Cyber Defense Hackpack

CU Cyber

Contents

1 General Information Concerning the Hackpack

1.1 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 thy 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

2 Competition Starting Checklists

2.1 Linux Checklist

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

For each system:

- Download toolset
  - `wget -qO- http://bit.ly/2GqAfTb | tar -xzv`
- Download busybox
  - `wget -qO- https://bit.ly/2N0a4KT >/bin/busybox && chmod +x /bin/busybox`
- Change the password for the root account
  - find path to 'passwd': `type passwd`
  - ensure passwd is not a script: `cat <path to passwd>`
  - `passwd <user>`
- Audit users and groups for invalid entries
  - `cat /etc/passwd`
  - `cat /etc/shadow`
  - `cat /etc/group`
  - '/etc/fstab' - owned by 'root:root' - has permission '0644'
  - '/etc/passwd', '/etc/shadow', & '/etc/group' are all owned by 'root:root'
  - '/etc/passwd' & '/etc/group' - has permission 644
  - '/etc/shadow' - has permission 400
- Check the crontab(s) for running tasks
  - `crontab -l`
  - `crontab -e`
  - Limit cron to root
    - `cd /etc/`
    - `/bin/rm -f cron.deny at.deny`
    - `echo root >cron.allow`
    - `echo root >at.allow`
    - `/bin/chown root:root cron.allow at.allow`
    - `/bin/chmod 400 cron.allow at.allow`
- Create a report of running processes
  - `ps aux`
- Create a report of running services
  - `ss -tulpn`
- Check for files with wide permissions and setuid
  - setuid bit: `find <dir> -perm -u=s`
  - world writable: `find <dir> -perm -o=w`
  - See 'Filesystem and Access Control Permissions' -> '/home' and '/var/www'
- Check mounted filesystems
  - `lsblk`

- Prevent device files, setuid files, and executables in globally writable directories
  - `mount -o remount,nodev,nosuid,noexec /tmp`
  - `mount -o remount,nodev,nosuid,noexec /var/tmp`
  - `mount -o remount,nodev,nosuid,noexec /dev/shm`
- Install important system and security updates
  - OpenSSL, OpenSSH, Apache, FTP, SMTP, DNS
  - Linux kernel (not necessarily to latest major version but to latest security update) - requires reboot
- Run a full system backup
  - See 'Backups and Restoration' -> 'Simple Backups'
- Check and configure '/etc/sudoers' and '/etc/sudoers.d/*'
- Harden the service(s) for your machine
  - Check for misconfigured files
  - Install and configure a firewall
    - 'ufw' or 'firewalld'
- Write an audit report containing changes made

2.2 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

3 Administrative Correspondence

3.1 Incident Response and Report

Below are steps to document and report an incident.

- Assign a case number
- Record details
- Time of incident and time of resolution
- Who was the first repsonder
- How the team was notified
- Response time
- Write a paragraph describing how and why the incident happened
- List the followed procedures to contain and recover from the incident
- List the preventative measures taken
- Estimate the financial impact and whether legal recourse is required

3.2 Handling Business Injects

Do **not** wait to complete injects. They are required for business function no matter how trivial. Below are steps to complete an inject satisfactorily.

- Understand what the inject is trying to accomplish. If the tool specified will not provide the intended information, use both the tool required and the tool most apt.
- Use your judgement on how to best complete the task.
- Complete the task writing down what you do
- Create a report
- Mark time of start and end
- Record who is completing the inject
- List information from your judgement on what the inject is trying to accomplish
- List the procedures taken

4 Authentication Modules and Network Protocols

4.1 Kerberos

Kerberos is a remote login service that allows a set of Linux and Windows servers to share users and groups. The current version of the protocol is version 5, and version 4 is deprecated and should not be used due to weak cryptography.

4.1.1 Installation

Kerberos can be configured to either authenticate against either Linux or a Windows Active Directory server.

Here is how to install and configure Kerberos to run on Linux:

```
#!/bin/sh
# if you can, use realmd (newer servers)
realm discover
realm join "realm_name"
realm permit -a

# which roughly does the following on the backend

#########################################################################
##this section is roughly based on the ArchLinux Wiki documentation##
##Which is available under the GNU Free Document License           ##
#########################################################################
# first install and configure NTP and name resolution for the servers
# next, configure the /etc/krb5.conf file as shown below

# verify that you can now login
kinit administrator@EXAMPLE.COM
klist

# if there are errors regarding a missing pam_winbind make a file called
# 'pam_winbind.conf' with the contents of the next section

# configure Samba as specified in the Samba series section

net ads join -U Administartor

# start and enable the required services
```

```
systemctl start smbd nmbd winbindd

# configure /etc/nsswitch.conf as shown below

# test winbind and nss(Windows Authentication service)
wbinfo -u
wbinfo -g
getent passwd
getent group
net ads info
net ads lookup
net ads status -U administrator

# configure PAM with the following config.

# modify applications as necessary to use Kerberos
# see the specific application for documentation

# finally configure smb shares and keytabs if desired using the following
```

/etc/pam_winbind.conf

```
[global]
  debug = no
  debug_state = no
  try_first_pass = yes
  krb5_auth = yes
  krb5_cache_type = FILE
  cached_login = yes
  silent = no
  mkhomedir = yes
```

/etc/pam.d/krb5

```
#%PAM-1.0

auth [success=1 default=ignore] pam_localuser.so
auth [success=2 default=die] pam_winbind.so
auth [success=1 default=die] pam_unix.so nullok
auth requisite pam_deny.so
auth      optional  pam_permit.so
auth      required  pam_env.so


account   required  pam_unix.so
account [success=1 default=ignore] pam_localuser.so
account required pam_winbind.so
account   optional  pam_permit.so
account   required  pam_time.so

password [success=1 default=ignore] pam_localuser.so
```

```
password [success=2 default=die] pam_winbind.so
password [success=1 default=die] pam_unix.so sha512 shadow
password requisite pam_deny.so
password  optional  pam_permit.so

session   required  pam_limits.so
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
session   required  pam_unix.so
session [success=1 default=ignore] pam_localuser.so
session required pam_winbind.so
session   optional  pam_permit.so
```

