

Cyber Defense Hackpack

CU Cyber

Contents

1	General Information	3
	The Ten Commandments of Cyber Defense	3
	Linux Checklist	3
	Windows Checklist	4
2	Backups and Restoration	5
	rsnapshot	5
	Summary	5
	Dependencies	5
	Configuration	5
	Simple Backups	7
	Summary	7
	Dependencies	7
	Commands	7
3	Firewalls and Configuration	8
	Firewall Basics	8
	FirewallD	8
	Config Files	8
	Commands	8
	Filtering	8
	Example Configuration	9
	iptables	10
	Config Files	10
	Commands	10
	Filtering	11
	Example Configuration	11
	pf	12
	Config Files	12
	Commands	12
	Filtering	12
	Example Configuration	12
	Uncomplicated Firewall	13
	Config Files	13
	Commands	13
	Filtering	14
	Example Configuration	14
4	Logging and Investigation	15
	auditd	15
	Installation	15
	Config Files	15

Commands	15
Example Configuration	15
Rsyslog	16
Config Files	16
5 Services and Applications	17
Apache	17
Installation	17
Chrooting	18
BIND	18
Config Files	18
Example Configuration	18
MySQL	20
Installation	20
Common Tasks	20
Samba	23
Example Configuration	23
OpenSSH	24
Best Practices	24
Config Files	24
Configuration	25
Apache Tomcat	25
Installation	26
Configuration	27
Wordpress	28
Setup	28
Securing	28
6 Appendix	30
The MIT License	30

General Information

The Ten Commandments of Cyber Defense

1. Thou shalt NEVER trust the red team
2. Thou shalt trust but verify everything else
3. Thou shalt know thy network
4. Thou shalt patch your services
5. Thou shalt make frequent backups
6. Thou shalt disable unused services
7. Thou shalt set and use strong passwords
8. Thou shalt always use a firewall
9. Thou shalt log everything
10. Thou shalt get your injects done on time

Linux Checklist

This checklist is designed for the first 30 minutes of competition.

For each system:

- Change the password for the root account
- Check for improper ssh config
- Check for improper sshd config
- Check the crontab (s) for running tasks
- Check with files with wider permissions and setuid
- Create a report of running services and processes and disable unnecessary processes
- Create a report of open ports
- Audit user, groups for invalid entries
- Check mount/nfs if it is running
- Install Updates
- Run a full system backup
- Check/Configure sudo and /etc/sudoers.d
- Harden the service for your machine
- Install/Configure a firewall
- Write an audit report containing changes made
- Configure ansible

For all systems:

- Scan the subnet for running servers
- Configure a provisioner such as Salt/Ansible master

Windows Checklist

This checklist is designed for the first 30 minutes of competition.

For each System:

- Change the password for the admin accounts
- Remove any nonessential user accounts
- Check the startup list
- Check the event logs
- Create a report of all running services
- Create a report of all open ports
- Install windows service packages
- Run a full backup of the system

Backups and Restoration

rsnapshot

Summary

rsnapshot is a utility to create incremental snapshot backups using rsync. It has minimal dependencies and should work even on very old Linux distributions.

Dependencies

- perl
- rsync
- openssh

Configuration

`/etc/rsnapshot.d/system`

```
config_version 1.2
```

```
no_create_root 1
```

```
lockfile      /var/run/rsnapshot.pid
```

```
cmd_cp        /bin/cp
```

```
cmd_rm        /bin/rm
```

```
cmd_rsync     /usr/bin/rsync
```

```
cmd_ssh       /usr/bin/ssh
```

```
link_dest     1
```

```
one_fs        1
```

```
snapshot_root /mnt/backup/
```

```
retain        system 8
```

```
exclude       /dev/**
```

```
exclude       /proc/**
```

```
exclude       /sys/**
```

```
exclude       /tmp/**
```

```

exclude    /var/cache/**
exclude    /var/lock/**
exclude    /var/run/**
exclude    /var/tmp/**

exclude    /usr/portage/distfiles/**

backup     root@example.local:/    example.local/

```

/etc/rsnapshot.d/application

```

config_version 1.2

no_create_root 1
lockfile       /var/run/rsnapshot.pid

cmd_cp         /bin/cp
cmd_rm         /bin/rm
cmd_rsync      /usr/bin/rsync
cmd_ssh        /usr/bin/ssh
link_dest      1

one_fs         1

snapshot_root  /mnt/backup/

retain         application 8

exclude        /dev/**
exclude        /proc/**
exclude        /sys/**

exclude        /tmp/**

exclude        /var/cache/**
exclude        /var/lock/**
exclude        /var/run/**
exclude        /var/tmp/**

exclude        /usr/portage/distfiles/**

backup         root@example.local:/etc/    example.local/
backup         root@example.local:/opt/    example.local/
backup         root@example.local:/var/    example.local/

```

/etc/cron.d/rsnapshot

```

0,15,30,45 * * * * root rsnapshot -c /etc/rsnapshot.d/application application
8 * * * * root rsnapshot -c /etc/rsnapshot.d/system system

```

Simple Backups

Summary

To create simple archive backups, use the tar command. These backups should be created as the initial backups during the beginning period of the competition.

