Debian - Wkstn

- □ Changed default passwords & notified team leads
- □ Checked for online users
  - □ Kicked and notified team leads if applicable
- □ Checked user permissions
- □ Checked open ports/processes
- □ Made Back-Ups
  - □ mkdir /root/bu
- □ Checked sudoers

Ubuntu Web Svr - APACHE

- □ Changed default passwords & notified team leads
- □ Checked for online users
  - □ Kicked and notified team leads if applicable
- □ Checked user permissions
- □ Checked open ports/processes
- □ Made Back-Ups
  - □ mkdir /root/bu
  - □ `/var/www` - Apache
- □ Checked sudoers

Ubuntu Wrkstn

- □ Changed default passwords & notified team leads
- □ Checked for online users
  - □ Kicked and notified team leads if applicable
- □ Checked user permissions
- □ Checked open ports/processes
- □ Made Back-Ups
  - □ mkdir /root/bu
- □ Checked sudoers

Splunk

- □ Changed default passwords & notified team leads
- □ Checked for online users
  - □ Kicked and notified team leads if applicable
- □ Checked user permissions
- □ Checked open ports/processes
- □ Made Back-Ups
  - □ mkdir /root/bu
  - □ `/opt/splunk` - Splunk
- □ Checked sudoers

CentOS

- □ Changed default passwords & notified team leads
- □ Checked for online users
  - □ Kicked and notified team leads if applicable
- □ Checked user permissions
- □ Checked open ports/processes
- □ Made Back-Ups
  - □ mkdir /root/bu
  - □ - Mail Server
- □ Checked sudoers

Fedora

- □ Changed default passwords & notified team leads
- □ Checked for online users
  - □ Kicked and notified team leads if applicable
- □ Checked user permissions
- □ Checked open ports/processes
- □ Made Back-Ups
  - □ mkdir /root/bu
  - □ `/var/log/dovecot` - Mail Server
- □ Checked sudoers

BACK-UP:

```
cp {{PATH_TO_DIR}} /root/bu/{{DIR_NAME}}-{{#}}
```

Check online userrs:

```
who -u
```

Kick users by name:

```
sudo pkill -HUP -u {{USERNAME}}
```

User perms:

```
cat /etc/passwd
cat /etc/sudoers
```

Open ports:

```
sudo netstat -tulpn | grep LISTEN
sudo nmap -sT -O localhost
Close Service:
sudo systemctl stop sshd OR service sshd stop OR kill PID
```

File access:

```
ls -l {{File}}
```

Cron:

```
cat /var/spool/cron/crontabs (or similar)
```

Watch:

```
#To watch the contents of a directory change, you could use
 watch -d ls -l
```

Backup: