

Hacked LAB (Cyber Defenders) - Walkthrough

Tuesday, September 10, 2024 5:30 AM

Story:

A soc analyst has been called to analyze a compromised Linux web server. Figure out how the threat actor gained access, what modifications were applied to the system, and what persistent techniques were utilized. (e.g. backdoors, users, sessions, etc).

- I attempted to mount the 'E01' file on my Kali system but was unsuccessful.
I used FTK Imager to tackle this issue.

Q1: What is the system timezone?

- You can find the file system timezone in the /etc/timezone file.

| Name | Size | Type | Date Modified |
|-----------------------|------|----------------|----------------------|
| subgid | | Regular File | 4/16/2016 1:09:24 PM |
| subgid- | | Regular File | 4/3/2016 4:36:02 PM |
| subuid | | Regular File | 4/16/2016 1:09:24 PM |
| subuid- | | Regular File | 4/3/2016 4:36:02 PM |
| sudocers | | Regular File | 2/10/2014 7:20:40 PM |
| sysctt.conf | | 3 Regular File | 4/1/2013 2:25:31 AM |
| timezone | | Regular File | 4/3/2016 4:33:16 PM |
| ucd.conf | | Regular File | 7/1/2013 1:01:00 AM |
| updatedb.conf | | Regular File | 6/20/2013 2:13:07 PM |
| upstart-xsessions | | Regular File | 4/11/2014 9:52:46 PM |
| vbrgb | | Symbolic Link | 4/3/2016 4:05:51 PM |
| wgetrc | | Regular File | 2/7/2014 6:04:20 PM |
| zsh_command_not_found | | Regular File | 6/26/2012 6:16:49 PM |

cat /etc/timezone

Q2: Who was the last user to log in to the system?

- To address this question, I exported the 'wtmp' file which located at '/var/log/wtmp' and used 'utmpdump' to parse it.

| | | | | | | | |
|-----|---------|--------|--------|---------|-------------------|-------------------|------------------------------------|
| [7] | [02999] | [ts/1] | [mail] | [pts/1] | [192.168.210.131] | [192.168.210.131] | [2019-10-05T11:21:04,107187+00:00] |
| [8] | [02999] | [|] | [pts/1] | [| [0.0.0.0] | [2019-10-05T11:21:45,539577+00:00] |
| [7] | [03108] | [ts/1] | [mail] | [pts/1] | [192.168.210.131] | [192.168.210.131] | [2019-10-05T11:23:34,640343+00:00] |
| [8] | [03108] | [|] | [pts/1] | [| [0.0.0.0] | [2019-10-05T11:24:11,772124+00:00] |

Q3: What was the source port the user 'mail' connected from?

- I exported the auth.log file located at '/var/log/auth.log' and filtered it by the user mail to find the last logged-in activity.

| |
|--|
| Search results: (40 hits) |
| Line 3327: Oct 5 13:21:11 VulnOSv2 su[3055]: pam_unix(su:session): session opened for user root by mail(uid=0) |
| Line 3331: Oct 5 13:21:30 VulnOSv2 sudo: mail : TTY=pts/1 : FWD=/var/mail : USER=root : COMMAND=/bin/su - |
| Line 3332: Oct 5 13:21:30 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0) |
| Line 3335: Oct 5 13:21:30 VulnOSv2 su[3082]: pam_unix(su:session): session opened for user root by mail(uid=0) |
| Line 3342: Oct 5 13:21:45 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session closed for user mail |
| Line 3343: Oct 5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2 |
| Line 3344: Oct 5 13:23:34 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session opened for user mail by (uid=0) |
| Line 3345: Oct 5 13:23:39 VulnOSv2 sudo: mail : TTY=pts/1 : FWD=/var/mail : USER=root : COMMAND=/bin/su - |
| Line 3346: Oct 5 13:23:39 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0) |
| Line 3349: Oct 5 13:23:39 VulnOSv2 su[3164]: pam_unix(su:session): session opened for user root by mail(uid=0) |
| Line 3353: Oct 5 13:24:11 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session closed for user mail |

Q4: How long was the last session for user 'mail'? (Minutes only)

- In the 'auth.log' logs, it shows that the duration of the last session was one minute.

Q5: Which server service did the last user use to log in to the system?

- In the 'auth.log' logs, it shows the user logged in via 'ssh2'.

Q6: What type of authentication attack was performed against the target machine?

