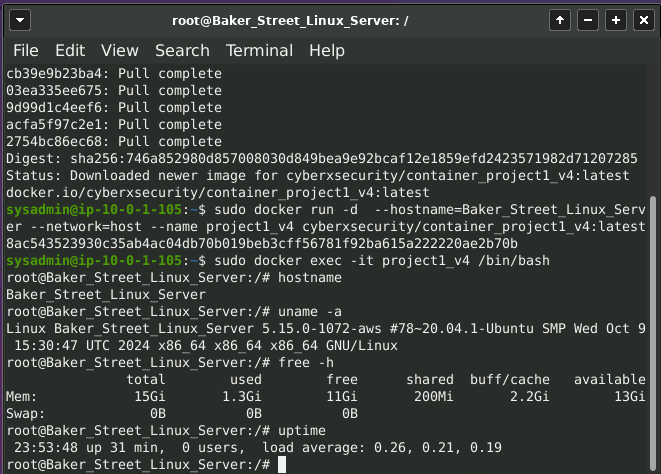


**OS Information**

| Customer | Baker Street Corporation |
| --- | --- |
| Hostname | **Hostname**  **Baker\_Street\_Linux\_Server** |
| OS Version | **uname -a**  **Linux Baker\_Street\_Linux\_Server 5.15.0-1072-aws #78~20.04.1-Ubuntu SMP Wed Oct 9 15:30:47 UTC 2024 x86\_64 x86\_64 x86\_64 GNU/Linux** |
| Memory information | **free -h**  **total used free shared buff/cache available**  **Mem: 15Gi 1.3Gi 11Gi 200Mi 2.2Gi 13Gi**  **Swap: 0B 0B 0B** |
| Uptime information | **Uptime**  **23:53:48 up 31 min, 0 users, load average: 0.26, 0.21, 0.19** |



