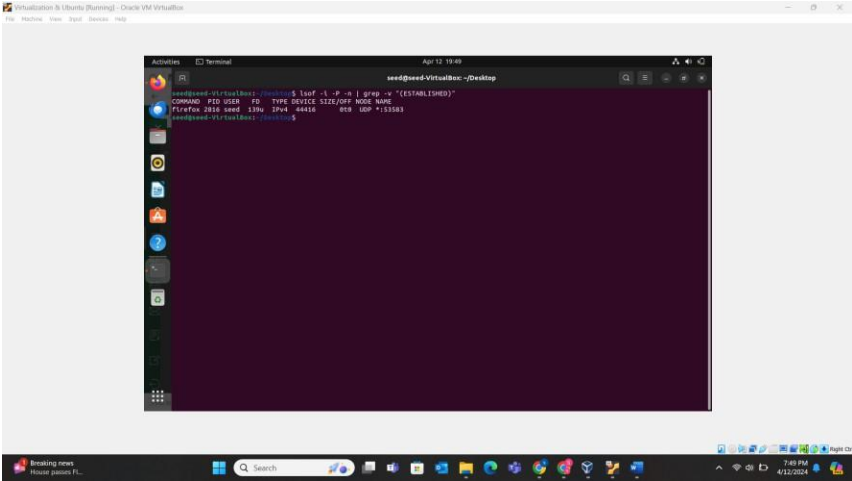


Saeed Rafee
Security Control Synopsis

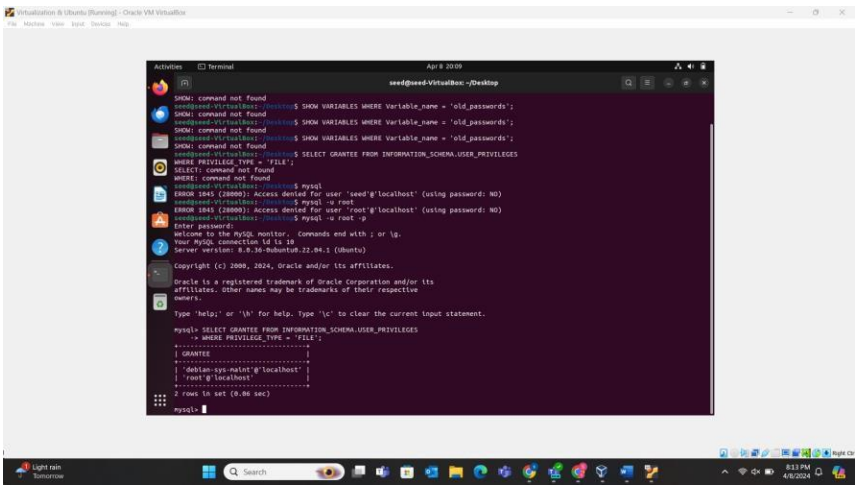
Objective:

This project presents my hands-on evaluation of 10 essential security controls implemented in a LAMP stack environment. Each control is based on established frameworks such as CIS Benchmarks, STIGs, and OWASP guidelines. The report outlines how I verified compliance, identified non-compliant configurations, and applied remediations where necessary. Screenshots and clear explanations are included to guide the reader through the full compliance and hardening process.

Security Control (1 of 10)

Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>CIS - Ubuntu 22</i>
Security Control ID:	<i>2.4</i>
Control/Rule Title:	<i>Ensure nonessential services are removed or masked (Manual)</i>
Checked Using:	<i>lsof -i -P -n grep -v "(ESTABLISHED)"</i>
Fix/Remediation:	<i>No fix needed</i>
Additional Steps Required for Compliance:	<i>Compliant! The only service identified as running on the system is Firefox, which is essential for the system's functionality. Firefox is operating on port 53583 using the UDP protocol.</i>
Comments:	<i>Can be found on page 278 of the CIS - Ubuntu 22 document.</i>
Screen Shots:	

Security Control (2 of 10)