/etc/krb5.conf

```
[libdefaults]
    #Default Realm must be unique on the network, by convention it is all caps
    default_realm = EXAMPLE.COM
    #if Windows Server 2008 and older require weak crypto; Think carefully before using
    allow_weak_crypto = true

[realms]
    EXAMPLE.COM = {
        #host where the auth server is running given as a fqdm:port
        admin_server = kerberos_server.example.com:749
        #Name(s) of a host running a Kerberos Key Distribution Server
        #These are nessisary if realm admins don't have SRV records in DNS
        kdc = kerberos_server.example.com:88
        kdc = kerberos_server2.example.com:88
    }
[domain_realm]
    #maps host names to kerberos realms
    #domains beginning with a . include all subdomains of the specified domain
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM

[logging]
    default = FILE:/var/log/krb5libs.log
```

4.2 login.defs

'/etc/login.defs' is a configuration file that controls login functionality on Linux machines using encrypted password files. It is one of 3 tools that can control this process (login.defs, pam, systemd-logind).

4.2.1 Best Practices

/etc/login.defs

- set `CONSOLE` to `/etc/securetty`
- set `PASS_MAX_DAYS` to 30
- set `PASS_MIN_DAYS` to 7

- set `PASS_WARN_DAYS` to 8
- set `PASS_MIN_LEN` to 8
- set `MAIL_DIR` to `/var/spool/mail`
- set `UMASK` to 077

/etc/securetty

```
console
tty1
tty2
tty3
tty4
tty5
tty6
```

4.3 PAM

PAM is short for Pluggable Authentication Module. It controls the authentication on Linux machines. By default, it reads the '/etc/shadow' file. It can also be configured to use LDAP or Kerberos for remote authentication.

In general the following should be configured:

- use `pam_cracklib retry=3 minlen=14 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1`
- use `pam_unix obscure sha512 remember=5`

4.3.1 Configuration

/etc/pam.d/system-auth

```
auth required pam_env.so
auth required pam_unix.so try_first_pass likeauth nullokf
auth required /lib/security/\$ISA/pam_tally.so onerr=fail no_magic_root

account required pam_unix.so
account required /lib/security/\$ISA/pam_tally.so per_user_deny=5 no_magic_root reset

password required pam_cracklib.so retry=3 minlength=8 difok=3
password required pam_unix.so try_first_pass use_authtok sha512 shadow

session required pam_limits.so
session required pam_env.so
session required pam_unix.so
```

4.4 Sudo

Sudo is short for super user do. It allows for non-root users to request elevated privileges on linux systems. Sudo has a variety of options that can be configured.

Here are some basic suggestions for managing systems that use sudo:

- Limit users permissions where possible, users should not have `ALL = (ALL) ALL`
- Avoid using groups with root permissions

The '/etc/sudoers' file should be edited as root using the `visudo` command which verifies the syntax before making changes. There are also other configuration files that can be found in '/etc/sudoers.d/'. These can be edited using `visudo -f <filename>`.

4.4.1 Configuration

The following script will create a sane configuration for sudo.

```
#!/bin/sh
cp -Ra /etc/sudoers.d /etc/sudoers.d~
groupdel wheel && groupadd wheel
cp -a /etc/sudoers /etc/sudoers~
cat >/etc/sudoers <<- EOF
root ALL=(ALL) ALL
%wheel ALL=(ALL) ALL
EOF

chown root:root /etc/sudoers
chmod 600 /etc/sudoers

# be sure to add administrators back to 'wheel' and
# merge stuff from '/etc/sudoers~' and '/etc/sudoers.d~/'
```

5 Backups and Restoration

5.1 rsnapshot

5.1.1 Summary

rnapshot 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

5.1.2 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
```

5.2 Simple Backups

5.2.1 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

5.2.2 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
```

6 Disaster Recovery

6.1 Linux

Here are some of the worst things that the red team can do and how to hopefully recover.

6.1.1 Empty Running Executable

If your interpreter or other running executable is an empty file, you can grab the binary from memory.

1. Find a PID of the process (e.g. `bash`) - `pgrep <process name>`
2. Copy the EXE to the location (e.g. `/bin/bash`) - `cp -f /proc/<pid>/exe <location>`

6.1.2 Invalid Password

The red team has changed the password to the root account.

1. Reboot and hold shift
2. Press 'e' at the grub prompt to edit the kernel command line
3. Add the option `init=/bin/bash` to the line that says linux
4. Mount the root filesystem, `mount -o remout,rw /`
5. Use 'vi' to edit the `/etc/passwd` file and remove the 'x' between the 2nd and 3rd colon on the root user
6. Write the file
7. Use 'passwd' to create a new root password
8. Reboot

6.1.3 Chmod Not Executable

While this initially might not seem like it is too bad, there is a problem where bash does not provide a built-in to fix this. This can be particularly devious if the entire root directory is marked not executable. If the entire file system is not executable, you are looking at a live CD or a slave mounted drive.

