CentOS E-Comm: Charlton

Ubuntu DB/MySQL: Ryan

Fedora Mail: Peter

QRadar: Martin

Martin is supposed to help with Windows if Matt is out of room.

When not doing QRadar he can:

SSH into three Linux servers and do IPTABLES.

Deploy the Ubuntu16 vm (hopefully during first two hours)

Deploy TENS

Injects like ClamAV, NMap, Mediawiki

# Fedora DB Strategy

Overall:

* Change local user passwords (root, any other)
* Dump database
* Backup etc
* Update SSH Config
* Kill Unneeded Listening Processes & Connections
* Disable IPv6
* Secure MySQL
* Update Web App Passwords
* Re-dump database
* Turn on Firewall
* Update change control forms
* Check Application Version/Exploits
* Check Config Files
* Check MySQL Permissions

Change local user passwords:

$ passwd

$ passwd otheruser

Dump Database:

$ mkdir /backup

$ chmod g+s /backup

$ chmod 600 /backup

$ mysqldump -u root -p --all-databases > /backup/mysql.dump

$ tar -zcP /backup/mysql.dump | openssl enc -aes-256-cbc -e > /backup/mysql.dump-pwd#.tar.gz.enc

$ # Verify

$ rm /backup/mysql.dump

Backup etc (run in background, takes a while):

$ tar -zcP /etc > openssl enc -aes-256-cbc -e > /backup/etc-pwd#.tar.gz.enc

Update SSH Config:

$ yum remove vim-minimal

$ yum install vim

$ mkdir -p ~/.ssh

$ echo '<public-key>' > ~/.ssh/authorized\_keys

$ cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.bak

$ vim /etc/ssh/sshd\_config

> PasswordAuthentication no

$ systemctl restart sshd

Kill Unneeded Listening Processes & Connections:

$ netstat -planet

$ kill -9 <pid>

Disable IPv6:

$ sysctl -w net.ipv6.conf.all.disable\_ipv6=1

$ sysctl -w net.ipv6.conf.default.disable\_i pv6=1

Secure MySQL:

$ mysql\_secure\_installation

Update Web App Passwords:

$ mysql -u root -p

> use mysql;

> select user,password,host from user;

> update user set password=PASSWORD("<new-password>") where user="<web-app>";

> flush privileges;

Re-dump Database:

$ mysqldump -u root -p --all-databases > /backup/mysql.dump

$ tar -zcP /backup/mysql.dump | openssl enc -aes-256-cbc -e > /backup/**mysql.dump.new**-pwd#.tar.gz.enc

$ # Verify

$ rm /backup/mysql.dump

Firewall:

systemctl disable firewalld

systemctl stop firewalld

iptables -F

iptables -A INPUT -p tcp --dport 3306 -s 192.168.1.25 -j ACCEPT

iptables -A INPUT -p tcp --dport 3306 -s 192.168.1.20 -j ACCEPT

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -s <ip of martin host> -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -s <ip of my host> -j ACCEPT

iptables -A INPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p tcp --sport 443 -j ACCEPT

iptables -A INPUT -p udp --sport 53 -j ACCEPT

iptables -A INPUT -j DROP

iptables -A OUTPUT -p udp --sport 53 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 -d <ip of my host> -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 -d <ip of martin host> -j ACCEPT

iptables -A OUTPUT -p tcp --sport 3306 -d 192.168.1.25 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 3306 -d 192.168.1.20 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

iptables -A OUTPUT -p udp --dport 53 -j ACCEPT

iptables -A OUTPUT -j DROP

iptables-save > /etc/sysconfig/iptables

systemctl enable iptables

**Update Change Control!**

Change control headers:

1st tab:

Unique ID: Branch DB

OS/Service/IP: Fedora 20, MySQL & DNS, 192.168.1.15

2nd tab:

Unique ID: Branch Ecom

OS/Service/IP: CentOS 5, Ecommerce, 192.168.1.20

3rd tab:

Unique ID: Branch Mail

OS/Service/IP: Ubuntu 14, SSH & SMTP & POP3, 192.168.1.25

4th tabb:

Unique ID: QRadar

OS/Service/IP: OS??, QRadar, IP??

Check Application Version/Exploits:

$ mysql -V

Compare against:

Ver 15.1 Distrib 5.5.43-MariaDB, for Linux (x86\_64) using readline 5.1

$ named -v

Compare Against: BIND 9.9.4-P2-RedHat-9.9.4-18.P2.fc20

Check Configuration Files:

* /etc/sudoers & /etc/sudoers.d/\*
* /etc/pam.d/\*
* /etc/cron.\* & crontab -l
* /etc/fstab
* /etc/host
* /etc/resolv.conf
* /etc/group

Check MySQL Permissions:

> show grants for 'user'@'host';

> revoke all privileges on \*.\* from 'user'@'host';

> grant all privileges on \*.\* to 'user'@'host';

> flush privileges;

**Update Change Control!**

Misc Security:

* Make sure MySQL and Bind are not running as root
  + ps aux | grep mysql
  + ps aux | grep bind
* Change log locations, make sure turned on
  + Backup my.cnf & named.conf
  + MySQL (my.cnf): log = /var/log/mysql-queries.log
  + MySQL (cmd): chown mysql:mysql /var/log/mysql-queries.log
  + Bind (/etc/bind/named.conf): include "/etc/bind/named.conf.log";
  + Bind (/etc/bind/named.conf.log):

logging {

channel bind\_log {

file "/var/log/bind/bind.log" versions 3 size 5m;

severity info;

print-category yes;

print-severity yes;

print-time yes;

};

category default { bind\_log; };

category update { bind\_log; };

category update-security { bind\_log; };

category security { bind\_log; };

category queries { bind\_log; };

category lame-servers { null; };

};

* + Bind (/etc/logrotate.d/bind):

/var/log/bind/bind.log {

daily

missingok

rotate 7

compress

delaycompress

notifempty

create 644 bind bind

postrotate

/usr/sbin/invoke-rc.d bind9 reload > /dev/null

endscript

}

* + Bind (cmd):

mkdir /var/log/bind

chown bind:bind /var/log/bind

service bind9 restart

logrotate -d /etc/logrotate.d/bind