Hurricane Labs

Strengthening & Protecting Linux Servers:
Top Ways to Harden Your Boxes

By: @theroxyd

whoiam

Work for @hurricanelabs doing vulnerability management and other stuff.

Yes, I purposely titled this slide as “whoiam” instead of “whoami” just to bother you.


Hurricane Labs
I Love Linux.
#1LinuxThingADay

Objectives

Let’s go over some security concepts to help you set up your servers!

Use this information to make a routine and checklist.

Hurricane Labs

10 Things

1. Restrict Access by IP

- Before any user can log in, they must send you their IP address so you can add it to a whitelist.
- **Exceptions:**
  - If the IP will change so much that it’s not worth constantly updating (you’ll have to accept risk).
  - There are too many users!
- But…maybe you can automate it!
- IPtables or UFW (Uncomplicated FireWall) would work. (https://help.ubuntu.com/community/UFW)

Hurricane Labs

UFW Demo

🙏 Ask the Demo Deities to please let this work 🙏

help.ubuntu.com/commuity/UFW

2. Data Integrity

- The integrity of your data (making sure it goes unchanged) is extremely important! Not all compromises involve loss of data.
- OSSEC (ossec.net) will notify you of any changes to files
  - e-mail
  - SIEM
- OSSEC is open source, free, and has a variety of other uses (it is a host-based Intrusion Detection System).

Hurricane Labs

3. Open Ports

- Don’t leave any ports open unnecessarily!
- Be sure to check and be aware of what is using which ports and why

Hurricane Labs

```
user@roxyd1:~$ sudo netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0    316 172.31.39.159:ssh       172.56.7.173:64697      ESTABLISHED
tcp        0      0 172.31.39.159:48970     52.94.225.236:https     ESTABLISHED
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:31297              [::]:*                  LISTEN
udp        0      0 *:bootpc                *:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    17685    /run/user/1001/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     17686    /run/user/1001/systemd/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     9119     /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     13186    /var/lib/lxd/unix.socket
unix  2      [ ACC ]     STREAM     LISTENING     13180    /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     13181    /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     13189    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     13190    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     13191    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     13278    @ISCSIADM_ABSTRACT_NAMESPACE
unix  3      [ ]         DGRAM                    8749     /run/systemd/notify
```

Hurricane Labs

```
user@roxyd1:~$ sudo netstat -atup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:ssh                   *:*                     LISTEN      1152/sshd
tcp        0      0 172.31.39.159:ssh       172.56.7.173:64697      ESTABLISHED 1568/sshd: user [pr
tcp        0      0 172.31.39.159:55592     52.94.233.158:https     ESTABLISHED 1145/amazon-ssm-age
tcp        0    332 172.31.39.159:ssh       172.56.7.173:40588      ESTABLISHED 1887/sshd: user [pr
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      1152/sshd
tcp6       0      0 [::]:31297              [::]:*                  LISTEN      1142/node
udp        0      0 *:bootpc                *:*                                 971/dhclient
```

Hurricane Labs

```
user@roxyd1:~$ sudo lsof -i
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
dhclient   971 root    6u  IPv4  12644      0t0  UDP *:bootpc
node      1142 root   10u  IPv6  16320      0t0  TCP *:31297 (LISTEN)
amazon-ss 1145 root    8u  IPv4  19278      0t0  TCP 172.31.39.159:48984->52.94.225.236:https (ESTABLISHED)
amazon-ss 1145 root   10u  IPv4  19275      0t0  TCP 172.31.39.159:56874->52.94.233.129:https (ESTABLISHED)
sshd      1152 root    3u  IPv4  14227      0t0  TCP *:ssh (LISTEN)
sshd      1152 root    4u  IPv6  14229      0t0  TCP *:ssh (LISTEN)
sshd      1568 root    3u  IPv4  17513      0t0  TCP 172.31.39.159:ssh->172.56.7.173:64697 (ESTABLISHED)
sshd      1629 user    3u  IPv4  17513      0t0  TCP 172.31.39.159:ssh->172.56.7.173:64697 (ESTABLISHED)
```

Hurricane Labs

4. SSH Configuration

Don’t use the default port - and do remember what it is.

