

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Динькиев Валерий

Содержание

1	Цель работы	4
2	Подготовка лабораторного стенда:	5
3	Выполнение лабораторной работы	7
4	Выводы	16

List of Figures

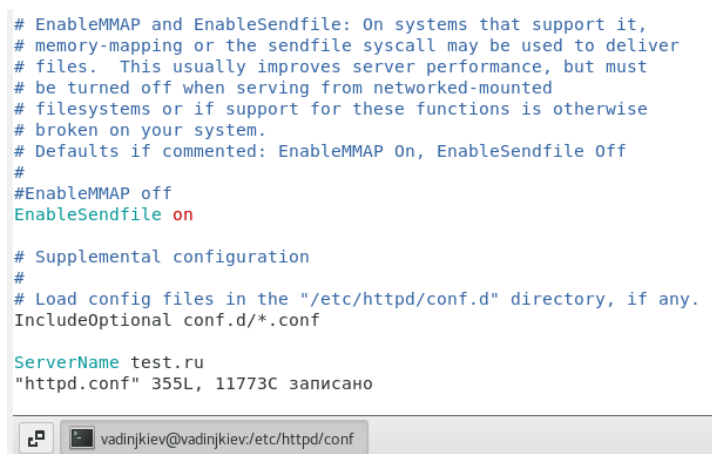
2.1	Параметр ServerName	5
2.2	Отключение фильтра	5
2.3	Отключение фильтра	6
2.4	Добавление разрешающих правил	6
3.1	Проверка через браузер	8
3.2	Проверка статуса	8
3.3	веб-сервер Apache	8
3.4	Просмотр переключателей SELinux для Apache	9
3.5	Статистика	10
3.6	Статистика	10
3.7	Создание файла	11
3.8	Проверка	11
3.9	Получение доступа к файлу через браузер	11
3.10	Изменение контекста, проверка	11
3.11	Получение доступа к файлу через браузер	12
3.12	Изменение порта 80 на 81	12
3.13	Анализ лог-файла	13
3.14	Просмотр файла /var/log/http/error_log	13
3.15	Просмотр файла /var/log/http/access_log	13
3.16	Просмотр файла var/log/audit/audit.log	13
3.17	Выполнение и проверка	14
3.18	Возвращение контекста	14
3.19	Получение доступа к файлу через браузер	14
3.20	Исправленный файл apache	14
3.21	Удаление привязки к 81 порту	14
3.22	Удаление файла /var/www/html/test.html	15

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Подготовка лабораторного стенда:

1. В конфигурационном файле /etc/httpd/httpd.conf задал параметр ServerName. (рис. 2.1).



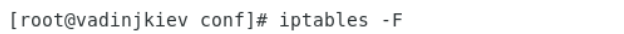
```
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf

ServerName test.ru
"httpd.conf" 355L, 11773C записано
```

Figure 2.1: Параметр ServerName

2. Также проследил, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключил фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавил разрешающие правила. (рис. 2.2), (рис. 2.3), (рис. 2.4).



```
[root@vadinjkiiev conf]# iptables -F
```

Figure 2.2: Отключение фильтра

```
[root@vadinjkiev conf]# iptables -P INPUT ACCEPT
[root@vadinjkiev conf]# iptables -P OUTPUT ACCEPT
[root@vadinjkiev conf]# █
```

Figure 2.3: Отключение фильтра

```
[root@vadinjkiev conf]# iptables -P INPUT ACCEPT
[root@vadinjkiev conf]# iptables -P OUTPUT ACCEPT
[root@vadinjkiev conf]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@vadinjkiev conf]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@vadinjkiev conf]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@vadinjkiev conf]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@vadinjkiev conf]# █
```

Figure 2.4: Добавление разрешающих правил

3 Выполнение лабораторной работы

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. ??).

```
[root@vadinjkiev conf]# getenforce
Enforcing
[root@vadinjkiev conf]# sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
[root@vadinjkiev conf]# █
```

2. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: `service httpd status` (рис. 3.1), (рис. 3.2).

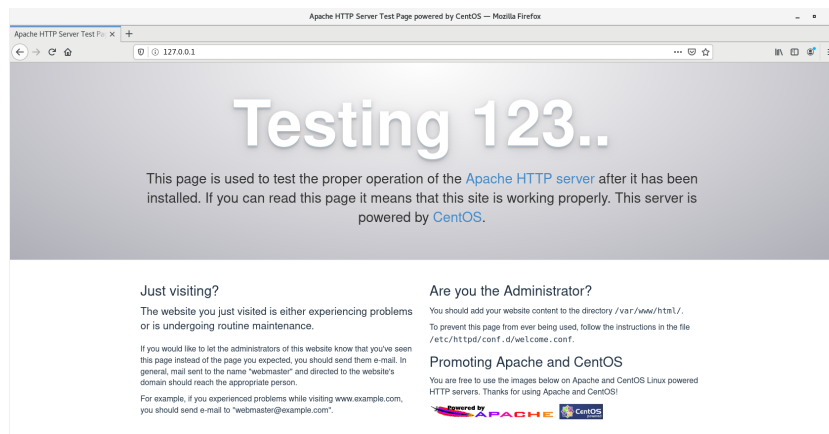


Figure 3.1: Проверка через браузер

```
[root@vadinjkiy conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3182  0.0  0.0 230448  628 ?        Ss   03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3185  0.0  0.0 232524  836 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3186  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3187  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3188  0.0  0.1 232660  1992 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3189  0.0  0.1 232660  1812 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4405  0.0  0.2 232524  2304 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4406  0.0  0.2 232524  2344 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4438  0.0  0.0 112832  976 pts/0  S+  03:42   0:00 grep --color=auto httpd
[root@vadinjkiy conf]#
```

Figure 3.2: Проверка статуса

3. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности. (рис. 3.3).

```
[root@vadinjkiy conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3182  0.0  0.0 230448  628 ?        Ss   03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3185  0.0  0.0 232524  836 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3186  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3187  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3188  0.0  0.1 232660  1992 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3189  0.0  0.1 232660  1812 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4405  0.0  0.2 232524  2304 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4406  0.0  0.2 232524  2344 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4438  0.0  0.0 112832  976 pts/0  S+  03:42   0:00 grep --color=auto httpd
[root@vadinjkiy conf]#
```

Figure 3.3: веб-сервер Apache

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратил внимание, что многие из них находятся в положении «off». (рис. 3.4).


```
[root@vadinjkiev conf]# sestatus -b httpd
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Max kernel policy version:    31

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system     off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap    off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content          off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write             off
cobbler_can_network_connect    off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_tcp_network_connect   off
condor_tcp_network_connect     off
conman_can_network             off
conman_use_nfs                 off
container_connect_any          off
cron_can_relabel               off
cron_system_cronjob_use_shares off
cron_userdomain_transition     on
cups_execmem                   off
cvs_read_shadow                off
daemons_dump_core              off
daemons_enable_cluster_mode   off
daemons_use_tcp_wrapper        off
daemons_use_tty                off
dbadm_exec_content             on
```

Figure 3.4: Просмотр переключателей SELinux для Apache

5. Посмотрел статистику по политике с помощью команды seinfo, также определил множество пользователей(8), ролей(14), типов(4793) (рис. 3.5).

```

[root@vadinjkiev conf]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1        Categories:       1024
Types:            4793     Attributes:        253
Users:            8        Roles:            14
Booleans:         316     Cond. Expr.:      362
Allow:            107834   Neverallow:        0
Auditallow:       158     Dontaudit:         10022
Type_trans:       18153   Type_change:       74
Type_member:      35      Role_allow:        37
Role_trans:       414     Range_trans:       5899
Constraints:      143     Validatetrans:     0
Initial SIDs:     27      Fs_use:            32
Genfscon:         103     Portcon:           614
Netifcon:         0       Nodecon:           0
Permissives:      0       Polcap:            5

[root@vadinjkiev conf]# █

```

Figure 3.5: Статистика

6. Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: `ls -lZ /var/www`.
7. Определил тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`.
8. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 3.6).

```

[root@vadinjkiev conf]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@vadinjkiev conf]#
[root@vadinjkiev conf]# ls -lZ /var/www/html
drwxr-xr-x. 2 root root 6 ноя 10 17:27 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 10 17:27 html
[root@vadinjkiev conf]# ls -l /var/www
итого 0
drwxr-xr-x. 2 root root 6 ноя 10 17:27 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 10 17:27 html
[root@vadinjkiev conf]# █

```

Figure 3.6: Статистика

9. Создал от имени суперпользователя (так как в дистрибутиве после

установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 3.7).



Figure 3.7: Создание файла

10. Проверил контекст созданного файла. httpd_sys_content_t (рис. 3.8).

```
[root@vadinjkiev html]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@vadinjkiev html]#
```

Figure 3.8: Проверка

11. Обратился к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедился, что файл был успешно отображён. (рис. 3.9).

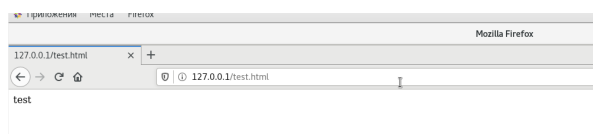


Figure 3.9: Получение доступа к файлу через браузер

12. Проверил контекст файла командой: `ls -lZ /var/www/html/test.html` (рис. 3.10).

13. Изменил контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t. После этого проверил, что контекст поменялся. (рис. 3.10).

```
[root@vadinjkiev html]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@vadinjkiev html]# chcon -t samba_share_t /var/www/html/test.html
[root@vadinjkiev html]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@vadinjkiev html]#
```

Figure 3.10: Изменение контекста, проверка

14. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получил сообщение об ошибке. (рис. 3.11).