There are a few options here roughly sorted by time to fix:

- Use a programming language like python, perl, or C to write your own chmod command to fix chmod
- Use the linker directly by running `/lib/ld-*.so /bin/chmod 755 /bin/chmod` as root
- Use a shell like busybox, zsh, or ksh that provides a built-in chmod
- Reinstall chmod from repos or a working machine
- Dump the bits of the binary and manually edit the permission bits
- Use a live CD
- Power off the machine, remove the hard drive, slave mount it to a different machine that has a working chroot, mount the drive, and fix it

Chmod Examples

C

```c
#include<sys/stat.h>

int main(int argc, char *argv[]) {
    chmod("/bin/chmod", S_IRWXU);
    return 0;
}
```

Perl

```perl
#!/bin/sh
perl -e 'chmod 0755, "/bin", "/bin/chmod"'
```

Python

```python
import os
os.chmod('/bin/chmod', 0755)
```

7 Filesystem Layout and Locations

7.1 Linux Filesystem Hierarchy

- `/etc`
  - Should be backed up
  - Contains configuration files
  - Notable system files and directories
    - `passwd` - user table
    - `shadow` - password hash table
    - `group` - group table
    - `pam.d` - PAM configuration
    - `sudoers` - sudo configuration
    - `crontab` and `cron.*` - cron configuration
  - Notable service files and directories
    - `sshd` - OpenSSH
    - `httpd` or `apache2` - Apache
    - `nginx` - NGINX
    - `named` or `bind` - BIND
- `/var`
  - Should be backed up
  - Contains changing permanent data (i.e. databases, logs, disk images, other service data)
  - Contains service home directories
  - Notable directories
    - `db` - databases
    - `lib` - service data
    - `log` - logs
    - `spool` - mail
    - `www` - web server files
    - `tmp` - temporary files that need to survive reboot
- `/tmp`
  - Temporary files that do not need to survive reboots
  - Sockets are often found here
    - `.X11-unix` and `.ICE-unix` - places for X11 sockets and sessions (not found and should be deleted on a headless server!)
- `/home`
  - User data files
- `/root`
  - Root user data files
- `/bin`
  - Contains core executables for running the system (e.g. `init`, `cp`, `ls`, `rm`)
- `/opt`
  - Contains special programs and services

  - Usually for locally compiled programs
- `/usr`
  - Contains non-critical system programs
  - Has its own `bin`, `lib`, and `libexec`
  - Notable directories
    * `share` - place for static program files that do not go in `/etc` or `/var`
- `/lib`
  - Core library files for running programs in `bin`
  - Executables should not be here
- `/libexec`
  - Library executables that should not be run as standalone programs
  - Scripts should probably not be here
- `/proc`
  - Contains process information
  - Is not stored on the filesystem
  - Red teams often use this to find information about processes
  - A core system feature of Linux
- `/dev`
  - Contains device files representing physical devices on the system
  - Red teams will go here to see if they can manipulate devices
  - A core system feature of Linux
- `/sys`
  - Contains system interfaces to retrieve or change features of Linux or the underlying hardware
  - Red teams will likely not use this, but it can be used to get yourself out of a jam if system utilities are not working
  - A core system feature of Linux

8 Dedicated Firewalls, System Firewalls, and Packet Filters

8.1 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.

8.1.1 Zones

Zones are distinct and physically or virtually separated portions of the network. A class example is the difference between LAN and WAN. Generally these are connected to ports on the firewall, but sometimes Virtual LANs or VLANs allow connecting multiple segregated zones to one port via hardware that supports it.

Common Zones

- DMZ (Demilitarized Zone) - separated zone that has no access to internal network
- WAN (Wide Area Network) - zone representing your upstream network connection, generally has your internet connection
- LAN (Local Area Network) - internal network that needs strict separation and access controls

8.1.2 Rules

TODO

8.1.3 Routes

TODO

8.2 NAT

TODO

8.3 FirewallD

8.3.1 Config Files

FirewallD references the following directories of files:

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

8.3.2 Commands

FirewallD uses only the `firewall-cmd` binary.

8.3.3 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 on the enp0s3 interface. It allows HTTPS traffic defined in the '/usr/lib/firewalld/services/https.xml' or overridden 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>FOO</short>
    <description>Foo is a program that allows bar</description>
    <port protocol="tcp" port="21"/>
    <module name="nf_conntrack_foo"/>
</service>
```

8.3.4 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
```

8.4 iptables

8.4.1 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

8.4.2 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.

8.4.3 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.

8.4.4 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
```

8.5 Palo Alto

The Palo Alto firewall is a common and relatively user friendly hardware firewall solution.

8.5.1 Lights Out

To disconnect a port, likely for the purposes of isolating the network from attack, use the following snippet with the desired interface (generally wan) to disconnect.

```
configure
set network interface ethernet <interface> link-state down
commit
```

8.5.2 Change Default Password

To change the admin password, use the following snippet.

```
configure
set mgt-config users admin password
commit
```

8.5.3 Basic Commands

The Palo Alto firewall works similar to Cisco systems in that the command line has various contexts it can be in. The default context gives access to basic network tools, such as ping or traceroute. To configure the firewall, use the `configure` context. While in the `configure` context, you can open various `edit` contexts that follow the hierarchical nature of the firewall configuration. For each `edit` context, it scopes the `set` command to those contexts so that the full path does not need to be specific for several set statements in a row. The `up` and `top` commands can travel up the hierarchy back to base contexts. Settings are not live until the `commit` command is run. You can use tab completion or the question mark key to complete written values and find potential options. The sections below will assume you are in the appropriate `edit` context given at the beginning of the section.

8.5.4 Interfaces

To edit network interfaces, such as the IP and mask of a particular subnet, enter the `edit network interface` context.

Set Interface Network

Use the following to set the interface to the `10.13.37.0/24` network with the address `10.13.37.3`.

```
edit ethernet <interface>
set layer3 ip 10.13.37.3/24
up
```

8.5.5 Routers

To edit virtual routers, such as the default, enter the `top` context.

Add Interface to Router

Use the following to add an interface to a virtual router.

```
edit network virtual-router <name>
set interface <interface>
up
```

8.5.6 Zones

To edit security zones, such as the LAN and DMZ, enter the `top` context.

Edit Zone Network

Use the following to set the interface for the named zone.

```
edit zone <name> network
set layer3 <interface>
up
up
```

8.5.7 Rules

To edit security rules, such as traffic barriers between interfaces, enter the `edit rulebase security` context. Rules between zones are default deny and rules within zones are default allow.

DMZ and LAN Interaction

The following rule enables a connection between the DMZ and LAN under specific circumstances, here a MySQL connection from webapps to database.