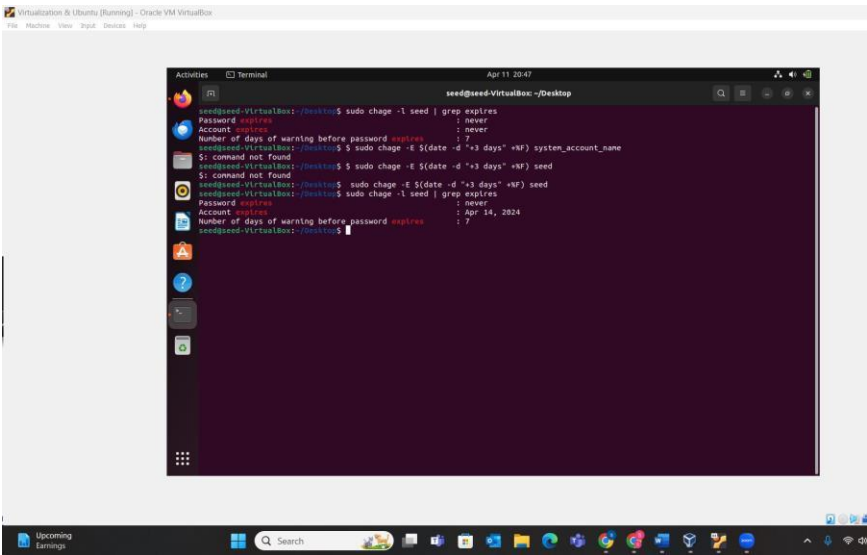
Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>CIS MariaDB</i>
Security Control ID:	<i>5.2</i>
Control/Rule Title:	<i>Ensure 'FILE' is Not Granted to Non-Administrative Users (Manual)</i>
Checked Using:	<i>Execute the following SQL statement to audit this setting:</i> <i>SELECT GRANTEE FROM INFORMATION_SCHEMA.USER_PRIVILEGES WHERE PRIVILEGE_TYPE = 'FILE';</i>
Fix/Remediation:	<i>No fix needed.</i>
Additional Steps Required for Compliance:	<i>No additional steps needed, file is not granted to non-admin users.</i>
Comments:	<i>We seem to be compliant with this security control, our file is only granted to administrative users as shown below. Also this security control can be found on page 111.</i>
Screen Shots:	 A screenshot of a terminal window titled 'Terminal' with a dark background. The terminal shows a series of commands and their outputs. The first few lines show 'cd: command not found' for several paths. Then, a MySQL command is executed: 'mysql -u root -p'. The prompt 'mysql>' appears. The user enters the SQL query: 'SELECT GRANTEE FROM INFORMATION_SCHEMA.USER_PRIVILEGES WHERE PRIVILEGE_TYPE = 'FILE';'. The output shows two rows: 'GRANTEE' and 'debian-sys-maint@localhost', and 'root@localhost'. The terminal also shows the MySQL version '8.0.30-Debian' and the user 'root'.

--	--

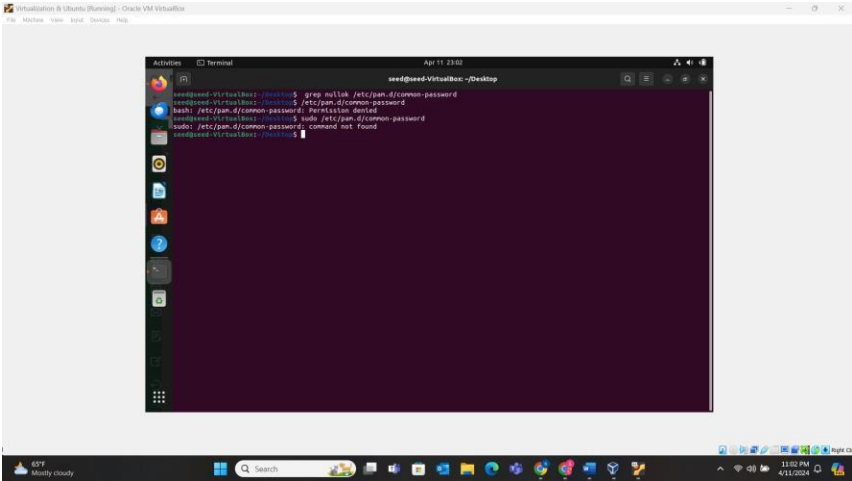
Security Control (3 of 10)

