

[Securing LDAP](#_4pz2oxg510hf) 46

[SMTP Server:](#_d2qf7enkw58z) 55

[DNS Server](#_f5grvx2z3j5p) 59

[SSH Checklist](#_t1wajh34o73o) 65

[LDAP](#_s9wf0mjqrujy) 69

[Web Server:](#_f0daa68x2y0d) 72

[FTP Checklist](#_9br0jw55u59s) 77

[MySQL](#_9a2aligdveuh) 80

[**Monitoring**](#_vaxck0pf4ip1) **82**

[Linux Monitoring](#_ogqtkfovxgg6) 82

[Windows](#_furo1dszqsfi) 85

[**Stryke**](#_t2ke8lbwgvme) **94**

[Forensics Checklist](#_tistdvhnc6lj) 94

# **Security Priorities**

## Security Priorities

the first thing that attackers do is look for low hanging fruit

1) change passwords, use different passwords for users/boxes

shared passwords create multiple security holes

be aware that once they have enough of a foothold, attacker no longer

needs to know your passwords

change your passwords often

In order to do this as efficiently as possible, there should be a master list of

passwords that is created before the competition. This list needs to be large

enough to allow for different systems to have different passwords which can be rotated

thoughout the competition. This rotation should occur at a fixed, predetermined interval.

By having a complete list of passwords prior to the start, it should be simple enough to write

which machine is using which password and for what round next to the password.

2) who's on there and who shouldn't be

tail -n 30 /etc/passwd

disable uneeded accounts

remove admin rights from accounts that don't need it

Obviously we won't be able to tell who needs admin rights and who doesn't before we have an understanding

of how the network works. The key here is to simply notate which users have certain permissions so

that we can go back and validate these users against required functionality.

Going along with this is checking your own OS, see the strike team guides for specific commands to identify

kernel arch and version

We can also see which services are running on our machine

sudo service --status-all

which processes are using the most cpu

top

what network connections look like

netstat -natp

netstat -tulpn

What network's we're connected to

ifconfig

inspect routing table

What's on the network?

To get a better understand of our network we can turn to nmap

nmap -F <host> # runs a quick scan of the 100 most common ports

nmap -sP 10.0.0.0/24 # scans the network listening for machines that respond to patching

nmap -A 1<host> # detect OS and services

common initial attacks are ssh\_login on linux and smb/psexec on windows

3) check ports 22 and 445

Similar to the user situation we won't know what machines need what ports until we understand the network

but keep track of what's open where so that we can close everything extra once we know.

your host firewall should be blocking port 445 unless it is absolutely necessary

change default ssh login credentials

look for dropped ssh keys, or ssh configuration that allows multiple users to use the same key

ls -la ~/.ssh

~/.ssh/authorized\_keys

if there's a key in .ssh that was added recently

when you look at authorized\_keys it gives you the key and the user associated with it if the same

key can log in to multiple users

they're getting in regardless but we would like to know how they're getting out

4) set up network monitoring

don't just focus on stopping post exploitation

in order for them to do stuff, information needs to come in and out

find out how it's happening and stop it

be aware of multiple ways to exfil data and what to look for

tcp

reverse shells

When something in your machine tries to call back to the attacker

look for high ports on your machine, odds are you're running standard services

so high ports making connections out of the network are signs that it's calling home

inbound shells

inbound connections to ports that aren't running known services

http

if it's just a website with a strange nonsense string on it then that could be c2

don't ask me how it works, i have no idea, but i know that it happens

dns tunneling

large number of requests to strange subdomains

block those domains

whitelist outbound ports

force web traffic through an authenticated proxy server to deny SYSTEM from exiting

now that we've taken closed the front door, close up holes in your walls

6) work on patching machines

ensure that those patches are applied and active

especially patch rce vulnerabilities

linux:

apt-get update

yum update

windows:

system security -> windows update -> view update history

-> restore hidden updates

check for updates

wmic qfe get hotfixid | find "<#>"

6) firewall

strict inbound and outbound rules

focus on whitelisting what we need

key to success is to defeat their persistence

7) how do they keep getting in?

indicators of compromise

hash values: Ssdeep and other fuzzy hash tools that might be able to match commercial malware

ip addresses: it's always good to block bad ips, but it's easy for attacker to change

domain names: little harder to change, necessary for dns tunneling

network artifacts:

uri patterns

c2 info in network protocols

This stuff comes from wireshark, once you are able to narrow down which addreses are malicious

you can try to watch the traffic in wireshark

distinctive http user agent strings

if you're using a proxy or some sort of custom request generator then they might not have bothered

to fill in the entire long user agent string

distinctive smtp mailer values

host artifacts:

registry keys and values: regshot

files with names that are similar to real windows files

especially stuff in system32, syswow64, program files, etc

stuff that will run at startup

alternate data streams in files

what processes are connecting to the internet and shouldn't

which processes are taking up way too much memory (process injection/reflective loading)

how to identify stuff that's bad

linux

ps -aux

netstat -napt

netstat -tulpn

lsof

suid programs

find <directory> -perm -4000

service --status-all

look through /proc/<pid> directories

chron

windows

sysinternals

procmon

tcpmon

autoruns

streams

regshot

task manager

Continually monitor network and conduct active defense throughout

8) watch for dirty tricks and a few of your own

static arp entries and arp poisoning

check service status

red team likes to stop services

and delete important files

so have a backup or know how to redo it

remove notepad.exe (default spawn process for cobalt strike and metasploit)

a note on shapshots

Reset to initial snapshot

vulnerable to default but it might manage to kick them off

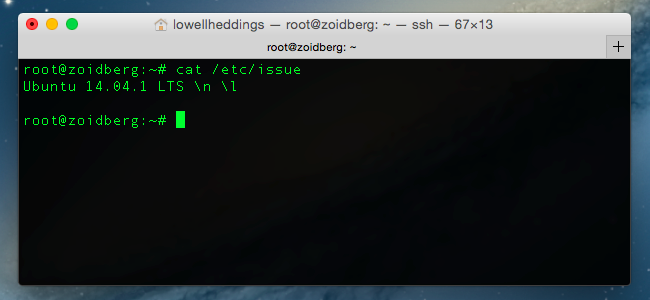
penalty???

don't want to rever to snapshot where they already were in the network

# **System**

## Specific Linux Checklists

Step One



After this proceed to the appropriate checklist

Centos 7 Hardening

1. Restrict root

#echo “tty1” > /etc/securetty

#chmod 700 /root

1. Set password policy
   1. Make them expire every 180 days

#perl -npe ‘s/PASS\_MAX\_DAYS\s+99999/PASS\_MAX\_DAYS 180/’ -i /etc/logins.defs

1. Can only be changed once a day

#perl -npe ‘s/PASS\_MIN\_DAYS\s+0/PASS\_MIN\_DAYS 1/g’ -i /etc/logins.defs

1. Update system to sha512 instead of md5

#authconfig --passalgo=sha512 --update

1. Restrict umask file sharing

#perl -npe ‘s/umask\s+0\d2/umask 077/g’ -i /etc/bashrc

#perl -npe ‘s/umask\s+0\d2/umask 077/g’ -i /etc/csh.cshrc

1. Reap idle users

#echo “readonly TMOUT=900” >> /etc/profile.d/os-security.sh

#echo “readonly HISTFILE” >> /etc/profile.d/os-security.sh

#chmod +x /etc/profile.d/os-security.sh

1. Restrict cron and AT to prevent cronjobs and timed scripts
   1. Cron:

#touch /etc/cron.allow

#chmod 600 /etc/cron.allow

#awk -F: '{print $1}' /etc/passwd | grep -v root > /etc/cron.deny

1. AT

#touch /etc/at.allow

#chmod 600 /etc/at.allow

#awk -F: '{print $1}' /etc/passwd | grep -v root > /etc/at.deny

Red Hat Enterprise Linux Checklist to Secure on Setup

1. Disable interactive setup
   1. Enter “PROMPT=no” in */etc/sysconfig/init* file
2. Ensure users create good passwords with one of two methods:
   1. Create passwords for users
   2. Verify that user created passwords are of acceptable quality
      1. Edit */etc/pam.d/passwd* file with appropriate settings

password required pam\_cracklib.so retry=3 minlen=8 minclass=4 maxsequence=3 maxrepeat=3

1. Edit the */etc/pam.d/login* file to lock inactive accounts after a certain number of days

chage -M <number of days> <username>

1. Edit */etc/security/access.conf* to customize access control based on login names following the access.conf(5) man page. Do the following to restrict logins from certain accounts:
2. In both /etc/pam.d/login and /etc/pam.d/gdm-\* files:

account required pam\_access.so

1. In the /etc/security/access.conf file:

- : <user you want to restrict> : ALL

1. Disable root access
   1. Set the root account's shell to */sbin/nologin* in the */etc/passwd* file
   2. Prevent root user from logging in with command echo > /etc/securetty in shell prompt
   3. Disable root SSH logins with “PermitRootLogin no” in */etc/ssh/ssh\_dconfig* file

\*For more detailed information look at Red Hat Enterprise Linux 6 Security Guide Chapter 2 pages 29-49

Ubuntu Checklist

1. Enable automatic security updates

#apt install unattended-upgrades

1. Install normal updates:

#apt update && apt upgrade

1. Configure PAM by installing pwquality and setting good configurations
2. Install pwquality: #apt install libpam-pwquality
3. Edit */etc/pam.d/common-password* with settings like the following (reference man pam\_pwquality for more info):

password requisite pam\_pwquality.so minlen=10 retry=3

1. Configure firewall and iptables to limit traffic:

\*\*\*Accept all incoming traffic on local interface\*\*\*

#iptables -A INPUT -I lo -j ACCEPT

\*\*\*Allow traffic to SSH (to port 2222), SMTP (25), and our web server (80, 443)\*\*\*

#iptables -A INPUT -p tcp -m tcp –dport 2222 -m state –state NEW,ESTABLISHED -j ACCEPT

#iptables -A INPUT -p tcp -m tcp –dport 25 -m state –state NEW,ESTABLISHED -j ACCEPT

#iptables -A INPUT -p tcp -m tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT

#iptables -A INPUT -p tcp -m tcp –dport 443 -m state –state NEW,ESTABLISHED -j ACCEPT

\*\*\*Drop all traffic in input chain\*\*\*

#iptables -A INPUT -j DROP

1. Make sure AppArmor is installed and is in *enforce* mode:

#sudo apt install apparmor-profiles (install)

#sudo aa\_status (checks status)

#sudo aa-enforce /path/to/bin (puts into *enforce* mode)

Fedora Hardening

* Either disallow root access. Three ways:
  + Change the root shell: edit the */etc/passwd* file to make the shell */sbin/nologin* instead of */bin/bash*
  + Empty */etc/securetty* file:

#echo > /etc/securetty

* + Edit the */etc/ssh/ sshd\_config* file and set the PermitRootLogin parameter to no.
    - Restart ssh with: #kill -HUP `cat /var/run/sshd.pid`
* Or limit root access via su and sudo:
  + Simplest way to control su access is adding specific users to the *wheel* group:

#usermod -G wheel <username>

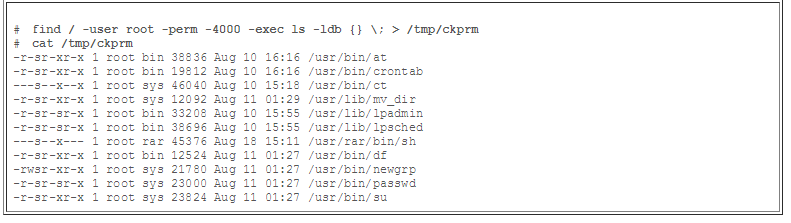
* Control sudo use by editing */etc/sudoers* file with the visudo command:

#visudo <username> ALL=(ALL) ALL

\*\*\*See Red Hat checklist for additional security measures because the two are pretty similar

## **End-user UNIX**

* Step One: Find out which version of OS and kernel are you dealing with
  + # lsb\_release -a ⇒ The lsb\_release command displays certain LSB (Linux Standard Base) and distribution-specific information. If this does not give you enough information try # cat /etc/\*-release.
  + # uname -a OR # uname -mrs ⇒ command to find out your kernel version. Sample output: Linux 2.6.32-5-amd64 x86\_64, where Linux is a Kernel name, 2.6.32-5 is a Kernel version and x86\_64 is machine hardware name(64 bit). Use # cat /proc/version if you want to see gcc version as well. Also, if you do not understand various parts of the output from the listed commands google them, but you should not need them. For the competition purposes knowing what distribution of \*Nix and kernel you have and their version numbers should be enough.
  + Take a note of the information you got from this step, you will need this for the various parts of the competition and to go through this checklist.
  + Keep Linux Kernel and Software Up to Date
    - # yum update OR # apt-get update && apt-get upgrade ⇒ Make sure you use both apt-get update and apt-get upgrade, first just gets you newest packages and the latter installs them all. Try to use yum first and if that does not work do the second one.
  + So, at the end of this step you should have an up to date OS on your box and you should know what version \*NIX OS and kernel are you running. Reference the Specific Unix Systems checklist for more info about your box’s OS version. (After you finish the rest of the steps from this checklist of course)
* Step Two: Check sensitive file permissions:
  + SetUID bit
    - You should be careful with files that have SetUID bit set
    - # find *{directory}* -user root -perm -4000 -exec ls -ldb {} \; >/tmp/ {*filename}* ⇒ Command to find files with setuid bit set. *Find {directory}* checks all mounted paths starting at the specified directory, which can be *root (/), sys, bin,* or *mail*. -user root displays files owned only by root. -perm -4000 displays files only with permissions set to 4000. -exec ls -ldb displays the output of the find command in ls -ldb format. ./tmp /{filename} writes results to this file.
      * Output Example:



* This output shows that a user named rar has made a personal copy of /usr/bin/sh, and has set the permissions as setuid to root. As a result, rar can execute /usr/rar/bin/sh and become the privileged user.
* To get rid of setuid bit:
* # sudo chmod g-s {filename} ⇒ g stands for group (also can be u -user, o -other, a-all), -s removes setuid bit (alternatively you can add it with +s). Verify changes with #ls -l {filename}.
* If numerical permissions work better for you do #sudo chmod 0664 {filename} (assuming the rest of the permissions are 664). Do not forget to verify.

Sensitive system files need to have the proper permissions set on them to prevent unauthorized changes:

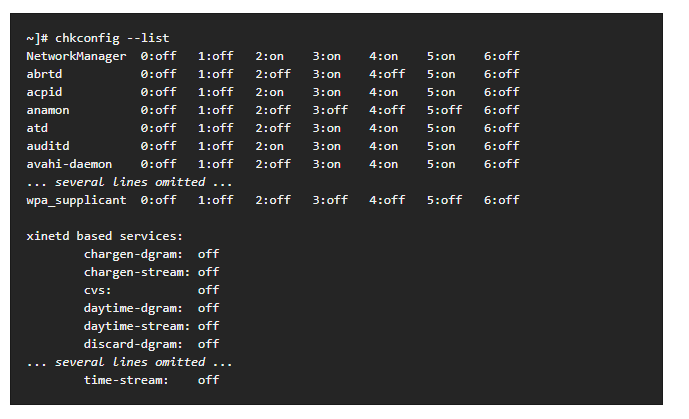
* + # ls -ldb /etc ⇒ Make sure the following permissions are as listed and if not change them
  + # chmod 0700 /etc/profile
  + # chmod 0700 /etc/hosts.allow
  + # chmod 0700 /etc/mtab
  + # chmod 0700 /etc/utmp
  + # chmod 0700 /var/adm/wtmp( or /var/log/wtmp)
  + # chmod 0700 /etc/syslog.pid( or /var/run/syslog.pid)
  + # chmod 0700 /etc/sysctl.conf
  + # chmod 0700 /etc/inittab
  + Verify:
    - Root.root and -rw-r--r--(644) ⇒ # ls -la /etc/fstab
    - Root.root and -rw-r--r--(644) ⇒ # ls -la /etc/passwd
    - Root.root and -rw-r------(400) ⇒ # ls -la /etc/shadow
    - Root.root and -rw-r--r--(644) ⇒ # ls -la /etc/group
    - Root.root and -rw-r--r--(644) ⇒ # ls -la /etc/sudoers
  + If you have time:
    - # ls -ldb /bin AND #ls -ldb /usr/bin ⇒ Verify permissions as specified below.
    - # chmod 02750 /bin/su
    - # chmod 02750 /bin/sudo
    - # chmod 02750 /bin/ping
    - # chmod 02750 /bin/ifconfig
    - # chmod 02750 /usr/bin/w
    - # chmod 02750 /usr/bin/who
    - # chmod 02750 /usr/bin/locate
    - # chmod 02750 /usr/bin/whereis
  + Get rid of World writable Files:
    - #find /dir -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
    - #find / -type d -perm +2 -ls ⇒ Either #chmod 750 those files or remove them (#rm)
  + Make Sure No Non-Root Accounts Have UID Set to 0
    - # awk -F: '($3 == "0") {print}' /etc/passwd ⇒ You should only see one line (root:x:0:0:root:/root:/bin/bash) if not do the following:
      * #usermod -u {newUID} {username} ⇒ {newUID} is the new user ID that you want to assign to the user {username} instead of the old “0”. New UID can be anything that has not been used before (check etc/user).
      * # groupmode -g {newGroupID} {groupName} ⇒ Same thing as above but for the groups.
      * # find / -group {oldGroupID} -exec chgrp -h {groupName} {} \; and # find / -user {oldUserID} -exec chgrp -h {userName} {} \; ⇒ This commands will change the group ID and user ID respectively for any files outside of user’s home directory.
      * To verify:
        + # ls -l /home/{username}
        + # id -u {username}
        + # id -u {groupname} ⇒ All of these commands should give the output that matches the parameters that you specified earlier. (Also, # awk -F: '($3 == "0") {print}' /etc/passwd command from earlier should give you only one line this time)

## 

## Step Three: Check for unwanted services and open ports (IMPORTANT):

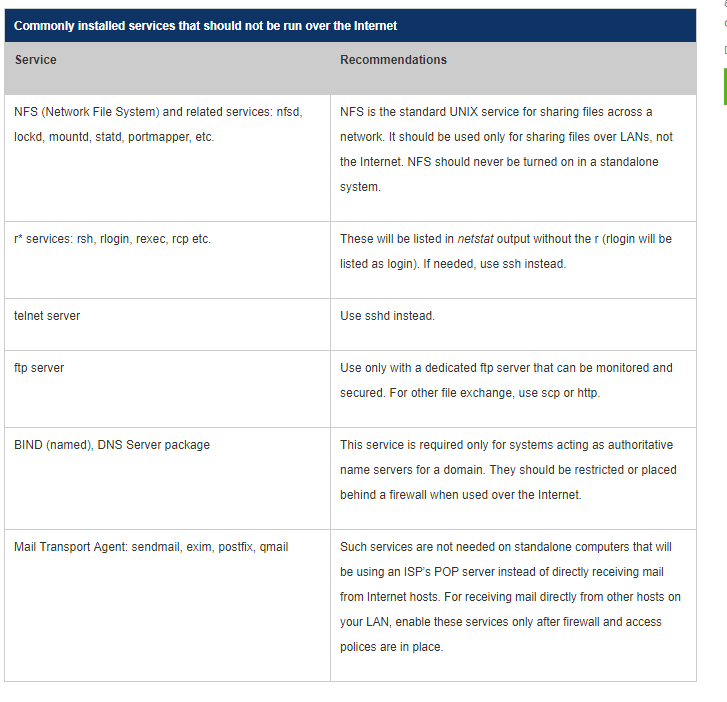
* + Disable Unwanted Services
    - # chkconfig --list | grep '3:on' OR # netstat -lp⇒ This will give you the list of services that are currently on. Carefully go through them and disable the ones that you do not need. More to follow on that in the next paragraph.