- In the 'auth.log' logs, we are able to see multiple failed logins to 'Root' user via SSH which indicates that is a 'Brute-Force' attack

| |
|--|
| Oct 5 12:39:16 VulnOSv2 sshd[1844]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:39:27 VulnOSv2 sshd[1822]: Failed password for root from 192.168.210.131 port 57190 ssh2 |
| Oct 5 12:39:33 VulnOSv2 sshd[1822]: Failed password for root from 192.168.210.131 port 57190 ssh2 |
| Oct 5 12:39:33 VulnOSv2 sshd[1822]: Connection closed by 192.168.210.131 [preauth] |
| Oct 5 12:39:33 VulnOSv2 sshd[1822]: PAM 1 more authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:33 VulnOSv2 sshd[1838]: Received disconnect from 192.168.210.131: 11: Bye Bye [preauth] |
| Oct 5 12:42:33 VulnOSv2 sshd[1838]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:33 VulnOSv2 sshd[1836]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:33 VulnOSv2 sshd[1838]: Failed password for root from 192.168.210.131 port 57200 ssh2 |
| Oct 5 12:42:35 VulnOSv2 sshd[1836]: Failed password for root from 192.168.210.131 port 57196 ssh2 |
| Oct 5 12:42:35 VulnOSv2 sshd[1842]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:35 VulnOSv2 sshd[1837]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:35 VulnOSv2 sshd[1839]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:35 VulnOSv2 sshd[1840]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:35 VulnOSv2 sshd[1841]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:40 VulnOSv2 sshd[1842]: Failed password for root from 192.168.210.131 port 57208 ssh2 |
| Oct 5 12:42:40 VulnOSv2 sshd[1837]: Failed password for root from 192.168.210.131 port 57198 ssh2 |
| Oct 5 12:42:40 VulnOSv2 sshd[1839]: Failed password for root from 192.168.210.131 port 57202 ssh2 |
| Oct 5 12:42:40 VulnOSv2 sshd[1840]: Failed password for root from 192.168.210.131 port 57204 ssh2 |
| Oct 5 12:42:40 VulnOSv2 sshd[1841]: Failed password for root from 192.168.210.131 port 57206 ssh2 |
| Oct 5 12:42:43 VulnOSv2 sshd[1840]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1835]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1844]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1851]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1850]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1849]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1849]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1857]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:44 VulnOSv2 sshd[1849]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:45 VulnOSv2 sshd[1846]: error: maximum authentication attempts exceeded for root from 192.168.210.131 port 57196 ssh2 [preauth] |
| Oct 5 12:42:45 VulnOSv2 sshd[1836]: Disconnecting: Too many authentication failures for root [preauth] |
| Oct 5 12:42:45 VulnOSv2 sshd[1841]: PAM 5 more authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root |
| Oct 5 12:42:45 VulnOSv2 sshd[1836]: PAM service(sshd) ignoring max retries; 6 > 3 |
| Oct 5 12:42:45 VulnOSv2 sshd[1838]: message repeated 5 times: [Failed password for root from 192.168.210.131 port 57200 ssh2] |
| Oct 5 12:42:45 VulnOSv2 sshd[1838]: error: maximum authentication attempts exceeded for root from 192.168.210.131 port 57200 ssh2 [preauth] |
| Oct 5 12:42:45 VulnOSv2 sshd[1838]: Disconnecting: Too many authentication failures for root [preauth] |

Q7: How many IP addresses are listed in the '/var/log/lastlog' file?

- To address this question, I exported the 'lastlog' file located at '/var/log/lastlog'.
After running the strings command on it, I discovered that the file contains only two IP addresses.

```
(kali@kali)-[~/Desktop]
$ strings lastlog
"3=wtty1
jpts/1
192.168.210.131
2=wtpts/0
192.168.56.101
)wtty1
```

Q8: How many users have a login shell?

- In the 'passwd' file which located in /etc/passwd, we are able to identify which users have a login shell (5)

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/bin/bash
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
php:x:999:999:/usr/php:/bin/bash
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false
landscape:x:103:109:/var/lib/landscape:/bin/false
vulnosadmin:x:1000:1000:vulnosadmin,,:/home/vulnosadmin:/bin/bash
myaql:x:104:113:MySQL Server,,:/nonexistent:/bin/false
webmin:x:1001:1001:/home/webmin:
ssh:x:105:65534:/var/run/ssh:/usr/sbin/nologin
postfix:x:106:114:/var/spool/postfix:/bin/false
postgres:x:107:116:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
```

Q9: What is the password of the mail user?

- To address this question, I took the encrypted password of the user from the '/etc/shadow' file and copied only the hash {56SzLa0LV8N\$BNxYZUxxXIZwb3UjBhCnxd9Mb02DDUF.GfMj1kblB.s/quBVtMM4QjOfOvmZvfqh7BuLxArRvsfPQ.gNlSprE} into a text file. The hash, recognized by ChatGPT as SHA512, was then cracked using John the Ripper to discover the password.

