CCDC PlayBook

AUGUSTA
UNIVERSITY

Contents

Windows

Linux

Checklist

- Uninstall netcat (sudo apt-get remove netcat)
- Users and Groups
  - Make new users
    - Useradd <username> -G sudo
    - Log into new user
    - Lock root with “usermod –L root”
  - Who has been using this machine?
  - Try to see if you can determine the point scorer using “host <insert scorer server name>” also dont kick yourself.
    - who / w
    - Last
    - You can kick a user using “pkill -9 –t <pts/# or tty#>”
  - /etc/passwd (passwd stores general user info)
    - uid/gid == 0 (Look for users have this but should not)
      - grep ":0:" /etc/passwd
    - Home Directories
    - Shells
      - Verify for who has bash with “cat /etc/passwd | grep bash”
      - Change their shell with “chsh -s /usr/bin/nologin <user>"
      - You can also lockout an account with “usermod –L <user>”
  - /etc/shadow (stores user passwd info)
    - Users with Passwords
    - Locked Accounts (locked accounts have !)
  - /etc/group
    - sudo, wheel, adm, etc
    - You can just delete the users with nano from groups
  - /etc/suoders{.d/*}
    - Use sudo visudo and comment out ones stating with sudo
    - Then add “<username> ALL=(ALL:ALL) ALL” under members of group sudo
  - PAM
    - /etc/pam.conf
    - /etc/pam.d/* (common.auth is a good one)
      - fallback should be pam_deny.so
  - Shell Configs
    - {.bashrc,.profile,.bash_profile}
    - /etc/bash.bashrc
    - alias
    - PATH
- File Persmissions
  - SUID/SGID files
    - find / -type f -executable -perm –{4,2,6}000
      - chmod –s <file> to remove setID
      - Should not be there (cat, zsh, false, nologin, non /usr/bin/bash)
  - World-writable files
    - find / -xdev -perm -o+w \(-type f -or -type d \)

        - Chmod the file to appropriate permissions (660) to remove others
- Network
    - Network Interfaces
        - Ifconfig
        - Ip -c a
    - Firewall
        - Iptables -L
        - nft list tables
        - ufw status
    - Open Ports
        - netstat -pant
        - ss -lpnt
- Processes
    - ps auxf
    - pkill -{u,g}
    - systemctl list-timers
    - systemctl list-units
- Services
    - SSH
        - authorized keys
            - find / -name authorized_keys*
        - /etc/sshd/sshd_config
            - PermitRootLogin no
            - PubkeyAuthentication / AuthorizedKeysFile
            - PasswordAuthentication
            - PermitEmptyPasswords no
            - AllowTcpFowarding
    - Cron
        - /etc/crontab
        - /etc/cron.*/*
        - /var/spool/cron/crontabs/*
    - Apache / PHP
        - ls -l /etc/apache2/*-enabled/
        - php.ini
            - disable_functions
            - open_basedir
        - find /var/www/ -name .htaccess
- Hardening
    - Run updates/upgrades
    - Configure a firewall
    - Package manager verify file checksums
        - Sha256sum <file>
    - Fail2Ban
    - Harden config files as needed
- Cheap Tricks
    - Install zsh, cronjob ***** pkill bash
    - chmod000 $(which,nc,wget,curl,sudo,...)
    - chattr +i /etc/{passwd,shadow,sudoers,...}

- SSH Forcecommand

User Management

Adding a User

To add a new user, you can use the useradd command followed by the username. For example, to add a user named newuser, you would use:

```
sudo useradd newuser
```

You can then set a password for the new user with the passwd command:

```
sudo passwd newuser
```

Deleting a User

To delete a user, you can use the userdel command. If you want to remove the user's home directory and mail spool, use the -r option. For example:

```
sudo userdel -r olduser
```

Modifying a User

The usermod command allows you to change a user's attributes. For example, to change a user's login name:

```
sudo usermod -l newname oldname
```

Viewing User Information

To view information about a user, you can use the id command:

```
id username
```

This will display the user's UID, GID, and the groups they belong to.