Restrict user access by putting them in a special directory. (https://www.cyberciti.biz/faq/debian-ubuntu-restricting-ssh-user-session-to-a-directory-chrooted-jail/)

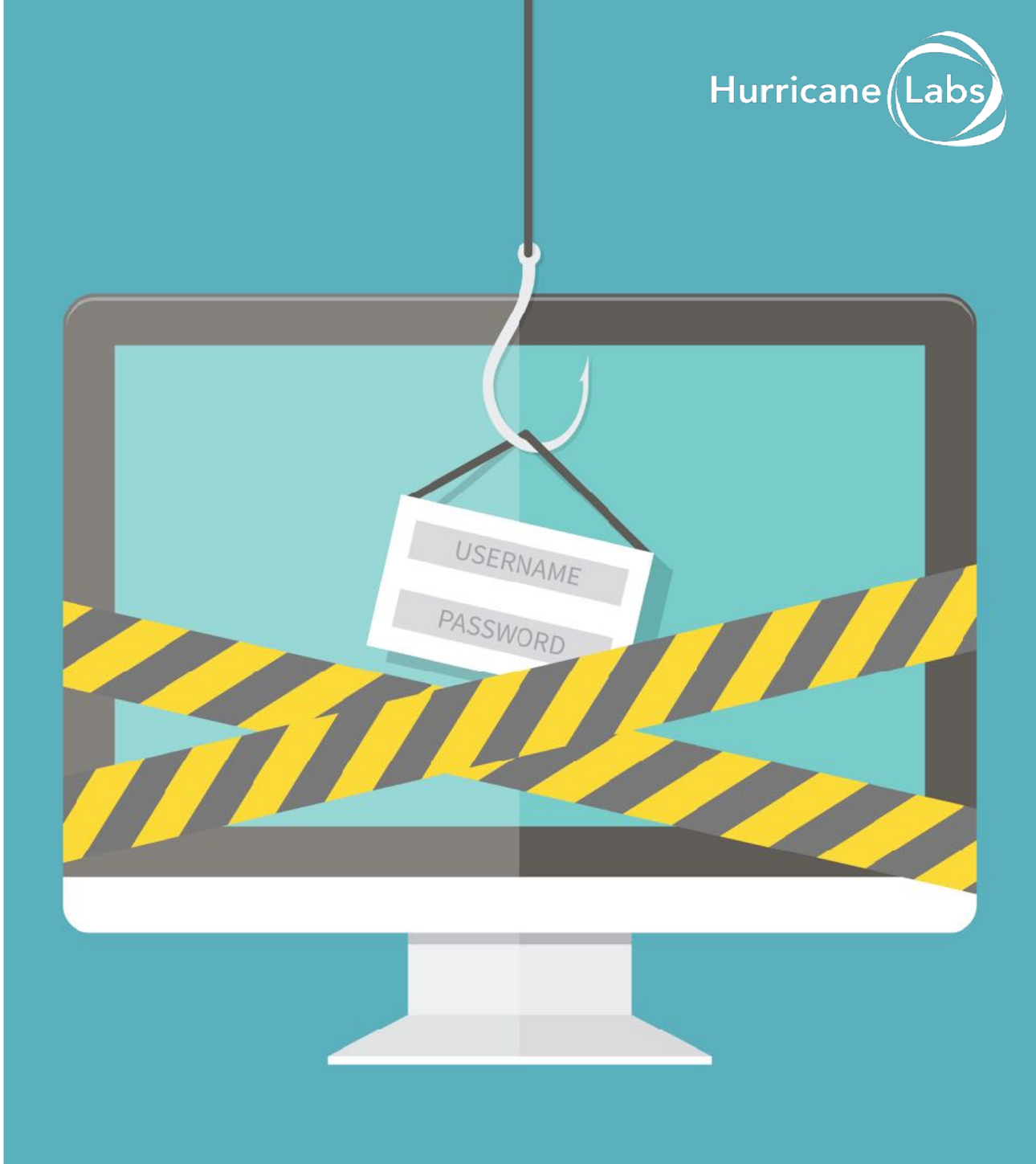
Hurricane Labs

SSH Config Demo

🙏 Ask the Demo Deities to please let this work 🙏

5. Logins

- Be aware of who is logging in.
- Just because everything seems okay, don’t assume!
- lastlog
- You can use OSSEC rules to notify you of suspicious login activity.



Hurricane Labs

6. Updates

Schedule updates and restarts.

Use CRON.

Don’t rely on yourself to remember
(I’m extremely guilty of this one).

7. Logging

If there’s no logs then…there’s no indication of compromise.

You need to know what happened when incidents occur.

Open Source: ELK stack; greylog

Splunk - there’s a free version and you can follow the guide on Hurricane Labs’ blog post:
“From Zero to Splunk…”

Hurricane Labs

8. Backup Schedule

- If data is not available, it is not secure. Keep a backup of data on another server or on a device stored separately.
- Schedule it!

9. Permissions

- Least privilege required.
- Audit users and permissions at least quarterly.
- OSSEC can alert you to changes.
- Document how you want things to happen on the server and make it available to all users.
- Even the BEST sysadmins make mistakes. Encourage them to use the documentation.

Hurricane Labs

10. Passwords

- Make a password policy!
- PAM

Hurricane Labs

Bye!

Get into a routine.

Experiment with different routines.

Document and share!

Q&A Time

List of all my www things:

roxyd.github.io

Email me!
roxy@hurricanelabs.com