Figure 3.11: Получение доступа к файлу через браузер

15. Проанализировал ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: `tail /var/log/messages` (рис. ??).



16. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`). Для этого в файле `/etc/httpd/httpd.conf` нашел строчку `Listen 80` и заменил её на `Listen 81` (рис. 3.12).

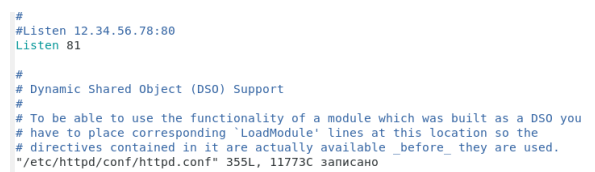


Figure 3.12: Изменение порта 80 на 81

17. Проанализировал лог-файлы. Просмотрел файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`. (рис. 3.13), (рис. 3.14), (рис. 3.15), (рис. 3.16).

```
[root@vadinjkiev html]# tail -n1 /var/log/messages
Nov 27 04:12:06 vadinjkiev systemd: Started The Apache HTTP Server.
[root@vadinjkiev html]#
```

Figure 3.13: Анализ лог-файла

```

[Sun Mar 27 03:12:53.929700000] [server] [pid 1302] 0/100000: Using protocol available, httpd running on content system, system "/usr/sbin/httpd"
[Sun Mar 27 03:12:53.949900000] [server] [pid 1302] 0/100000: module mechanism could not load: /usr/sbin/libmod.so
[Sun Mar 27 03:12:54.000000000] [server] [pid 1302] 0/100000: determine the server's fully qualified domain name, using vhostlookup to lookup the dns
[Sun Mar 27 03:12:54.000000000] [server] [pid 1302] 0/100000: The 'ServerName' directive globally to suppress this message
[Sun Mar 27 03:12:54.010000000] [server] [pid 1302] 0/100000: [warn] (pid 1302) is listening on a non-ipv6 network interface [::]
[Sun Mar 27 03:12:54.010000000] [server] [pid 1302] 0/100000: new pre-forked list of pid 1302: 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325, 1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1560, 1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1572, 1573, 1574, 1575, 1576, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588, 1589, 1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616, 1617, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1630, 1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1640, 1641, 1642, 1643, 1644, 1645, 1646, 1647, 1648, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658, 1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1673, 1674, 1675, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1683, 1684, 1685, 1686, 1687, 1688, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1696, 1697, 1698, 1699, 1700, 1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1710, 1711, 1712, 1713, 1714, 1715, 1716, 1717, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1757, 1758, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1770, 1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1779, 1780, 1781, 1782, 1783, 1784, 1785, 1786, 1787, 1788, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1796, 1797, 1798, 1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826, 1827, 1828, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1850, 1851, 1852, 1853, 1854, 1855, 1856, 1857, 1858, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868, 1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1878, 1879, 1880, 1881, 1882, 1883, 1884, 1885, 1886, 1887, 1888, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1896, 1897, 1898, 1899, 1900, 1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908, 1909, 1910, 1911, 1912, 1913, 1914, 1915, 1916, 1917, 1918, 1919, 1
```

Figure 3.14: Просмотр файла /var/log/httpd/error_log

```

123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

```

Figure 3.15: Просмотр файла /var/log/http/access log

[illegible]Figure 3.16: Просмотр файла `var/log/audit/audit.log`

18. Выполнил команду: `semanage port -a -t http_port_t -p tcp 81`. После этого проверил список портов командой: `semanage port -l | grep http_port_t`. Убедился, что порт 81 появился в списке. (рис. 3.17).

```
[root@vadinjkiy httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 уже определен
[root@vadinjkiy httpd]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@vadinjkiy httpd]#
```

Figure 3.17: Выполнение и проверка

19. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test». (рис. 3.18), (рис. 3.19).

```
[root@vadinjkiy httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vadinjkiy httpd]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 ноя 27 03:53 /var/www/html/test.html
[root@vadinjkiy httpd]# ls -lZ /var/www/html/test.html
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@vadinjkiy httpd]#
```

Figure 3.18: Возвращение контекста



Figure 3.19: Получение доступа к файлу через браузер

20. Исправил обратно конфигурационный файл `apache`, вернув `Listen80`. (рис. 3.20).



Figure 3.20: Исправленный файл `apache`

21. Удалил привязку `http_port_t` к 81 порту. (рис. 3.21).

```
[root@vadinjkiy httpd]# semanage port -d -t http_port_t -p tcp 81
```

Figure 3.21: Удаление привязки к 81 порту

22. Удалил файл /var/www/html/test.html. (рис. 3.22).

```
[root@vadinjkiév httpd]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@vadinjkiév httpd]#
```

Figure 3.22: Удаление файла /var/www/html/test.html

4 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.