```
edit rulebase security
set rules database from dmz to lan source <webapps> destination <database>
  application mysql service application-default action allow
up
```

Incoming Traffic

The following rule enables a connection between the public interface and LAN under specific circumstances, here an HTTP connection to webapps. Replace `application-default` with a port number if different from default.

```
edit rulebase security
set rules webapps from public to lan source any destination <webapps>
  application web-browsing service application-default action allow
up
```

Outgoing Traffic

The following rule enables outgoing communication to specific websites for package management and for DNS lookups.

```
edit rulebase security
set rules package from any to public source any
  destination [ <centos archive> <debian archive> ]
  application web-browsing service application-default action allow
set dns from any to public source any destination <dns server>
  application dns service application-default action allow
up
```

8.6 pf

8.6.1 Config Files

pf references the following files:

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

8.6.2 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

8.6.3 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.

8.6.4 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
```

8.7 Uncomplicated Firewall

8.7.1 Config Files

Uncomplicated Firewall references mainly the following files:

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

8.7.2 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
- `ufw status` verbose - display the current firewall rules (if active)

8.7.3 Sample Usage

- `ufw allow 8080/tcp` - adds a rule that allows incoming traffic on tcp port 22
- `ufw delete allow 8080/tcp` - deletes the previous rule

8.7.4 Filtering

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

8.7.5 Example Configuration

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

9 Logging, Investigation, and Auditing

9.1 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.

9.1.1 Installation

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

9.1.2 Config Files

The userspace 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 userspace commands.

9.1.3 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'

9.1.4 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 unsucessful calls
# the -F flag filters out based on various
# options see man auditctl for more details
auditctl -a always,exit -S all -F sucess=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
```

9.2 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.

9.2.1 Config Files

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

/etc/syslog.conf

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

9.3 Script

The `script` command can be used to record commands run for audit logs.

9.3.1 Usage

```
#!/bin/sh
# use default interactive interpreter
script <file>

# use specified interactive interpreter
script -c bash <file>
```

10 Operating System Utilities

10.1 Advanced Packaging Tool (apt)

10.1.1 Archive Mirrors

If you are running a particularly old version of Debian, you should set up the archive mirrors to get a working package manager.

/etc/apt/sources.list

```
deb http://archive.debian.org/debian/ [version]/main
deb http://archive.debian.org/debian-security/ [version]/updates
deb http://archive.debian.org/debian-volatile/ [version]/volatile
```

10.2 sh

10.2.1 Backgrounding

Often you will want to be able to run processes in the background during the contest. There are a few ways to do this:

- job control - this is the legacy job control system.
- tmux/screen - if they are installed, these are more full featured tools

```
#!/bin/sh
# run an update with yum in the background writing the log to
# '/var/log/yum_updates' that will continue running even if the user logs out
nohup yum update -y >>/var/log/yum_updates 2>&1 &

# see the running list of jobs
jobs -l

# send a job to the background
bg

# send a job to the foreground
fg

# disown a process after you start it
disown
```

10.2.2 Scripting

```
#!/bin/sh
# for loop that outputs 1 2 3 4 5 6 7 8 9 10 a b c
for i in {1..10} a b c
do
    echo $i
done

# conditional testing for an empty string
foo="bar"
if [ -z "$foo" ]; then
    echo $foo
fi

# conditional testing equal stings
if [ "$foo" == "bar" ]; then
    echo $foo
fi

# conditional testing numeric values
if [ 1 -eq 2 ]; then
    echo $foo
fi

# example function
foobar(){
    echo $1
}
foobar "this echos this statement"
```

11 Filesystem and Access Control Permissions

11.1 /dev

The following command will fix permissions for all device files to reasonable defaults:

```
#!/bin/sh
# find devices with execute permissions and remove the execute permissions
find /dev \( -type c -or -type b -or -type f \) -perm -+x -exec chmod -x {} \;
```

11.2 /home

The following command will fix permissions for all home files to reasonable defaults:

```
#!/bin/sh
# barring unusual circumstances, files in a home directory should be 640
sed -i -e "s/^umask [0-9][0-9][0-9]$/umask 027/" /etc/profile
for file in $(find /home/*); do
    if [ -d "$file" ]; then
        #Directories must have execute permissions
        chmod 750 "$file"
    elif [ -x "$file" ]; then
        #Some users will have scripts in there home directory
        read "Should this file be executable ($file) ?" yes
        if [ $yes -eq "y" ]; then
            chmod 750 "$file"
        else
            chmod 640 "$file"
        fi
    else
        #If it is not a file or directory, mark it 640
        chmod 640 "$file"
    fi
done
```

11.3 /tmp

Remount '/tmp', '/var/tmp', and '/dev/shm' with `nodev`, `nosuid`, and `noexec` to prevent executables or device files from being dropped into a globally writable directory and used maliciously.

```
#!/bin/sh
# remount with nodev, nosuid, and noexec
mount -o remount,nodev,nosuid,noexec /tmp
mount -o remount,nodev,nosuid,noexec /var/tmp
mount -o remount,nodev,nosuid,noexec /dev/shm
```

11.4 /var/www

The following command will fix permissions for all www files to reasonable defaults:

```
#!/bin/sh
find /var/www -type d -exec chmod 750 {} \;
find /var/www -type f -exec chmod 640 {} \;
chown -R root:apache /var/www
chmod 770 /var/www/[any directories that need to be writable by the web application]
```

12 Scripts and Other Useful Snippets

12.1 Add Group

The following scripts takes an accounts.csv file with headers 'Firstname,Lastname,SAM,Email' and adds them to the current Active Directory 'Administrators' group.

```
$Users = Import-Csv -Path "accounts.csv"

ForEach($user in $Users){
    Add-ADGroupMember -Identity Administrators -Member $user.SAM
}
```

12.2 Bulk Users

The following scripts takes an accounts.csv file with headers 'Firstname,Lastname,SAM,Email' and adds them to the current Active Directory.

```
$Users = Import-Csv -Path "accounts.csv"
foreach ($User in $Users)
{
    $Displayname = $User.Firstname + " " + $User.Lastname
    $UserFirstname = $User.Firstname
    $UserLastname = $User.Lastname
    $SAM = $User.SAM
    $UPN = $User.Email
    $Password = "CUCyber9."
    New-ADUser -Name "$Displayname" -DisplayName "$Displayname" `
        -GivenName "$UserFirstname" -Surname "$UserLastname" -SamAccountName $SAM `
        -AccountPassword (ConvertTo-SecureString $Password -AsPlainText -Force) `
        -Enabled $true -ChangePasswordAtLogon $true
}
```

12.3 Parallel

The following script takes in a file then command parameter in and for every server in the file, it runs the command on that server.

```
#!/bin/sh
file="$1"
cmd="${*:2}"
```

```
while read server; do
  (ssh $server $cmd) &
done <"$file"
wait
```

13 System Services and Network Applications

13.1 Apache

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

13.1.1 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
- Remove compromising or information leaking modules
    - mod_status
    - mod_info
    - mod_autoindex
    - mod_cgi

13.1.2 Remove Override Functionality

Web application override functionality should be disabled as they are a major security flaw in the Apache system. The functionality is easy to disable, `AllowOverride None` everywhere it is referenced, but the '.htaccess' files should be merged into a global configuration file. This can be done using the following snippet.

```
<Location "[absolute directory of .htaccess file]">
    [contents of .htaccess file]
</Location>
```

13.1.3 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
```

13.1.4 Configuring SSL

Modify the below snippet to your site's needs and add it to your configuration file.

```
LoadModule ssl_module modules/mod_ssl.so

Listen 443
<VirtualHost *:443>
    ServerName www.example.com
    SSLEngine on
    SSLCertificateFile "/path/to/www.example.com.cert"
    SSLCertificateKeyFile "/path/to/www.example.com.key"
</VirtualHost>
```

13.1.5 Prevent Leaking Web Application Data

The following files should be edited to prevent common ways web applications leak data.

robots.txt

```
User-agent: *
Disallow: /
```

13.2 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.

13.2.1 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.

13.2.2 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, queries, and insecure options
   allow-transfer { "none"; };
   version "none";
   fetch-glue no;

   # if we have another DNS recursor, disable recursion
   recursion no;
   allow-query { "none"; };

   # if we are a DNS recursor, only allow queries
   # from the local network or only  for specific hosts
   #recursion yes;
   #allow-query { 10.0.0.0/24; localhost; };
   #allow-query { "none"; };
};

# 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
```

13.3 MySQL

MariaDB, and its predecessor MySQL, is a quick database for small to medium size organizations.

13.3.1 Installation

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

13.3.2 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 config file
- Restart MySQL after making any configuration changes

13.4 OpenSSL

OpenSSL is a toolkit for the TLS protocol and a general purpose cryptography library.

13.4.1 Generate TLS Certificates

Below is a command to generate a key file and TLS certificate for use in Apache or other server. Copy the generated files to the appropriate place (e.g. '/etc/httpd/conf/ssl.key' and '/etc/httpd/conf/ssl.crt') and make them writable only by root and readable by the web server group (e.g. `chown -R root:httpd /etc/httpd/conf/ssl.{key,crt} && chmod 640 /etc/httpd/conf/ssl.{key,crt}`). The output files are `example.pem`, the key, and `example.crt`, the certificate.

```
#!/bin/sh
openssl req -x509 -newkey rsa:2048 -nodes -sha256 -days 365 \
    -keyout example.pem -out example.crt \
    -subj '/O=Example, Inc./CN=example.com'
```

13.5 PHP

TODO

13.5.1 Eval

Some web applications allow web requests to include data which gets sent to `eval()`, generally to allow the front-end to execute back-end commands. Doing this is very bad for security as it allows clients to execute potentially arbitrary code. This sort of problem can often be found with the following command:

```
#!/bin/sh
grep -r "eval(" /var/www # replace /var/www with the web root
```

13.6 Postfix

Postfix is a secure replacement for Sendmail. It features very strong process and privilege separation while keeping an interface roughly consistent with Sendmail. It should work out of the box for local mail delivery and relaying given the mail hostname.

13.6.1 Full MTA

/etc/postfix/main.cf

```
myhostname = [hostname]
```

13.6.2 Send Only

Postfix should be used in place of Sendmail for the case of sending emails. It is easy to install and for send-only has minimal required configuration.

/etc/postfix/main.cf

Apply the below configuration where the original options are in the main configuration file. These will only allow connections from localhost and disable local delivery.

```
inet_interfaces = loopback-only
local_transport = error:local delivery is disabled
```

13.7 Samba

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

13.7.1 Example Configuration

The following configuration allows the machine to authneticate 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
```

13.8 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 vary 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 backup tool rsnapshot for secure connections. In general there are a few best practices to follow for using ssh.

13.8.1 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.

13.8.2 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

13.8.3 Configuration

/etc/ssh/sshd_config

```
Protocol 2
PermitRootLogin no
PermitEmptyPasswords no
IgnoreRhosts yes
RhostsAuthentication no
RhostsRSAAuthentication no
HostbasedAuthentication no
UsePAM yes
UsePrivilegeSeparation sandbox
AcceptEnv LANG LC_*
LoginGraceTime 15s
SyslogFacility AUTH
ClientAliveInterval 300
ClientAliveCountMax 0
AllowUsers <user1> <user2> ...
MaxAuthTries 1
```

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.

