CDX Event

Your team has just been hired as network and security administrators at a small company and will be taking administrative control of their web server. Your team knows very little about the network, what security level has been maintained, or what software has been installed. Your team has a limited time frame to familiarize yourself with the network and systems and to begin the securing and patching before competitors start actively attacking your company.

Services You Must Provide:

Your team has been told to keep the following services available:

- Apache+PHP
- MySQL (for the purpose of supporting the existing WordPress site)
- WordPress site must continue providing the content in the MONITOR THIS entry, at the same URL (http://<Your IP>/wordpress/?p=4), and must continue to function as a WordPress site
- The daytime service must continue providing the time of day on the server
- FTP must continue providing anonymous access to log in and download any files hosted there
- The print service (ipp) must be running
- Your IP address must respond to ICMP ECHO REQUESTs (ping) per RFC 1122

Accounts:

The OS you have been given boots into account 'student' without supplying a username and password. Since 'student' is in the '/etc/sudoers' file a user 'student' only has to run 'sudo su' to become root (although initially this is blocked). After becoming root you should immediately change the password of 'student' since all VMs given to teams have the same password and someone is bound to figure out what that is. Here are all the credentials you need:

- username: student / password: see above

For the administrator of both MySQL databases:

- username: root / password: (empty)

Both MySQL databases are owned by the following:

- username: student / password: student
The Contest
There exists a Scorer that interrogates each VM at regular intervals - approximately every minute or two. Interrogation is round-robin so all VMs are checked by the Scorer (approximately) the same number of times during the contest. For each service that the Scorer finds is 'up' a point is given to that VM. At the end of the contest teams are ranked according to the sum over all their VMs.

CDX Activities
The OS given to each team has vulnerabilities. The protocol used to check that services are running also has vulnerabilities. This gives teams an opportunity to prevent adversaries from keeping their services up. Therefore, the following activity is recommended:

- examine the supplied VM and improve the security posture with changes to configuration files, code, etc.

Using a VM other than the one provided is not allowed. When the contest is over, submit a final report which includes the following:

- What vulnerabilities were discovered and how they were fixed to prevent exploitation.
- List attacks made against your VM and use a kill chain description of those attacks including command-and-control if they got that far.
- Say whether the attack was successful and, if so, what could have been done to prevent it or, if not, what did you do, if anything, that caused the attack to fail.
- Pinpoint the exact time the attack occurred and, if possible, what IP address(es) was(were) used in the attack.
- List attacks that were attempted by you.
- Say whether the attack was successful and, if not, say what the target of the attack did to stop it.
- Pinpoint the exact time of the attack and what IP address was the target.

The CDX period begins at 6:00AM, December 1 and ends 11:00PM, December 3.

The final report is due 11:59PM, December 10 (OK, if you are a little late and I have some other reports to read I will still accept it).

Attacking Rules of Engagement
Students may join together in a team, as they wish. Students may even switch teams during the contest. Teams are encouraged to attack competing teams’ VMs and the Scoring protocol. But the following rules will be enforced:

- It is not OK to attempt to break out of the CDX network. That is, team members should stick to poking IP address 192.168.42.XX, where XX is a number between 10 and 254.
- If a VM is compromised (that is, password is discovered and adversary can enter the VM to become root) it is not OK to attempt to open a connection to UC’s network from the compromised VM.
Defending Rules of Engagement
The following rules apply to defending against attacks:

- Recovery using a snapshot is allowed only in emergencies such as the VM has become completely useless. This rule is invoked because using snapshots violates the spirit of a CDX where we are trying to improve skills of recovery from attack.
- It is OK to block ports that are not used to provide necessary services.
- It is not OK to transfer files between the VM and a UC node.
- It is OK to create new accounts, change passwords, add or remove users and groups in the VM. All changes need to be documented in the final report (the change and the date and time).
- It is OK to block IP addresses but the Scorer will randomly select an IP address from which to interrogate a team's VM so blocking one or more IP addresses may prevent a score from increasing even though services are up. Please document blocking in the final report (include date and time it was done and undone).
- Points are deducted where the final report indicates an attack that was actually benign traffic or has no mention of an attack that occurred.
- It is OK to add or remove packages from the VM. For example, you may want to add some analysis tools and remove some potentially dangerous packages that are not needed. But you have to figure out how to do this.

Detailed Instructions, Hints, and Corrections

- Each student will get access to a contest OS VM with a particular IP address and access to a Kali Linux VM with a different IP address. All addresses are unique with respect to contestant and function and will be of the form 192.168.42.XX where XX is a number between 10 and 254.
- The contest will be run on the Ohio Cyber Range (OCR). See OCR-doc for instructions on how to access your VMs on the OCR.
- A scoreboard will be available at http://192.168.42.2/standings.html. It will be updated at intervals of less than 60 seconds.
- More instructions will follow.

Hint 1
Make sure your important services are up! Use nmap to find out. Use nmap from the VM like this: nmap localhost. Use nmap from the Kali Linux OS like this: nmap 192.168.42.XX where 192.168.42.XX is the address of your VM. The outputs should agree!

Hint 2
To make sendmail public do this as root:

```
edit /etc/mail/sendmail.mc /* make ports 25 & 587 public */
replace occurrences of "127.0.0.1" with "0.0.0.0" /* in two places */
save
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```
service sendmail restart /* restart sendmail service */

**Hint 3**  
To make MySQL public do this as root:

```
edit /etc/mysql/my.cnf /* make port 3306 public */  
set bind-address = 0.0.0.0 /* was 127.0.0.1 */  
save
service mysql restart /* restart mysql */
```

**Hint 4**  
To make CUPS public do this as root:

```
edit /etc/cups/cupsd.conf /* make port 631 public */  
change "Listen localhost:631" to "Listen 0.0.0.0:631"
save
service cups restart /* restart cups */
```

**Prizes**  
First place: $150  
Second place: $100  
Third place: $50

Winners may choose between cash, Amazon gift card, or Walmart gift card.  
Prizes are awarded based on points shown on the scoreboard at the end of the contest.  
Report grades have no influence on prizes.  
If a scoreboard is manipulated by one or more players, it does not matter: the scoreboard results are final!!