Analyst Name:	Saeed Rafee
Control Source:	CIS MARIADB
Security Control ID:	5.6
Control/Rule Title:	Ensure 'CREATE USER' is Not Granted to Non-Administrative Users (Manual)
Checked Using:	SELECT GRANTEE FROM INFORMATION_SCHEMA.USER_PRIVILEGES WHERE PRIVILEGE_TYPE = 'CREATE USER';
Fix/Remediation:	No fix needed.
Additional Steps Required for Compliance:	Create user is not granted for non-admins.
Comments:	We are compliant with this security control, no further steps needed for compliance.
Screen Shots:	<p>The screenshot shows a terminal window titled 'Terminal' with a dark background. The user is logged in as 'saeed' on a system named 'VirtualBox'. The terminal displays the output of the command 'cat /etc/my.cnf', showing various MySQL configuration options like 'max_buffer_length', 'select_limit', 'max_join_size', etc. Below the configuration, the user has entered the MySQL command 'select * from information_schema.user_privileges where privilege_type = \'CREATE USER\';'. The output shows that the 'GRANTEE' is 'debian-sys-maint@localhost' and the 'PRIVILEGE_TYPE' is 'CREATE USER'. The terminal also shows the MySQL prompt 'mysql>'.</p>

Security Control (4 of 10)

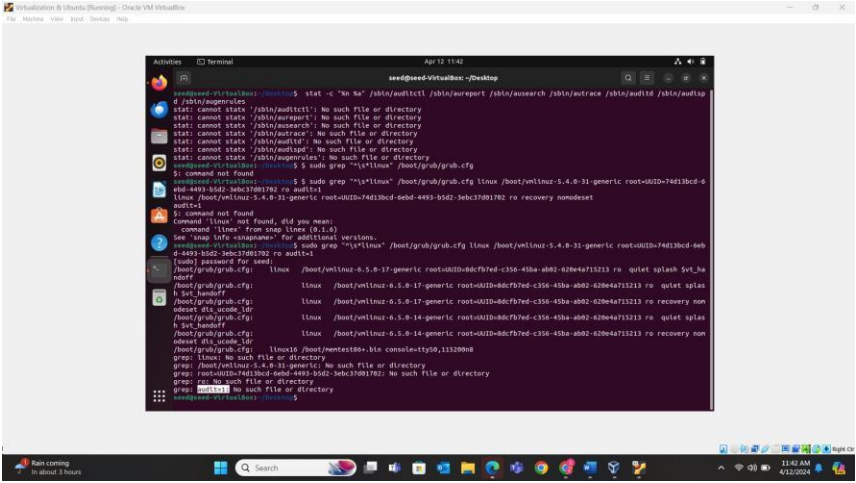
Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>STIG - Ubuntu 20</i>
Security Control ID:	SV-238196r653763_rule
Control/Rule Title:	The Ubuntu operating system must provision temporary user accounts with an expiration time of 72 hours or less.
Checked Using:	<code>\$ sudo chage -l system_account_name grep expires</code>
Fix/Remediation:	<code>\$ sudo chage -E \$(date -d "+3 days" +%F) system_account_name</code>
Additional Steps Required for Compliance:	<i>I ran \$ sudo chage -E \$(date -d "+3 days" +%F) system_account_name then checked if we were complaint with the checked using.</i>
Comments:	<i>NOT compliant! See fix/remediation for fix.</i>
Screen Shots:	 <p>The screenshot shows a terminal window with the following output:</p> <pre>seed@seed-VirtualBox: ~/Desktop seed@seed-VirtualBox:~/Desktop\$ sudo chage -l seed grep expires Password expires : never Account expires : never Number of days of warning before password expires : 7 seed@seed-VirtualBox:~/Desktop\$ sudo chage -E \$(date -d "+3 days" +%F) system_account_name \$! command not found seed@seed-VirtualBox:~/Desktop\$ sudo chage -E \$(date -d "+3 days" +%F) seed \$! command not found seed@seed-VirtualBox:~/Desktop\$ sudo chage -E \$(date -d "+3 days" +%F) seed seed@seed-VirtualBox:~/Desktop\$ sudo chage -l seed grep expires Password expires : never Account expires : Apr 14, 2024 Number of days of warning before password expires : 7 seed@seed-VirtualBox:~/Desktop\$</pre>