Sample output for the chkonfig command (note that in this output example we did not filter for the services that are on)



Each line consists of the name of the service followed by its status (*on* or *off*) for each of the seven numbered runlevels. For example, in the listing above, NetworkManager is enabled in runlevel 2, 3, 4, and 5, while abrtd runs in runlevel 3 and 5. The xinetd based services are listed at the end, being either *on*, or *off*.

Here is the list of the services that should not be running on your system:



* + - \*\*\*\* MAKE SURE YOU ARE NOT TURNING OFF THE SERVICE THAT YOU NEED FOR COMPETITION, TURN ONE OFF ONLY IF YOU ARE ABSOLUTELY SURE THAT TEAM DOES NOT NEED IT. CONSULT IT WITH SYSTEMS TEAM/LEADERSHIP \*\*\*\*\*
    - There are tons of other services, go through them (do not take forever looking at them though) and research the ones that seem weird to you (something you do not know what it is or completely out of context). If you are not sure, ask! Somebody in the team should know something about that service.
    - # service {serviceName} stop ⇒ Stop the service
    - # chkconfig {serviceName} off ⇒ Stop the Service

## Find Listening Network Ports

* + - #sudo lsof -i -P -n⇒ list the network open ports on your Linux server and the process that owns them
      * Sample output:

sshd 85379 root 3u IPv4 0xffff80000039e000 0t0 TCP 10.86.128.138:22 (LISTEN)

-sshd is the name of the application

-10.86.128.138 is the IP address to which sshd bind to (LISTEN)

- 22 is the TCP port that is being used (LISTEN)

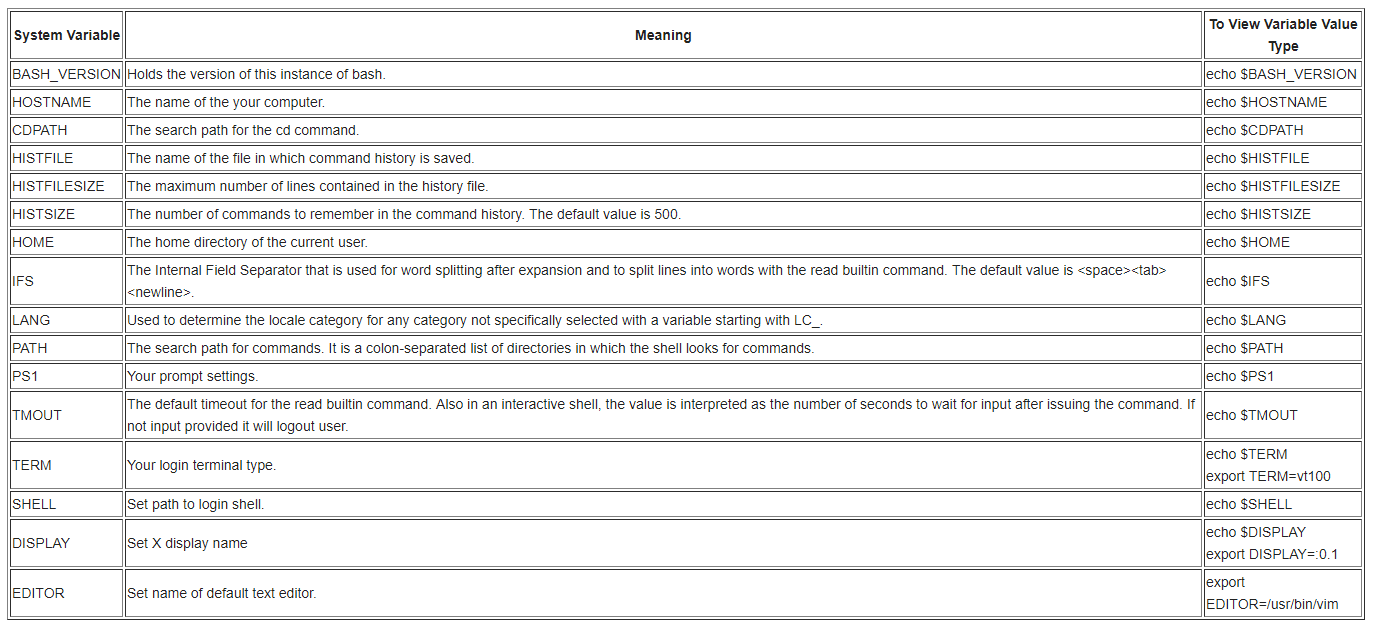
-85379 is the process ID of the sshd process

* + - Most people use netstat though to get the same info so here is the syntax for it as well:
      * #netstat -tulpn | less ⇒ Does the same thing
    - Other Useful Commands:
      * #lsof -i :{portNumber} ⇒ To see which process is bound to port {portNumber}
      * #ls -l /proc/{PID} ⇒ See More Info for Process with PID
      * #whatis {COMMAND}
      * #pwdx {PID} ⇒ Report current working directory of proves with PID.
* Step Four: Preventing other common vulnerabilities
  + Verify No accounts have empty passwords
    - # awk -F: '($2 == "") {print}' /etc/shadow
    - If any empty ones disable it or even delete it ⇒ #passwd -l {username}
  + NoLogin

Set users shell to nologin if you do not want them to access shell. NoLogin puts linux shell access restrictions for the services like FTP or telnet and refuses them politely not to log in. YOU most likely would want to make sure that www-data has set its shell to nologin, but there might be other users as well that will need this option.

* + - # less /etc/shells ⇒ You should see the nologin shell in the output. If not, add using the command #echo “/sbin/nologin” >> /etc/shells if you are using Debian modify the path to “usr/sbin/nologin”.
    - # usermod -s /sbin/nologin {username} ⇒ Block shell access to user {username}. User {username} must exist when you use this command. Once again, if you are using Debian modify path to “usr/sbin/nologin”.
  + Environmental Variables
    - # set ⇒ Display current Environment variables. In case if you want to look at them all.
    - # echo “${variableName}” ⇒ Display the content of the environmental variable

Following is the list of most common environmental variables:



* + - You can modify environmental variables using export command. Here is the example:
      * #export PATH=${PATH}:/home/{username}/bin ⇒ Note that this changes to environmental variables are not permanent, they will be flushed if you reboot the system or logout or even if you open a new shell. Since we are not allowed to reboot in this competition this should not be a problem, but in case if you want to make it permanent use this command : #vi `/.bash\_profile (any other editor will work), append your change, so for our example command it would be #export PATH=${PATH}:/home/{username}/bin, save and close the file. Alternatively, you always can change them manually every time you login if that makes you happy.
    - PATH variable
      * Make sure “./” (your home directory) is not in there or if it is, it is at the end not anywhere else. Note, PATH variable tells the shell which directories to search for executable files in response to commands issued by user. Each directory is separated by column.
        + One way to remove something from your PATH variable is to redefine it completely and excluding your home directory. So it will be something like # export PATH = {only directories I want}
        + More sophisticated but dirty way to do it:

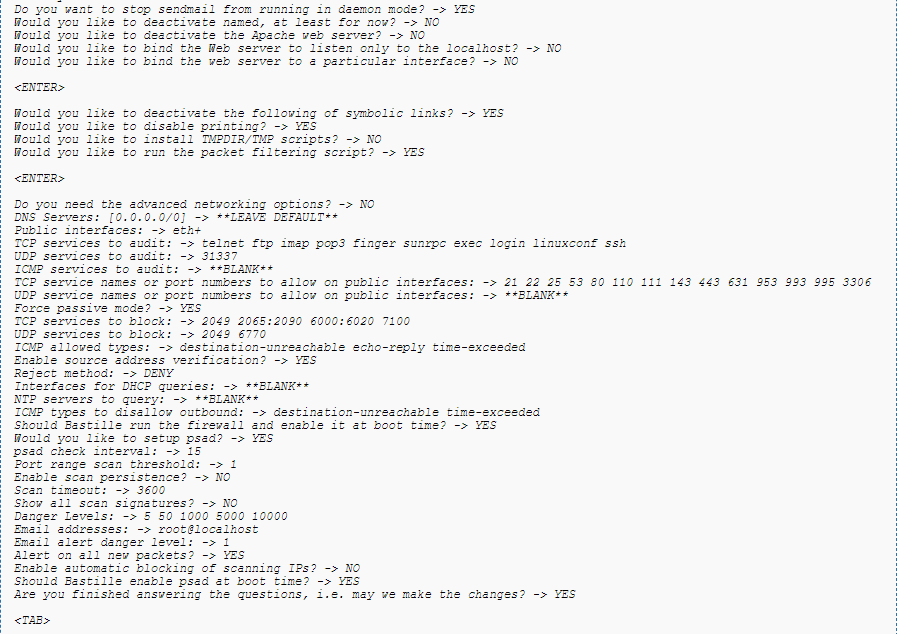
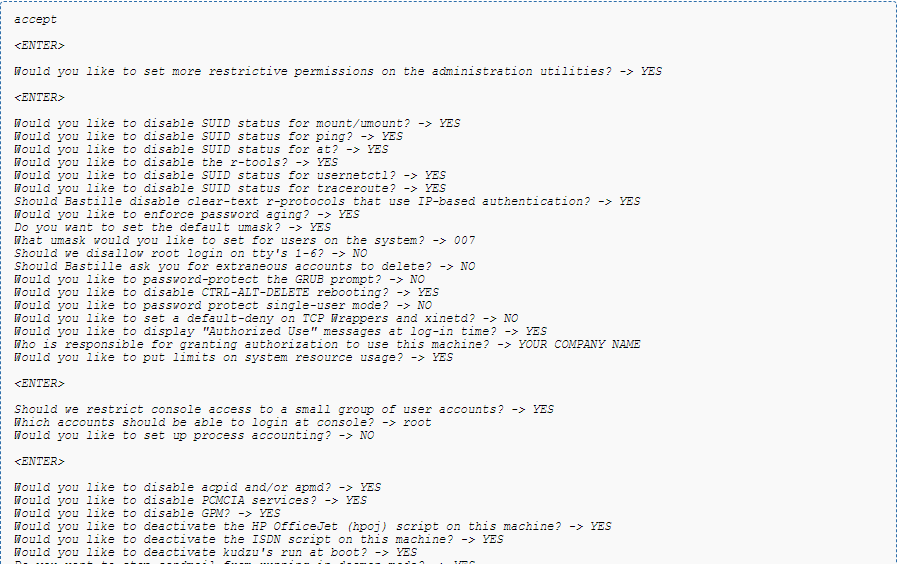
export PATH="$( echo $PATH| tr : '\n' |grep -v raj | paste -s -d: )"

separate each dir in your PATH by line using tr

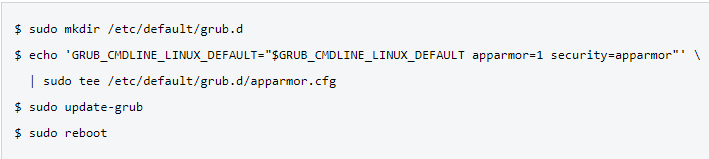
remove what you don't want (path matching "raj") using grep -v, and

collapse back into a long ":" delimited string using paste.

* Step 5 (Tentative depending whether monitoring team does this or not): Setup Logs
  + Track and Log Failed Login Attempt Records
    - # vi /etc/pam.d/system-auth
      * Modify As Follows:
        + *auth required pam\_tally.so no\_magic\_root*
        + *account required pam\_tally.so deny=3 no\_magic\_root lock\_time=120*
      * Other Useful Commands:
        + #faillog -u {username} ⇒ Display Login Attempts for {username}
        + #faillog -M MAX -u {username} ⇒ Set Maximum Number of Login Failures MAX for the {username}.
        + #faillog -r OR #faillog -r -u {username} ⇒ Reset counter of all login failure OR for {username}
      * On that Note:
        + #passwd -l {username} ⇒ To Lock Account
        + #passwd -u {username} ⇒ To Unlock Account
* Bastille
  + # apt-get install bastille
  + Once installed: #bastille -c to configure bastille
  + The following screengrabs show the correct configurations:



* Apparmor
  + Install: #apt-get install apparmor-profiles apparmor-utils
  + Enable:



* + #apparmor \_status (to see current profiles and associated modes)
  + #man apparmor (for more details of what to do with that information)

## 

## **End-User Windows**

Windows 2000 Hardening

Open Local Security Policy:

1. Log on to the computer with administrative rights.
2. In a Windows 2000 Professional computer, Administrative Tools is not displayed as a Start menu option by default. To view the Administrative Tools menu option in Windows 2000 Professional, click Start, point to Settings, and select Taskbar and Start Menu. In the Taskbar and Start Menu Properties window, click the Advanced tab. Check the Display Administrative Tools checkbox in the Start Menu Settings dialog box. Click the OK button to complete the setting.
3. Click Start, point to Programs, point to Administrative Tools, and then click Local Security Policy. This opens the Local Security Settings console.

Set password policy:

1. Open the applicable security policy through Local Security Policies
2. Expand Security Settings.
3. Within Security Settings, expand Account Policies to reveal the Password, Account Lockout, and Kerberos policies.
4. Click on the Password Policy object. The right-hand details pane will reveal the configurable Password Policy settings.
5. Set the Password Policy as follows:
   1. Set limit on how often password may be reused:
      1. Double click Enforce password history
      2. Check Define this policy setting box
      3. Set passwords remembered to 24
   2. Set max password age:
      1. Double click Maximum password age
      2. Check Define this policy setting box
      3. Set days to 70
   3. Set min password age:
      1. Double click Minimum password age
      2. Check Define this policy setting box
      3. Set days to 2
   4. Set min password length:
      1. Double click Minimum password length
      2. Check Define this policy setting box
      3. Set characters to 8
   5. Enable password complexity

Set local rights and privileges:

1. Expand security settings
2. Within Security Settings, expand Local Policies to reveal the Audit, User Rights Assignment, and Security Options policies.
3. Click on the User Rights Assignment object. Assign the following rights and privileges:
   1. Access this computer from the network:
      * Administrators
      * Backup Operators
      * Power Users
      * Users
      * Authenticated Users
   2. Log on Locally:
      * Administrators
      * Backup Operators
      * Power Users
   3. Shut Down the System
      * Administrators

Set security options:

1. Navigate to Windows Settings > Security Settings > Local Policy > Security Options
2. Set the following options:
   1. Additional Restrictions for Anonymous Connections: No access without explicit anonymous permissions
   2. Allow System to Be Shut Down Without Having to Log On: Disabled
   3. Audit Use of Backup and Restore Privilege: Enabled
   4. Clear Virtual Memory Pagefile When System Shuts Down: Enabled
   5. Digitally Sign Client Communication (Always): Enabled
   6. Disable CTRL-ALT-DEL Requirement for Logon: Disabled
   7. Do Not Display Last User Name in Logon Screen: Enabled
   8. Prevent Users From Installing Printer Drivers: Enabled
   9. Recovery Console: Allow Automatic Administrative Logon: Disabled
   10. Rename Administrator Account: (Provide a good name)
   11. Restrict CD-ROM Access to Locally Logged-On User Only: Enabled

Audit Log management (Up to monitoring team to determine if these changes are worth it):

1. Navigate to Start > Programs > Administrative tools > Event viewer
2. Right-click on Security Log object and click Properties
3. Set the following:
   * Set Maximum Security Log Size: 20MB
   * Restrict Guest Access to the Application Log: Enabled
   * Restrict Guest Access to the Security Log: Enabled
   * Restrict Guest Access to the System Log: Enabled
   * Retention Method for Application Log: Overwrite events as needed
   * Retention Method for Security Log: Overwrite events as needed