13.9 Apache Tomcat

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

13.9.1 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 `$CATALINA_HOME` owned by `tomcat_admin:tomcat` with permissons 750
  - Make `$CATALINA_BASE` owned by `tomcat_admin:tomcat` with permissons 750
  - Make `$CATALINA_HOME/conf` owned by `tomcat_admin:tomcat` with permissons 770
  - Make `$CATALINA_HOME/logs` owned by `tomcat_admin:tomcat` with permissons 770
  - Make `$CATALINA_HOME/temp` owned by `tomcat_admin:tomcat` with permissons 770
  - Make `$CATALINA_HOME/bin` owned by `tomcat_admin:tomcat` with permissons 750
  - Make `$CATALINA_HOME/webapps` owned by `tomcat_admin:tomcat` with permissons 750
  - Make `$CATALINA_HOME/conf/catalina.policy` owned by `tomcat_admin:tomcat` with permissons 600
  - Make `$CATALINA_HOME/conf/catalina.properties` owned by `tomcat_admin:tomcat` with permissons 600
  - Make `$CATALINA_HOME/conf/logging.properties` owned by `tomcat_admin:tomcat` with permissons 600
  - Make `$CATALINA_HOME/conf/server.xml` owned by `tomcat_admin:tomcat` with permissons 600
  - Make `$CATALINA_HOME/conf/tomcat-users.xml` owned by `tomcat_admin:tomcat` with permissons 600
  - Make `$CATALINA_HOME/conf/web.xml` owned by `tomcat_admin:tomcat` with permissons 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 SSLEngine 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` to `sun., org.apache.catalina., org.apache.coyote., org.apache.tomcat., org.apache.jasper.` 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"`

13.9.2 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-contraint>
#   <user-data-constraint>
#      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
#   </user-data-constraint>
# </security-contraint>
```

13.10 VSFTPD

When an FTP server needs to be created or migrating to a more secure box, the FTP server of choice is vsftpd. Apply the following changes to the configuration file to reduce privileges and spoof the banner as the Windows FTP server. If migrating the server, copy all of the FTP files from the old server to '/home/ftp' using the `ftp` command.

/etc/vsftpd.conf

```
nopriv_user=ftp
ftpd-banner=Windows FTP Server
```

13.11 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.

See the PHP section for more details of general PHP hardening.

13.11.1 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.

13.11.2 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

14 Sniffers and Information Gathering

14.1 Nmap

Nmap is a network exploration tool, port scanner, and service scanner. It is useful for preforming host enumeration on IPv4 networks and auditing ports and services on specific hosts on IPv4 and IPv6 networks.

14.1.1 Common Options

There are several main use cases and common options here:

```
#!/bin/sh
# most common options

# ping scan of a IPv4 network
nmap -sn 192.168.1.0/24

# agressive scan of a IPv4 host
nmap -T4 -A 192.168.1.1/32

# agressive scan of a hostname resolved via dns
nmap -T4 -A www.foobar.com

# agressive scan of a IPv6 host
nmap -6 -T4 -A 2::dead:beaf:cafe/128

# agressive scan of a file of hosts/networks separated by newlines
nmap -T4 -A -iL inputfile.txt
```

Host Discovery Options

For host discovery, the most important flag is `-sn`. It sends an ICMP ECHO to each target host. In IPv4 networks, this is a fast and easy way to enumerate hosts for a deeper scan.

In IPv6 networks, the address space is probably too large to do this effectively. On solution in this case to examine the network switch MAC table or to use tcpdump or wireshark to sniff for packets.

To conduct discovery using different types of packets use the `-P{n,S,A,U,Y}` option which uses no pings, SYN, ACK, UDP, and SCTP packets respectively.

Port Scanning Options

By default, Nmap scans the 1000 most commonly used ports. To use Nmap to scan for specific ports, use the `-p` flag to specify which ports to scan. It accepts hyphen separated ranges and comma separated lists. To scan all ports, use the –allports long option. To use a different type of packets use the `-s{S,T,A,W,U,Y}` option which tests with SYN, TCP connect, ACK, UDP, and SCTP INIT packets respectively.

Service Scanning Options

There are several commons flags to use here:

- `-O` will run OS detection against the target
- `-sV` will run service version detection against the target
- `-sC` will run common default scripts against the target to detect various things
- `--script="<script_name>"` will specify a script or group of scripts to run against the targets
- `-A` will enable OS detection, version detection, script scanning, and traceroute

Scripts that are available can often be found the '/usr/share/nmap' directory. Refer to these for examples on how to write scripts.

Timing and Optimization

Nmap has a series of timing and optimizations that can be run. The most useful is -T[1-5] which specifies how quickly packets are to be sent, 1 is the slowest and 5 is the fastest. You can also specify max retries via the –max-retries long option. You can also specify max timeout via the –host-timeout long option.

Evasive Options

If you are running Nmap offensively, there are several flags that control how evasive Nmap behaves. These allow for spoofing of IP address (`-S`) and MAC address (`--spoof-mac`) and for setting various options for sending custom packets.

Output Options

There are various output options the most important are:

- `-oN <file_name>` will send normal output to a file
- `-oG <file_name>` will send grep-able output to a file
- `-oX <file_name>` will output XML to a file

14.2 Wireshark

Wireshark is a GUI and command line tool for network monitoring and analysis. You can use it to record and later analyze or recreate network traffic. You can also use it to find malicous traffic on the network. It can run with promiscuous mode, where all network traffic on the interface is recorded, or without it, where only network traffic originating from or going to the monitoring computer is recorded. It must be run as an administrator to capture traffic (`sudo -E wireshark-gtk` on Linux systems).

14.2.1 Color Scheme

In the traffic pane, the traffic will be highlighted to correspond with different types of packets.

- Green - TCP traffic
- Dark Blue - DNS traffic
- Light Blue - UDP traffic
- Black - TCP packets with problems

14.2.2 Capture Filters

```
# bidirection capture
# capture IPv4 or IPv6 packets to and from a specific host
host 192.168.1.1

