2. Banners de servidores

Wednesday, November 4, 2020 8:03 AM

Los banners exponen el nombre del servidor web y/o la versión que está corriendo en el servidior. Algunos, incluso, exponen la tecnología backend usada y su versión.

Por esta razón siempre debemos probar los banners en nuestros servidores para verificar que no dejamos al descubierto información sensible.

```
#!/usr/bin/python3
# Obtain server banner

import socket
import argparse


if __name__ == "__main__":
    parser = argparse.ArgumentParser(description='Obtain server banner')
    # Main arguments
    parser.add_argument("-target", dest="target", help="target IP / domain", required
    parser.add_argument("-port", dest="port", help="Port", type=int, required=True)
    parsed_args = parser.parse_args()

    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((parsed_args.target, parsed_args.port))
    sock.settimeout(2)

    targetBytes = parsed_args.target.encode()
    http_get = b"GET /index.html HTTP/1.1\r\nHost: "+targetBytes+b"\r\nAccept: */*\r\
    data = ''
    try:
        sock.sendall(http_get)
        data = sock.recvfrom(1024)
        print (data[0].decode())
    except socket.error:
        print ("Socket error", socket.errno)
    finally:
        print("closing connection")
        sock.close()
```

```
C:\Users\marle\Downloads\Investigación web>python BannerServer.py -target www.fcfm.uanl.mx
HTTP/1.1 404 Not Found
Date: Wed, 04 Nov 2020 23:19:07 GMT
Server: Apache/2.4.38 (Debian)
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: es
X-Frame-Options: SAMEORIGIN
X-Generator: Drupal 7 (http://drupal.org)
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

4ebb
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML+RDFa 1.1//EN">
<html lang="es" dir="ltr" version="HTML+RDFa 1.1"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:dc="http://purl.org/dc/terms/"
  xmlns:foaf="http://xmlns.com/foaf/0.1/"
```

```
  xmlns:og="http://ogp.me/ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:sioc="http://rdfs.org/sioc/ns#"
  xmlns:sioct="http://rdfs.org/sioc/types#"
  xmlns:skos="http://www.w3.org/2004/02/skos/core#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#">
<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta na
closing connection
```