Set group memberships:

1. Navigate to Start > Administrative tools > Active Directory and Computers
2. Double click the domain node
3. Go to Users container
4. Right click the account name and select Properties
5. Click on Member Of tab and then Set Primary Group to edit
6. Set the following:
   * DnsUpdateProxy don’t edit
   * Domain Admins don’t edit
   * Domain Guests don’t edit
   * Domain Users: remove Guest account and disable TsInternetUser account
   * Enterprise Admins don’t add non-Administrative accounts
   * Group Policy Creator Owner don’t add non-Administrative accounts
   * Schema Admins don’t add non-Administrative accounts

Secure the registry:

1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand Security Settings.
3. Within Security Settings, right-click on Registry.
4. Select Add key.
5. From the Select Registry Key window, navigate to and select the desired key.
6. Click the OK button. A window labeled Database Security for *path* Properties will appear.
7. Set permissions as outlined below:
   1. \SOFTWARE\Microsoft\Windows NT\CurrentVersion:
      * Users: Read; This key and subkeys
      * Power Users: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER:Full Control; Subkeys only
      * TERMINAL SERVER USER: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
   2. \SOFTWARE\Microsoft\Windows NT\CurrentVersion
      * Authenticated Users: Read; This key and subkeys
      * Server Operators: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER: Full Control; Subkeys only
   3. \SOFTWARE\Microsoft\Windows NT\CurrentVersion
      * Users: Read; This key and subkeys
      * Power Users: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER: Full Control; Subkeys only
   4. \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
      * Authenticated Users: Read; This key and subkeys
      * Server Operators: Read; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER: Full Control; Subkeys only
   5. \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
      * Users: Read; This key and subkeys
      * Power Users: Read; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER: Full Control; Subkeys only
   6. HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
      * Users:Read; This key and subkeys
      * Power Users:Read; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER: Full Control; Subkeys only
   7. HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AEDebug
      * Users:Read; This key and subkeys
      * Power Users:Read; This key and subkeys
      * Administrators: Full Control; This key and subkeys
      * SYSTEM: Full Control; This key and subkeys
      * CREATOR OWNER: Full Control; Subkeys only
   8. Edit the following with the same settings:
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Accessibility
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Classes
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\EFS
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Windows
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Time Zones
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Svchost
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\SecEdit
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Perflib
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AEDebug
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Accessibility
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Classes
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Classes
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\EFS
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\FontMapper
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Windows
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Time Zones
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Svchost
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\SecEdit
      * HKLM\System\Software\Microsoft\Windows NT\CurrentVersion\Perflib

\*\*\*The above applies specifically to Windows 2000 but can also be used in later versions

# **Network**

## **Router**

1. Check version of cisco on machine

* show version

2. Check all commands placed onto router

* show run
  + - make sure that service password encryption is set
    - make sure hostname is set
    - make sure that enable secret is set
    - make sure domain name is set
    - make sure username is set
    - make sure passwords are encrypted (ex. password 7 1P312A910I)
    - make sure “no ip http server” is set
    - make sure that a default route is set (ex. ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1)
    - make sure created access lists are on
    - make sure telnet is disabled and ssh is enabled (“login local” and “transport input ssh should be set” on line vty 0 4)

3. Check ip addresses (machines that you are directly connected to)

* show ip int OR show ip int brief
  + - make sure ip addresses correlate to what your ip allocations/network

4. Check all possible routes for network traffic

* show ip route
  + - make sure that a default route is set
    - make sure that any routing protocols (ex. ospf) are within the designated network (ex: no network 0.0.0.0 255.255.255.255 area 0)
    - make sure routes are not going to an unknown address

5. Check neighbor machines (machines that you are directly connected to)

* show cdp neighbor
  + - make sure no unknown neighbors are there

6. Check all access lists on router

* show ip access-lists
  + make sure no unwanted traffic is going in or out of network

7. Check hosts

* sh hosts
  + make sure that the hosts designated have the correct ips and hostnames
* delete any hosts that should not be designated a hostname

8. Check Logging configuration and log messages

* show logging (shows logging configuration
* show logging message (shows list of log messages)

9. Ping loopback

* should get replies

10. Ping devices within network

* should get replies

11. Ping devices outside of network

* \*replies depend

Configuring a router

* Passwords
* service password-encryption (sets encryption to password)
* enable secret <cisco> (set password to cisco)
* Configure a hostname
  + hostname <name>
* Configure domain name and ip for domain name server (DNS)
  + ip domain name <name> (sets domain name)
  + ip name-server <server ip> (sets ip for domain name)
* Configure to no ip domain look ups
* no ip domain-lookup
* Configure an Interface and its ip address
* int <g0/0> (configure int g0/0)
* ip address <#.#.#.#.> (set ip address for interface)
* no shutdown (Turns interface on)
* Configure a Vlan Interface and its ip address
  + int <g0/0.1> (configure int g0/0.1)
  + ip address <#.#.#.#.> (set ip address for interface)
  + no shutdown (Turns interface on)
* Configure OSPF
* router <ospf 1>(starts ospf process 1)
* network <172.16.10.0> <0.0.0.255> <area 0> ( Any interface with an address of 172.16.10.0~255 is to be put in area 0 )
* Configure ip route
* int <g0/0>
* ip route <0.0.0.0> <0.0.0.0> (route traffic from a certain src ip to a specific destination)
* Set SSH and turn off telnet
* username <Roland> password <tower> (creates username/password for SSH connection)
* ip domain-name <name> (creates a host domain name for the router)
* crypto key generate rsa (enable ssh server for local and remote authentication on router and generates RSA key pair)
* ip ssh version 2 (enables ssh version 2 on device)
* line vty 0 4 (move to vty config mode)
* login local ( enable password checking)
* transport input ssh (limits remote connectivity to ssh)
* Apply Standard Access Lists
* access-list <10> <permit> <172.16.0.0> <0.0.255.255>(All packets with source ip of 172.16.x.x. will be permitted to come through)
* int <g0/0> (move to interface)
* ip access-group <10> <in> (takes access list 10’s lines and applies to packets going into interface)
* Apply Extended Access Lists
* access-list <110> <permit> <tcp> <172.16.0.0> <0.0.0.255> <192.168.100.0> <0.0.0.255> <eq 80> ( HTTP packets (port 80) with a source ip address of 172.16.0.x will be permitted to travel to the destination address 192.168.100.x).
* Enable Logging
  + logging enable
* Turn off ip http server
  + no ip http server

## **Switch**

0. Check version of cisco on machine

* show version

1. Check all commands placed onto switch

* + show run
    - make sure that service password encryption is set
    - make sure hostname is set
    - make sure that enable secret is set
    - make sure domain name is set
    - make sure username is set
    - make sure passwords are encrypted (ex. password 7 1P312A910I)
    - make sure Portfast and BPDU and used on the correct interfaces (ex. on interface GigabitEthernet0/4 “spanning-tree portfast trunk” is set)
    - make sure Vlan interfaces have ips/subnets (ex. on interface Vlan4 “ip address 10.1.7.129 255.255.255.240”)
    - make sure that a default gateway is set (ex. ip default-gateway 10.1.7.142)
    - make sure “no ip http server” is set
    - make sure created access lists are on
    - make sure telnet is disabled and ssh is enabled (“login local” and “transport input ssh should be set” on line vty 0 15)

2. Check ip addresses (machines that you are directly connected to)

* show ip int OR show ip int brief
  + - make sure ip addresses are correct

3. Check all possible routes for network traffic

* + show ip route
    - make sure that a default route is set
    - make sure routes are not going to an unknown address

4. Check neighbor machines (machines that you are directly connected to)

* + show cdp neighbor
    - make sure no unknown neighbors are there

5. Check all access lists on switch

* show ip access-lists

6. Check Vlan status

* show vlan
  + make sure vlans are active
  + make sure vlan interface is correct
* show interface trunk
  + make sure trunks are active/inactive
  + make sure vlan interface for trunks are correct
* show spanning-tree root (displays information for the root bridge)
* make sure correct protocol is used for switch (ex. dot1q)
* make sure access ports and trunk ports are correctly allocated to interfaces

7. Check hosts

* sh hosts
  + make sure that the hosts designated have the correct ips and hostnames
* delete any hosts that should not be designated a hostname

9. Ping loopback

* should get replies

10. Ping devices within network

* should get replies

11. Ping devices outside of network

* \*replies depend

Configuring a switch

* Passwords
* service password-encryption (sets encryption to password)
* enable secret cisco (set password to cisco)
* Configure a hostname
* hostname <name>
* Set default gateway
* ip default-gateway <172.16.10.1>
* Set ip on switch
* interface vlan1
* ip address <172.16.10.2> <255.255.255.0>
* no shutdown (Turns interface on)
* Configure a hostname
* hostname <name>
* Configure domain name and ip for domain name server (DNS)
  + ip domain name <name> (sets domain name)
  + ip name-server <server ip> (sets ip for domain name)
* Configure to no ip domain look ups
* no ip domain-lookup
* Configure VLANs
* vlan3 (creates VLAN 3)
* name <Engineer> (assigns name to VLAN)
* interface <f0/0> (moves to interface)
* switchport mode access (changes port to access mode. \*Other modes such as trunk exist)
* switchport access <vlan 10> (assigns port to VLAN 10)
* Configure access ports
* interface <f0/0> (moves to interface)
* switchport access <vlan 3> (switches interface to access port for vlan 3)
* switchport mode <access> (force link to be a access link)
* Configure trunk ports
* interface <f0/0> (moves to interface)
* switchport trunk encapsulation <dot1q> (put trunk port into appropriate mode; in this case dot1q)
* switchport mode <trunk> (force link to be a trunk link)
* Set SSH and turn off telnet
* username <Roland> password <tower> (creates username/password for SSH connection)
* ip domain-name (creates a host domain name for the router)
* crypto key generate rsa (enable ssh server for local and remote authentication on router and generates RSA key pair)
* ip ssh version 2 (enables ssh version 2 on device)
* line vty 0 15 (move to vty config mode)
* login local ( enable password checking)
* transport input ssh (limits remote connectivity to ssh)
* Turn off ip http server
  + no ip http server

## **Linux Firewall**

Troubleshooting:

1. Check UFW status, enable if necessary (https://help.ubuntu.com/community/UFW)

* + ufw status
  + ufw enable

2. Get UFW Info

* + grep 'DEFAULT\_' /etc/default/ufw
  + ufw app list
  + ufw app info <profile>
  + ufw app default ALLOW
  + ufw app update
  + ufw app update --add-new <profile>

3. Ensure logging is enabled

* + sudo ufw logging on

4. If a singular service doesn’t work

* + ufw allow|deny service|port

OR

* + ufw allow|deny [proto <protocol>] [from <address> [port <port>]] [to <address> [port <port>]]

5. Manage incoming and outcoming traffic

* + sudo ufw deny from 15.15.15.51
  + sudo ufw deny in on eth0 from 15.15.15.51

6. Confirm mirroring on ports  
 More research needed

Common Services:

SSH - 22

HTTP - 80

HTTPS - 443

MySQL - 3306

PostgreSQL - 5432

SMTP - 25, 587 outbound

IMAP - 143

IMAPS - 993

POP3 - 110

POP3S - 995

Useful file paths:

/etc/default/ufw: high level configuration, such as default policies, IPv6 support and kernel modules to use

/etc/ufw/before[6].rules: rules in these files are evaluated before any rules added via the ufw command

/etc/ufw/after[6].rules: rules in these files are evaluated after any rules added via the ufw command

/etc/ufw/sysctl.conf: kernel network tunables

/var/lib/ufw/user[6].rules or /lib/ufw/user[6].rules (0.28 and later): rules added via the ufw command (should not normally be edited by hand)

/etc/ufw/ufw.conf: sets whether or not ufw is enabled on boot, and in 9.04 (ufw 0.27) and later, sets the LOGLEVEL

/etc/ufw/after.init: initialization customization script run after ufw is initialized (ufw 0.34 and later)

/etc/ufw/before.init: initialization customization script run before ufw is initialized (ufw 0.34 and later)

/var/log/ufw.log: default location of log files

Other Commands:

ufw [--dry-run] [options] [rule syntax]

ufw reload (update changes)

ufw reset (reset to defaults)

iptables

1. Check current settings/tables

* sudo iptables -S
* sudo iptables -L

2. Ensure Persistence

* sudo apt-get install iptables-persistent

## **Windows Server 2008/2012/2016 GUI Firewall Checklist**

1. Initial diagnosis

* Open Notification tab in top right corner
  + Read any highlighted alerts
* Find applicable section

2. Confirm Firewall is enabled.

* Change Firewall state to “On”
  + Find the switch labeled “Turn on Windows Firewall”
  + Move switch to “On”

3. Specifically, what is wrong?

* Click red highlighted alerts
* Open the “Detail View” dialog box
* Read description of error

4. For which roles or servers is the problem occurring?

* Click the “Go To” button (opens the role or group home page)
* Write down the names of the roles or groups listed

5. Are there notifications about failed tasks or processes, and Task Details messages?

* Look at the Notifications area (top right corner)
  + If there is a red exclamation mark, there is an alert
  + If there is no exclamation mark, there is no alert
    - Click any alerts to open the “Task Details” dialog box (often identifies the source of the problem)
* Look at the Manager tab(top, top right of screen)
  + If there is a red exclamation mark, there is an alert
  + If there is no exclamation mark, there is no alert

7. Explore Manager

* Click on the Manager tab
* Ensure “All Servers” option is selected
* Right click on error process messages
  + Read for description

8. Respond to Errors

* Authentication errors require Active Directory or permissions updates/checks
  + Confirm devices listed with errors are added in the right groups with the right permissions (Communicate with Active Directory Team to complete this task)
* Name resolution errors come from conflicts in naming (special characters) or location (correct domain/ domain controller)
  + Confirm no inappropriate special characters are used (“,/\{}()[])
  + Confirm device correctly managed in Active Directory (Communicate with Active Directory Team to complete this task)

9. General Connection Issues

* Confirm you are trying to connect to a Windows machine
  + Open device
  + Observe Operating System
* Confirm the target is on
  + Turn it on if it is off
* Confirm the target is physically connected
  + View physical ports for wired connection
    - Push cables into ports completely
* Confirm the target has proper baseline configurations (i.e. proper static IPs for servers, in correct domain for users, etc.)
  + ipconfig /all
  + Compare given information with expected information
  + As necessary, change IP addresses, domains, groups, etc.
* Confirm you are using the correct username/password to log in
  + Refer to credential source document
  + Type username/password carefully

10. Firewall Blockage/Conneciton refused

* Ensure Windows Management Framework 3.0 is used
  + Open Powershell
  + Run (host).Version
* Check blocked ports for conflict
  + View existing firewall rules
  + Confirm rules are in proper order
* Check logs
  + Listed on homepage under name of each server

11. What is the update status of the server?

* If necessary, check for updates.
  + Control Panel>System and Security>Windows Update>Check for Update
* If problem persists, repeat at step 1

12. Dear God, what is going on?

* <https://social.technet.microsoft.com/wiki/contents/articles/13443.windows-server-2012-server-manager-troubleshooting-guide-part-i-overview.aspx>
* <https://docs.microsoft.com/en-us/windows-server/networking/sdn/troubleshoot/troubleshoot-windows-server-software-defined-networking-stack>

## 

## **Windows XP/Vista/7/8/10 Firewall Checklis**t

Windows User Firewalls is user-friendly and very GUI-dependent

Group policies can be leveraged to mandate certain firewall rules.

1. Check status

* Ensure Windows Firewall is turned on
  + Click on Windows button
  + Type “firewall”
  + Click first result
  + If all bars are red
    - Not “recommended settings”
    - Might all be “Off”
    - Expand all bars and make sure none are listed as “Windows Firewall state: Off”
    - As necessary to not conflict with services or the Group Policy, look at panel on left
      * Click “Turn Windows Firewall on or off”
      * Select proper status of firewall
  + If some bars are red
    - Most likely
    - Not “recommended settings”
    - Expand all bars and make sure none are listed as “Windows Firewall state: Off”
    - As necessary to not conflict with services or the Group Policy, look at panel on left
      * Click “Turn Windows Firewall on or off”
      * Select proper status of firewall
  + If all bars are green
    - Windows Firewall ‘works’

2. Update Microsoft Firewall

* Click “Troubleshoot my network”
  + Install any updates

3. Check Individual Rules

* Click “Advanced settings”
  + If group policy, ensure group policy enabled
  + If not
    - Click “Inbound Rules”

Observe current rules, compare to connection issues

* + - * + Click on rules to edit existing rules
        + Click “Add Rule” to add new rules

Select rule type from list

Choose program(s), protocol(s), port(s), and/or address(es) affected

Choose action to take

Choose when to apply rule

Name the rule

Give appropriate description

* + - Click “Outbound Rules”

Observe current rules, compare to connection issues

* + - * + Click on rules to edit existing rules
        + Click “Add Rule” to add new rules
  + Click on “Monitoring”
    - Click on services you would like monitored
    - Take note of file path of log

# **Services**

## Squid Proxy Server Checklist (Linux)

1. -Go into the configuration file with sudo gedit /etc/squid/squid.conf &

-Find the #acl localnet src line that corresponds to your network/IP address and ensure that it is uncommented

-For example, if my network is 192.168.1.0/255.255.255.0, uncomment #acl localnet src 192.168.1.0/24

1. Modify configuration file

-Reduce Squid’s configuration file to a more readable/useful one that takes out empty lines and documentation

mv /etc/squid/squid.conf /etc/squid/squid.conf.bkp

grep –Eiv ‘(^#|^$)’ /etc/squid/squid.conf.bkp > /etc/squid/squid.conf

-This creates a .bkp file that is the original file, and squid.conf now only contains the useful lines.