Dependencies

- tar

Commands

Backup

```
#!/bin/sh
useradd flynn
mkdir -p /home/flynn/
tar cjpf /home/flynn/kevin \
    --exclude={"/sys/*,/dev/*,/proc/*,/tmp/*,/run/*"} \
    --exclude=/home/flynn/* /
chown flynn:flynn /home/flynn/kevin
chmod 640 /home/flynn/kevin
```

Extract

```
#!/bin/sh
tar xjpf /home/flynn/kevin --wildcards "$@"
```

Restore

```
#!/bin/sh
cd /
tar xjpf /home/flynn/kevin
```


Firewalls and Configuration

Firewall Basics

Firewalls are essentially sets of rules that allow network traffic in and out of a machine. In general, firewalls should be configured to allow the minimum required access. For Windows, the firewall is called Windows Firewall. For Linux, iptables is the built-in low-level firewall and ufw and firewalld are the most common high-level firewalls. For BSD, pf, the base of the pfSense enterprise firewall, is the default. For dedicated equipment, such as the Cisco ASA, custom firewalls or firewalls based on Linux and on occasion BSD are common.

In general, there are 3 major elements of firewall security:

- Use a default reject policy to avoid admitting unwanted traffic.
- Open only the required ports to make the services to work.
- Log any unusual traffic that hits the firewall.

Firewalld

Config Files

Firewalld references the following directories of files:

- /usr/lib/firewalld - where package default rules reside
- /etc/firewalld - where user overrides rules reside

Commands

Firewalld uses only the `firewall-cmd` binary.

Filtering

Firewalld is the new Linux firewall from RedHat. It provides a usability layer on top of iptables by focusing on zones and services. Firewalld therefore inherits iptables's first match rule.

Zones

Zones are affiliated with source addresses or interfaces. Zones have short names they are referenced by.

The following zone example affects all incoming traffic with the enp0s3 interface. It allows HTTPS traffic defined in the /usr/lib/firewalld/services/https.xml or overwritten in /etc/firewalld/services/https.xml. It also blocks traffic on the 10.0.0.0/8 subnet by dropping and logging the packets.

```
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</public>
  <description>This is our external interface</description>
  <interface name="enp0s3"/>
  <service name="https"/>
  <rule family="ipv4">
    <source address="10.0.0.0/8"/>
    <log>
      <limit address="5/m"/>
    </log>
    <drop/>
  </rule>
</zone>
```

Services

Services define the ports and protocols that will be used by an application. Services have short names they are referenced by.

The following service example allows traffic on TCP port 21. It uses a kernel module to help track and filter the traffic. This is not required for all modules, but is used for some services such as FTP.

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>F00</short>
  <description>Foo is a program that allows bar</description>
  <port protocol="tcp" port="21"/>
  <module name="nf_conntrack_foo"/>
</service>
```

Example Configuration

```
#!/bin/bash

# get the name of the device used for the default route
ext_if=$(ip route | head -n 1 | awk '{print $5}')

# list of devices that should be blocked on the external interface
# WARNING! assumes that there are separate interfaces
#           for the external network
# NOTE the 192.168.0.0/16 subnet should be excluded
#           if there is only one interface
broken="224.0.0.22 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, \
        10.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, \
        192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24, \
        169.254.0.0/16, 0.0.0.0/8, 240.0.0.0/4, 255.255.255.255/32"

firewall-cmd --zone=public --add-interface=$ext_if
```

```

for addr in $broken; do
    firewall-cmd --zone=public \
        --add-rich-rule="rule family='ipv4' service=ssh \
            source address=\"$addr\" log limit value='5/m' drop"
    firewall-cmd --zone=public \
        --add-rich-rule="rule family='ipv4' service=http \
            source address=\"$addr\" log limit value='5/m' drop"
    firewall-cmd --zone=public \
        --add-rich-rule="rule family='ipv4' service=https \
            source address=\"$addr\" log limit value='5/m' drop"
done

firewall-cmd --zone=public --add-service=ssh
firewall-cmd --zone=public --add-service=http

firewall-cmd --direct --add-rule ipv4 filter INPUT_direct 0 \
    -p tcp --dport ssh -m state --state NEW -m recent --set
firewall-cmd --direct --add-rule ipv6 filter INPUT_direct 0 \
    -p tcp --dport ssh -m state --state NEW -m recent --set
firewall-cmd --direct --add-rule ipv4 filter INPUT_direct 1 \
    -p tcp --dport ssh -m state --state NEW -m recent --update \
    --seconds 30 --hitcount 6 -j REJECT --reject-with tcp-reset
firewall-cmd --direct --add-rule ipv6 filter INPUT_direct 1 \
    -p tcp --dport ssh -m state --state NEW -m recent --update \
    --seconds 30 --hitcount 6 -j REJECT --reject-with tcp-reset

firewall-cmd --runtime-to-permanent

```

iptables

Config Files

iptables stores the majority of its configuration in a series of files:

- /etc/sysconfig/iptables - iptables configuration (RedHat-based distributions)
- /etc/iptables - iptables configuration (Debian-based distributions)
- /etc/services - an optional file that maps service names to port numbers

Commands

iptables uses the following binaries:

- iptables - view and modify the firewall
- iptables-save - prints the running configuration to stdout; used to save the running configuration to a file
- iptables-restore - reads a file and sets the firewall configuration

While a save format exists, iptables is normally configured via shell commands to avoid inconsistencies between save file versions.

Filtering

iptables will stop processing a packet when it matches the first rule. The only exception to this is the LOG target. When the LOG target is matched, matching will continue; but the traffic will be logged in the kernel log.

Example Configuration