```
(kali@kali)-[~/Desktop]
└─$ john --format=sha512crypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
forensics (?)
1g 00:00:00:28 DONE (2024-09-11 09:07) 0.03467g/s 2041p/s 2041c/s 2041c/s gabriel13..bluedolphin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Q10: Which user account was created by the attacker?

- I filtered the auth.log file for the keyword 'useradd' and found that the command was executed by 'root' to add a user named 'php'.

```
Oct 5 13:06:38 Vuln0Sv2 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 5 13:06:38 Vuln0Sv2 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: new group: name=php, GID=999
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: new user: name=php, UID=999, GID=999, home=/usr/php, shell=/bin/bash
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: add 'php' to group 'sudo'
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: add 'php' to shadow group 'sudo'
```

Q11: How many user groups exist on the machine?

- To address this question, I exported the /etc/group file and found that there are 58 groups.

```
# Group 0:
1: daemon:x:1:
2: bin:x:2:
3: sys:x:3:
4: adm:x:4:
5: log:x:5:
6: utmp:x:6:
7: lp:x:7:
8: mail:x:8:
9: news:x:9:
10: uucp:x:10:
11: nobody:x:65534:
12: libuuid:x:100:
13: syslog:x:101:
14: messagebus:x:102:
15: landscape:x:103:
16: vulnosadmin:x:1000:
17: myaql:x:104:
18: webmin:x:1001:
19: ssh:x:105:
20: postfix:x:106:
21: postgres:x:107:
22: group:x:108:
23: nobody:x:65534:
24: libuuid:x:100:
25: syslog:x:101:
26: messagebus:x:102:
27: landscape:x:103:
28: vulnosadmin:x:1000:
29: myaql:x:104:
30: webmin:x:1001:
31: ssh:x:105:
32: postfix:x:106:
33: postgres:x:107:
34: group:x:108:
35: nobody:x:65534:
36: libuuid:x:100:
37: syslog:x:101:
38: messagebus:x:102:
39: landscape:x:103:
40: vulnosadmin:x:1000:
41: myaql:x:104:
42: webmin:x:1001:
43: ssh:x:105:
44: postfix:x:106:
45: postgres:x:107:
46: group:x:108:
47: nobody:x:65534:
48: libuuid:x:100:
49: syslog:x:101:
50: messagebus:x:102:
51: landscape:x:103:
52: vulnosadmin:x:1000:
53: myaql:x:104:
54: webmin:x:1001:
55: ssh:x:105:
56: postfix:x:106:
57: postgres:x:107:
58: group:x:108:
59: nobody:x:65534:
60: libuuid:x:100:
61: syslog:x:101:
62: messagebus:x:102:
63: landscape:x:103:
64: vulnosadmin:x:1000:
65: myaql:x:104:
66: webmin:x:1001:
67: ssh:x:105:
68: postfix:x:106:
69: postgres:x:107:
70: group:x:108:
71: nobody:x:65534:
72: libuuid:x:100:
73: syslog:x:101:
74: messagebus:x:102:
75: landscape:x:103:
76: vulnosadmin:x:1000:
77: myaql:x:104:
78: webmin:x:1001:
79: ssh:x:105:
80: postfix:x:106:
81: postgres:x:107:
82: group:x:108:
83: nobody:x:65534:
84: libuuid:x:100:
85: syslog:x:101:
86: messagebus:x:102:
87: landscape:x:103:
88: vulnosadmin:x:1000:
89: myaql:x:104:
90: webmin:x:1001:
91: ssh:x:105:
92: postfix:x:106:
93: postgres:x:107:
94: group:x:108:
95: nobody:x:65534:
96: libuuid:x:100:
97: syslog:x:101:
98: messagebus:x:102:
99: landscape:x:103:
100: vulnosadmin:x:1000:
101: myaql:x:104:
102: webmin:x:1001:
103: ssh:x:105:
104: postfix:x:106:
105: postgres:x:107:
106: group:x:108:
107: nobody:x:65534:
108: libuuid:x:100:
109: syslog:x:101:
110: messagebus:x:102:
111: landscape:x:103:
112: vulnosadmin:x:1000:
113: myaql:x:104:
114: webmin:x:1001:
115: ssh:x:105:
116: postfix:x:106:
117: postgres:x:107:
118: group:x:108:
119: nobody:x:65534:
120: libuuid:x:100:
121: syslog:x:101:
122: messagebus:x:102:
123: landscape:x:103:
124: vulnosadmin:x:1000:
125: myaql:x:104:
126: webmin:x:1001:
127: ssh:x:105:
128: postfix:x:106:
129: postgres:x:107:
130: group:x:108:
131: nobody:x:65534:
132: libuuid:x:100:
133: syslog:x:101:
134: messagebus:x:102:
135: landscape:x:103:
136: vulnosadmin:x:1000:
137: myaql:x:104:
138: webmin:x:1001:
139: ssh:x:105:
140: postfix:x:106:
141: postgres:x:107:
142: group:x:108:
143: nobody:x:65534:
144: libuuid:x:100:
145: syslog:x:101:
146: messagebus:x:102:
147: landscape:x:103:
148: vulnosadmin:x:1000:
149: myaql:x:104:
150: webmin:x:1001:
151: ssh:x:105:
152: postfix:x:106:
153: postgres:x:107:
154: group:x:108:
155: nobody:x:65534:
156: libuuid:x:100:
157: syslog:x:101:
158: messagebus:x:102:
159: landscape:x:103:
160: vulnosadmin:x:1000:
161: myaql:x:104:
162: webmin:x:1001:
163: ssh:x:105:
164: postfix:x:106:
165: postgres:x:107:
166: group:x:108:
167: nobody:x:65534:
168: libuuid:x:100:
169: syslog:x:101:
170: messagebus:x:102:
171: landscape:x:103:
172: vulnosadmin:x:1000:
173: myaql:x:104:
174: webmin:x:1001:
175: ssh:x:105:
176: postfix:x:106:
177: postgres:x:107:
178: group:x:108:
179: nobody:x:65534:
180: libuuid:x:100:
181: syslog:x:101:
182: messagebus:x:102:
183: landscape:x:103:
184: vulnosadmin:x:1000:
185: myaql:x:104:
186: webmin:x:1001:
187: ssh:x:105:
188: postfix:x:106:
189: postgres:x:107:
190: group:x:108:
191: nobody:x:65534:
192: libuuid:x:100:
193: syslog:x:101:
194: messagebus:x:102:
195: landscape:x:103:
196: vulnosadmin:x:1000:
197: myaql:x:104:
198: webmin:x:1001:
199: ssh:x:105:
200: postfix:x:106:
201: postgres:x:107:
202: group:x:108:
203: nobody:x:65534:
204: libuuid:x:100:
205: syslog:x:101:
206: messagebus:x:102:
207: landscape:x:103:
208: vulnosadmin:x:1000:
209: myaql:x:104:
210: webmin:x:1001:
211: ssh:x:105:
212: postfix:x:106:
213: postgres:x:107:
214: group:x:108:
215: nobody:x:65534:
216: libuuid:x:100:
217: syslog:x:101:
218: messagebus:x:102:
219: landscape:x:103:
220: vulnosadmin:x:1000:
221: myaql:x:104:
222: webmin:x:1001:
223: ssh:x:105:
224: postfix:x:106:
225: postgres:x:107:
226: group:x:108:
227: nobody:x:65534:
228: libuuid:x:100:
229: syslog:x:101:
230: messagebus:x:102:
231: landscape:x:103:
232: vulnosadmin:x:1000:
233: myaql:x:104:
234: webmin:x:1001:
235: ssh:x:105:
236: postfix:x:106:
237: postgres:x:107:
238: group:x:108:
239: nobody:x:65534:
240: libuuid:x:100:
241: syslog:x:101:
242: messagebus:x:102:
243: landscape:x:103:
244: vulnosadmin:x:1000:
245: myaql:x:104:
246: webmin:x:1001:
247: ssh:x:105:
248: postfix:x:106:
249: postgres:x:107:
250: group:x:108:
251: nobody:x:65534:
252: libuuid:x:100:
253: syslog:x:101:
254: messagebus:x:102:
255: landscape:x:103:
256: vulnosadmin:x:1000:
257: myaql:x:104:
258: webmin:x:1001:
259: ssh:x:105:
260: postfix:x:106:
261: postgres:x:107:
262: group:x:108:
263: nobody:x:65534:
264: libuuid:x:100:
265: syslog:x:101:
266: messagebus:x:102:
267: landscape:x:103:
268: vulnosadmin:x:1000:
269: myaql:x:104:
270: webmin:x:1001:
271: ssh:x:105:
272: postfix:x:106:
273: postgres:x:107:
274: group:x:108:
275: nobody:x:65534:
276: libuuid:x:100:
277: syslog:x:101:
278: messagebus:x:102:
279: landscape:x:103:
280: vulnosadmin:x:1000:
281: myaql:x:104:
282: webmin:x:1001:
283: ssh:x:105:
284: postfix:x:106:
285: postgres:x:107:
286: group:x:108:
287: nobody:x:65534:
288: libuuid:x:100:
289: syslog:x:101:
290: messagebus:x:102:
291: landscape:x:103:
292: vulnosadmin:x:1000:
293: myaql:x:104:
294: webmin:x:1001:
295: ssh:x:105:
296: postfix:x:106:
297: postgres:x:107:
298: group:x:108:
299: nobody:x:65534:
300: libuuid:x:100:
301: syslog:x:101:
302: messagebus:x:102:
303: landscape:x:103:
304: vulnosadmin:x:1000:
305: myaql:x:104:
306: webmin:x:1001:
307: ssh:x:105:
308: postfix:x:106:
309: postgres:x:107:
310: group:x:108:
311: nobody:x:65534:
312: libuuid:x:100:
313: syslog:x:101:
314: messagebus:x:102:
315: landscape:x:103:
316: vulnosadmin:x:1000:
317: myaql:x:104:
318: webmin:x:1001:
319: ssh:x:105:
320: postfix:x:106:
321: postgres:x:107:
322: group:x:108:
323: nobody:x:65534:
324: libuuid:x:100:
325: syslog:x:101:
326: messagebus:x:102:
327: landscape:x:103:
328: vulnosadmin:x:1000:
329: myaql:x:104:
330: webmin:x:1001:
331: ssh:x:105:
332: postfix:x:106:
333: postgres:x:107:
334: group:x:108:
335: nobody:x:65534:
336: libuuid:x:100:
337: syslog:x:101:
338: messagebus:x:102:
339: landscape:x:103:
340: vulnosadmin:x:1000:
341: myaql:x:104:
342: webmin:x:1001:
343: ssh:x:105:
344: postfix:x:106:
345: postgres:x:107:
346: group:x:108:
347: nobody:x:65534:
348: libuuid:x:100:
349: syslog:x:101:
350: messagebus:x:102:
351: landscape:x:103:
352: vulnosadmin:x:1000:
353: myaql:x:104:
354: webmin:x:1001:
355: ssh:x:105:
356: postfix:x:106:
357: postgres:x:107:
358: group:x:108:
359: nobody:x:65534:
360: libuuid:x:100:
361: syslog:x:101:
362: messagebus:x:102:
363: landscape:x:103:
364: vulnosadmin:x:1000:
365: myaql:x:104:
366: webmin:x:1001:
367: ssh:x:105:
368: postfix:x:106:
369: postgres:x:107:
370: group:x:108:
371: nobody:x:65534:
372: libuuid:x:100:
373: syslog:x:101:
374: messagebus:x:102:
375: landscape:x:103:
376: vulnosadmin:x:1000:
377: myaql:x:104:
378: webmin:x:1001:
379: ssh:x:105:
380: postfix:x:106:
381: postgres:x:107:
382: group:x:108:
383: nobody:x:65534:
384: libuuid:x:100:
385: syslog:x:101:
386: messagebus:x:102:
387: landscape:x:103:
388: vulnosadmin:x:1000:
389: myaql:x:104:
390: webmin:x:1001:
391: ssh:x:105:
