NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO:

Consider a program that attempts to connect to Google’s SMTP server using the method smtplib.SMTP. The `ssl.create_default_context` function returns a new `SSLContext` object with default settings (e.g., default protocol, options, and cipher) for the given purpose (client authentication or server authentication). The arguments `cafile`, `capath`, and `cadata` represent optional CA certificates to trust for certificate verification. The `SSLContext` class returned by `ssl.create_default_context` helps manage settings and certificates that can be inherited by SSL sockets. The method `SMTP.starttls` puts the SMTP connection in TLS (Transport Layer Security) mode. After that, all SMTP commands that follow will be encrypted. Answer the following questions using this snippet of code.

```
# import whatever is needed
smtp = smtplib.SMTP("smtp.google.com", port=587)
ctx = ssl.create_default_context()
smtp.starttls(context = ctx)
# continue to communicate to the SMTP server...
```

Questions:

1. What will the program do when executed?

2. What type of verification occurs when `SMTP.starttls` is executed?
a. hostname authentication (i.e. checking the hostname against the CN of the certification)
b. server identity authentication (i.e. checking the certification authenticity and validity)
c. a and b
d. None of the above

[Other statistical questions will be imported here while creating the survey.}

NOTE: ANSWER IS TO BE SHOWN TO THE PUZZLE TAKER AT THE END OF THE SESSION.

ANSWERS:

1. The program will attempt to connect to the SMTP server using the created ssl context.

2. c
Since `ssl.create_default_context` is used, the hostname verification and server identification are enabled by default.

NOTE: THE REST OF THIS DOCUMENT CONTAINS EXTRA INFORMATION FOR THE PROJECT RESEARCHERS. IT IS NOT TO BE SHOWN TO THE PUZZLE TAKERS.

TAGS:
python, ssl, certificate-validation,

CATEGORIES:
Blindspot - NO
Type - SSL
Number of distinct functions - 3
Number of total functions - 3
Blindspot function - N/A
Function call omitted - YES
Blindspot type - N/A
Number of parameters in the blindspot function - N/A
Cyclomatic complexity - 2

NAME:
ssl.create_default_context

DESCRIPTION:
The program returns a new SSLContext object with default settings for the given purpose. The settings are chosen by the ssl module, and usually represent a higher security level than when calling the SSLContext constructor directly.

The settings are: PROTOCOL_SSLv23, OP_NO_SSLv2, and OP_NO_SSLv3 with high encryption cipher suites without RC4 and without unauthenticated cipher suites. Passing SERVER_AUTH as purpose sets verify_mode to CERT_REQUIRED and either loads CA certificates (when at least one of cafile, capath or cadata is given) or uses SSLContext.load_default_certs() to load default CA certificates.

BLINDSPOT:
#N/A

CORRECT USE EXAMPLE:
#N/A

MORE INFORMATION:
#N/A

REFERENCES:

1. https://docs.python.org/3/library/ssl.html#ssl-security