```
#!/bin/bash

# clear out the current configuration
iptables -F && iptables -X

# allow traffic on the loopback interface
iptables -A INPUT -i lo -j ACCEPT

# ext_if is the device with the default route
ext_if=$(ip route | head -n 1 | awk '{print $5}')

# broken is a list of address that should be blocked on the external interface
# WARNING! Assumes that there is an internal and an external interface
# note that 192.168.0.0/16 should not be blocked if there is only one interface
broken="224.0.0.22 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, \
      10.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, \
      192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24, \
      169.254.0.0/16, 0.0.0.0/8, 240.0.0.0/4, 255.255.255.255/32"

# use a default drop policy
iptables -P INPUT DROP

# disable all ipv6 traffic; Syntax is the same as ipv4 if required
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# log traffic that is dropped by the firewall
iptables -N LOGDROP
iptables -A LOGDROP -m log --log-level info --log-prefix "IPTABLES" \
      -m limit --limit 5/m --limit-burst 10 -j LOG
iptables -A LOGDROP -j DROP

# block bad packets and http and ssh traffic from broken addresses
iptables -A INPUT -m conntrack --ctstate INVALID -j LOGDROP
iptables -t raw -I PREROUTING -m rpfilter -j LOGDROP
for addr in $broken; do
    iptables -A INPUT -p tcp -i $ext_if -s $addr --dport 80 -j REJECT
    iptables -A INPUT -p tcp -i $ext_if -s $addr --dport 443 -j REJECT
    iptables -A INPUT -p tcp -i $ext_if -s $addr --dport 22 -j REJECT
done

# allow established traffic to applications
iptables -I INPUT 1 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
# allow new traffic to applications
iptables -A INPUT -m limit --limit 5/m --limit-burst 10 -m conntrack \
    --ctstate NEW -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -m limit --limit 5/m --limit-burst 10 -m conntrack \
    --ctstate NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m limit --limit 5/m --limit-burst 10 -m conntrack \
    --ctstate NEW -p tcp --dport 443 -j ACCEPT

# drop all other traffic
iptables -A INPUT -j DROP
```

pf

Config Files

pf references the following files:

- /etc/rc.conf - as with all services, pf must be enabled here
- /etc/pf.conf - pf configuration file

Commands

pf uses the following binaries:

- pfctl -f /etc/pf.conf - load the firewall configuration
- pfctl -sa - see the current configuration status
- kldload pf - load the pf kernel module

Filtering

All of the configuration for pf is stored in /etc/pf.conf. There is no way to modify the running configuration except to overwrite the running configuration with the saved configuration. Unlike other firewalls, the last rule to match will be the rule that is applied. This behavior can be overridden by using the **quick** keyword.

Example Configuration

```
# adapted from bsdnow tutorial

# variables for convenience
ext_if = "em0"
broken="224.0.0.22 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, \
    10.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, \
    192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24, \
    169.254.0.0/16, 0.0.0.0/8, 240.0.0.0/4, 255.255.255.255/32"
# use a default drop policy
set block-policy drop

# skip the local loopback interface
set skip on lo0
```

```

# block invalid packets
match in all scrub (no-df max-mss 1440)
block in all
pass out quick on $ext_if inet keep state
antispoof quick for ($ext_if) inet

# block ipv6 if it is not needed
block out quick inet6 all
block in quick inet6 all

# block any packet we can't find a valid route back to
block in quick from { $broken urpf-failed no-route } to any
block out quick on $ext_if from any to { $broken no-route }

# block bad actors
table <childrens> persist
block in log quick proto tcp from <childrens> to any

# block Chinese address to ssh and web
table <chuugoku> persist file "/etc/cn.zone"
block in quick proto tcp from <chuugoku> to any port { 80 22 }

# allow traffic thought the firewall
pass in on $ext_if proto tcp from any to any port 80 flags S/SA synproxy state
pass in on $ext_if proto tcp from 1.2.3.4 to any port { 137, 139, 445, 138 }
pass in on $ext_if proto tcp to any port ssh flags S/SA keep state \
(max-src-conn 5, max-src-conn-rate 5/5, overload <childrens> flush)
pass inet proto icmp icmp-type echoreq

# adapted from the http://www.bsdnow.tv/tutorials/pf
# which is distrusted under CC-BY-SA

```

Uncomplicated Firewall

Config Files

Uncomplicated Firewall references mainly the following files:

- `/etc/default/ufw` - high level configuration
- `/etc/ufw/sysctl.conf` - kernel tunables

Commands

- `ufw enable` - enables and reloads the firewall
- `ufw default` - sets default action
- `ufw allow` - allows service or port
- `ufw deny` - blocks a service or port
- `ufw limit` - allows with connection rate limiting

Filtering

Uncomplicated Firewall is based on iptables and therefore inherits iptables's first match rule.

Example Configuration

