Cleaning Linux Box Checklist

NOTE: If you need to remove anything in the below steps, do NOT delete it. Simply zip up the file or directory and leave it in the same directory it was found in.

During Prep:

- ❑ Look for users that are not in the default configuration in the /etc/password file.
- ❑ Change default creds that are given to blue teams
- ❑ Check which users have passwords by looking at the /etc/shadow file.
    - ❑ The “nobody” user should not have a password in most cases.
    - ❑ The “games” user should not have a password in most cases.
    - ❑ The “www-data” user should not have a password in most cases.
    - ❑ The “backup” user should not have a password in most cases.
- ❑ Look in the home directory for every user for files that are out of place. For example, a file called “reset.sh”.
- ❑ Look for home directories for users that aren’t users on the box. These directories should most likely not be there.
- ❑ Verify that only certain users can SSH onto the box by checking the SSH config at /etc/ssh/sshd_config.
    - ❑ Verify that every user needs to put a password in to SSH.
    - ❑ Verify that there isn’t a rule in there that allows every user to SSH. Note: You can make specific rules to make it so specific people or groups can SSH onto the box.
- ❑ Find if there are any SSH keys on the box.
    - ❑ Check if there are any unnecessary or unknown SSH keys in /root/.ssh
    - ❑ Try SSHing into the box and verify that you can’t do it with every user.
    - ❑ Check if there are any Putty SSH keys by checking the /root/.putty/sshostkeys file.
- ❑ Check who is listed as a sudo user by checking /etc/sudoers.
    - ❑ Verify that not all the users have sudo privileges. If this is the case, add rules for individual groups or users rather than having this blanket rule.
    - ❑ Verify that no user can run sudo without providing a password.
- ❑ Check for any files that have setuid permissions. If you find any that have this permission level, their permissions need to be demoted if it is possible.
- ❑ Kill all running processes when making changes to see if there are persistence steps in place. Running the “pstree” command will show you all running processes. Use “kill” to kill off processes.
    - ❑ Particular focus on network services. Use “Netstat -tulapn/ss -IForgetTheFlags” or “netstat -tulpan”

- ❏ Skim through the /root directory for any suspicious looking files or directories.
- ❏ Look through the cron jobs to see if there are any cron jobs that look malicious.
    - ❏ Check the /etc/cron.hourly directory
    - ❏ Check the /etc/cron.daily directory
    - ❏ Check the /etc/cron.monthly directory
- ❏ Setup SSH keys for every user on the blueteam.
- ❏ Check for scripts in systemd/init
- ❏ Add authentication through an active directory if the scenario allows and your team chooses to do that. If you add AD authentication, remove all users that aren't needed besides root and a user for the blue team members to log in with.
- ❏ Use LinEnum (https://github.com/rebootuser/LinEnum) to verify you've cleaned everything.
- ❏ Run nmap on the box if it isn't a SCADA device and the competition allows it.
- ❏ Check for malicious scripts in the /etc/rc.local directory
- ❏ Check that users are not able to SSH into the box using the root account.

Right Before Competition:

- ❏ Change passwords for all users unless the scenario restricts it.
- ❏ Kill all processes on the box and reboot the box.

NOTE: This checklist is only there to get you started. There may be other things wrong with the box.

Make sure only the required services are running at any given time.