**Checklist**

| **Completed** | **Activity** | **Script(s) used / Tasks completed / Screenshots** |
| --- | --- | --- |
|  |  |  |
|  | OS backup | * + *sudo tar -cvpzf /baker\_street\_backup.tar.gz --exclude=/baker\_street\_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /*   Created a backup of the file systems while excluding areas not pertinent to the backup.  Screenshot: |
|  | Auditing users and groups | Removed all staff who have been **terminated** and also removed all home directories and files:  cat /etc/passwd  Terminated list:  **lestrade**  **irene**  **mary**  **gregson**  sudo userdel -r lestrade  sudo userdel -r irene  sudo userdel -r mary  sudo userdel -r gregson      Locked all user accounts of staff on **temporary leave**:  LOA List:  **moriarty**  **mrs\_hudson**  sudo usermod -L moriarty  sudo usermod -L mrs\_hudson    Unlocked any users who are **employed**:  Current Staff List:  **sherlock**  **watson**  **mycroft**  **toby**  **adler**  sudo passwd -u sherlock  sudo passwd -u watson  sudo passwd -u mycroft  sudo passwd -u toby  sudo passwd -u adler  Also set a password for any users who could not be unlocked due to having no initial password:  sudo passwd toby  sudo passwd adler    Checked to move all the employees who were in the marketing department to a new group called **research**. Created this group since it doesn't exist:  sudo groupadd research  getent group marketing    Nobody is in marketing as shown by marketing:x:1014:  The command to add someone from marketing to research would be in the format:  sudo usermod -aG research name1  Removed the marketing group as the marketing department was closed this year:  sudo groupdel marketing  Screenshot: |
|  | Updating and enforcing password policies | Edited the file: **/etc/pam.d/common-password**  sudo nano /etc/pam.d/common-password  Updated requirements for secure passwords:  **minlen**: Minimum length 8 characters.  **dcredit**: No digits are required  **ucredit:** At least one uppercase character required  **lcredit**: At least 6 lowercase characters required  **ocredit:** At least one special character required  **retry**: Allow two retries if the user enters a bad password.  So updated the entry as:  password requisite pam\_pwquality.so minlen=8 ucredit=-1 ocredit=-1 retry=2  Screenshot: |
|  | Updating and enforcing sudo permissions | Check which users have sudo:  getent group sudo    Check contents of the sudoers file:  sudo cat /etc/sudoers    Edit sudoers:  Sudo visudo    Sherlock can have all sudo:  sherlock ALL=(ALL:ALL) ALL  Removed any other entries giving sudo access that is not expressed.  Watson and Mycroft should only have sudo privileges to run a script located here:  /var/log/logcleanup.sh  watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh  mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh  All employees who belong to the **research** group should have sudo privileges to run the following script:  /tmp/scripts/research\_script.sh  %research ALL=(ALL) NOPASSWD: /tmp/scripts/research\_script.sh  Screenshots: |
|  | Validating and updating permissions on files and directories | There should be no files that have any world permissions to r, w, x:  sudo find /home -type f -exec chmod o-rwx {} \;    Find executable scripts:  sudo find -iname '\*engineering\*' -exec chown :engineering {} +    sudo find -iname '\*research\*' -exec chown :research {} +    sudo find -iname '\*finance\*' -exec chown :finance {} +    Set permissions:  sudo chmod 770 /tmp/scripts/\*engineering\*  sudo chmod 770 /tmp/scripts/\*research\*  sudo chmod 770 /tmp/scripts/\*finance\*    Search for files containing passwords:  sudo grep -r -i -l 'password\|passwd\|secret\|login' /home  Did not find any user created files - only some system files:    If any files happen to be found in the future, remove with command:  sudo rm /path/to/found\_file  Exit:  **sshd** |
|  | Optional: Updating password hashing configuration |  |
|  | Auditing and securing SSH | Configured SSH to **not** allow the ability to: SSH with empty passwords, SSH with the root user, SSH with any other ports besides 22. As well, enable SSH protocol 2.  sudo nano /etc/ssh/sshd\_config    Add/revise entries:  PermitEmptyPasswords no    PermitRootLogin no    Port 22    Enabled the SSH protocol 2:  Protocol 2  (also shown: closed 4 additional ports 2222-2225 to leave only Port 22 open)    Allowed only the current active staff to SSH:  **sherlock**  **watson**  **mycroft**  **toby**  **Adler**  Saved the sshd\_config file    Restarted the SSH service to apply changes:  sudo service ssh restart  Screenshots: |
|  | Reviewing and updating system packages | Ran sudo *apt update*      Ran sudo apt upgrade -y    Use apt list –installed to place all installed packages into a new file:  apt list --installed > package\_list.txt  cat package\_list.txt    Check if telnet and/or rsh-client is in the list. Yes they are both installed:      Remove unwanted packages: telnet and rsh-client  sudo apt remove telnet rsh-client -y    Telnet should be removed because a more secure protocol SSH is now the standard. Telnet can be easily used by a bad actor to transmit data without encryption. Eavesdropping and packet sniffing are easily done.  https://www.ssh.com/academy/ssh/telnet  RSH is also outdated because it is also unencrypted and can be used in IP spoofing and ARP hijacking attacks  https://www.beyondsecurity.com/resources/vulnerabilities/rsh-detection  Cleaned up dependencies:  sudo apt autoremove -y    Installed 3 packages as requested:  sudo apt install ufw lynis tripwire -y    Hardening features:  UFW (Uncomplicated Firewall). By default UFW will deny incoming connections unless set to be allowed. You can also set rules for ports and subnets to deny or allow traffic. Logging features for auditing and checking for intrusion attempts. Can also limit rapid incoming traffic that may represent a brute force attack.  Lynis. This Linux security software will audit the server for configuration of the operating system and running services. Can audit password policies and sudo permissions in case they are incorrect. You can also review file permissions and check software packages for the newest version. All of this will harden the server against attack.  Tripwire. Can check for unauthorized changes to important files and directories and when and by who. Similar to Varonis in Windows. Can alert IT when a breach has occurred and records the logs for auditing. |
|  | Disabling unnecessary services | List all services and redirect to a file:  service --status-all > service\_list.txt    Identify if any of the following services are running and stop, disable and remove them:  mysql  samba  Check the status:  sudo service mysql status  (Mysql service is Stopped)    sudo service samba status  (samba is an unrecognized service)    Tried again:  sudo service smbd status  Smbd (samba) service is Running.        Stop the services:  sudo service mysql stop  sudo service smbd stop    Disable the services:  sudo service mysql disable  sudo service smbd disable    Remove the packages:  sudo apt remove mysql-server -y    sudo apt remove samba -y      Remove any dependencies:  sudo apt autoremove -y |
|  | Enabling and configuring logging | Access */etc/systemd/journald.conf*  Edit the file:  sudo nano /etc/systemd/journald.conf    Set “**storage=persistent”**  Set “**systemMaxUse=300M”**  Save settings  Screenshot:      Access /etc/logrotate.conf  sudo nano /etc/logrotate.conf  Changed the log rotation from weekly to daily:    Adjusted line to: daily  Rotated out the logs after 7 days:    Adjusted the line to: rotate 7    Save settings  Screenshot:    Exit |
|  | Scripts created | nano hardening\_script1.sh        chmod +x hardening\_script1.sh  ./hardening\_script1.sh  Script Day 1 Results:      nano hardening\_script2.sh      chmod +x hardening\_script2.sh  ./hardening\_script2.sh  Script Day 2 Results: |
|  | Scripts scheduled with cron | crontab -e  Set schedule for Day 1 scripted activities to run once a month on the first of the month  0 0 1 \* \* /hardening\_script1.sh  Set schedule for Day 2 scripted activities to run once a week, every Friday  0 0 \* \* 1 /hardening\_script2.sh  crontab -l |