```
#!/bin/sh
ufw default deny
ufw allow ssh/tcp
ufw logging on
ufw enable
```

Logging and Investigation

auditd

Linux has a built-in auditing framework that acts in kernel space. This portion of the kernel communicates with the userspace auditd server. It can be configured to monitor files and syscalls.

Installation

```
#!/bin/sh
dnf install audit
systemctl start auditd
```

Config Files

The user space auditing commands, can be used to configure logs. Audit can stores its rules in `/etc/audit/audit.rules` or in files inside `/etc/audit/audit.d/`. The syntax for these files is the same as the user space commands.

Commands

Viewing the auditlog can be done in a few ways:

- aureport - query logs for a specific event
- ausearch - view a summary of recent events
- syslog - view logs typically stored in `/var/log/audit/audit.log`

Example Configuration

```
#!/bin/sh
# remove all rules
auditctl -D

# see a list of rules
auditctl -l

# watch a file for writes
auditctl -w /etc/passwd -p wa -k passwd_access

# watch a directory and all its children for writes
```



```
auditctl -w /etc/ -p wa -k etc_writes

# watch for use of a specific syscalls
auditctl -a always,exit -S stime.* -k time_changes
auditctl -a always,exit -S setrlimit.* -k setrlimits
auditctl -a always,exit -S unlink -S rmdir -k deleting_files

# watch for unsuccessful calls
# the -F flag filters out based on various
# options see man auditctl for more details
auditctl -a always,exit -S all -F success=0

# make the default audit log buffer larger
auditctl -b 1024

# lock audit rules so that they cannot be edited until reboot
auditctl -e 2
```

Rsyslog

Rsyslog is a client and server that conforms to the syslog protocol. On systems with systemd (i.e. RedHat and newer Debian distributions), journald is typically used instead, but both programs can be used to compliment each other.

Config Files

Rsyslog is generally configured by `/etc/syslog.conf` and `/etc/syslog.conf.d/` most other syslog daemons.

`/etc/syslog.conf`

<code>*.err;kern.debug</code>	<code>/dev/console</code>
<code>auth.notice;authpriv.none</code>	<code>/dev/console</code>
<code>*.err;*.crit;*.emerg</code>	<code>/var/log/critical.log</code>
<code>*.notice</code>	<code>/var/log/messages</code>
<code>auth,authpriv.none</code>	<code>/var/log/messages</code>
<code>auth,authpriv.debug</code>	<code>/var/log/auth.log</code>
<code>cron.info</code>	<code>/var/log/cron.log</code>
<code>news,kern,lpr,daemon,ftp,mail.info</code>	<code>/var/log/daemon.log</code>
<code>*.err;user.none</code>	<code>root</code>
<code>*.emerg;user.none</code>	<code>*</code>

Services and Applications

Apache

Apache is a one of the most popular web servers with a large variety of features.

Installation

There is a large variety of steps that are important for securing Apache.

- Install Mod Security either from repos or from www.modsecurity.org
- Configure the Apache to use the Mod Security core rules from the repos or www.modsecurity.org
- Remove unnecessary options and text from Apache's `httpd.conf` file and `/etc/httpd/conf.d` (sometimes located at `/etc/apache2/conf/extra`)
- Remove all unnessisary modules entries from Apache's `httpd.conf` file
- Create an Apache user and group without a shell
- Configure Apache to run using this user and group
- Restrict access to the webserver via the `Order allow,deny` line in `httpd.conf`
- Prevent access to root file system
- Allow only read access to web directory `/var/www/html`
- Disable the following functionality if possible:
 - ExecCGI - Allow scripts to be run by apache from this directory.
 - FollowSymLinks - allow the server to follow symlinks
 - SymLinksIfOwnerMatch - has large performance costs.
 - Includes - permists the execution of server side includes
 - IncludesNOEXEC - same as above except prohibit executing scripts
 - Indexes - create an a directory listing in directories without an `index.html`
 - AllowOverride - allows overrides in `.htaccess` files
 - Multiviews - allows for the same request to ask for multiple files.
- Use `RewriteEngine`, `RewriteCond`, and `RewriteRule` to force HTTP 1.1
- Configure the web server to only server allowed file types.
- Configure to protect from DoS attacks
 - Timeout - set this to a low value like 10 seconds
 - KeepAlive - set this to on (unless RAM is a problem)
 - KeepAliveTimeout - set to 15
 - AcceptFilter http data - require content to open connection
 - AcceptFilter https data - require content to open connection
- Configure to protect against Buffer Overflows
 - LimitRequestBody 64000 - Limit requests to 10k in size
 - LimitRequestFeilds 32 - Limit number of request fields
 - LimitRequestFeildSize 8000 - Limit size of request lines
 - LimitRequestLine 4000 - Maximum size of the request line
- Use `Mod_SSL` if possible (see `openssl` section for generating a sever certificate)

- Set ServerTokens to ProductOnly
- Use custom error pages via the ErrorDocument directive
- Remove default files and cgi-scripts
- Do not keep Apache Source after installation
- Ensure that web sever binaries are owned by root
- Allow only root to read the apache config or logs ‘/usr/lib/apache/{conf,logs}’
- Move apache to a chroot if possible - see below
- Use Mod_Log_Forensic

Chrooting