1. Restart Squid

sudo service squid restart

-Every time the configuration file is changed, restart Squid.

1. Check the version of Squid

-In the terminal, execute

/usr/sbin/squid –v

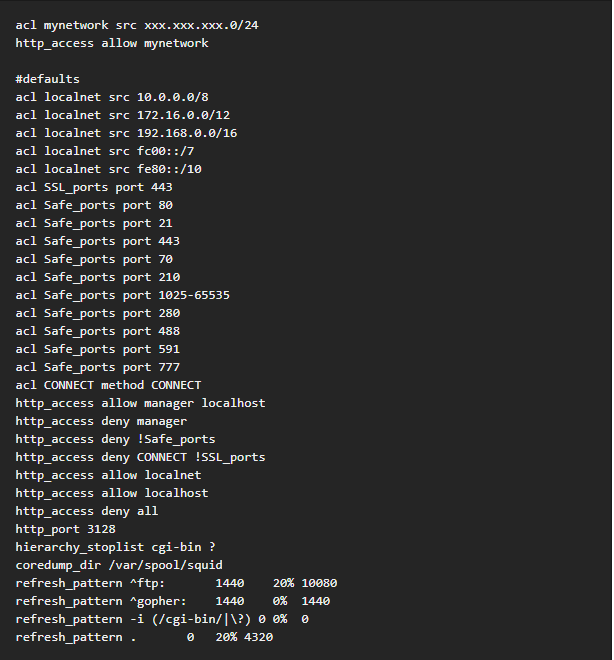
-You should see anything from version 2.6 to the most current version, 3.5. These versions are pretty stable and do not have serious vulnerabilities. Earlier versions like 2.5, however, do have some issues. These are not vulnerabilities so much as problems with the program itself that may result in the proxy doing something you didn’t think you configured it to do. For instance, it “does not trigger a fatal error when it identifies missing or invalid ACLs in the http\_access configuration, which could lead to less restrictive ACLs than intended by the administrator.” The worst issue is that “when processing the configuration file, Squid 2.5 parses empty Access Control Lists (ACLs), including proxy\_auth ACLs without defined auth schemes, in a way that effectively removes arguments, which could allow remote attackers to bypass intended ACLs if the administrator ignores the parser warnings.” These problems are good to look for, but even if you have Squid 2.5 or below, following the steps below will still result in a good configuration setup.

1. Check configuration file

-Go back into the config file

sudo gedit /etc/squid/squid.conf &

-If you have version 3.5, the most current version, you should see something like this:



-These are the default settings for Squid. Earlier versions of squid have similar default files, except sometimes the order changes for the commands. Either way, this should generally be what it looks like. Check to see if there are any significant changes that look out of place. One example from a previous competition is that there were a few ACLs in the Squid configuration file that were blocking a few websites from being accessed. Simply remove those lines to get back to the default stage.

1. To use Squid with Firefox, complete the following commands in the Firefox browser:

-Edit

-Preferences

-Advanced

-Network

-Settings

-Check Manual proxy configuration

-Next to HTTP Proxy, enter your IP address, and enter Port 3128.

-OK

-Close

1. Basic Configurations
   1. To see what squid is doing on the network, you can look at /var/log/squid/access.log or /var/log/squid/cache.log
   2. Configure an ACL to block certain IPs

-Make a new file called bad\_hosts.txt and put it in /etc/squid (cd /etc/squid, then cat > bad\_hosts.txt)

-Add to that new file a list of IPs to block

-Edit squid.conf (sudo gedit /etc/squid/squid.conf &) and add the following lines:

acl bad\_hosts src “/etc/squid/bad\_hosts.txt”

http access deny bad\_hosts

1. Add Squid to the firewall

firewall-cmd –add-port=3128/tcp –permanent

-This will only work if the firewall is already enabled.

1. Restrict access by user authentication

-Go back into squid.conf with sudo gedit /etc/squid/squid.conf &

-Add the following lines:

auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/passwd

auth\_param basic credentialsttl 30 minutes

auth\_param basic casesensitive on

auth\_param basic realm Squid proxy-caching web server for Tecmint’s LFCE series

acl ncsa proxy\_auth REQUIRED

http\_access allow ncsa

-Then back in the console, type in the following command to add credentials for a given user (in this case Username) that will be accepted by Squid:

htpasswd –c /etc/squid/passwd Username

-You will be prompted to create a password.

-Now, anytime you need to use a web browser, you will need to enter the username and password you specified to gain access.

AnalogX Proxy Server Checklist (Windows)—Use if you see a green P in the taskbar

For windows in general, proxy servers are largely handled at the firewall level. Likely the best approach is to do a cursory check of the proxy setup and then consult the firewall checklist for further configurations.

1. HTTP’s proxy server is at port 6588.
2. How to test if the proxy server’s connection is working/configure your browser to use the proxy:
   1. Hit the windows button, and search “Internet Options”
   2. Click on “Internet Options”
   3. Click on the Connections tab
   4. Click on LAN settings
   5. Under Proxy server, check the box that says “Use a proxy server for your LAN”
   6. In the address box, type in the IP address of that computer
   7. In the Port box type: 6588
   8. Click Ok, then Ok
   9. Open a web browser and you should be able to access the internet

Other port numbers for services that AnalogX can support:

|  |  |
| --- | --- |
| HTTP/HTTPS | 6588 |
| SOCKS4 (TCP proxying) | 1080 |
| SOCKS4a (TCP proxying w/ DNS lookups) | 1080 |
| SOCKS5 (only partial support, no UDP) | 1080 |
| NNTP (usenet newsgroups) | 119 |
| POP3 (receiving email) | 110 |
| SMTP (sending email) | 25 |
| FTP (file transfers) | 21 |

1. Configuring the proxy:
   1. Make sure the proxy is on by searching for “AnalogX” and clicking on Proxy
   2. There should be a green P in the taskbar (up arrow in the bottom right-hand corner)
   3. All configurations are completed through the “Configure” menu
   4. When in this menu the proxy is disabled (you'll notice the tray icon will be red), and when done, it will automatically start back up.
   5. Security Configurations:
      1. By default the proxy binds to all TCP/IP interfaces on your computer - this is primarily to make it easy to get running, but it also means that it will service requests from the Internet as well. You can force Proxy to only bind to your local IP address in the Configuration menu, at the 'Proxy Bind' option. If this is set to 'disabled', then it will bind to all interfaces, but if a valid TCP/IP address is entered, the proxy will ONLY bind to that - so if you enter 10.0.0.1, and that's your server's IP address, then the proxy will only talk to machines that connect to that IP, in other words, only your local network.

Squid Proxy Server Checklist (Windows)—Use if you see a blue squid in the taskbar

-Again, check the firewall with the firewall checklist.

-Search for “Windows Firewall with Advanced Security” and open up the Rules (both Inbound and Outbound).

-Check for a rule with a Name with the word “Squid” in it. This is where you will see ACLs associated with the Squid proxy. Examine this rule to check for discrepancies similar to the ones described in the Linux section for Squid.

-Besides that, configuration is the same as for AnalogX, so look at that checklist for advice on how to use that for internet browsing.

## 

## **Securing LDAP**

* Identify server
  1. nslookup -type=srv \_ldap.\_tcp.DOMAINNAME (DOMAINNAME is your domain name)
* List OUs in ldap (linux)

$name = "username";

$pass = "password";

$adServer = "127.0.0.1";

$ldapconn = ldap\_connect($adServer) or die("Could not connect to LDAP server.");

ldap\_set\_option($ad, LDAP\_OPT\_PROTOCOL\_VERSION, 3) or die ("Could not set ldap protocol");

ldap\_set\_option($ad, LDAP\_OPT\_REFERRALS, 0) or die ("Could not set option referrals");

$account = $name;

$password = $pass;

$ldaprdn = $account."@foobar.com";

$ldappass = $password;

if ($ldapconn) {

$ldapbind = ldap\_bind($ldapconn, $ldaprdn, $ldappass) or die("Couldn't bind to AD!");

}

$dn = "ou=Agencies,dc=foobar,dc=com";

$filter="(objectClass=organizationalunit)";

$justthese = array("dn", "ou");

$sr=ldap\_search($ldapconn, $dn, $filter, $justthese);

$info = ldap\_get\_entries($ldapconn, $sr);

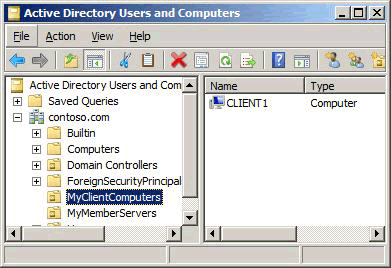
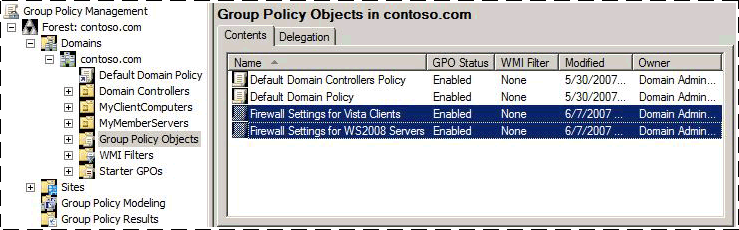
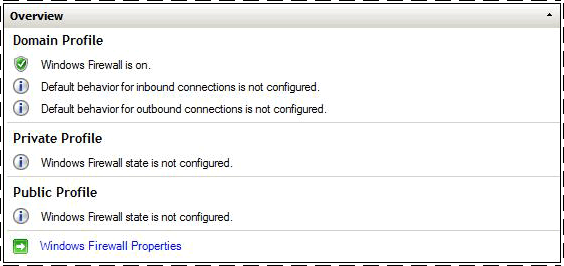
for ($i=0; $i < $info["count"]; $i++) {

echo $info[$i]["dn"]."<br>";

}

ldap\_free\_result($sr);

ldap\_unbind($ldapconn);

* List OUs (windows)
  1. Get-ADOrganizationalUnit -Filter <string> [-ResultPageSize <int>] [-ResultSetSize <System.Nullable[System.Int32]>] [-SearchBase <string>] [-SearchScope {<Base> | <OneLevel> | <Subtree>}] [-AuthType {<Negotiate> | <Basic>}] [-Credential <PSCredential>] [-Partition <string>] [-Properties <string[]>] [-Server <string>] [<CommonParameters>]
* Change root passwords
  1. Slappasswd
  2. New password: [enter new password]
  3. Re-enter new password: [re enter new password]
  4. Password will print, highlight and copy
  5. Vim chrotpw.ldif [new password in “olcRootPW” section]
  6. dn: olcDatabase={0}config,cn=config
  7. Changetype: modify
  8. Add: olcRootPW
  9. olcRootPW: [paste new password you copied]
  10. Ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.lfdif
* Change directory manager password
  1. Same as a-d in previous section
  2. Vim chdomain.lfdif
  3. Dn: olcDatabase={1}monitor,cn=config
  4. Changetype: modify
  5. Replace: olcAccess
  6. olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=srv,dc=world" read by \* none
  7. dn: olcDatabase={2}bdb,cn=config
  8. changetype: modify
  9. replace: olcSuffix
  10. olcSuffix: dc=srv,dc=world
  11. dn: olcDatabase={2}bdb,cn=config
  12. changetype: modify
  13. replace: olcRootDN
  14. olcRootDN: cn=Manager,dc=srv,dc=world
  15. dn: olcDatabase={2}bdb,cn=config
  16. changetype: modify
  17. add: olcRootPW
  18. olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx
  19. dn: olcDatabase={2}bdb,cn=config
  20. changetype: modify
  21. add: olcAccess
  22. olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=Manager,dc=srv,dc=world" write by anonymous auth by self write by \* none
  23. olcAccess: {1}to dn.base="" by \* read olcAccess: {2}to \* by dn="cn=Manager,dc=srv,dc=world" write by \* read
  24. Ldapmodofy -Y EXTERNAL -H ldapi:/// -f chdomain.ldif
* Configure LDAP to use SSL (Windows)
  1. \*LDAP sends unsecured traffic and TLS over port 389 and SSL over 636
  2. \*need to install certificate and store it on the Local computer personal certificate directory (specify your own for linux, MY certificate store for windows)
     + Certificate must contain Server Authentication OID 1.3.6.1.5.5.7.3.1
  3. Open MMC
  4. File > Add/Remove Snap-In
  5. Select Certificates, click Add
  6. In Certs snap in, select Computer Account, click Next
  7. In select computer, select Local, click Ok, then Finish
  8. Click Ok in Add or Remove Snap-Ins
  9. In console tree, expand certificates, right click Certificates, select All Tasks [if unsuccessful, you are connected to a remote DC]
  10. In Certificate Enrollment, click Next
  11. In the Select Certificate Enrollment Policy, choose Active Directory Enrollment Policy (default) and click Next.
  12. Select a certificate that allows for server authentication. You may want to use a custom certificate as described in Publishing a Certificate that Supports Server Authentication. Now go ahead and click Enroll
  13. The process may take a few seconds to complete. Click Finish in the Certificate Enrollment dialog box
  14. Click the Details tab. In the Field column, go ahead and select Enhanced Key Usage. You’ll want to confirm that the Server Authentication (1.3.6.1.5.5.7.3.1) is listed
  15. \*To test if LDAP over TLS works properly, use the ldp.exe tool.
  16. Open a command prompt and type ldp. Click Enter. The LDP application window appears.
  17. Select Connection, then Connect. The Connect dialog box appears.
  18. In the Server text box, type the name of your AD server. For this example, type the fully qualified domain name (FQDN) of the DC, just as it appears in the Subject Alternative Name (SAN) of the Digital Certificate.
  19. In the Port text box, type 636.
  20. Check the box for SSL.
  21. Click OK. Now, without the above procedure you will not be able to connect.
  22. Select the Connection menu, click Bind, and then click OK.
      + The command output should display the username and domain name that you used for binding, if LDAPS is configured properly. You can start browsing through the AD tree.
* Configure SSL connections (Linux)
  1. Sudo apt-get install openssh-server
  2. sudo mkdir -v /etc/ldap/ssl
  3. pushd /etc/ldap/ssl
  4. sudo openssl req -newkey rsa:1024 -x509 -nodes -out slapd.pem -keyout slapd.pem -days 3650
     + # Make this readable to openldap only ..
  5. sudo chown -v openldap:openldap /etc/ldap/ssl/slapd.pem
  6. sudo chmod -v 400 /etc/ldap/ssl/slapd.pem
  7. Popd
* Set server LDAP signing requirement
  1. Click Start, click Run, type mmc.exe, and then click OK.
  2. On the File menu, click Add/Remove Snap-in.
  3. In the Add or Remove Snap-ins dialog box, click Group Policy Management Editor, and then click Add.
  4. In the Select Group Policy Object dialog box, click Browse.
  5. In the Browse for a Group Policy Object dialog box, click Default Domain Policy under the Domains, OUs and linked Group Policy Objects area, and then click OK.
  6. Click Finish.
  7. Click OK.
  8. Expand Default Domain Controller Policy, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
  9. Right-click Domain controller: LDAP server signing requirements, and then click Properties.
  10. In the Domain controller: LDAP server signing requirements Properties dialog box, enable Define this policy setting, click to select Require signing in the Define this policy setting drop-down list, and then click OK.
  11. In the Confirm Setting Change dialog box, click Yes.
* Set Client LDAP signing requirement through local computer policy (windows)
  1. Click Start, click Run, type mmc.exe, and then click OK.
  2. On the File menu, click Add/Remove Snap-in.
  3. In the Add or Remove Snap-ins dialog box, click Group Policy Object Editor, and then click Add.
  4. Click Finish.
  5. Click OK.
  6. Expand Local Computer Policy, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
  7. Right-click Network security: LDAP client signing requirements, and then click Properties.
  8. In the Network security: LDAP client signing requirements Properties dialog box, click to select Require signing in the drop-down list, and then click OK.
  9. In the Confirm Setting Change dialog box, click Yes.
* Set the client LDAP signing requirement through a domain group policy object (windows)
  1. Click Start, click Run, type mmc.exe, and then click OK.
  2. On the File menu, click Add/Remove Snap-in.
  3. In the Add or Remove Snap-ins dialog box, click Group Policy Object Editor, and then click Add.
  4. Click Browse, and then select Default Domain Policy (or the Group Policy Object for which you want to enable client LDAP signing).
  5. Click OK.
  6. Click Finish.
  7. Click Close.
  8. Click OK.
  9. Expand Default Domain Policy, expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
  10. In the Network security: LDAP client signing requirements Properties dialog box, click to select Require signing in the drop-down list, and then click OK.
  11. In the Confirm Setting Change dialog box, click Yes.
* Create OUs and put computer accounts into them (windows servers up to 2008)
  1. On DC1, click Start, click Administrative Tools, and then click Active Directory Users and Computers. Alternatively, you can use Server Manager. Expand Roles, expand Active Directory Domain Services, and then expand Active Directory Users and Computers [DC1.contoso.com].
  2. n the navigation pane, right-click contoso.com, click New, and then click Organizational Unit.
  3. In the Name box, type MyMemberServers, and then click OK.
  4. Right-click contoso.com again, and then click New, and then click Organizational Unit.
  5. In the Name box, type MyClientComputers, and then click OK.
  6. In the navigation pane, click Computers.
  7. In the results pane, right-click CLIENT1, and then click Move.
  8. In the Move dialog box, click MyClientComputers, and then click OK.
  9. In the results pane, right-click MBRSVR1, and then click Move.
  10. In the Move dialog box, click MyMemberServers, and then click OK.
  11. When you have finished, your display resembles the following figure.
  12. 
  13. Close the Active Directory Users and Computers snap-in.
* Create new Group Policy Object (windows)
  1. On MBRSVR1, click Start, click Administrative Tools, and then click Group Policy Management.
  2. Alternatively, if you use Server Manager, expand Features, and then expand Group Policy Management.
  3. In the navigation pane, expand Forest: contoso.com, expand Domains, and then expand contoso.com.
  4. In the navigation pane, right-click Group Policy Objects, and then click New.
  5. In the Name box, type Firewall Settings for Windows Servers, and then click OK.
  6. In the navigation pane, right-click Group Policy Objects, and then click New.
  7. In the Name box, type Firewall Settings for Windows Clients, and then click OK.
  8. Select the Group Policy Objects node, and your display resembles the following figure.
  9. 
* Add GPO setting to enable firewall on member client computers
  1. On MBRSVR1, in Group Policy Management, click Group Policy Objects, right-click Firewall Settings for Windows Clients, and then click Edit.
  2. In Group Policy Management Editor, right-click the top node Firewall Settings for Windows Clients [DC1.contoso.com] Policy, and then click Properties.
  3. Select the Disable User Configuration settings check box.
  4. In the Confirm Disable dialog box, click Yes, and then click OK.
  5. Under Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand Windows Firewall with Advanced Security.
  6. Click the node Windows Firewall with Advanced Security - LDAP://cn={*GUID*},cn=policies,cn=system,DC=contoso,DC=com, where *GUID* is a unique number assigned to your domain.
  7. In the results pane, under Overview, notice that for each network location profile Windows Firewall state is not configured, and then click Windows Firewall Properties.
  8. On the Domain Profile tab, click the drop-down list next to Firewall state, and then click On (recommended).
  9. Click OK to save your changes. Note in the results pane that Domain Profile now shows Windows Firewall is on.
  10. 
  11. Close Group Policy Management Editor.
* Deploy initial GPO with test firewall settings
  1. On MBRSVR1, in Group Policy Management, in the navigation pane, right-click MyClientComputers, and then click Link an Existing GPO.
  2. In the Group Policy objects list, click Firewall Settings for Windows Clients, and then click OK.
* Confirm receipt and application of GPO policies
  1. On CLIENT1, open an administrator command prompt.
  2. At the command prompt window, type gpupdate /force, and then press ENTER. Wait until the command finishes before moving to the next step.
  3. To validate that the GPO was correctly applied, run gpresult /r /scope computer. In the output, look for the section Applied Group Policy Objects. Confirm that it contains entries for both Firewall Settings for Windows Clients and the Default Domain Policy.
  4. Open the Windows Firewall with Advanced Security snap-in.
  5. Right-click the top node Windows Firewall with Advanced Security on Local Computer, and then click Properties.
  6. Note that the Firewall State setting is On (recommended), and that the list control is disabled. It is now controlled by Group Policy and cannot be changed locally, even by an administrator.
  7. Close the Properties dialog box, and the Windows Firewall with Advanced Security snap-in
* Prevent computer from using rules and settings defined by local admin
  1. On MBRSVR1, in Group Policy Management, click Group Policy Objects, right-click Firewall Settings for Windows Clients, and then click Edit.
  2. In Group Policy Management Editor, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand Windows Firewall with Advanced Security.
  3. Right-click Windows Firewall with Advanced Security - LDAP://cn={*GUID*},cn=policies,cn=system,DC=contoso,DC=com, and then click Properties.
  4. On the Domain Profile tab, in the Settings section, click Customize.
  5. Change the Display a notification setting to No. This prevents Windows from displaying a notification to the user whenever a program is blocked.
  6. In the Rule merging section, change the Apply local firewall rules list to No.
  7. In the Rule merging section, change the Apply local connection security rules list to No.
  8. Click OK two times to return to Group Policy Management Editor.
* Test new restrictions
  1. On CLIENT1, in Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes.
  2. In the Windows Firewall with Advanced Security snap-in, in the list of Outbound Rules, right-click A Test Rule, and then click Enable Rule.
  3. In Administrator: Command Prompt, run ping dc1.
  4. The ping command works even though A Test Rule appears to be enabled. The rule is listed as enabled on the local computer, but when you set the Apply local firewall rules to No on the GPO in the previous procedure, you blocked the merging of local rules with the rules delivered in the GPO.
  5. In the navigation pane of the Windows Firewall with Advanced Security snap-in, expand Monitoring, and then click Firewall to see the list of rules active on the local computer.
  6. No rules are listed. You have not yet created any rules applied by GPO, and no local rules are active because of the settings that you included in the GPO.
  7. Before proceeding, delete your rule. On CLIENT1, in the navigation pane, click Outbound Rules. In the results pane, right-click A Test Rule, click Delete, and then click Yes on the confirmation dialog box.
  8. Leave both Administrator: Command Prompt and the Windows Firewall with Advanced Security snap-in open.