# capture packets to and from a subnet of IP addresses in CIDR notation
net 192.168.1.1/24

# capture packets to and from a subnet of IP addresses in network mask notation
net 192.168.1.1 mask 255.255.255.0

# capture traffic only from one source
src net 192.168.1.1

# capture traffic only from a subnet of hosts in CIDR notation
src net 192.168.1.1/24

# capture packets from a range of IPs in subnet format
net 192.168.1.1 mask 255.255.255.0

# capture traffic on specific ports
port 21

# capture traffic for specific services
http
dns
ftp

# capture port range with specific protocol
tcp portrange 1-65535

# capture only IPv4 traffic
# useful when trying to observe traffic other than ARP and STP
ip

# capture only unicast traffic
# good for when you are trying to clear up noise on network
not broadcast and not multicast

# capture heartbleed attempts
tcp src port 443 and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4] = 0x18)
  and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4 + 1] = 0x03)
  and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4 + 2] < 0x04)
  and ((ip[2:2] - 4 * (ip[0] & 0x0F) - 4 * ((tcp[12] & 0xF0) >> 4) > 69)rc
```

```
port 443
and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4] = 0x18)
and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4 + 1] = 0x03)
and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4 + 2] < 0x04)
and ((ip[2:2] - 4 * (ip[0] & 0x0F) - 4 * ((tcp[12] & 0xF0) >> 4) > 69))
```

15 Appendix

15.1 Copyright

All documentation is licensed under the Creative Commons Attribution-ShareAlike 4.0 license. All code examples, unless otherwise specified, are licensed under the BSD 2-Clause license. The build system is licensed under the MIT license.

15.1.1 Creative Commons Attribution-ShareAlike 4.0 International Public License

By exercising the Licensed Rights (defined below), You accept and agree to be bound by the terms and conditions of this Creative Commons Attribution-ShareAlike 4.0 International Public License ("Public License"). To the extent this Public License may be interpreted as a contract, You are granted the Licensed Rights in consideration of Your acceptance of these terms and conditions, and the Licensor grants You such rights in consideration of benefits the Licensor receives from making the Licensed Material available under these terms and conditions.

Section 1 - Definitions.

1. **Adapted Material** means material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor. For purposes of this Public License, where the Licensed Material is a musical work, performance, or sound recording, Adapted Material is always produced where the Licensed Material is synched in timed relation with a moving image.
2. **Adapter's License** means the license You apply to Your Copyright and Similar Rights in Your contributions to Adapted Material in accordance with the terms and conditions of this Public License.
3. **BY-SA** Compatible License means a license listed at creativecommons.org/compatiblelicenses, approved by Creative Commons as essentially the equivalent of this Public License.
4. **Copyright and Similar Rights** means copyright and/or similar rights closely related to copyright including, without limitation, performance, broadcast, sound recording, and Sui Generis Database Rights, without regard to how the rights are labeled or categorized. For purposes of this Public License, the rights specified in Section 2-2-1 are not Copyright and Similar Rights.
5. **Effective Technological Measures** means those measures that, in the absence of proper authority, may not be circumvented under laws fulfilling obligations under Article 11 of the WIPO Copyright Treaty adopted on December 20, 1996, and/or similar international agreements.
6. **Exceptions and Limitations** means fair use, fair dealing, and/or any other exception or limitation to Copyright and Similar Rights that applies to Your use of the Licensed Material.
7. **License Elements** means the license attributes listed in the name of a Creative Commons Public License. The License Elements of this Public License are Attribution and ShareAlike.

8. **Licensed Material** means the artistic or literary work, database, or other material to which the Licensor applied this Public License.
9. **Licensed Rights** means the rights granted to You subject to the terms and conditions of this Public License, which are limited to all Copyright and Similar Rights that apply to Your use of the Licensed Material and that the Licensor has authority to license.
10. **Licensor** means the individual(s) or entity(ies) granting rights under this Public License.
11. **Share** means to provide material to the public by any means or process that requires permission under the Licensed Rights, such as reproduction, public display, public performance, distribution, dissemination, communication, or importation, and to make material available to the public including in ways that members of the public may access the material from a place and at a time individually chosen by them.
12. **Sui Generis Database Rights** means rights other than copyright resulting from Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended and/or succeeded, as well as other essentially equivalent rights anywhere in the world.
13. **You** means the individual or entity exercising the Licensed Rights under this Public License. **Your** has a corresponding meaning.

Section 2 - Scope.

1. **License grant.**
    1. Subject to the terms and conditions of this Public License, the Licensor hereby grants You a worldwide, royalty-free, non-sublicensable, non-exclusive, irrevocable license to exercise the Licensed Rights in the Licensed Material to:
        1. reproduce and Share the Licensed Material, in whole or in part; and
        2. produce, reproduce, and Share Adapted Material.
    2. **Exceptions and Limitations.** For the avoidance of doubt, where Exceptions and Limitations apply to Your use, this Public License does not apply, and You do not need to comply with its terms and conditions.
    3. **Term.** The term of this Public License is specified in Section 6-1.
    4. **Media and formats; technical modifications allowed.** The Licensor authorizes You to exercise the Licensed Rights in all media and formats whether now known or hereafter created, and to make technical modifications necessary to do so. The Licensor waives and/or agrees not to assert any right or authority to forbid You from making technical modifications necessary to exercise the Licensed Rights, including technical modifications necessary to circumvent Effective Technological Measures. For purposes of this Public License, simply making modifications authorized by this Section 2-1-4 never produces Adapted Material.
    5. **Downstream recipients.**
        1. **Offer from the Licensor – Licensed Material.** Every recipient of the Licensed Material automatically receives an offer from the Licensor to exercise the Licensed Rights under the terms and conditions of this Public License.
        2. **Additional offer from the Licensor – Adapted Material.** Every recipient of Adapted Material from You automatically receives an offer from the Licensor to exercise the Licensed Rights in the Adapted Material under the conditions of the Adapter's License You apply.
        3. **No downstream restrictions.** You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, the Licensed Material if doing so restricts exercise of the Licensed Rights by any recipient of the Licensed Material.