```
#!/bin/sh
mkdir -p /jail/apache/usr/local
cd /usr/local
mv apache /jail/apache/usr/local

echo "SecChrootDir /jail/apache" >> $HTTPD_CONF
/usr/local/apache/bin/apachectl startssl
```

BIND

BIND is a common, featured DNS server. To make it more secure and less vulnerable to attacks, it is recommended to only run BIND as an authoritative nameserver and not as a recursive nameserver.

Config Files

The configuration for BIND is usually stored in either:

- /etc/bind/ (Debian-based distributions)
- /etc/named/ (other distributions)
- /etc/named.conf (RedHat-based distributions)
- /var/named/ (RedHat-based distributions)

Utilize the named-checkconf utility to check configuration before applying it.

Example Configuration

Below is a set of example configuration files for securely configuring BIND as an authoritative nameserver with forward and reverse records.

/etc/named.conf

```
options {
    # disable zone transfers
    allow-transfer { "none"; };
    version "none";
    fetch-glue no;

    # if we have another DNS recursor, disable queries and recursion
    allow-query { "none"; };
```

```

recursion no;

# if we are a DNS recursor, only allow queries
# from the local network
#allow-query { 10.0.0.0/24; localhost; };
};

# if we are a DNS recursor,
# set forwarding addresses to another nameserver
#forwarders {
#    8.8.8.8;
#    8.8.4.4;
#};

```

/var/named/example.com.conf

```

# replace example.com with the actual domain
zone "example.com" {
    type master;
    # rhel puts these in /var/named
    file "/etc/bind/zones/db.example.com";

    # allow queries to this zone from anywhere
    allow-query { any; };
};

# 10.0.0.0/24 subnet, put address octets backwards
zone "0.0.10.in-addr.arpa" {
    type master;
    # rhel puts these in /var/named
    file "/etc/bind/zones/db.10.0.0";

    # allow queries to this zone from anywhere
    allow-query { any; };
};

```

/var/named/db.example.com

```

$ORIGIN example.com.

; TTL of 10 minutes for quick change during competitions
$TTL    600

; hostmaster.example.com. is the email hostmaster@example.com
@       IN      SOA      ns1.example.com. hostmaster.example.com. (
                                1          ; Serial
                                600        ; Refresh
                                600        ; Retry
                                2419200   ; Expire
                                600        ; Negative Cache TTL
                                ; (how long to cache
                                ; negative (e.g. NXDOMAIN)
                                ; responses)

```

```

)
IN      NS      ns1          ; this box
IN      MX      10 mail       ; mail box
IN      A        10.0.0.103   ; www box (resolve example.com
                                to the same address as
                                www.example.com)

ns1      IN      A          10.0.0.101
mail     IN      A          10.0.0.102
www      IN      A          10.0.0.103

/var/named/db.10.0.0

; put address octets backwards
$ORIGIN 0.0.10.in-addr.arpa.

; TTL of 10 minutes for quick change during competitions
$TTL      600

; hostmaster.example.com. is the email hostmaster@example.com
@          IN      SOA      ns1.example.com. hostmaster.example.com. (
                                1          ; Serial
                                600        ; Refresh
                                600        ; Retry
                                2419200   ; Expire
                                600        ; Negative Cache TTL
                                ; (how long to cache
                                negative (e.g. NXDOMAIN)
                                responses)
                                )
          IN      NS      ns1          ; this box

; if on a bigger subnet, put octets backwards (i.e. 101.0.0)
101      IN      PTR      ns1          ; 10.0.0.101
102      IN      PTR      mail         ; 10.0.0.102
103      IN      PTR      www          ; 10.0.0.103

```

MySQL

MySQL is a quick database for small to medium size organizations.

Installation

Install from the repositories then use the command `mysql_secure_installation`.

Common Tasks

```

-----
-- Listing Databases and Tables:
-----

```

```

SHOW DATABASES; -- lists every db, make sure to DROP the ones you don't need
USE openemr; -- selects a certain database so future operations run on it
SHOW TABLES; -- displays every table in the current database

-----

-- Verify all database users:
-----

# mysql -u root -p -- Login with root
-- Type in root password in prompt. If root doesn't have a password, you should set one now:
UPDATE mysql.User SET Password=PASSWORD('new root password') WHERE User='root';
-- Get list of all users:
SELECT Host, User, Password from mysql.User;

--If there are users that shouldn't be there, delete
--them (remember that % and _ are wildcards, % means 0 or more
--characters and _ means exactly one character).

--Delete all bad users. This should include all anonymous users, and any user
--that has a Host OTHER than 'localhost' (especially root!)

DROP USER 'username'@'hostname';
-- repeat for each undesired user
FLUSH PRIVILEGES;
-- run this after you finish deleting users and/or changing user passwords

--If this is at the beginning of competition, you should delete all non
--root@localhost users and only add them back if you need to. Chances are the
--server is set up to allow an anonymous user or a user with root-like access
--and a weak password full control over the database(s), so the best way to
--prevent an intrusion from Red Team is to outright delete these users. You
--(probably) do not need to worry about copying down password hashes, as if
--some application is using MySQL the password will be stored in plaintext in
--that application, and if not then you should be able to submit a Memo to
--White Team to change a user's password. That said, it might be a good idea
--anyways as long as you store it somewhere that Red Team can't get at and it
--isn't against Policy.