## **SMTP Server:**

1. Harden POSTFIX with /etc/postfix/main.cf:
   1. # line 75: uncomment and specify hostname

myhostname = mail.srv.world

# line 83: uncomment and specify domain name

mydomain = srv.world

# line 99: uncomment

myorigin = $mydomain

# line 116: change

inet\_interfaces = all

# line 164: add

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

# line 264: uncomment and specify your local network

mynetworks = 127.0.0.0/8, 10.0.0.0/24

# line 419: uncomment (use Maildir)

home\_mailbox = Maildir/

# line 574: add

smtpd\_banner = $myhostname ESMTP

# add follows to the end

# limit an email size for 10M

message\_size\_limit = 10485760

# limit a mailbox for 1G

mailbox\_size\_limit = 1073741824

# for SMTP-Auth

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

smtpd\_sasl\_security\_options = noanonymous

smtpd\_sasl\_local\_domain = $myhostname

smtpd\_recipient\_restrictions = permit\_mynetworks,permit\_auth\_destination,permit\_sasl\_authenticated,reject

1. Ensure firewall allows smtp:
   1. Firewall-cmd --add-service=smtp --permanent
   2. Firewall-cmd --add-service=smtps --permanent
   3. Firewall-smd --reload

Harden Dovecot with:

1. Vim /etc/dovecot/dovecot.conf

# line 24: uncomment

protocols = imaps pop3s lmtp

# line 30: uncomment and change ( if not use IPv6 )

listen = \*

1. Vim /etc/dovecot/conf.d/10-auth.conf

# line 10: uncomment and change ( allow plain text auth )

disable\_plaintext\_auth = no

# line 100: add

auth\_mechanisms = plain login

1. Vim /etc/dovecot/conf.d/10-mail.conf

# line 30: uncomment and add

mail\_location = maildir:~/Maildir

1. Vim /etc/dovecot/conf.d/10-master.conf

# line 96-98: uncomment and add like follows

# Postfix smtp-auth

unix\_listener /var/spool/postfix/private/auth {

mode = 0666

user = postfix

group = postfix

}

1. Vim /etc/dovecot/conf.d/10-ssl.conf

# line 8: change

ssl = yes

# line 14,15: specify certificates, ensure they are in correct directory

ssl\_cert = </etc/pki/tls/certs/server.crt

ssl\_key = </etc/pki/tls/certs/server.key

1. Firewall:
   1. Firewall-cmd --add-service=imaps --permanent
   2. Firewall-cmd --add-service=pop3s --permanent
   3. Firewall-cmd --reload

Mail log report:

1. Yum install postfix-perl-scripts
2. Perl /usr/sbin/pflogsumm -d yesterday /var/log/maillog
   1. Generates log summary for yesterday
3. Yum --enablerepo+epel install awstats
4. Vim /etc/awstats/awstats.(hostname).conf

###awstats automatically creates the .conf file

# line 50: change

LogFile="/usr/share/awstats/tools/maillogconvert.pl standard < /var/log/maillog |"

# line 62: change

LogType=M

# line 122: comment out and add like follows

#LogFormat=1

LogFormat="%time2 %email %email\_r %host %host\_r %method %url %code %bytesd"

# line 848: change like follows

LevelForBrowsersDetection=0

LevelForOSDetection=0

LevelForRefererAnalyze=0

LevelForRobotsDetection=0

LevelForSearchEnginesDetection=0

LevelForKeywordsDetection=0

LevelForFileTypesDetection=0

LevelForWormsDetection=0

# line 966: change like follows

ShowMonthStats=UHB

ShowDaysOfMonthStats=HB

ShowDaysOfWeekStats=HB

ShowHoursStats=HB

ShowDomainsStats=0

ShowHostsStats=HBL

ShowRobotsStats=0

ShowEMailSenders=HBML

ShowEMailReceivers=HBML

ShowSessionsStats=0

ShowPagesStats=0

ShowFileTypesStats=0

ShowOSStats=0

ShowBrowsersStats=0

ShowOriginStats=0

ShowKeyphrasesStats=0

ShowKeywordsStats=0

ShowMiscStats=0

ShowHTTPErrorsStats=0

ShowSMTPErrorsStats=1

1. Vim /etc/httpd/conf.d/awstats.conf

# line 30: add IP range you allow to access

Require ip 10.0.0.0/24

1. Access at “http://(hostname)/awstats/awstats.pl

## **DNS Server**

## 1) What Version the DNS Server it is and Run Status

### a) BIND (Linux) Version

$ /usr/sbin/named -v

### b) BIND Status

$ service named status

### c) Update BIND

patch -Np1 -i ../bind-9.11.2-use\_iproute2-1.patch

## 2) Change BIND configuration files (CentOS)

Now the named.conf file, which is the main file for BIND, must be configured for safer authorizations.. Open the file with any program you favor. For this example, I will be using vim.

vim /etc/named.conf

This is also where one can determine if the server is a slave or master. Normally you define one master server and all others are slave servers:

zone "example.com"{   
 type master;   
 file "example.com";   
 notify yes; // Add this line to enable Notifications }

The following will be what should be on the named.conf file should look like. Pay attention to the underlined and bolded text. This text will be comments for what the highlighted configuration should be and why:

options {

# change ( listen all )

listen-on port 53 { any; }; change ‘any’ to specific host (IP)

# change if not use IPv6

listen-on-v6 { none; }; if not explicitly stated or nothing there, assume it’s any

directory "/var/named";

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

memstatistics-file "/var/named/data/named\_mem\_stats.txt";

# query range ( set internal server and so on )

allow-query { localhost; 10.0.0.0/24; }; Only allow authorized IPs to query

# transfer range ( set it if you have secondary DNS )

For the DNS servers in your network that are exposed to the Internet, if zone transfer must be enabled, restrict DNS zone transfers to either DNS servers identified in the zone by name server (NS) resource records or to specific DNS servers in your network.

allow-transfer { localhost; 10.0.0.0/24; };

By default, recursion is not disabled for the DNS Server service. This makes it possible for the DNS server to perform recursive queries on behalf of its DNS clients and DNS servers that have forwarded DNS client queries to it. Recursion may be used by attackers to deny the DNS Server service. Therefore, if a DNS server in your network is not intended to receive recursive queries, it should be disabled.

recursion no;

dnssec-enable yes;

dnssec-validation yes;

dnssec-lookaside auto;

/\* Path to ISC DLV key \*/

bindkeys-file "/etc/named.iscdlv.key";

managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

# change all from here

view "internal" {

match-clients {

localhost;

10.0.0.0/24;

};

zone "." IN {

type hint;

file "named.ca"; };

zone "srv.world" IN {

type master;

file "srv.world.lan";

allow-update { none; }; ensure that zones are not allowed to be updated by other servers or zones

};

zone "0.0.10.in-addr.arpa" IN {

type master;

file "0.0.10.db";

allow-update { none; };ensure that zones are not allowed to be updated by other servers or zones

};

## 2) Restart Service

The service MUST be restarted after any changes have been made in order for the changes to apply:

systemctl restart named

## 3) CentOS DNS Troubleshooting

If the DNS server does not seem to be running, here is a checklist of some commands you can run to update/see what possible errors there may be:

1. sudo ntpdate time.nist.gov
   1. Sometimes DNS server times are out of whack, this command will update the time
2. sudo named-checkconf
   1. This allows one to see if there are any errors
3. service named status
   1. Shows if service is running, and brief overview if there is an error
4. dig [ip or address]
   1. Shows where the information came from
   2. Shows who the system was looking for
   3. Shows IP to name or reverse
5. If you have edited the files, but you get a failure or you are not able to resolve anything, remember your First, confirm configurations! Take a hard look at the documents you created and ensure you have the right “.” or space or ip address where they should be. Look for little misspellings. Errors messages can help you narrow the search. Try the following command right after your server fails to restart:  
     
   tail -f /var/log/syslog  
     
   This command should give you the last fews lines of errors in your syslog file, which should capture what went wrong and give you a hint as to what to fix. Often there will be a line number of the db file that has the issue! Second, if it is not clear what the issue is from tracing through the configs, it is time to confirm the network from layer 1 and up. Is layer 1 and layer 2 properly configured, i.e. are your interface cards correct and connected to the virtual infrastructure? Do you have layer 3 connectivity? Can you ping end-to-end? A layer 7 protocol, like DNS, cannot work if the lower layers are broken! Often, one link in the chain is broken, causing issues.

## 4) Secure Windows DNS Server Checklist

Windows DNS is more of a GUI. Below will be how to secure your DNS server and zones.

### a) Restrict DNS server to listen only on selected addresses

1. Open DNS Manager.
   1. To open DNS Manager, click Start, point to Administrative Tools, and then click DNS.
2. In the console tree, click the applicable DNS server. Where?
   1. DNS/*applicable DNS server*
3. On the Action menu, click Properties.
4. On the Interfaces tab, click Only the following IP addresses.
5. In IP address, type an IP address to be enabled for this DNS server , and then click Add.
6. Repeat the previous step as necessary to specify other server IP addresses to be enabled for this DNS server. To remove an IP address from the list, click it, and then click Remove.

### b) Secure the Server Cache Against Names Pollution

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server. Where?
   * DNS/*applicable DNS server*
3. On the Action menu, click Properties.
4. Click the Advanced tab.
5. In Server options, select the Secure cache against pollution check box, and then click OK.

### c) Disable Recursion

1. Open DNS Manager.
2. In the console tree, right-click the applicable DNS server, then click Properties. Where?
   1. DNS/*applicable DNS server*
3. Click the Advanced tab.
4. In Server options, select the Disable recursion check box, and then click OK.

### d) Disable Root Hints

This ensures that if you have an internal DNS root infrastructure, that root hints only point to the DNS root in the internal network not hosts in the internet root domain.

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server. Where?
   * DNS/*applicable DNS server*
3. On the Action menu, click Properties.
4. Click the Root Hints tab.
5. Modify server root hints as follows:
   * To add a root server to the list, click Add, and then specify the name and IP address of the server to be added to the list.
   * To modify a root server in the list, click Edit, and then specify the name and IP address of the server to be modified in the list.
   * To remove a root server from the list, select it in the list, and then click Remove.
   * To copy root hints from a DNS server, click Copy from server, and then specify the IP address of the DNS server from which you want to copy a list of root servers to use in resolving queries. These root hints will not overwrite any existing root hints.

## **SSH Checklist**

### Linux

## 1) Version and Update

### a) How to tell what version of ssh is running

sshd -V

### b) Below is multiple ways of updated SSH

* pkg-add -r openssh-portable
* cd /usr/ports/security/openssh && make install clean
* portupgrade security/openssh-portable

## 2) Install Service (CentOS)

If only telnet is installed, SSH needs to be utilized since it’s more secure.

yum -y install openssh-clients

## 2) Configure Server Passwords Settings (CentOS)

The following changes need to be made in the following file:

vim /etc/ssh/sshd\_config

SSH allows for users to login as root, so it should be disabled. If you need access you can use the sudo command. The following is what needs to be changed in this file:

# line 48: uncomment and change(prohibit root login remotely)  
PermitRootLogin no

Ensure that there needs to be user authentication:

# line 77: uncomment  
PermitEmptyPasswords no  
PasswordAuthentication yes

If necessary, limit which users can use SSH. In this example Alice and Bob are the users:

AllowUsers alice bob

Ensure that SSH2 is being used and not SSH1, since SSH2 is the newer protocol. Meaning it is more secure:

#Uncomment Protocol 2,1 and change it to:  
Protocol 2

IMPORTANT! Every time a change is made, you MUST restart the SSH service

systemctl restart sshd

## 3) Authenticate Keys (CentOS)

Having authorized key pairs will allow for more authentication throughout the network. The following is how to create and copy a key pair to the local SSH directory:

### Create Key Pair

ssh-keygen -t rsa

[mv](https://www.server-world.info/en/command/html/mv.html) ~/.ssh/id\_rsa.pub ~/.ssh/authorized\_keys

[chmod](https://www.server-world.info/en/command/html/chmod.html) 600 ~/.ssh/authorized\_keys

### Copy Secret Key to Local SSH Directory

[mkdir](https://www.server-world.info/en/command/html/mkdir.html) ~/.ssh

[chmod](https://www.server-world.info/en/command/html/chmod.html) 700 ~/.ssh

scp cent@10.0.0.30:/home/cent/.ssh/id\_rsa ~/.ssh/

ssh -i ~/.ssh/id\_rsa cent@10.0.0.30

### Restart Service

systemctl restart sshd

## 4) SCP

#### Copy the file "foobar.txt" from a remote host to the local host

$ scp your\_username@remotehost.edu:foobar.txt /some/local/directory

#### Copy the file "foobar.txt" from the local host to a remote host

$ scp foobar.txt your\_username@remotehost.edu:/some/remote/directory

#### Copy the directory "foo" from the local host to a remote host's directory "bar"

$ scp -r foo your\_username@remotehost.edu:/some/remote/directory/bar

#### Copy the file "foobar.txt" from remote host "rh1.edu" to remote host "rh2.edu"

#### Copying the files "foo.txt" and "bar.txt" from the local host to your home directory on the remote host

* $ scp your\_username@rh1.edu:/some/remote/directory/foobar.txt \
* your\_username@rh2.edu:/some/remote/directory/
* $ scp foo.txt bar.txt your\_username@remotehost.edu:~

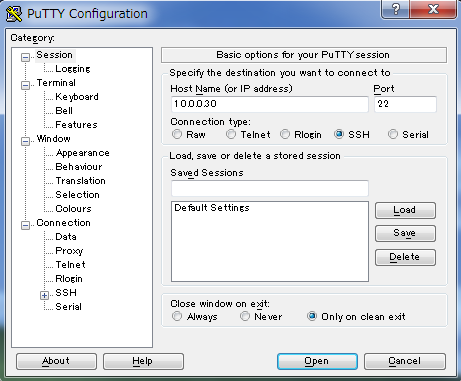
Copy the file "foobar.txt" from the local host to a remote host using port 2264

$ scp -P 2264 foobar.txt [your\_username@remotehost.edu](mailto:your_username@remotehost.edu):/some/remote/directory

### Windows

## 4) Configure SSH Client (Windows)

An SSH client is need for windows, so for this example I will be using Putty (need a safe link to download). Below is how the window should look like. Ensure to put the correct host name (IP), and then select open. A command prompt should open asking for a password.



