Appsec: Full initial checklist

Further description of topics covered

Type of Systems: Linux
Necessary Skills: Linux admin, Checklist Sheet
Complete Goal: Obtain the best balance of security and efficiency in first ~hour or so
ONE PERSON per network: `nmap -sV <network> AND nmap -Pn <network>`
Steps on your workstation:

1. Make note of what is scored on the machine, and what other services are noted in the topology. Also note other services on topology
2. Go to parts A and B, C if possible/necessary, in Linux Server Checklist.
3. Secure SSH
   a) Turn off SSH if it's not scored, and a locally accessible machine.
   b) check for ssh keys in ~/.ssh/authorized_keys
   c) whitelist users in /etc/sshd_config: AllowUsers <user>@<hostname or ip>

----------Stop and do steps 1 and 2 in "other machines" ----------

4. If your workstation doesn't have a GUI, install it sometime around here (or don't)
5. Wicked Quick Linux firewalls as soon as possible.

----------Whoever gets to this point first should start on ELK ----------

6. Install Filebeat, and possibly auditd turn on Auditd module
7. When you have a moment later on, do D and E in Nick's Linux Server Checklist, as well as make sure (checking with team members) that all important services credentials have been updated.

Steps on other machines you're responsible for:

1. Make note of what is scored on the machine, and what other services are noted in the topology. Also note other services on topology
2. Go through parts A and B, C if the machine is running any services, in Linux Server Checklist.
3. Wicked Quick Linux firewalls ASAP
4. Install Auditd and Filebeat, turn on Auditd module
5. When you have a moment later on, do D and E in Nick's Linux Server Checklist, as well as make sure (checking with team members) that all important services credentials have been updated.
6. For any web servers, make sure to change credentials on the website