-----

-- Creating new users:
-----

--You should only create users with specific access
--to a specific database (e.g. one user per application that uses a database).
--Additionally, you should restrict the Host as much as possible. If your
--webapp is running on the same box as the db server, make the host localhost,
--otherwise make the host the IP of the box running the webapp. ONLY IF REMOTE
--DATABASE ACCESS IS REQUIRED BY THE INJECT should you open up the host to
--something outside of your team's network (e.g. '%')

--Create the database first

```

```

CREATE DATABASE webapp_name;

--Now add a user to it with a secure password:
--With minimal write access (can add/delete records, but not add/drop tables or
--table structures)

GRANT INSERT, UPDATE, SELECT, DELETE ON webapp_name.* TO
    'database_user'@'hostname per above' IDENTIFIED BY 'password goes here';
--With full write access to the given database
GRANT ALL PRIVILEGES ON webapp_name.* TO
    'database_user'@'hostname per above' IDENTIFIED BY 'password goes here';

-----
-- Get a user's Perms:
-----

SHOW GRANTS FOR 'user'@'host';

SELECT * FROM mysql.User where User='user' and Host='host';
--If you see a lot of Y's and the user ISN'T root@localhost, something is wrong.

-----
-- Backing up and restoring the database:
-----
--This should be in your list of things to do at
--the beginning of competition, as well as semi-frequently throughout when you
--do installations of new webapps, etc. Each command will prompt you to type
--the root password into the terminal. This is safer than providing the
--password in the command line because it does not get saved in .bash_history
--and possibly other places.

-- # is beginning of shell (Linux):
--Backup:
-- # mysqldump --all-databases -u root -p > backup.sql
--Restore:
-- # mysql -u root -p < backup.sql

-----
-- Reset root password:
-----
--Stop MySQL
-- # mysqld -u mysql --skip-grant-tables
-- # mysql -u root --Connect as root

UPDATE mysql.User SET Password=PASSWORD('new root password') WHERE User='root';
FLUSH PRIVILEGES;

--to re-load the grant tables and make root and all other users
--have passwords again

```

Securing

- Make sure it is only listening on localhost unless remote access is required by an inject (or the scoring engine) or you are running the webapps on a different server
- Look for bind-address in the [mysqld] section and ensure it is set to 127.0.0.1 for allowing local connections only or 0.0.0.0 for allowing remote connections
- Disable the LOCAL INFILE queries, which allows someone (i.e. red team) to upload files from their computers into your database, by adding local-infile = 0 to the [mysqld] section of the conf file
- Restart MySQL after making any configuration changes

Samba

Samba is reimplementaion of the Serial Message Block Protocol from Windows.

Example Configuration

The following configuration allows the machine to authenticate to a Windows AD via Kerberos.

samba.conf

this config file based on the Archlinux Wiki which is published under the GFDL

[Global]

```
#Server information
netbios name = EXAMPLEHOST
workgroup = EXAMPLE
realm = EXAMPLE.COM
server string = %h Host

#Authentication
security = ads
encrypt passwords = yes
password server = ad_server.example.com
idmap config * : backend = rid
idmap config * : range = 10000-20000

#Windows domain authentication
winbind use default domain = Yes
winbind enum users = Yes
winbind enum groups = Yes
winbind nested groups = Yes
winbind separator = +
winbind refresh tickets = yes
winbind offline logon = yes
winbind cache time = 300

#New User Template
template shell = /bin/bash
template homedir = /home/%D/%U

preferred master = no
```



```

dns proxy = no
wins server = ad_server.example.com
wins proxy = no

inherit acls = Yes
map acl inherit = Yes
acl group control = yes

load printers = no
debug level = 3
use sendfile = no

```

smb.conf

```

[ExampleShare]
comment = Example Share
path = /srv/exports/example
read only = no
browseable = yes
valid users = @NETWORK+"Domain Admins" NETWORK+test.user

```

OpenSSH

SSH or Secure Shell is a remote administration protocol. It allows the user to send remote commands to Linux machines (and soon to versions of Windows 10 or later). It can be a very powerful tool for system administration, but can also be a powerful exploit target if not secured. It is used with a variety of tools, including the provisioning tool Ansible and back up tool rsnapshot for secure connections. In general there are a few best practices to follow for using ssh.

Best Practices

- Disable root login.
- Disable password authentication (default).
- Disable host-based authentication (default).
- Ensure that ssh is not setuid to prevent host-based authentication.
- Use at least public key authentication and use 2-factor authentication where possible.
- During competition revoke all authorized keys except when required by the scoring engine.
- Use sandbox privilege separation to prevent privilege escalation attacks on the daemon (default).
- Use PAM (pluggable authentication module) (default).
- Block excessive connections to ssh at the firewall.
- Do not forward the SSH Agent to untrusted/compromised servers.

Config Files

Important system level configuration directories and files:

- /etc/sshd/sshd_config - daemon configuration
- /etc/hosts.equiv - used for insecure host based authentication; remove when found
- /etc/shosts.equiv - used for insecure host based authentication; remove when found
- /etc/ssh/ssh_known_hosts - system wide list of host keys

- /etc/ssh/ssh_host_*key - private keys used for host-based authentication and fingerprints
- /etc/ssh/sshrc - commands that are executed when the user logs on

Important user level configuration directories and files:

- ~/.rhosts - used for insecure host based authentication; remove when found
- ~/.shosts - used for insecure host based authentication; remove when found
- ~/.ssh/known_hosts - list of hosts that are not already in /etc/ssh/ssh_known_hosts
- ~/.ssh/authorized_keys/ - list of keys that can be used to authenticate as this user
- ~/.ssh/config - per user configuration options for ssh
- ~/.ssh/environment - environment options for the user
- ~/.ssh/id*.pub - public key for the user
- ~/.ssh/id* - private key for the user

Configuration

/etc/ssh/sshd_config

```
PermitRootLogin no
UsePAM yes
UsePrivilegeSeparation sandbox
AcceptEnv LANG LC_*
ClientAliveInterval 300
ClientAliveCountMax 0
```

Purge User Keys

```
for key_dir in $(awk 'BEGIN { FS=":" } {print $6}' /etc/passwd); do
    if [ -d "$key_dir/.ssh" ]; then
        test -f "$key_dir/.ssh/authorized_keys" && \
            mv "$key_dir/.ssh/authorized_keys" "$key_dir/.ssh/authorized_keys~" &>/dev/null
        test -f "$key_dir/.ssh/rhosts" && \
            mv "$key_dir/.ssh/rhosts" "$key_dir/.ssh/rhosts~" &>/dev/null
        test -f "$key_dir/.ssh/shosts" && \
            mv "$key_dir/.ssh/shosts" "$key_dir/.ssh/shosts~" &>/dev/null
        ls "$key_dir/.ssh/id*" &> /dev/null && echo "found keys at $key_dir/.ssh"
    fi
done
```

Purge System Keys

```
test -f /etc/hosts.equiv && mv /etc/hosts.equiv /etc/hosts.equiv~ &> /dev/null
test -f /etc/shosts.equiv && mv /etc/shosts.equiv /etc/shosts.equiv~ &> /dev/null
```

Do not forget to restart sshd after configuration.

Apache Tomcat

Apache Tomcat is a web server designed to serve Java Server Page (JSP) web applications.

Installation

- Avoid running tomcat with other services
- Remove the sample server files
- Do not reveal excess information
 - Do not advertise version information
 - Disable X-Powered-By HTTP header by setting `xpoweredBy="false"` in the Connectors
 - Disable Allow Trace HTTP header by setting `allowTrace="false"` in the Connectors
 - Disable Client facing Stack Traces
- Protect shutdown port by either disable by setting port to -1 or setting shutdown value to a random value
- Ensure that file permissions are correct
 - Make `$CATALINA_HOME` owned by `tomcat_admin:tomcat` with permissions 750
 - Make `$CATALINA_BASE` owned by `tomcat_admin:tomcat` with permissions 750
 - Make `$CATALINA_HOME/conf` owned by `tomcat_admin:tomcat` with permissions 770
 - Make `$CATALINA_HOME/logs` owned by `tomcat_admin:tomcat` with permissions 770
 - Make `$CATALINA_HOME/temp` owned by `tomcat_admin:tomcat` with permissions 770
 - Make `$CATALINA_HOME/bin` owned by `tomcat_admin:tomcat` with permissions 750
 - Make `$CATALINA_HOME/webapps` owned by `tomcat_admin:tomcat` with permissions 750
 - Make `$CATALINA_HOME/conf/catalina.policy` owned by `tomcat_admin:tomcat` with permissions 600
 - Make `$CATALINA_HOME/conf/catalina.properties` owned by `tomcat_admin:tomcat` with permissions 600
 - Make `$CATALINA_HOME/conf/logging.properties` owned by `tomcat_admin:tomcat` with permissions 600
 - Make `$CATALINA_HOME/conf/server.xml` owned by `tomcat_admin:tomcat` with permissions 600
 - Make `$CATALINA_HOME/conf/tomcat-users.xml` owned by `tomcat_admin:tomcat` with permissions 600
 - Make `$CATALINA_HOME/conf/web.xml` owned by `tomcat_admin:tomcat` with permissions 600
- Use better authentication
 - Configure Realms to not use MemoryRealm in server.xml
 - Configure Realms to use LockOutRealms
 - If possible use Client-Cert Authentication by setting `clientAuth="True"` in server.xml
- Use SSL where possible
 - Ensure that `SSLEnabled` is set to `True` for Sensitive Connectors in server.xml
 - Set the scheme to “https” in connectors in server.xml
 - Ensure that `secure` is set to `false` on connectors that are not using SSL in sever.xml.
 - Ensure that the `sslProtocol` is “TLS” for all connectors using `SSL Engine` in server.xml.
- Configure Logging
 - Ensure the following lines are in `logging.properties` `handlers=org.apache.juli.FileHandler, java.util.logging.ConsoleHandler`
 - Ensure the following lines are in `logging.properties` `org.apache.juli.FileHandler.level=FINEST`
 - Ensure that `className` is set to `org.apache.catalina.valves.FastCommonAccessLogValve` in `$CATALINA_BASE/<app name>/META-INF/context.xml`
 - Ensure that `directory` is set to `$CATALINA_HOME/logs` | in `$CATALINA_BASE/<app name>/META-INF/context.xml`
 - Ensure that `pattern` is set to `%t % U %a %A %m %p %q %s` in `$CATALINA_BASE/<app name>/META-INF/context.xml`
- Prevent unexpected code execution
 - Set `package.access = sun.,org.apache.catalina.,org.apache.coyote.,org.apache.tomcat.,org.apache.ja` in `conf/catalina.properties`
 - Ensure that Tomcat is started with `-security`
 - Ensure that `autoDeploy="false"` in server.xml
 - Ensure that `deployOnStartup="false"` in server.xml
- Protect the manager application

- Ensure that the valves with the class RemoteAddrValve is set to allow on 127.0.0.1 only in server.xml
- Ensure that the valves with the class RemoteAddrValve is set to allow on 127.0.0.1 only in “webapps/host-manager/manager.xml” if it must be used
- Force SSL to access manager if it must be used
- Rename the manager application by renaming the xml file and moving the app to a new corresponding directory
- Disable insecure startup settings
 - Ensure that `-Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true` is set in startup script
 - Ensure that `-Dorg.apache.catalina.connector.RECYCLE_FACADES=false` is set in startup script
 - Ensure that `-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=false` is set in startup script
 - Ensure that `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=false` is set in startup script
 - Ensure that `-Dorg.apache.coyote.USE_CUSTOM_STATUS_MSG_IN_HEADER=false` is set in startup script
- Do not allow symbolic linking in context.xml by setting `allowLinking="false"`
- Do not run applications as privileged in context.xml by setting `privileged="false"`
- Do not allow cross context requests in context.xml by setting `crossContext="false"`
- Do not allow resolving hosts on logging Valves by setting `resolveHosts="false"`

Configuration