## 5) SSH File Transfer (Windows)

If the system we have uses Windows, we can us WinSCP. However, [WinSCP](https://winscp.net/eng/download.php) needs to be installed in order to be used. Once installed, here are the steps:

1. Select New
2. Input the correct information and file that is wanted to be transfered
3. Move to the 'Directory' section on the left menu and input remote server's directory and local client directory you want to login. Next, click login button.
4. Insert Password
5. Once logged in, you can upload or download files in WinSCP

## **LDAP**

## [1] Install OpenLDAP Server. [root@dlp ~]# yum -y install openldap-servers openldap-clients [root@dlp ~]# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG [root@dlp ~]# chown ldap. /var/lib/ldap/DB\_CONFIG [root@dlp ~]# systemctl start slapd [root@dlp ~]# systemctl enable slapd

[2] Set OpenLDAP admin password.  
# generate encrypted password  
[root@dlp ~]# slappasswd   
New password:  
Re-enter new password:  
{SSHA}xxxxxxxxxxxxxxxxxxxxxxxx  
[root@dlp ~]# vi chrootpw.ldif  
# specify the password generated above for "olcRootPW" section  
 dn: olcDatabase={0}config,cn=config  
changetype: modify  
add: olcRootPW  
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx  
  
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif   
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0  
modifying entry "olcDatabase={0}config,cn=config"

[3] Import basic Schemas.  
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif   
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0  
adding new entry "cn=cosine,cn=schema,cn=config"  
  
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif   
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0  
adding new entry "cn=nis,cn=schema,cn=config"  
  
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif   
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0  
adding new entry "cn=inetorgperson,cn=schema,cn=config"

[4] Set your domain name on LDAP DB.  
# generate directory manager's password  
[root@dlp ~]# slappasswd   
New password:  
Re-enter new password:  
{SSHA}xxxxxxxxxxxxxxxxxxxxxxxx  
[root@dlp ~]# vi chdomain.ldif  
# replace to your own domain name for "dc=\*\*\*,dc=\*\*\*" section  
# specify the password generated above for "olcRootPW" section  
 dn: olcDatabase={1}monitor,cn=config  
changetype: modify  
replace: olcAccess  
olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"  
 read by dn.base="cn=Manager,dc=srv,dc=world" read by \* none  
  
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
replace: olcSuffix  
olcSuffix: dc=srv,dc=world  
  
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
replace: olcRootDN  
olcRootDN: cn=Manager,dc=srv,dc=world  
  
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
add: olcRootPW  
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx  
  
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
add: olcAccess  
olcAccess: {0}to attrs=userPassword,shadowLastChange by  
 dn="cn=Manager,dc=srv,dc=world" write by anonymous auth by self write by \* none  
olcAccess: {1}to dn.base="" by \* read  
olcAccess: {2}to \* by dn="cn=Manager,dc=srv,dc=world" write by \* read  
  
[root@dlp ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif   
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0  
modifying entry "olcDatabase={1}monitor,cn=config"  
  
modifying entry "olcDatabase={2}hdb,cn=config"  
  
modifying entry "olcDatabase={2}hdb,cn=config"  
  
modifying entry "olcDatabase={2}hdb,cn=config"  
  
[root@dlp ~]# vi basedomain.ldif  
# replace to your own domain name for "dc=\*\*\*,dc=\*\*\*" section  
 dn: dc=srv,dc=world  
objectClass: top  
objectClass: dcObject  
objectclass: organization  
o: Server World  
dc: Srv  
  
dn: cn=Manager,dc=srv,dc=world  
objectClass: organizationalRole  
cn: Manager  
description: Directory Manager  
  
dn: ou=People,dc=srv,dc=world  
objectClass: organizationalUnit  
ou: People  
  
dn: ou=Group,dc=srv,dc=world  
objectClass: organizationalUnit  
ou: Group  
  
[root@dlp ~]# ldapadd -x -D cn=Manager,dc=srv,dc=world -W -f basedomain.ldif   
Enter LDAP Password: # directory manager's password  
adding new entry "dc=srv,dc=world"  
  
adding new entry "cn=Manager,dc=srv,dc=world"  
  
adding new entry "ou=People,dc=srv,dc=world"  
  
adding new entry "ou=Group,dc=srv,dc=world"

[5] If Firewalld is running, allow LDAP service. LDAP uses 389/TCP.  
[root@dlp ~]# firewall-cmd --add-service=ldap --permanent   
success  
[root@dlp ~]# firewall-cmd --reload   
Success

Source: https://www.server-world.info/en/note?os=CentOS\_7&p=openldap

## **Web Server:**

1. What OS model are we using?
   1. Cat /etc/issue OR cat /etc/version
      1. This will tell you if you are utilizing Ubuntu, or CentOS
2. Make appropriate updates to OS:
   1. Sudo yum update OR sudo apt-get update
3. What type of web server do you have?
   1. Cd /etc
      1. Locate apache2 OR httpd folders
   2. Service apache2|httpd status
      1. This will inform you if service is running
4. Make appropriate changes to .conf files (from now on i will utilize httpd)
   1. Cd /etc/httpd/httpd.conf
      1. Locate following:
         1. ServerAdmin
            1. Who will be notified if needed?

[name@ide.com](mailto:name@ide.com)

* + - 1. ServerName
         1. Change to your server name and port

[www.myserver.edu:80](http://www.myserver.edu:80)

* + - 1. DirectoryIndex
         1. File server can access only with directory name

Index.html

* + - 1. KeepAlive
         1. Turn on
      2. DocumentRoot
         1. Where are all your files located?

/var/www/

This can depend on how you develop virtual hosts

Verify .html documents in directory

* + - 1. AllowOverride
         1. Do not allow. This disables .htaccess
      2. Options
         1. Remove ‘indexes’ from options. This will disable CGI-Bin and other scripts
      3. AddHandler
         1. Remove all scripts

1. Validate DocumentRoot with Virtual Hosts:
   1. Cd /etc/httpd/conf.d/vhost.conf
      1. Verify document root location
      2. Cd ‘documentRoot’
         1. Verify .html files in each directory
2. Disable userdir
   1. Vim /etc/httpd/conf.d/userdir.conf
      1. UserDir disabled
3. If using LDAP:
   1. Vim /etc/httpd/conf.d/auth\_ldap.conf
      1. Add to end:
         1. <Directory /var/www/html/auth-ldap>  
            SSLRequireSSL  
            AuthName “LDAP Authentication”  
            AuthType Basic  
            AuthBasicProvider ldap  
            AuthLDAPURL ldap://dlp.srv.world/dc=srv,dc=world,?uid?sub?(objectClass=\*)  
            Require ldap-filter objectClass=posixAccount  
            </Directory>
4. Disable proxy capabilities:
   1. Vim /etc/httpd/conf.d/f\_proxy.conf
      1. module is enabled by default so create new
         1. <IfModule mod\_proxy.c>

ProxyRequests off

<Proxy \*>

# access permission

Require ip 127.0.0.1 10.0.0.0/24

</Proxy>

# specify the way of load balancing with "lbmethod". it's also possible to set "bytraffic".

ProxyPass / balancer://cluster lbmethod=byrequests

<proxy balancer://cluster>

BalancerMember http://node01.srv.world/ loadfactor=1

BalancerMember http://node02.srv.world/ loadfactor=1

</proxy>

</IfModule>

Additional Services:

1. Access Log Analyzer: AWstats
   1. Install: sudo yum --enablerepo=epel -y install awstats
      1. awstats.(hostname).conf created. Modify with:
         1. Sudo vim /etc/awstats/awstats.(hostname).conf
            1. # line 122: change

# if your config for log format in httpd.conf is 'combined' Set here '1'

# If log-config is 'common' set here '4', but in this case, some info unavailable (browser info etc.)

LogFormat=1

# line 153: specify your hostname

SiteDomain="[www.srv.world](http://www.srv.world)"

# line 168: set IP address you'd like to exclude

HostAliases="localhost 127.0.0.1 REGEX[server\.world$] REGEX[^10\.0\.0\.]"

1. vi /etc/httpd/conf.d/awstats.conf
   1. # line 30: IP address you permit to access

Require ip 10.0.0.0/24

1. Set cron to update log every hour:

/usr/share/awstats/wwwroot/cgi-bin/awstats.pl -config+[www.srv.world](http://www.srv.world) -update

1. Access at “[http://(hostname)/awstats/awstats.pl](about:blank)

Harden against DDoS:

1. Install: sudo yum --enablerepo=epel install mod\_evasive
2. Vim /etc/httpd/conf.d/mod\_evasive.conf

# line 18: threshhold for the number of requests for the same page per page interval

DOSPageCount 5

# line 24: threshhold for the total number of requests for any object by the same client on the same listener per site interval

DOSSiteCount 50

# line 28: The interval for the page count threshhold

DOSPageInterval 1

# line 32: The interval for the site count threshhold

DOSSiteInterval 1

# line 41: amount of time (in seconds) that a client will be blocked for if they are added to the blocking list

DOSBlockingPeriod 300

# line 48: notification address if IP address becomes blacklisted

DOSEmailNotify root@localhost

# line 66: specify log directory

DOSLogDir "/var/log/mod\_evasive"

1. Mkdir /var/log/mod\_evasive
2. Chown apache. /var/log/mod\_evasive
3. Systemctl restart httpd
4. Use to test:

Perl /usr/share/doc/mod\_evasive-\*/test.pl

\*\*\*should get 40 forbidden in a bit

ll /var/log/mod\_evasive

\*\*logs are saved

Mail

\*\*shows email to ServerAdmin stating what IP was blacklisted

Utilize mod\_security:

1. Sudo yum install mod\_security
2. Add rules only to SecRuleEngine!!!

Vim /etc/httpd/conf.d/mod\_security.conf

\*\*\*note, default rules are set.

1. Test rules and verify:

Vim /etc/httpd/modsecurity.d/activated\_rules/rules-01.conf

# default action when matching rules

SecDefaultAction "phase:2,deny,log,status:406"

# "etc/passwd" is included in request URI

SecRule REQUEST\_URI "etc/passwd" "id:'500001'"

# "../" is included in request URI

SecRule REQUEST\_URI "\.\./" "id:'500002'"

# "<SCRIPT" is included in arguments

SecRule ARGS "<[Ss][Cc][Rr][Ii][Pp][Tt]" "id:'500003'"

# "SELECT FROM" is included in arguments

SecRule ARGS "[Ss][Ee][Ll][Ee][Cc][Tt][[:space:]]+[Ff][Rr][Oo][Mm]" "id:'500004'"

systemctl restart httpd

1. Logs are stored in directory:

Cat /var/lg/httpd/modsec\_audit.log

1. General rules are provided from official repository

Sudo yum install mod\_security\_crs

# rules are placed like follows

# they are linked into the directory /etc/httpd/modsecurity.d/activated\_rules

ll /usr/lib/modsecurity.d/base\_rules

## **\*\*FTP Checklist\***\*

1. First you must check to see that the FPT service is running
   1. [root@www ~]# service vsftpd status or OR netstat -pant (look for port 21)
   2. Find out your FTP type:
      1. If VSFTPD, continue to 2
      2. If ProFTPD, continue to 3
      3. If Pure-FTPD, continue to 4
2. Verify your Config file with: [root@www ~]# vi /etc/vsftpd/vsftpd.conf
   1. Ensure anonymous login is disabled
      1. # line 12: no anonymous  
         anonymous\_enable=NO
   2. Ensure ascii capabilities are enabled
      1. # line 82,83: uncomment ( allow ascii mode )  
         ascii\_upload\_enable=YES  
         ascii\_download\_enable=YES
   3. Ensure users are CHROOT’ed
      1. # line 100, 101: uncomment ( enable chroot )  
         chroot\_local\_user=YES  
         chroot\_list\_enable=YES
      2. # line 103: uncomment ( specify chroot list )  
         chroot\_list\_file=/etc/vsftpd/chroot\_list
   4. Ensure Recursive is disabled
      1. # line 109: uncomment  
         ls\_recurse\_enable=NO
   5. Make sure using IPv4
      1. # line 114: change ( if use IPv4 )  
         listen=YES  
         # line 123: change  
         listen\_ipv6=NO
   6. Esure root directory is specified
      1. local\_root=public\_html
   7. Examine chrooted users list
      1. [root@www ~]# vi /etc/vsftpd/chroot\_list  
         # add users you allow to move over their home directory
3. Verify your config file with: [root@www ~]# vi /etc/proftpd.conf
   1. Ensure your naming is custom to what you want
      1. # line 77: change to your own hostname  
         ServerName "[www.srv.world](http://www.srv.world)"
      2. # line 79: change to your email address  
         ServerAdmin root@srv.world
   2. Ensure logging is enabled
      1. # line 113: add  
         # get access log & get auth log  
         ExtendedLog /var/log/proftpd/access.log WRITE,READ default  
         ExtendedLog /var/log/proftpd/auth.log AUTH auth
   3. Ensure you are blocking bad users
      1. [root@www ~]# vi /etc/ftpusers  
         # add users you prohibit to FTP access
   4. Enable the service
      1. [root@www ~]# systemctl start proftpd   
         [root@www ~]# systemctl enable proftpd
4. Verify your config file with: [root@www ~]# vi /etc/pure-ftpd/pure-ftpd.conf
   1. Ensure anonymous login is disabled
      1. # line 77: change (no Anonymous)

NoAnonymous yes

* 1. Ensure the service is enabled
     1. [root@www ~]# systemctl start pure-ftpd

[root@www ~]# systemctl enable pure-ftpd

1. Ensure FTP is allowed over your firewall
   1. [root@dlp ~]# firewall-cmd --add-service=ftp --permanent   
      [root@dlp ~]# firewall-cmd --reload
2. Ensure enabled FTP on SELinux
   1. [root@dlp ~]# setsebool -P ftpd\_full\_access on
3. Fix Firewall for Security
   1. [root@dlp ~]# firewall-cmd --add-port=21000-21010/tcp --permanent   
      [root@dlp ~]# firewall-cmd --reload

Resource - <https://www.server-world.info/en/note?os=CentOS_7&p=ftp&f=1>

Resource - <https://www.server-world.info/en/note?os=CentOS_7&p=ftp&f=4>

Resource - <https://www.server-world.info/en/note?os=CentOS_7&p=ftp&f=5>

## **MySQL**

\*\*\*NEVER RUN AS ROOT USER\*\*\*

1. Ensure your MySQL database is running
   1. service mysqld status
      1. Even If the service is running, run the following
         1. sudo mysql\_secure\_installation
            1. Enter password

If no password:

sudo service mysql stop

sudo dpkg-reconfigure mysql-server-5.5

sudo service mysql start

Return to step ‘a’

1. Check user based security
   1. Ensure all users have passwords
      1. SELECT User,Host,Password FROM mysql.user;
      2. For those who don't have passwords:
         1. UPDATE mysql.user SET Password=PASSWORD('newPassWord') WHERE User="demo-user";
      3. For those who have a “%’ in the host field
         1. UPDATE mysql.user SET Host='localhost' WHERE User="demo-user";
      4. If there is a blank username:
         1. DELETE FROM mysql.user WHERE User="";
   2. Check the privileges on each user
      1. See all grants: show grants for 'demo-user'@'localhost';
      2. Remove unnecessary grants: REVOKE UPDATE ON testDB.\* FROM 'demo-user'@'localhost';
   3. Ensure the root user has a username other than ‘root’
      1. rename user 'root'@'localhost' to 'newAdminUser'@'localhost';
   4. When you have completed all steps run the command: FLUSH PRIVILEGES
2. Check the config file
   1. sudo vi /etc/mysql/my.cnf
   2. Ensure your ‘bind-address’ is set to ‘127.0.0.1’ (Local machine only)
   3. Ensure ‘local-infile’ is set to ‘0’ (add this if not exist)
   4. Ensure youre using the proper log file:
      1. log=/var/log/mysql-logfile
3. Check the MySQL log file
   1. sudo ls -l /var/log/mysql\*
   2. Check the ‘.err’ and ‘.log’ files to make sure they aren’t world readable
4. Ensure MySQL is capable of running with firewall:
   1. [root@www ~]# firewall-cmd --add-service=mysql --permanent   
      [root@www ~]# firewall-cmd --reload