392: postfix:x:106:
393: postgres:x:107:
394: group:x:108:
395: nobody:x:65534:
396: libuuid:x:100:
397: syslog:x:101:
398: messagebus:x:102:
399: landscape:x:103:
400: vulnosadmin:x:1000:
401: myaql:x:104:
402: webmin:x:1001:
403: ssh:x:105:
404: postfix:x:106:
405: postgres:x:107:
406: group:x:108:
407: nobody:x:65534:
408: libuuid:x:100:
409: syslog:x:101:
410: messagebus:x:102:
411: landscape:x:103:
412: vulnosadmin:x:1000:
413: myaql:x:104:
414: webmin:x:1001:
415: ssh:x:105:
416: postfix:x:106:
417: postgres:x:107:
418: group:x:108:
419: nobody:x:65534:
420: libuuid:x:100:
421: syslog:x:101:
422: messagebus:x:102:
423: landscape:x:103:
424: vulnosadmin:x:1000:
425: myaql:x:104:
426: webmin:x:1001:
427: ssh:x:105:
428: postfix:x:106:
429: postgres:x:107:
430: group:x:108:
431: nobody:x:65534:
432: libuuid:x:100:
433: syslog:x:101:
434: messagebus:x:102:
435: landscape:x:103:
436: vulnosadmin:x:1000:
437: myaql:x:104:
438: webmin:x:1001:
439: ssh:x:105:
440: postfix:x:106:
441: postgres:x:107:
442: group:x:108:
443: nobody:x:65534:
444: libuuid:x:100:
445: syslog:x:101:
446: messagebus:x:102:
447: landscape:x:103:
448: vulnosadmin:x:1000:
449: myaql:x:104:
450: webmin:x:1001:
451: ssh:x:105:
452: postfix:x:106:
453: postgres:x:107:
454: group:x:108:
455: nobody:x:65534:
456: libuuid:x:100:
457: syslog:x:101:
458: messagebus:x:102:
459: landscape:x:103:
460: vulnosadmin:x:1000:
461: myaql:x:104:
462: webmin:x:1001:
463: ssh:x:105:
464: postfix:x:106:
465: postgres:x:107:
466: group:x:108:
467: nobody:x:65534:
468: libuuid:x:100:
469: syslog:x:101:
470: messagebus:x:102:
471: landscape:x:103:
472: vulnosadmin:x:1000:
473: myaql:x:104:
474: webmin:x:1001:
475: ssh:x:105:
476: postfix:x:106:
477: postgres:x:107:
478: group:x:108:
479: nobody:x:65534:
480: libuuid:x:100:
481: syslog:x:101:
482: messagebus:x:102:
483: landscape:x:103:
484: vulnosadmin:x:1000:
485: myaql:x:104:
486: webmin:x:1001:
487: ssh:x:105:
488: postfix:x:106:
489: postgres:x:107:
490: group:x:108:
491: nobody:x:65534:
492: libuuid:x:100:
493: syslog:x:101:
494: messagebus:x:102:
495: landscape:x:103:
496: vulnosadmin:x:1000:
497: myaql:x:104:
498: webmin:x:1001:
499: ssh:x:105:
500: postfix:x:106:
501: postgres:x:107:
502: group:x:108:
503: nobody:x:65534:
504: libuuid:x:100:
505: syslog:x:101:
506: messagebus:x:102:
507: landscape:x:103:
508: vulnosadmin:x:1000:
509: myaql:x:104:
510: webmin:x:1001:
511: ssh:x:105:
512: postfix:x:106:
513: postgres:x:107:
514: group:x:108:
515: nobody:x:65534:
516: libuuid:x:100:
517: syslog:x:101:
518: messagebus:x:102:
519: landscape:x:103:
520: vulnosadmin:x:1000:
521: myaql:x:104:
522: webmin:x:1001:
523: ssh:x:105:
524: postfix:x:106:
525: postgres:x:107:
526: group:x:108:
527: nobody:x:65534:
528: libuuid:x:100:
529: syslog:x:101:
530: messagebus:x:102:
531: landscape:x:103:
532: vulnosadmin:x:1000:
533: myaql:x:104:
534: webmin:x:1001:
535: ssh:x:105:
536: postfix:x:106:
537: postgres:x:107:
538: group:x:108:
539: nobody:x:65534:
540: libuuid:x:100:
541: syslog:x:101:
542: messagebus:x:102:
543: landscape:x:103:
544: vulnosadmin:x:1000:
545: myaql:x:104:
546: webmin:x:1001:
547: ssh:x:105:
548: postfix:x:106:
549: postgres:x:107:
550: group:x:108:
551: nobody:x:65534:
552: libuuid:x:100:
553: syslog:x:101:
554: messagebus:x:102:
555: landscape:x:103:
556: vulnosadmin:x:1000:
557: myaql:x:104:
558: webmin:x:1001:
559: ssh:x:105:
560: postfix:x:106:
561: postgres:x:107:
562: group:x:108:
563: nobody:x:65534:
564: libuuid:x:100:
565: syslog:x:101:
566: messagebus:x:102:
567: landscape:x:103:
568: vulnosadmin:x:1000:
569: myaql:x:104:
570: webmin:x:1001:
571: ssh:x:105:
572: postfix:x:106:
573: postgres:x:107:
574: group:x:108:
575: nobody:x:65534:
576: libuuid:x:100:
577: syslog:x:101:
578: messagebus:x:102:
579: landscape:x:103:
580: vulnosadmin:x:1000:
581: myaql:x:104:
582: webmin:x:1001:
583: ssh:x:105:
584: postfix:x:106:
585: postgres:x:107:
586: group:x:108:
587: nobody:x:65534:
588: libuuid:x:100:
589: syslog:x:101:
590: messagebus:x:102:
591: landscape:x:103:
592: vulnosadmin:x:1000:
593: myaql:x:104:
594: webmin:x:1001:
595: ssh:x:105:
596: postfix:x:106:
597: postgres:x:107:
598: group:x:108:
599: nobody:x:65534:
600: libuuid:x:100:
601: syslog:x:101:
602: messagebus:x:102:
603: landscape:x:103:
604: vulnosadmin:x:1000:
605: myaql:x:104:
606: webmin:x:1001:
607: ssh:x:105:
608: postfix:x:106:
609: postgres:x:107:
610: group:x:108:
611: nobody:x:65534:
612: libuuid:x:100:
613: syslog:x:101:
614: messagebus:x:102:
615: landscape:x:103:
616: vulnosadmin:x:1000:
617: myaql:x:104:
618: webmin:x:1001:
619: ssh:x:105:
620: postfix:x:106:
621: postgres:x:107:
622: group:x:108:
623: nobody:x:65534:
624: libuuid:x:100:
625: syslog:x:101:
626: messagebus:x:102:
627: landscape:x:103:
628: vulnosadmin:x:1000:
629: myaql:x:104:
630: webmin:x:1001:
631: ssh:x:105:
632: postfix:x:106:
633: postgres:x:107:
634: group:x:108:
635: nobody:x:65534:
636: libuuid:x:100:
637: syslog:x:101:
638: messagebus:x:102:
639: landscape:x:103:
640: vulnosadmin:x:1000:
641: myaql:x:104:
642: webmin:x:1001:
643: ssh:x:105:
644: postfix:x:106:
645: postgres:x:107:
646: group:x:108:
647: nobody:x:65534:
648: libuuid:x:100:
649: syslog:x:101:
650: messagebus:x:102:
651: landscape:x:103:
652: vulnosadmin:x:1000:
653: myaql:x:104:
654: webmin:x:1001:
655: ssh:x:105:
656: postfix:x:106:
657: postgres:x:107:
658: group:x:108:
659: nobody:x:65534:
660: libuuid:x:100:
661: syslog:x:101:
662: messagebus:x:102:
663: landscape:x:103:
664: vulnosadmin:x:1000:
665: myaql:x:104:
666: webmin:x:1001:
667: ssh:x:105:
668: postfix:x:106:
669: postgres:x:107:
670: group:x:108:
671: nobody:x:65534:
672: libuuid:x:100:
673: syslog:x:101:
674: messagebus:x:102:
675: landscape:x:103:
676: vulnosadmin:x:1000:
677: myaql:x:104:
678: webmin:x:1001:
679: ssh:x:105:
680: postfix:x:106:
681: postgres:x:107:
682: group:x:108:
683: nobody:x:65534:
684: libuuid:x:100:
685: syslog:x:101:
686: messagebus:x:102:
687: landscape:x:103:
688: vulnosadmin:x:1000:
689: myaql:x:104:
690: webmin:x:1001:
691: ssh:x:105:
692: postfix:x:106:
693: postgres:x:107:
694: group:x:108:
695: nobody:x:65534:
696: libuuid:x:100:
697: syslog:x:101:
698: messagebus:x:102:
699: landscape:x:103:
700: vulnosadmin:x:1000:
701: myaql:x:104:
702: webmin:x:1001:
703: ssh:x:105:
704: postfix:x:106:
705: postgres:x:107:
706: group:x:108:
707: nobody:x:65534:
708: libuuid:x:100:
709: syslog:x:101:
710: messagebus:x:102:
711: landscape:x:103:
712: vulnosadmin:x:1000:
713: myaql:x:104:
714: webmin:x:1001:
715: ssh:x:105:
716: postfix:x:106:
717: postgres:x:107:
718: group:x:108:
719: nobody:x:65534:
720: libuuid:x:100:
721: syslog:x:101:
722: messagebus:x:102:
723: landscape:x:103:
724: vulnosadmin:x:1000:
725: myaql:x:104:
726: webmin:x:1001:
727: ssh:x:105:
728: postfix:x:106:
729: postgres:x:107:
730: group:x:108:
731: nobody:x:65534:
732: libuuid:x:100:
733: syslog:x:101:
734: messagebus:x:102:
735: landscape:x:103:
736: vulnosadmin:x:1000:
737: myaql:x:104:
738: webmin:x:1001:
739: ssh:x:105:
740: postfix:x:106:
741: postgres:x:107:
742: group:x:108:
743: nobody:x:65534:
744: libuuid:x:100:
745: syslog:x:101:
746: messagebus:x:102:
747: landscape:x:103:
748: vulnosadmin:x:1000:
749: myaql:x:104:
750: webmin:x:1001:
751: ssh:x:105:
752: postfix:x:106:
753: postgres:x:107:
754: group:x:108:
755: nobody:x:65534:
756: libuuid:x:100:
757: syslog:x:101:
758: messagebus:x:102:
759: landscape:x:103:
760: vulnosadmin:x:1000:
761: myaql:x:104:
762: webmin:x:1001:
763: ssh:x:105:
764: postfix:x:106:
765: postgres:x:107:
766: group:x:108:
767: nobody:x:65534:
768: libuuid:x:100:
769: syslog:x:101:
770: messagebus:x:102:
771: landscape:x:103:
772: vulnosadmin:x:1000:
773: myaql:x:104:
774: webmin:x:1001:
775: ssh:x:105:
776: postfix:x:106:
777: postgres:x:107:
778: group:x:108:
779: nobody:x:65534:
780: libuuid:x:100:
781: syslog:x:101:
782: messagebus:x:102:
783: landscape:x:103:
784: vulnosadmin:x:1000:
785: myaql:x:104:
786: webmin:x:1001:
787: ssh:x:105:
788: postfix:x:106:
789: postgres:x:107:
790: group:x:108:
791: nobody:x:65534:
792: libuuid:x:100:
793: syslog:x:101:
794: messagebus:x:102:
795: landscape:x:103:
796: vulnosadmin:x:1000:
797: myaql:x:104:
798: webmin:x:1001:
799: ssh:x:105:
800: postfix:x:106:
801: postgres:x:107:
802: group:x:108:
803: nobody:x:65534:
804: libuuid:x:100:
805: syslog:x:101:
806: messagebus:x:102:
807: landscape:x:103:
808: vulnosadmin:x:1000:
809: myaql:x:104:
810: webmin:x:1001:
811: ssh:x:105:
812: postfix:x:106:
813: postgres:x:107:
814: group:x:108:
815: nobody:x:65534:
816: libuuid:x:100:
817: syslog:x:101:
818: messagebus:x:102:
819: landscape:x:103:
820: vulnosadmin:x:1000:
821: myaql:x:104:
822: webmin:x:1001:
823: ssh:x:105:
824: postfix:x:106:
825: postgres:x:107:
826: group:x:108:
827: nobody:x:65534:
828: libuuid:x:
```