Summary of Key Findings

Security Analyst: Kevin Arnold

Date: January 6, 2025

This cybersecurity assessment checked a wide scope of critical infrastructure for the Baker Street Corporation (BSC) including BSC’sLinux server’s users, groups, files, and directories. Next, a close examination of the SSH, system packages, services, and logging configurations was conducted. Finally, the needed tasks were scripted and scheduled routinely for the future-proofing all the improvements.

As requested, the necessary updates have been conducted to ensure a hardened Linux system and overall organization security.

By proactively addressing some security concerns, BSC has set a new standard for their security policies and greatly diminished the risk of data breaches on their Linux server.

Detailed Findings

Users, Groups and Permissions

Users and groups were examined and cleaned up to current levels. This reflects a new principle of least privilege for BSC - to have only the current staff with valid user accounts and as well, those accounts having access to only the minimal required data. Extra accounts lingering on the network have been removed, so can no longer be potentially used by cyber criminals to access protected data.

It was important to remove any access from current accounts having high levels of access to prevent unauthorized access. Especially for sudo access and only Sherlock has ALL sudo access.

Only the research, engineering and finance groups remain and have appropriate membership. The risk of users assigned to unintended groups can lead to access to sensitive files, resources and data leakage. An attacker who compromises one account can move laterally within the system if they have access to several groups. This can lead to modifying critical services and cause organizational downtime.

Since there should be no files that have any world permissions to read, write and execute, this was addressed and mitigated. The risks of having the files open in such a way can lead to anyone on the system having that access and changing config files. As well, if the file is a script and owned by a privileged user, others can modify it to execute malicious commands. It is recommended to educate users of the risks of placing too much permission on the files.

Packages and Services

Applications have been checked and updated. Telnet and RSH have been removed because of their weak security.

Telnet was removed because a more secure protocol SSH is now the standard. Telnet can be easily used by a bad actor to transmit data without encryption. Eavesdropping and packet sniffing are easily done.

https://www.ssh.com/academy/ssh/telnet

RSH is also outdated because it is also unencrypted and can be used in IP spoofing and ARP hijacking attacks.

https://www.beyondsecurity.com/resources/vulnerabilities/rsh-detection

SSH has been secured to **not** allow the ability to: SSH with empty passwords, SSH with the root user, SSH with any other ports besides 22. As well, enabled SSH protocol 2. (Additional ports 2222-2225 and only Port 22 remain open). The risks of having other ports open invite malicious attackers to connect to the network, bypassing firewalls and in fact modifying the SSH configurations . Once modified, they can allow password-based login to the network resources.

As requested three packages have been installed to further protect the BSC infrastructure:

UFW (Uncomplicated Firewall). By default UFW will deny incoming connections unless set to be allowed. You can also set rules for ports and subnets to deny or allow traffic. Logging features for auditing and checking for intrusion attempts. Can also limit rapid incoming traffic that may represent a brute force attack.

Lynis. This Linux security software will audit the server for configuration of the operating system and running services. Can audit password policies and sudo permissions in case they are incorrect. You can also review file permissions and check software packages for the newest version. All of this will harden the server against attack.

Tripwire. Can check for unauthorized changes to important files and directories and when and by who. Similar to Varonis in Windows. Can alert IT when a breach has occurred and records the logs for auditing.

MySQL and samba have been removed and their services stopped due to the severity of risk that these two packages pose. MySQL invites unauthorized access through brute force, trying common credentials. It can be used for SQL injection whereby attackers can execute arbitrary SQL commands and extract sensitive data. Also Denial of Service (DoD) risks because purposefully causing excessive requests can cause MySQL to crash.

Likewise, Samba introduces the risk of Man in the MIddle (MitM) attacks. Without encryption, attackers can intercept or modify SMB traffic.

Logging

The logging with journald.conf was checked and updated with sufficient retention. In the event of a security breach, these logs will be important for the investigation. If logs are kept indefinitely, it will eventually lead to a lack of disk space and causing critical services to fail.

Conclusion

A variety of security aspects were checked and mitigated. It is recommended to continue running the scheduled scripts that have been supplied and periodically repeat the audit on a regular basis. When there are organizational changes to users, groups, files, directories, packages and tools, it will impact the overall security strategy. User education is important and it is recommended to do regular user training and testing to ensure a healthy network.