Source - <https://www.server-world.info/en/note?os=CentOS_7&p=mysql57>

Source - <https://www.linode.com/docs/databases/mysql/install-mysql-on-ubuntu-14-04>

Source - <https://dev.mysql.com/doc/refman/5.7/en/security-against-attack.html>

Source - <https://www.digitalocean.com/community/tutorials/how-to-secure-mysql-and-mariadb-databases-in-a-linux-vps>

# **Monitoring**

## **Linux Monitoring**

Step by step on how to setup and monitor important log information (i.e. logins, connections, running systems)

Set up central logging server rsyslog/ElasticSearch

1. Ensure rsyslog is downloaded on machine
   1. If not (sudo apt OR apt-get install rsyslog OR sudo yum install rsyslog)
2. IF SELinux enabled- Enable SElinux (semanage -a -t syslogd\_port\_t -p udp 514)
3. Open the config file ( sudo vi /etc/rsyslog.conf)
4. Uncomment 4 lines in modules section
   1. #module(load="imudp")
   2. ​#input(type="imudp" port="514")
   3. #module(load="imtcp")
   4. ​#input(type="imtcp" port="514")
5. Restart server (sudo systemctl rsyslog restart)
6. Unlock firewall for this port (iptables -A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT)
7. Check rsyslog file (sudo rsyslogd -N1)

Set up clients on all machines that want to be monitored rsyslog/ElasticSearch

1. Ensure rsyslog is downloaded on machin(s)
   1. If not (sudo apt install rsyslog OR sudo yum install rsyslog)
2. Open config file (sudo vi /etc/rsyslog.d/50-default.conf)
3. Add to bottom of the file (\*.\* @@SERVERIPADDRESS:514)
4. Create new file (sudo vim /etc/rsyslog.d/10-rsyslog.conf)
5. Add to top of file replacing private\_ip\_of\_ryslog\_server with (@@ SERVERIPADDRESS:514)
6. Restart rsyslog (sudo systemctl rsyslog restart)
7. Check rsyslog file (sudo rsyslogd -N1)

Testing the server

Client

[root@server2 ~]# logger Test from system   
 [root@server2 ~]# tail /var/log/messages   
 Dec 25 00:00:01 server2 root: Test from system

Server

[root@server1 ~]# tail /var/log/messages   
 Dec 25 00:00:01 server2 root: Test from system

Common log files within linux and where to find them

* /var/log/message – Where whole system logs or current activity logs are available.
* /var/log/auth.log – Authentication logs.
* /var/log/kern.log – Kernel logs.
* /var/log/cron.log – Crond logs (cron job).
* /var/log/maillog – Mail server logs.
* /var/log/boot.log – System boot log.
* /var/log/mysqld.log – MySQL database server log file.
* /var/log/secure – Authentication log.
* /var/log/utmp or /var/log/wtmp : Login records file.
* /var/log/yum.log: Yum log files
* /var/log/syslog - logs critical information, beside auth logs

\*How to parse log files\*

* Use head/tail to focus on smaller portion of log files
* Grep WORD TO LOOK FOR logpath
  + Use grep to search for keywords within files
    - Grep “authentication failure” /var/log/auth.log
* Awk REGEXPRESSION logpath
  + Uses REGEX to parse for very specific files
    - awk ‘/sshd.\*invalid user/’ /var/log/auth.log

Helpful tools for monitoring outside of log’s

Monitor running processes

* 1. Linux
     1. System processes (top / htop)
     2. Apache Monitoring (apachetop)
     3. FTP monitoring (ftptop)
     4. SQL monitoring (mytop)

Monitor Desktop processes

* 1. Linux
     1. If Internet is Available (ntopng)
        1. Provides windowed server to analyze ip address connections, usage by each one, and where they originated from.
     2. Built in service similar to wireshark (iftop/jnettop)
        1. Watches packets being sent and received from the computer
     3. Monitor Connections (netstat)
        1. For focusing on one specific tcp packet (justsniffer/tcpdump)
     4. Ultimately if possible download and use wireshark because we have all previously used it and provides the most information for packet and transport layer communications

Monitor entire system

* 1. Linux
     1. Monitorix
        1. Provides default http page with information about the current system it is downloaded on, reports on all mechanisms within the machine
     2. Uptime
        1. Shows the information on run time and how many users are currently logged on. (can be helpful to ensure only the users you know are on the system)
     3. acct / psacct
        1. Acct (for when the system uses apt-get)
           1. Monitors the commands that are entered on the machine (can be used to ensure commands that are malicious are not entered and if they are quickly seen)
        2. Psacct (for when the system uses yum)
           1. Monitors the commands that are entered on the machine (can be used to ensure commands that are malicious are not entered and if they are quickly seen)

## **Windows**

Event Logging API (Windows 2003, XP, 2000)

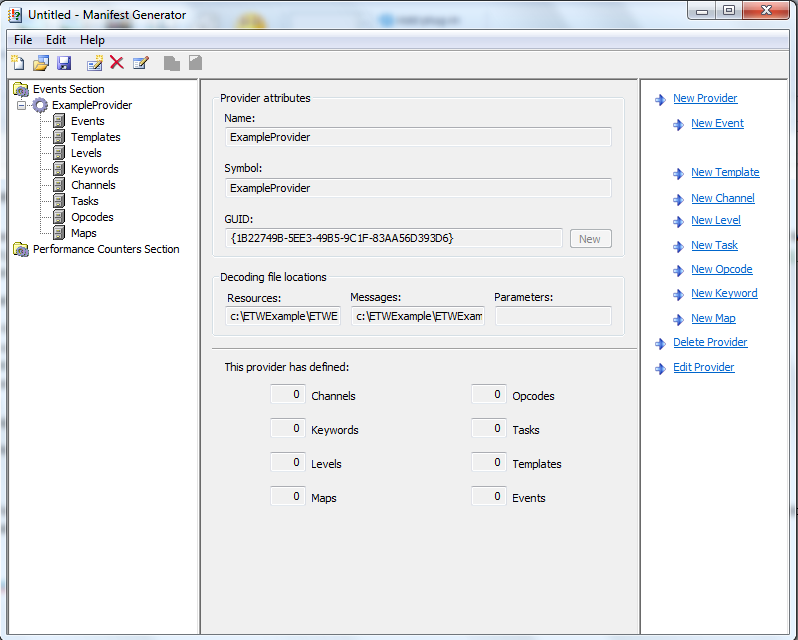
* Use the following C++ code to query for events logged in API
  + <https://msdn.microsoft.com/en-us/library/windows/desktop/bb427356(v=vs.85).aspx>
  + Puts all logged events on a buffer and prints the contents of the buffer
* Use the following C++ code to receive notifications of event logs
  + <https://msdn.microsoft.com/en-us/library/windows/desktop/aa363677(v=vs.85).aspx>
  + Loops through all event logs and if a new event appears, displays a notification

Windows Event Log (Vista-Win10)

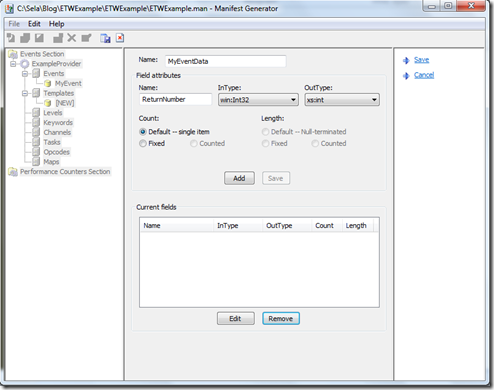
* Download Windows SDK
  + <https://www.microsoft.com/en-us/download/details.aspx?id=8279>
  + Windows tool kit that allows users to create applications. We’ll use this to create an application for log monitoring
* Choose which events your event manifest will record
  + Recommended:
    - Authentication successes/ failures
    - Authorization failures
    - Application and related systems start-ups and shut-downs, and logging initialization (starting, stopping or pausing)
    - Use of higher-risk functionality e.g. network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, etc.
* Create an event manifest
  + Run ECManGen.exe from Windows SDK \bin directory

1. Create a new event provider. This step requires two actions:

* First, select the “Events Section” node in the far left pane and then “New Provider” in the far right pane.
* Second, give the provider a name, symbol, and GUID. Set the Resources and Messages boxes to the full path where the application will be installed. Click “Save” in the far right pane.
  + Use the example from the example section for each of the events you are going to be putting in your event manifest

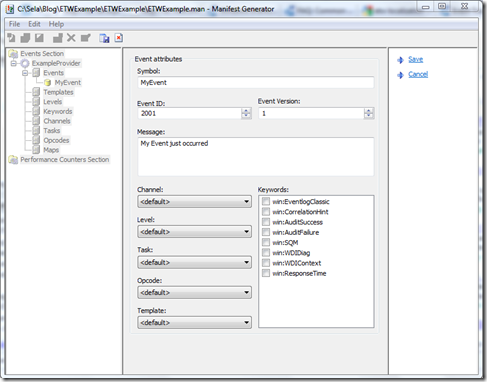


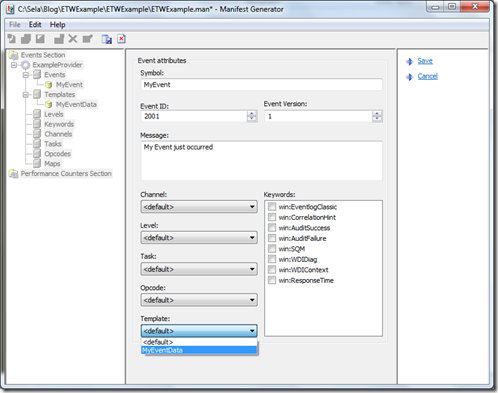
2. Create a new template to define parameter types for each message that requires input parameters.



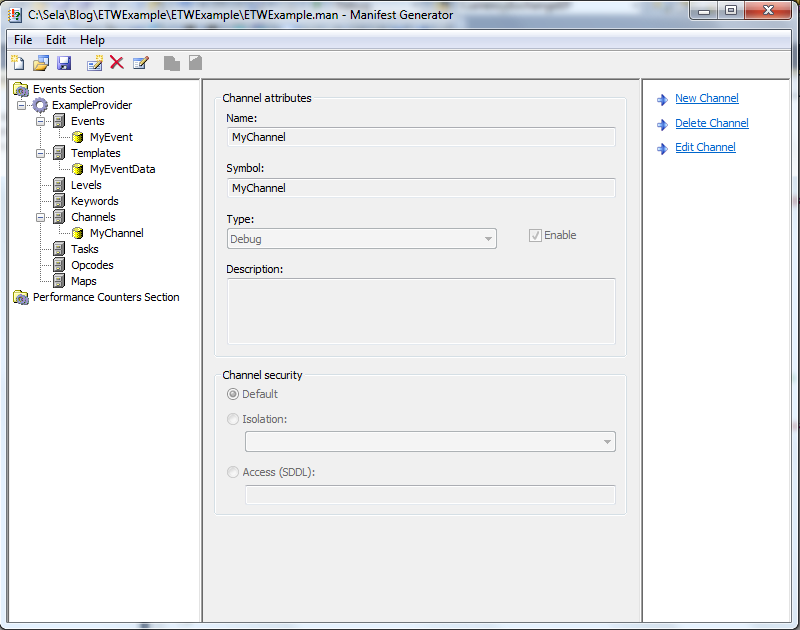
3. Define metadata used to tag events.

4. Create events by giving each a symbol, event ID, message text and template. When you write the message text, use %1, %2, %3, …, %12 to specify the positions of each parameter. Make sure the event template matches the format of the message text with parameters. Assign any channels, levels, tasks, keywords, and opcodes which apply to the event. Save the event. Do the same for all remaining event messages your application will produce.





5. Save the event manifest to your project directory.



Windows Defender

* Download most recent version
  + Note:this will not run on anything earlier than Windows XP SP2
  + https://www.microsoft.com/en-us/windows/comprehensive-security
* Set up a more frequent scan to search for malware
  + Search for and open schedule tasks
  + In the left pane, expand Task Scheduler Library > Microsoft > Windows and then scroll down and double click the Windows Defender folder
  + In the top center pane, double click Windows Defender Scheduled Scan
  + Select the Triggers tab, and then select New
  + Set your time and frequency (every half hour?) and then select OK

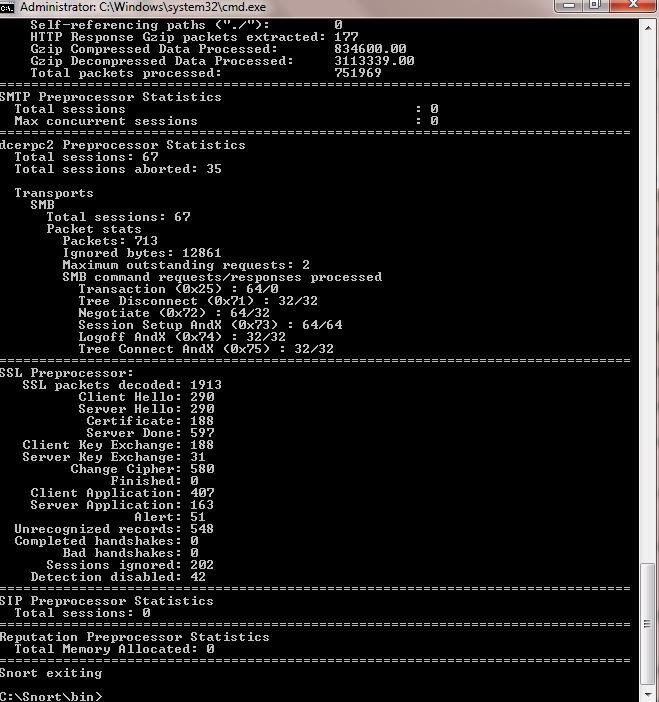
Snort (IDS mode)

* Ensure you have WinPcap installed
  + https://www.winpcap.org/install/
* Download most recent version from snort.org/snort-downloads
* Download Rules
  + <https://www.snort.org/snort-rules>
  + Extract Rules file
  + Copy and paste extracted files to C:\Snort\rules
  + Copy the “snort.conf” file from the “etc” folder of the extracted folder into “C:\Snort\etc”
* Edit the conf file
  + var HOME\_NET 192.168.1.0/24
    - Change the address on this line to your network address
  + Repeat for DNS servers
* Open a command prompt and navigate to “C:\Snort\bin”
* Change the RULE\_PATH variable to the path of rules folder.
  + It should now read “var RULE\_PATH c:\snort\rules”
* Change the path of all library files with the name and path on your system. and you must change the path of snort\_dynamicpreprocessorvariable.
* C:\Snort\lib\snort\_dynamiccpreprocessor
  + Do this to all library files in the “C:\Snort\lib” folder. The old path might be: “/usr/local/lib/…”. you will need to replace that path with your system path. Using C:\Snort\lib
* Change the path of the “dynamicengine” variable value in the “snort.conf” file
* Add the paths for “include classification.config” and “include reference.config” files.
  + include c:\snort\etc\classification.config
  + include c:\snort\etc\reference.config
* Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.
  + include $RULE\_PATH/icmp.rules
* You can also remove the comment of ICMP-info rules comment, if it is commented.
  + include $RULE\_PATH/icmp-info.rules
* To add log files to store alerts generated by snort, search for the “output log” test in snort.conf and add the following line:
  + output alert\_fast: snort-alerts.ids
* Comment (add a #) the whitelist $WHITE\_LIST\_PATH/white\_list.rules and the blacklist
* Change the nested\_ip inner , \ to nested\_ip inner #, \
* Comment out (#) following lines:
  + #preprocessor normalize\_ip4
  + #preprocessor normalize\_tcp: ips ecn stream
  + #preprocessor normalize\_icmp4
  + #preprocessor normalize\_ip6
  + #preprocessor normalize\_icmp6
* Save snort.conf file
* Run on command line
* snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3

Example output:



After done scanning:



(Windows Hardening)

* Change all default passwords
* Have firewall filter on port 445
  + Defends against ms08\_067\_netpai
* In the Security Policy Editor under “Local Policies->User Rights Assignment” there is a policy called “Deny access to the computer from this network”
  + Ensure this is enabled to defend against remote access to local accounts, specifically admin
* Set the RunAsPPL registry key for the LSA
  + Prevents code injection that can compromise credentials
    - Prevents code injection that can compromise credentials
      * Open the registry editor (regEdit.exe) and navigate to the registry key that is located at: HKEY\_LOCAL\_MACHINES\SYSTEM\CurrentControlSet\Control\Lsa
      * Set value of the registry key to “RunAsPPL”=dword:00000001.

