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 security updates and patches before the red team starts actively attacking your company. Your company operates servers on three IP addresses which have been given to the team.

Services You Must Provide:
Your team has been told to keep the following services available on all three IP addresses:

- 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 OSes you have been given boot 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 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 OSes given to each team have 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 that 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 VMs 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
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 10.8.0.1XX, where XX is 00 to 99.
• If a VM is compromised (that is, password is discovered and adversary team 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.
• It is **not OK** to attack before 6:00AM on December 1 or after 11:00PM on December 3.
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 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 OK to transfer files between the host OS and the VM but it is not OK to transfer files between the VM and a UC node. This means it is not OK to transfer a file from the VM to the host then from the host to 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.

Detailed Instructions, Hints, and Corrections

- Each team will get three IP addresses. All addresses will be of the form 10.8.0.1XX where XX between 00 and 99.
- The contest will be run using OpenVPN. The OpenVPN server will be located at 10.52.10.254 (boole.ececs.uc.edu) behind the UC firewall.
- Use these instructions to connect to the contest network. The files contest.conf, run.proxy, run.client, stop.proxy, stop.client will be provided to teams before a practice session a week ahead of the contest and will be used again during the contest.
- A scoreboard will be available at http://gauss.ececs.uc.edu/standings.html. It will be updated at intervals of less than 60 seconds.
- More instructions will follow.

**Hint 1:**

if the connection resets every 5 seconds you may have a second openvpn session running. This is possible because ubuntu installs openvpn to start automatically. To kill the other session do this:

```
sudo killall openvpn
```

then try again.
**Socks Proxy**
Use the following command from a shell on your Ubuntu VM to establish a socks proxy connection to UC:

```
ssh -N -f -C -D 8080 visitor@helios.ececs.uc.edu
```

Use password 'iwarsdemo'. If you use a socks proxy (port 8080) you will have to uncomment the following line into your client.conf file before starting openvpn:

```
;socks-proxy 127.0.0.1 8080
```

To uncomment, open client.conf in a text editor and remove the semi-colon from the beginning of the line.

**Staying Alive**
In order to stay alive regardless of activity you will need to edit `/etc/ssh/ssh_config` before running the command above. The important lines to add are:

```
ServerAliveInterval 30
ServerAliveCountMax 5
```

**Test**
After starting openvpn you should see a new internet interface called tap0 or tap1. If you execute `ifconfig tap0` (alternatively, tap1) you will get something like this:

```
tap0      Link encap:Ethernet  HWaddr 4a:5b:ac:d0:39:c6
          inet addr:10.8.0.152  Bcast:10.8.0.255  Mask:255.255.255.0
          inet6 addr: fe80::485b:acff:fed0:39c6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:808 (808.0 B)  TX bytes:578 (578.0 B)
```

where the 152 could be anything from 100 to 199. We may occasionally have a VM connected at 10.8.0.200. Connect to it like this:

```
[franco@franco ~]$ ssh student@10.8.0.200
The authenticity of host '10.8.0.200 (10.8.0.201)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.8.0.200' (ECDSA) to the list of known hosts.
no such identity: /home/franco/.ssh/id_ed25519: No such file or directory
student@10.8.0.200's password:
Last login: Mon Nov 3 13:00:35 2020 from 10.8.0.1
student@cyber-box:-$
```

The password is 'student'. The authenticity message shows up only the first time you log in. Please note that the connectivity to this test machine is flaky because it is connected via wireless, so the above not working does not mean your setup is not working.
Setup the VM
Make sure openvpn is running without errors as above. Assuming you downloaded CDX-2020.ova and you have installed the latest virtualbox and guest additions, start virtualbox, drop the 'File'menu and select 'Import Appliance'. The next step is critical: Click 'Expert Mode' to reveal a screen such as this:

![Expert Mode Screen](image)

Check the box labeled 'Reinitialize the MAC address of all network cards' as shown in the figure. If you do not do this all hell will break loose: if the MAC of your NIC ends in C75A, then it will conflict with everyone else who has not reinitialized it, so check it. The result of not reinitializing is incredibly slow communication. Next, click the tiny icon to the right of thetextfield and select the downloaded ova file. Progress through the installation, clicking the obvious boxes (and not trying to customize), which takes several minutes to finish. Now find the new VM in a list on the left side of the starting screen of virtualbox, select it, drop the settings menu and select network. Make sure the setting is bridged adapter.

Click on the green arrow at the top to start the VM.

When the VM is up, you will likely see a 'Downloads' icon to the upper left, a column of icons in the left margin, and a row of small icons at the top of the screen. Click the margin icon that looks like a terminal to open a shell. Execute `ifconfig`. You will see something that looks like this:

```
eth0 Link encap:Ethernet  HWaddr 08:00:27:47:c7:5a
inet addr:10.8.0.152  Bcast:10.8.0.255  Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe47:c75a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:3768 errors:0 dropped:0 overruns:0 frame:0
TX packets:661 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:463732 (463.7 KB)  TX bytes:87036 (87.0 KB)
```
where eth0 may be tap0 or tap1. Observe that the IP address is 10.8.0.70. This must be changed. In the top row there is a network icon that is normally one up arrow next to a down arrow (indicating an established connection).

**Important**
Beginning two days before the CDX we may ask you via email to make some minor changes to the OS. If you do not make those changes the Scorekeeper might think that one or more of your services is down. Those changes will also be written on this page below.

**Hint 2**
If you are getting connection resets every 5 seconds after using

```
sudo openvpn client.conf
```

it may be caused by having an openvpn session already open. This is unlikely because the VM I gave you does not have openvpn installed. Do this to see if there is an openvpn session running:

```
pstree | grep openvpn
```

Do this to kill a running openvpn:

```
sudo killall openvpn
```

Another reason, as mentioned above, for connection resets is that you are using a socks proxy but you did not uncomment the socks-proxy line in client.conf. If there is a ';' before the socks-proxy line, remove it - but only if you are using the socks proxy.

**Hint 3**
If you can connect to the CDX network while at UC but not while outside UC's perimeter look at the 'remote' line in 'client.conf'. If it has 10.52.10.253 or 10.52.10.252 try changing it to 10.52.10.254 or boole.ececs.uc.edu and restart openvpn (hopefully via run.client).

**Hint 4**
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 host like this: nmap 10.8.0.XXX where 10.8.0.XXX is the tap0 address of your VM. The outputs should agree!

**Hint 5**
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 6**
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 7**
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 */
```

**Hint 8**
We have to have a DNS server added. Do this as root:

```
ant-get install bind9
```

The server should start on its own. Configuration is as follows:

- Download files `named.conf.local`, `db.myzone`, and `db.reverse`
- Edit the files: replace my email address with yours and 10.8.0.199 with your VM's CDX IP address. Do not use @. You can change the name of the domain, if you wish.
- Dump all three files into `/etc/bind`, overwriting the existing `named.conf.local`
- Restart the nameserver like this as root: `/etc/init.d/bind9 restart`
- **Important:** every time you edit `db.reverse` or `db.myzone` you need to add 1 to the serial number before restarting the nameserver.