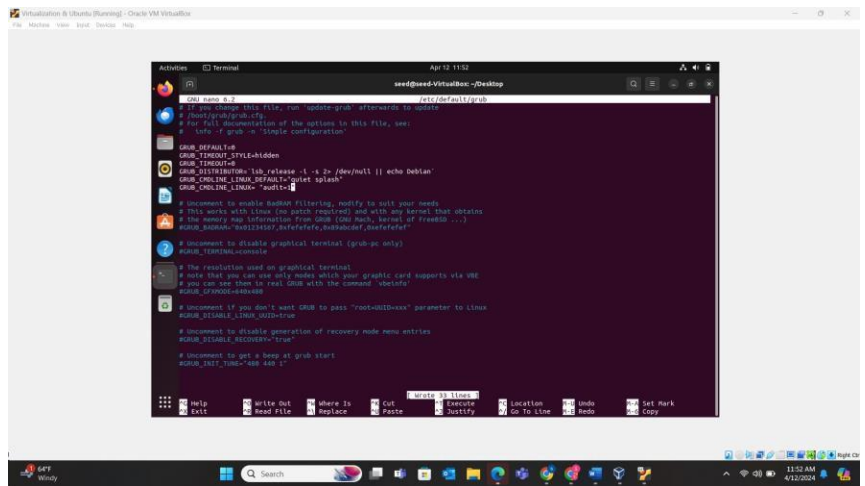
Security Control (5 of 10)

Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>STIG - Ubuntu 20</i>
Security Control ID:	<i>V-251504</i>
Control/Rule Title:	The Ubuntu operating system must not allow accounts configured with blank or null passwords.
Checked Using:	<i>\$ grep nullok /etc/pam.d/common-password</i>
Fix/Remediation:	<i>Remove any instances of the "nullok" option in "/etc/pam.d/common-password" to prevent logons with empty passwords.</i>
Additional Steps Required for Compliance:	<i>/etc/pam.d/common-password command then remove nullok, to prevent null passwords log in.</i>
Comments:	<i>Not compliant, I tried to remove nullok but I was denied permission.</i>
Screen Shots:	 <p>The screenshot shows a terminal window titled 'saeed@saed-VirtualBox: ~/Desktop'. The user has entered the command <code>grep nullok /etc/pam.d/common-password</code>. The output of the command is <code>hash: /etc/pam.d/common-password: Permission denied</code>. The terminal window is open on a desktop environment with a taskbar at the bottom showing various application icons and the system clock indicating 11:03 PM on 4/11/2024.</p>

--	--

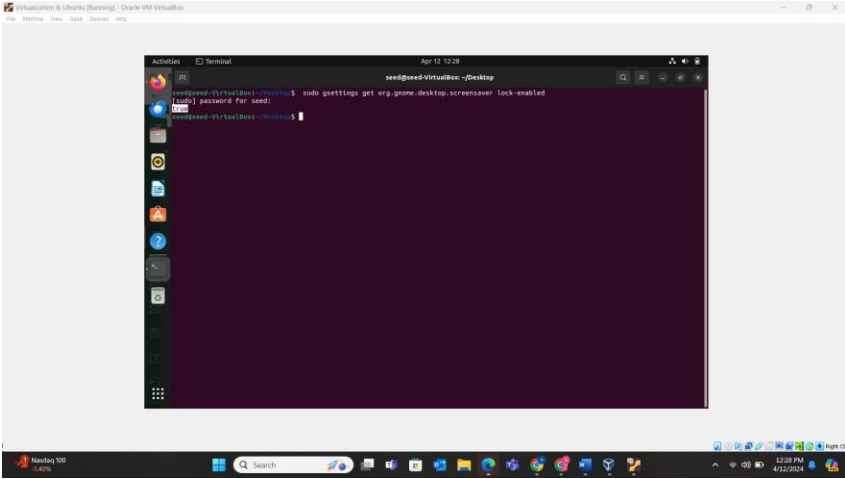
Security Control (6 of 10)