# **STRYKE Forensics Checklist** Strike/Forensics Checklist (Initial Vulnerability) No. Control 1 Initial System Vulnerability Scan: Linux/UNIX http://www.openvas.org/ ⇒ OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Networks' commercial vulnerability management solution from which developments are contributed to the Open Source community since 2009. How to get OpenVas web interface running:https://www.digitalocean.com/community/tutorials/how-to-use-openvas-to-audit-the-security-of-remote-systems-on-ubuntu-12-04 Greenbone Security Assist: http://docs.greenbone.net/src/gsa/7.0/index.html This is very powerful tool but it is really hard to setup and configure. If links provided are not enough just google it. You will get a lot of assistance out there. Lynis - Lynis is an open source security auditing tool. Used by system administrators, security professionals, and auditors, to evaluate the security defenses of their Linux and Unix-based systems. It runs on the host itself, so it performs more extensive security scans than vulnerability scanners. Quick how to run Lynis scan: git clone https://github.com/CISOfy/Lynis cd lynis ./lynis audit system -Q Lynis Get Started Guide: https://cisofy.com/documentation/lynis/get-started/ Installation: yum install lynis or git clone https://github.com/CISOfy/lynis + cd lynis Running Lynis: ./lynis lynis audit system - a basic scan without any preconfiguration lynis audit system --quick - running without pauses Example Commands: Command Description audit system Perform a system audit show commands Show available Lynis commands show help Provide a help screen show profiles Display discovered profiles show settings List all active settings from profiles show version Display current Lynis version Options: Option Abbreviated Description --auditor "Given name Surname" Assign an auditor name to the audit (report) --cronjob Run Lynis as cronjob (includes -c -Q) --debug Show debug information, useful for troubleshooting and development --help -h Shows valid parameters --man-page View man page --no-colors Do not use any colors --pentest Perform a penetration test scan (non-privileged) --quick -Q Don't wait for user input, except on errors --quiet -q Only show warnings (includes --quick, but doesn't wait) --reverse-colors Use a different color scheme for lighter backgrounds --verbose Show more screen output Tips: If Lynis is not installed as package (with included man page), use --man or nroff -man ./lynis.8 For systems where the shell background is light, use --nocolors or --reverse-colors Use command show options to see all available parameters of Lynis Windows (not for Windows 10) https://msdn.microsoft.com/en-us/library/ff647642.aspx ⇒ Microsoft Baseline Security Analyzer (MBSA) checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server. MBSA also scans a computer for insecure configuration settings. When MBSA checks for Windows service packs and patches, it includes in its scan Windows components, such as Internet Information Services (IIS) and COM+. MBSA uses Microsoft Update and Windows Server Update Services (WSUS) technologies to determine needed updates. This Microsoft Update data source is obtained either directly from the Microsoft Update Web site or, if offline or in a secure environment, from an offline catalog file named Wsusscn2.cab. This one is not the best tool to guarantee security but most software for windows vulnerability scans are commercial so this one is probably the best we can do. Better way to enhance windows security would be manually going through all the configuration details that systems team provides for Windows OS and having secure configurations for the running services. Download Link : https://www.microsoft.com/en-us/download/details.aspx?id=7558 Double click to open MBSA. Click "Scan a computer". Make sure the options “Check for Windows Administrative vulnerabilities”, “Check for weak passwords” and “Check for security updates“ are checked. You can uncheck the options “Cech for IIS vulnerabilities” and “Check for SQL vulnerabilities” if you don’t have them installed. How to interpret the MBSA scan report: Administrative vulnerability check: Red X - critical check failed (black password) Yellow X - non-critical check failed (password that doesn’t expire) Green check - check passes Blue asterisks - for more info about the computer Security update checks: Red X - security update missing Yellow X - warning (not the latest update) Green check - good Blue asterisks - update not available (not approved on the Update Services server) You can click “Result details” for info on how to fix it. 2 Volatile Memory Analysis: Volatility ⇒ The Volatility Foundation is an independent 501(c) (3) non-profit organization. The foundation’s mission is to promote the use of Volatility and memory analysis within the forensics community, to defend the project’s intellectual property (trademarks, licenses, etc.) and longevity, and to help advance innovative memory analysis research. Download Link : http://www.volatilityfoundation.org/releases Ubuntu: apt-get install volatility Git repo: git clone https://github.com/volatilityfoundation/volatility.git How to use Volatility: https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/ Volatility Analysis: Identify the supported “profiles”: volatility-2.4.standalone.exe imageinfo -f memdump3.raw Get a list of running process in the memory dump examples with profile = Win7SP0x86: volatility-2.4.standalone.exe --profile=Win7SP0x86 pslist -f memdump3.raw Display the processes in tree (parent/child) format. Identify the parent process of the malicious program: volatility-2.4.standalone.exe --profile=Win7SP0x86 pstree -f memdump3.raw The following command with malfind switch is used to dump the malicious DLL's in “output” directory. (Run with PID of all suspicious processes; Process ID: 1120 (svchost.exe)) volatility-2.4.standalone.exe --profile=Win7SP0x86 malfind -D E:\output/pid-1120 -p 1120 -f memdump3.raw No malicious DLL found: Found malicious DLL: Example output dump: The dumps of the malicious programs are scanning using Windows defender and Malware bytes. Command history (CMD history): Scan for the history of commands run on the machine: volatility-2.4.standalone.exe --profile=Win7SP0x86 cmdscan -f memdump3.raw Network Connection: As we know that network connection can be found in the memory analysis, so “netscan” plug-in is run against the memory image and the result shows that malicious program “iexplore” opened several connections on the victim machine. volatility-2.4.standalone.exe" --profile=Win7SP0x86 netscan -f memdump3.raw General Info and commands: Used: git clone https://github.com/volatilityfoundation/volatility.git Basic Usage: python vol.py [plugin] -f [image] --profile=[profile] Example: python vol.py pslist -f /path/to/memory.img --profile=Win7SP1x64 List of Plugins/Readme: https://github.com/volatilityfoundation/volatility/blob/master/README.txt GitHub repo with installation instructions : https://github.com/volatilityfoundation/volatility/wiki/Installation More installation instructions : https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/ Interesting Usages: http://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/#gref 3 Network: Universal Tools: Nmap; Nessus (free of charge for personal use in a non-enterprise environment) Nmap: Check if Nmap is already installed: nmap --version Download: https://nmap.org/download.html Nmap cheat sheet: Basic Scanning Techniques Scan a single target —> nmap [target] Scan multiple targets —> nmap [target1,target2,etc] Scan a list of targets —-> nmap -iL [list.txt] Scan a range of hosts —-> nmap [range of IP addresses] Scan an entire subnet —-> nmap [IP address/cdir] Scan random hosts —-> nmap -iR [number] Excluding targets from a scan —> nmap [targets] –exclude [targets] Excluding targets using a list —> nmap [targets] –excludefile [list.txt] Perform an aggressive scan —> nmap -A [target] Scan an IPv6 target —> nmap -6 [target] Discovery Options Perform a ping scan only —> nmap -sP [target] Don’t ping —> nmap -PN [target] TCP SYN Ping —> nmap -PS [target] TCP ACK ping —-> nmap -PA [target] UDP ping —-> nmap -PU [target] SCTP Init Ping —> nmap -PY [target] ICMP echo ping —-> nmap -PE [target] ICMP Timestamp ping —> nmap -PP [target] ICMP address mask ping —> nmap -PM [target] IP protocol ping —-> nmap -PO [target] ARP ping —> nmap -PR [target] Traceroute —> nmap –traceroute [target] Force reverse DNS resolution —> nmap -R [target] Disable reverse DNS resolution —> nmap -n [target] Alternative DNS lookup —> nmap –system-dns [target] Manually specify DNS servers —> nmap –dns-servers [servers] [target] Create a host list —-> nmap -sL [targets] Advanced Scanning Options TCP SYN Scan —> nmap -sS [target] TCP connect scan —-> nmap -sT [target] UDP scan —-> nmap -sU [target] TCP Null scan —-> nmap -sN [target] TCP Fin scan —> nmap -sF [target] Xmas scan —-> nmap -sX [target] TCP ACK scan —> nmap -sA [target] Custom TCP scan —-> nmap –scanflags [flags] [target] IP protocol scan —-> nmap -sO [target] Send Raw Ethernet packets —-> nmap –send-eth [target] Send IP packets —-> nmap –send-ip [target] Port Scanning Options Perform a fast scan —> nmap -F [target] Scan specific ports —-> nmap -p [ports] [target] Scan ports by name —-> nmap -p [port name] [target] Scan ports by protocol —-> nmap -sU -sT -p U:[ports],T:[ports] [target] Scan all ports —-> nmap -p “\*” [target] Scan top ports —–> nmap –top-ports [number] [target] Perform a sequential port scan —-> nmap -r [target] Version Detection Operating system detection —-> nmap -O [target] Submit TCP/IP Fingerprints —-> http://www.nmap.org/submit/ Attempt to guess an unknown —-> nmap -O –osscan-guess [target] Service version detection —-> nmap -sV [target] Troubleshooting version scans —-> nmap -sV –version-trace [target] Perform a RPC scan —-> nmap -sR [target] Timing Options Timing Templates —-> nmap -T [0-5] [target] Set the packet TTL —-> nmap –ttl [time] [target] Minimum of parallel connections —-> nmap –min-parallelism [number] [target] Maximum of parallel connection —-> nmap –max-parallelism [number] [target] Minimum host group size —–> nmap –min-hostgroup [number] [targets] Maximum host group size —-> nmap –max-hostgroup [number] [targets] Maximum RTT timeout —–> nmap –initial-rtt-timeout [time] [target] Initial RTT timeout —-> nmap –max-rtt-timeout [TTL] [target] Maximum retries —-> nmap –max-retries [number] [target] Host timeout —-> nmap –host-timeout [time] [target] Minimum Scan delay —-> nmap –scan-delay [time] [target] Maximum scan delay —-> nmap –max-scan-delay [time] [target] Minimum packet rate —-> nmap –min-rate [number] [target] Maximum packet rate —-> nmap –max-rate [number] [target] Defeat reset rate limits —-> nmap –defeat-rst-ratelimit [target] Firewall Evasion Techniques Fragment packets —-> nmap -f [target] Specify a specific MTU —-> nmap –mtu [MTU] [target] Use a decoy —-> nmap -D RND: [number] [target] Idle zombie scan —> nmap -sI [zombie] [target] Manually specify a source port —-> nmap –source-port [port] [target] Append random data —-> nmap –data-length [size] [target] Randomize target scan order —-> nmap –randomize-hosts [target] Spoof MAC Address —-> nmap –spoof-mac [MAC|0|vendor] [target] Send bad checksums —-> nmap –badsum [target] Output Options Save output to a text file —-> nmap -oN [scan.txt] [target] Save output to a xml file —> nmap -oX [scan.xml] [target] Grepable output —-> nmap -oG [scan.txt] [target] Output all supported file types —-> nmap -oA [path/filename] [target] Periodically display statistics —-> nmap –stats-every [time] [target] 133t output —-> nmap -oS [scan.txt] [target] Troubleshooting and debugging Help —> nmap -h Display Nmap version —-> nmap -V Verbose output —-> nmap -v [target] Debugging —-> nmap -d [target] Display port state reason —-> nmap –reason [target] Only display open ports —-> nmap –open [target] Trace packets —> nmap –packet-trace [target] Display host networking —> nmap –iflist Specify a network interface —> nmap -e [interface] [target] Nmap Scripting Engine Execute individual scripts —> nmap –script [script.nse] [target] Execute multiple scripts —-> nmap –script [expression] [target] Script categories —-> all, auth, default, discovery, external, intrusive, malware, safe, vuln Execute scripts by category —-> nmap –script [category] [target] Execute multiple scripts categories —-> nmap –script [category1,category2, etc] Troubleshoot scripts —-> nmap –script [script] –script-trace [target] Update the script database —-> nmap –script-updatedb Ndiff Comparison using Ndiff —-> ndiff [scan1.xml] [scan2.xml] Ndiff verbose mode —-> ndiff -v [scan1.xml] [scan2.xml] XML output mode —-> ndiff –xml [scan1.xm] [scan2.xml] Other: Wireshark Useful Wireshark filters: Display Filters ip.addr == 10.0.0.1 - Sets a filter for any packet with 10.0.0.1, as either the source or dest ip.addr==10.0.0.1 && ip.addr==10.0.0.2 - sets a conversation filter between the two defined IP addresses http or dns - sets a filter to display all http and dns tcp or udp - sets a filter to display all http and dns tcp.port==4000 - sets a filter for any TCP packet with 4000 as a source or dest port tcp.analysis.flags - filter for all tcp packets with flags (no responce etc.) tcp.flags.reset==1 - displays all TCP resets http.request - displays all HTTP GET requests http.response - displays all HTTP GET response tcp contains traffic - displays all TCP packets that contain the word ‘traffic’. Excellent when searching on a specific string or user ID !(arp or icmp or dns) - masks out arp, icmp, dns, or whatever other protocols may be background noise. Allowing you to focus on the traffic of interest udp contains 33:27:58 - sets a filter for the HEX values of 0x33 0x27 0x58 at any offset tcp.analysis.retransmission - displays all retransmissions in the trace. Helps when tracking down slow application performance and packet loss tcp.flags.syn==1 - show only tcp SYN packets tcp.flags.reset==1 - show all tcp resets sip && rtp - show all Session Initiation Protocol packets (Internet telephone calls, multimedia distribution, and multimedia conferences) and Real-time Transport (transmitting audio, video or simulation data) Network Miner Xplico 4 Malware: Chkrootkit: a shell script that checks system binaries for rootkit modification (for Linux) \* ifpromisc.c: checks if the network interface is in promiscuous mode. \* chklastlog.c: checks for lastlog deletions. \* chkwtmp.c: checks for wtmp deletions. \* check\_wtmpx.c: checks for wtmpx deletions. (Solaris only) \* chkproc.c: checks for signs of LKM trojans. \* chkdirs.c: checks for signs of LKM trojans. \* strings.c: quick and dirty strings replacement. \* chkutmp.c: checks for utmp deletions. Download: http://www.chkrootkit.org/download/ Installation: To compile the C programs type: make sense After that it is ready to use and you can simply type: ./chkrootkit Usage: chkrootkit must run as root. The simplest way is: ./chkrootkit This will perform all tests. You can also specify only the tests you want, as shown below: Usage: ./chkrootkit [options] [testname ...] Options: -h show this help and exit -V show version information and exit -l show available tests -d debug -q quiet mode -x expert mode -r dir use dir as the root directory -p dir1:dir2:dirN path for the external commands used by chkrootkit -n skip NFS mounted dirs Where testname stands for one or more from the following list: aliens asp bindshell lkm rexedcs sniffer w55808 wted scalper slapper z2 chkutmp amd basename biff chfn chsh cron crontab date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf identd init killall ldsopreload login ls lsof mail mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vdir w write Example Uses: Checks for trojaned ps and ls binaries and also checks if the network interface is in promiscuous mode. ./chkrootkit ps ls sniffer The `-q' option can be used to put chkrootkit in quiet mode -- in this mode only output messages with `infected' status are shown. With the `-x' option the user can examine suspicious strings in the binary programs that may indicate a trojan -- all the analysis is left to the user. Lots of data can be seen with: ./chkrootkit -x | more Pathnames inside system commands: ./chkrootkit -x | egrep '^/' To use, for example, binaries in /cdrom/bin: ./chkrootkit -p /cdrom/bin It is possible to add more paths with a `:' ./chkrootkit -p /cdrom/bin:/floppy/mybin Specify a new rootdir with the `-r' option.For example, suppose the disk you want to check is mounted under /mnt, then: ./chkrootkit -r /mnt Output Messages: The following messages are printed by chkrootkit (except with the -x and -q command options) during its tests: "INFECTED": the test has identified a command probably modified by a known rootkit; "not infected": the test didn't find any known rootkit signature. "not tested": the test was not performed -- this could happen in the following situations: a) the test is OS specific; b) the test depends on an external program that is not available; c) some specific command line options are given. (e.g. -r ). "not found": the command to be tested is not available; "Vulnerable but disabled": the command is infected but not in use. (not running or commented in inetd.conf) 5 File Carving/Parsing/Metadata: AnalyzeMTF - A Python Script analyzeMFT.py is designed to fully parse the MFT file from an NTFS file system. (git repo: https://github.com/dkovar/analyzeMFT ) Installation =========== You should now be able to install analyzeMFT with pip: pip install analyzeMFT Alternatively: git clone https://github.com/dkovar/analyzeMFT.git cd analyzeMFT python setup.py install (or, just run it from that directory) Usage =========== Usage: analyzeMFT.py [options] Options: -h, --help show this help message and exit -v, --version report version and exit File input options: -f FILE, --file=FILE read MFT from FILE File output options: -o FILE, --output=FILE write results to FILE -c FILE, --csvtimefile=FILE write CSV format timeline file -b FILE, --bodyfile=FILE write MAC information to bodyfile Options specific to body files: --bodystd Use STD\_INFO timestamps for body file rather than FN timestamps --bodyfull Use full path name + filename rather than just filename Other options: -a, --anomaly turn on anomaly detection -l, --localtz report times using local timezone -e, --excel print date/time in Excel friendly format -d, --debug turn on debugging output -s, --saveinmemory Save a copy of the decoded MFT in memory. Do not use for very large MFTs -p, --progress Show systematic progress reports. -w, --windows-path Use windows path separator when constructing the filepath instead of linux Output ========= analyzeMFT can produce output in CSV or bodyfile format. CSV output --------- The output is currently written in CSV format. Due to the fact that Excel automatically determines the type of data in a column, it is recommended that you write the output to a file without the .csv extension, open it in Excel, and set all the columns to "Text" rather than "General" when the import wizard starts. Failure to do so will result in Excel formatting the columns in a way that misrepresents the data. I could pad the data in such a way that forces Excel to set the column type correctly but this might break other tools. GUI: You can turn off all the GUI dependencies by setting the noGUI flag to 'True'. This is for installations that don't want to install the tk/tcl libraries. Exiftool - reading, writing and editing meta information in image, audio and video files. Foremost - Foremost is a console program to recover files based on their headers, footers, and internal data structures. RegRipper - For Windows Registry Hives 6 (Monitoring) Auditing: System helps system administrators create an audit trail, a log for every action on the server. We can track security-relevant events, record the events in a log file, and detect misuse or unauthorized activities by inspecting the audit log files. Windows : https://technet.microsoft.com/en-us/library/dd277403.aspx Windows 2000 server: Viewing the Security Log: Open Shared Folders. Click Start, select Programs, select Administrative Tools, click Computer Management. In the console tree, click Event Viewer. Double-click Security and in the details pane, examine the list of audit events Linux/UNIX: https://www.isaca.org/Journal/archives/2015/Volume-4/Pages/auditing-linux-unix-server-operating-systems.aspx