```
# remove sample resources
rm -rf $CATALINA_HOME/webapps/{js-examples,servlet-example,webdav,tomcat-docs,balancer}
rm -rf $CATALINA_HOME/webapps/{ROOT/admin,examples}
rm -rf $CATALINA_HOME/server/webapps/{host-manager,manager}
rm -rf $CATALINA_HOME/conf/Catalina/localhost/{host-manager,manager}.xml

# ensure that only needed connectors are configured remove unused connectors
grep "Connector" $CATALINA_HOME/conf/server.xml

# edit the server properties string to hide properties
#tomcat 5.5
cd $CATALINA_HOME/server/lib
#tomcat 6.0
cd $CATALINA_HOME/lib
#both
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
vim org/apache/catalina/util/ServerInfo.properties
jar uf catalina.jar

# disable client facing stack traces
vim error.jsp
# create a error page with out useful information
vim $CATALINA_HOME/conf/web.xml
# add a section that looks like this in the <web-app> element
# <error-page>
#   <exception-type>java.lang.Throwable</exception-type>
#   <location>/path/to/error.jsp</location>
# </error-page>
```

```
# configure LockOutRealms
vim $CATALINA_HOME/conf/server.xml
# add a section that looks like this wrapping the main realm
# <Realm className="org.apache.catalina.realm.LockOutRealm" failureCount="3"
#     lockOutTime="600" cacheSize="1000" cacheRemovalWarningTime="3600">
#     ... MAIN REALM ...
# </Realm>

# force SSL when accessing the manager application
vim $CATALINA_HOME/{server/,}webapps/manager/WEB-INF/web.xml
# add lines that look like this
# <security-constraint>
#     <user-data-constraint>
#         <transport-guarantee>CONFIDENTIAL</transport-guarantee>
#     </user-data-constraint>
# </security-constraint>
```

Wordpress

Wordpress is a PHP content management system. It has reasonable security in a new default install, but has a poor track record for remote execution exploits. The best way to secure Wordpress is to update it if possible and remove all unnecessary or old plugins.

Setup

Download the latest tarball available at '<https://wordpress.org/latest.tar.gz>' and untar it into the document root (i.e. /var/www). Create and configure the necessary using the following SQL commands.

```
CREATE USER wordpress@localhost IDENTIFIED BY 'password';
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE ON wordpress.* TO wordpress@localhost;
FLUSH PRIVILEGES;
```

Navigate to the setup page at '<http://localhost/wordpress/>' and follow the setup instructions. Proceed below with how to add a few extra layers of security to a Wordpress installation.

Securing

- Make sure file permissions are restrictive
 - '/' needs to be writable only by the owning user account (e.g. 'www')
 - '/wp-content' needs to be writable by web server (e.g. 'apache')
 - '/wp-content/plugins' needs to be writable only by the owning user account (e.g. 'www')
- Remove unnecessary database permissions
 - reduce database permissions for the SQL user by running the following command, replacing **wordpress.*** with the Wordpress tables and **wordpress@localhost** with the Wordpress user if necessary.
 - **REVOKE ALL PRIVILEGES ON wordpress.* from wordpress@localhost; GRANT SELECT,INSERT,UPDATE,DELETE ON wordpress.* TO wordpress@localhost; FLUSH PRIVILEGES;**
- Disable file editing from wp-admin
 - add **define('DISALLOW_FILE_EDIT', true);** to 'wp-config.php'
- Move 'wp-config.php' to the directory above the Wordpress root

- Add 'AskApache Password Protect' which enables HTTP authentication preventing wp-admin from being exploited

Appendix

The MIT License

Copyright (c) 2016, CU Cyber cyber@clemson.edu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.