Analyst Name:	Saeed Rafee
Control Source:	STIG - Ubuntu 20
Security Control ID:	V-238299
Control/Rule Title:	The Ubuntu operating system must initiate session audits at system start-up.
Checked Using:	<p><code>sudo grep "\s*linux" /boot/grub/grub.cfg linux /boot/vmlinuz-5.4.0-31-generic root=UUID=74d13bcd-6ebd-4493-b5d2-3ebc37d01702 ro audit=1 linux /boot/vmlinuz-5.4.0-31-generic root=UUID=74d13bcd-6ebd-4493-b5d2-3ebc37d01702 ro recovery nomodeset audit=1</code></p> <p>Then to update the grub config file run: \$ <code>sudo update-grub</code></p>
Fix/Remediation:	Edit the "/etc/default/grub" file and add "audit=1" to the "GRUB_CMDLINE_LINUX" option.
Additional Steps Required for Compliance:	If any linux lines do not contain "audit=1", this is a finding. We're not compliant. As shown in the screenshot below.
Comments:	Not compliant see fix for further steps.
Screen Shots:	

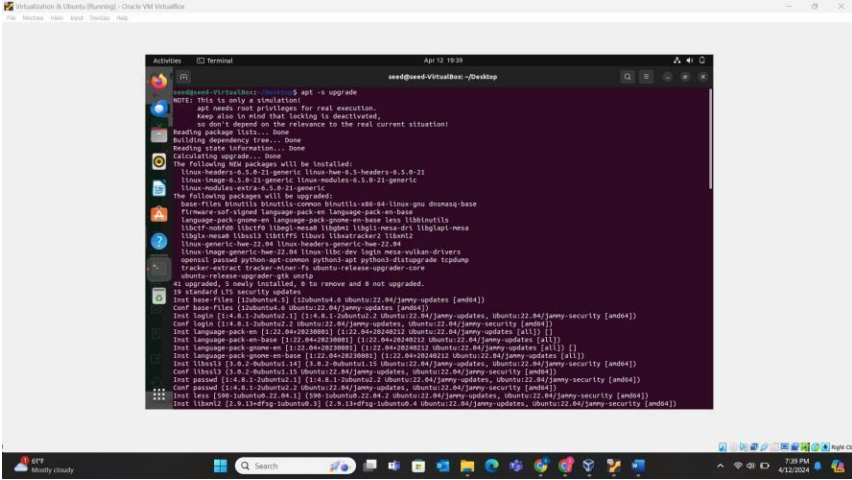


Fix^

Security Control (7 of 10)

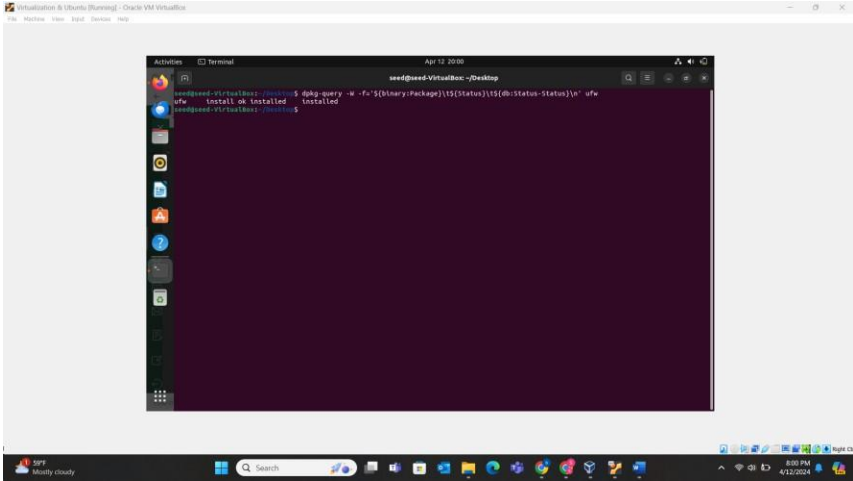
Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>STIG - Ubuntu 20</i>
Security Control ID:	<i>V-238199 R</i>
Control/Rule Title:	<i>The Ubuntu operating system must retain a user's session lock until that user reestablishes access using established identification and authentication procedures.</i>
Checked Using:	<i>sudo gsettings get org.gnome.desktop.screensaver lock-enabled you're compliant if the output is true.</i>
Fix/Remediation:	<i>No fix needed.</i>
Additional Steps Required for Compliance:	<i>Output was true so no need for further steps.</i>
Comments:	<i>We're compliant with this control.</i>
Screen Shots:	 <p>The screenshot shows a terminal window titled 'Terminal' with the prompt 'seed@seed-virtualbox: ~/Desktop'. The command 'sudo gsettings get org.gnome.desktop.screensaver lock-enabled' has been entered, and the output 'true' is displayed. The terminal window is overlaid on a desktop environment with various icons and a taskbar at the bottom.</p>