Q14: What command did the attacker use to gain root privilege? (Answer contains two spaces).

- In the 'auth.log', I searched keyword 'COMMAND' and found the command 'sudo su -' which executed by the compromised user.

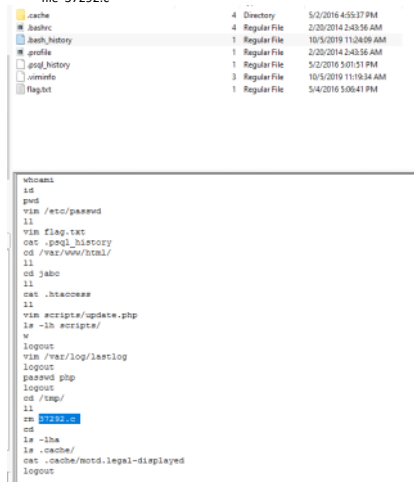
```

Line 2280: Oct 5 13:06:38 Vuln0sV2 sudo: root: TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/sbin/useradd -d /usr/php -m --system --shell /bin/bash --skel
Line 2297: Oct 5 13:14:04 Vuln0sV2 sudo: mail: TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2310: Oct 5 13:19:21 Vuln0sV2 sudo: mail: TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2323: Oct 5 13:21:11 Vuln0sV2 sudo: mail: TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2331: Oct 5 13:21:30 Vuln0sV2 sudo: mail: TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2345: Oct 5 13:23:39 Vuln0sV2 sudo: mail: TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -

```

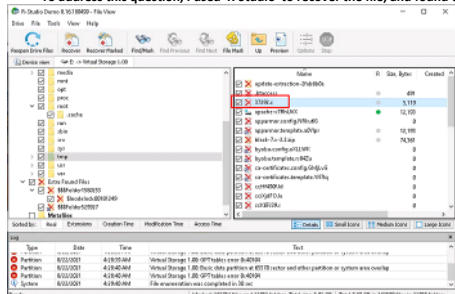
Q15: Which file did the user 'root' delete?

- In the 'Bash_history' file which located at '/root' directory, you are able to see the deletion of the file '37292.c'



Q16:Recover the deleted file, open it and extract the exploit author name.

- To address this question, I used 'R-Studio' to recover the file, and found the author is 'rebel'



Q17: What is the content management system (CMS) installed on the machine?

- To address the question of identifying the installed CMS, I accessed the `/var/www/html/jabc` directory, which is a common directory for CMS installations. Upon inspecting the contents of the `.htaccess` file, I found that the installed CMS is **Drupal**.

This was confirmed through typical Drupal configurations found within the .htaccess file, which is often used for URL rewrites, access control, and security settings specific to Drupal installations.

Q18: What is the version of the CMS installed on the machine?

- I just navigated in '/var/www/html/jab' files and found in the 'profiles/testing/testing.info' file which included the version of the CMS system.

```
; Information added by Drupal.org packaging script on 2014-01-15
version = "7.26"
project = "drupal"
datestamp = "1389815930"
```

Q19: Which port was listening to receive the attacker's reverse shell?

- I accessed the 'access.log' and found suspicious POST request, after URL decoding, we are able to see the port 4444.

[illegible]