    6. **No endorsement.** Nothing in this Public License constitutes or may be construed as permission to assert or imply that You are, or that Your use of the Licensed Material is, connected with, or sponsored, endorsed, or granted official status by, the Licensor or others designated to receive attribution as provided in Section 3-1-1-1-1.
2. **Other rights.**
    1. Moral rights, such as the right of integrity, are not licensed under this Public License, nor are publicity, privacy, and/or other similar personality rights; however, to the extent possible, the

Licensor waives and/or agrees not to assert any such rights held by the Licensor to the limited extent necessary to allow You to exercise the Licensed Rights, but not otherwise.
2. Patent and trademark rights are not licensed under this Public License.
3. To the extent possible, the Licensor waives any right to collect royalties from You for the exercise of the Licensed Rights, whether directly or through a collecting society under any voluntary or waivable statutory or compulsory licensing scheme. In all other cases the Licensor expressly reserves any right to collect such royalties.

Section 3 - License Conditions.

Your exercise of the Licensed Rights is expressly made subject to the following conditions.

1. **Attribution.**
    1. If You Share the Licensed Material (including in modified form), You must:
        1. retain the following if it is supplied by the Licensor with the Licensed Material:
            1. identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);
            2. a copyright notice;
            3. a notice that refers to this Public License;
            4. a notice that refers to the disclaimer of warranties;
            5. a URI or hyperlink to the Licensed Material to the extent reasonably practicable;
        2. indicate if You modified the Licensed Material and retain an indication of any previous modifications; and
        3. indicate the Licensed Material is licensed under this Public License, and include the text of, or the URI or hyperlink to, this Public License.
    2. You may satisfy the conditions in Section 3-1-1 in any reasonable manner based on the medium, means, and context in which You Share the Licensed Material. For example, it may be reasonable to satisfy the conditions by providing a URI or hyperlink to a resource that includes the required information.
    3. If requested by the Licensor, You must remove any of the information required by Section 3-1-1-1 to the extent reasonably practicable.
2. **ShareAlike.** In addition to the conditions in Section 3-1, if You Share Adapted Material You produce, the following conditions also apply.
    1. The Adapter's License You apply must be a Creative Commons license with the same License Elements, this version or later, or a BY-SA Compatible License.
    2. You must include the text of, or the URI or hyperlink to, the Adapter's License You apply. You may satisfy this condition in any reasonable manner based on the medium, means, and context in which You Share Adapted Material.
    3. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, Adapted Material that restrict exercise of the rights granted under the Adapter's License You apply.

Section 4 – Sui Generis Database Rights.

Where the Licensed Rights include Sui Generis Database Rights that apply to Your use of the Licensed Material:

1. for the avoidance of doubt, Section 2-1-1 grants You the right to extract, reuse, reproduce, and Share all or a substantial portion of the contents of the database;

2. if You include all or a substantial portion of the database contents in a database in which You have Sui Generis Database Rights, then the database in which You have Sui Generis Database Rights (but not its individual contents) is Adapted Material, including for purposes of Section 3-2; and
3. You must comply with the conditions in Section 3-1 if You Share all or a substantial portion of the contents of the database.

For the avoidance of doubt, this Section 4 supplements and does not replace Your obligations under this Public License where the Licensed Rights include other Copyright and Similar Rights.

Section 5 – Disclaimer of Warranties and Limitation of Liability.

1. **Unless otherwise separately undertaken by the Licensor, to the extent possible, the Licensor offers the Licensed Material as-is and as-available, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply to You.**
2. **To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of this Public License or use of the Licensed Material, even if the Licensor has been advised of the possibility of such losses, costs, expenses, or damages. Where a limitation of liability is not allowed in full or in part, this limitation may not apply to You.**
3. The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability.

Section 6 – Term and Termination.

1. This Public License applies for the term of the Copyright and Similar Rights licensed here. However, if You fail to comply with this Public License, then Your rights under this Public License terminate automatically.
2. Where Your right to use the Licensed Material has terminated under Section 6-1, it reinstates:
    1. automatically as of the date the violation is cured, provided it is cured within 30 days of Your discovery of the violation; or
    2. upon express reinstatement by the Licensor.

    For the avoidance of doubt, this Section 6-2 does not affect any right the Licensor may have to seek remedies for Your violations of this Public License.
3. For the avoidance of doubt, the Licensor may also offer the Licensed Material under separate terms or conditions or stop distributing the Licensed Material at any time; however, doing so will not terminate this Public License.
4. Sections 1, 5, 6, 7, and 8 survive termination of this Public License.

Section 7 – Other Terms and Conditions.

1. The Licensor shall not be bound by any additional or different terms or conditions communicated by You unless expressly agreed.
2. Any arrangements, understandings, or agreements regarding the Licensed Material not stated herein are separate from and independent of the terms and conditions of this Public License.

Section 8 – Interpretation.

1. For the avoidance of doubt, this Public License does not, and shall not be interpreted to, reduce, limit, restrict, or impose conditions on any use of the Licensed Material that could lawfully be made without permission under this Public License.
2. To the extent possible, if any provision of this Public License is deemed unenforceable, it shall be automatically reformed to the minimum extent necessary to make it enforceable. If the provision cannot be reformed, it shall be severed from this Public License without affecting the enforceability of the remaining terms and conditions.
3. No term or condition of this Public License will be waived and no failure to comply consented to unless expressly agreed to by the Licensor.
4. Nothing in this Public License constitutes or may be interpreted as a limitation upon, or waiver of, any privileges and immunities that apply to the Licensor or You, including from the legal processes of any jurisdiction or authority.

15.1.2 BSD 2-Clause

Copyright (c) 2018, CU Cyber cyber@clemson.edu

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

15.1.3 The MIT License

Copyright (c) 2018, 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.