Security Control (8 of 10)

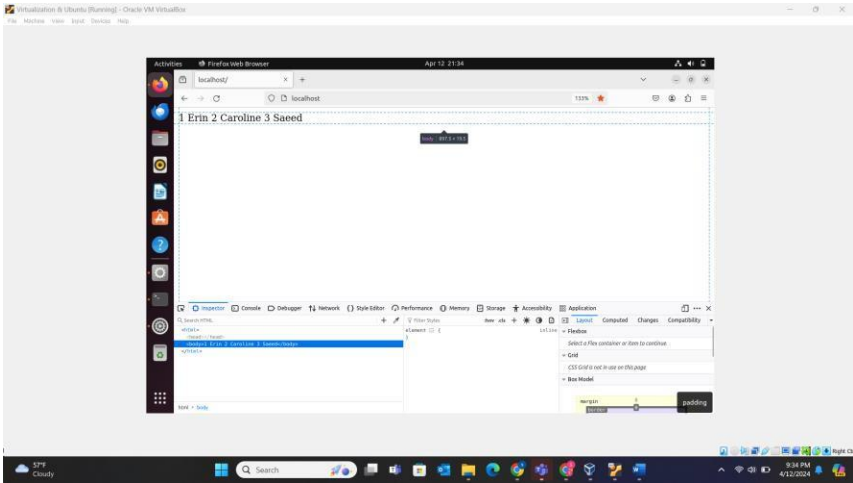
Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>STIG - MariaDB</i>
Security Control ID:	<i>1.9</i>
Control/Rule Title:	<i>Ensure updates, patches, and additional security software are installed (Manual)</i>
Checked Using:	<i>apt -s upgrade</i>
Fix/Remediation:	<i>apt upgrade enter sudo if needed or denied</i>
Additional Steps Required for Compliance:	<i>See fix for further steps.</i>
Comments:	<i>Not compliant updates need to be installed.</i>
Screen Shots:	



Security Control (9 of 10)

Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>CIS - Ubuntu 22</i>
Security Control ID:	<i>3.5.1.1</i>
Control/Rule Title:	<i>Ensure ufw is installed.</i>
Checked Using:	<i>dpkg-query -W -f='\${binary:Package}\t\${Status}\t\${db:Status-Status}\n' ufw</i>
Fix/Remediation:	<i>No fix needed.</i>
Additional Steps Required for Compliance:	<i>UFW is installed.</i>
Comments:	<i>We're compliant with this security control.</i>
Screen Shots:	 <p>The screenshot shows a terminal window titled 'Terminal' with the command <code>dpkg-query -W -f='\${binary:Package}\t\${Status}\t\${db:Status-Status}\n' ufw</code> entered. The output is <code>ufw install ok installed installed</code>. The terminal is running on a system with a desktop environment, as evidenced by the Ubuntu logo and icons on the left side of the terminal window.</p>

Security Control (10 of 10)

Analyst Name:	<i>Saeed Rafee</i>
Control Source:	<i>OWASP testing guide</i>
Security Control ID:	<i>OTG-CLIENT-004</i>
Control/Rule Title:	<i>Testing for Client Side URL Redirect</i>
Checked Using:	<i>URL</i>
Fix/Remediation:	<i>Educate developers on secure coding practices to prevent the introduction of Client Side URL Redirect vulnerabilities in future development efforts.</i>
Additional Steps Required for Compliance:	<i>For our yoga application, the URL can be similar like in a typo squatting event to make the URL seem alike but redirect to a malicious page.</i>
Comments:	<i>Client Side URL Redirect vulnerabilities can be exploited by attackers to conduct phishing attacks.</i>
Screen Shots:	 <p>The screenshot shows a web browser window titled 'Firefox Web Browser' with the address bar set to 'localhost/'. The page content displays a list of names: '1 Erin 2 Caroline 3 Saeed'. Below the browser window, several developer tools are visible, including the 'Inspector' panel showing the DOM tree with a selected element containing the text 'Erin 2 Caroline 3 Saeed'. The browser is running on a virtual machine (Ubuntu 20.04 LTS) with various development tools open. The system tray at the bottom shows the date and time as 6:34 PM on 6/11/2024.</p>