Managing User Groups

To add a user to a group, use the usermod command with the -aG option:

(Use this if you wish to add a user to the sudo group)

```
sudo usermod -aG groupname username
```

To remove a user from a group, use the gpasswd command with the -d option:

```
sudo gpasswd -d username groupname
```

Locking/Unlocking Account

```
usermod (-L/-U) <username>
```

File Permissions

Summary

- **r**(ead) has the value of **4**
- **w**(rite) has the value of **2**
- (e)**x**(ecute) has the value of **1**
- **no permission** has the value of **0**

The privileges are summed up and depicted by one number. Therefore, the possibilities are:

- **7 –** for read, write, and execute permission
- **6 –** for read and write privileges
- **5** – for read and execute privileges
- **4** – for read privileges

Change file permissions

```
chmod ### <file>
```

File Immutability

Check for file Immutability

`lsattr <file>` look for an “i”

Edit file immutability

```
chattr i <file>
```

SSH

View Authorized SSH Keys:

```
cat ~/.ssh/authorized_keys
```

This command displays the authorized keys for the currently logged-in user.

Deleting SSH Keys:

To remove an SSH key, you can edit the authorized_keys file manually or use the following command:

```
ssh-keygen -R <hostname|ip>
```

The public key(s) associated with the specified server will be removed from the authorized_keys file.

FTP

Installation

```
sudo apt install vsftpd
```

Managing the Service

```
sudo systemctl (enable/start/stop/status) vsftpd
```

Configure vsftpd:

```
sudo nano /etc/vsftpd.conf
```

Customize settings as needed:

Set anonymous_enable=NO to disable anonymous access.

Configure user-specific settings (e.g., local_enable=YES).
Optionally, enable SSL/TLS for secure connections.

Apache

Installation

```
sudo apt install apache2
```

Managing the Service

```
sudo systemctl start apache2
sudo systemctl stop apache2
sudo systemctl restart apache2
```

Config Files

Main configuration file: `/etc/apache2/apache2.conf`

Virtual host files: `/etc/apache2/sites-available.`

Content

Replace the default content in the htdocs folder with your own website files.

Edit the index.html file to display your content.

Fail2ban

Installation

```
sudo apt install fail2ban
```

Make backups of config files

```
sudo cp /etc/fail2ban/fail2ban.conf /etc/fail2ban/fail2ban.local
        sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

If you want to make any changes for any jail (or for all the jail), like the maximum retries, ban time, find time etc., you should edit the jail.local file.

Check status of sshd jail

```
sudo fail2ban-client status sshd
```

Enable and start the service

```
        systemctl start fail2ban
        systemctl enable fail2ban
```

Check Status of the service

```
systemctl status fail2ban
```

To Check Logs

```
cat /var/log/fail2ban.log
```

Lynis System Checker

Installation

```
sudo apt install lynis
```

Run a scan

```
lynis audit system
```

Logs can be found at

```
Test and debug information     /home/<user>/lynis.log
```

Report data: /home/<user>/lynis-report.dat

ClamAV

Installation

```
sudo apt install clamav
sudo freshclam (might error, but this updates the virus database)
```

Running a Scan

```
    sudo clamscan -r /path/to/scan
```

Snoopy

Installation

```
    wget -q -O install-snoopy.sh https://github.com/a2o/snoopy/raw/install/install/install-snoopy.sh &&
    chmod 755 install-snoopy.sh &&
    ./install-snoopy.sh stable
```

Restart terminal to test it

Logs can be found at

CentOS, /var/log/secure,
Debian, /var/log/auth.log,
Ubuntu, /var/log/auth.log,
(others), /var/log/messages, (potentially, could be elsewhere)

You can do a constant check using watch –n 1 <command> | grep –v <unwanted command>

One important example of this command is

```
    watch -n 1 ss -anpt | grep <ip to look for> | grep ESTAB | grep –v <ip to ignore>
```

Other comannds i find neat

ps -aef –forest (lets you see proccess in a forsest view)