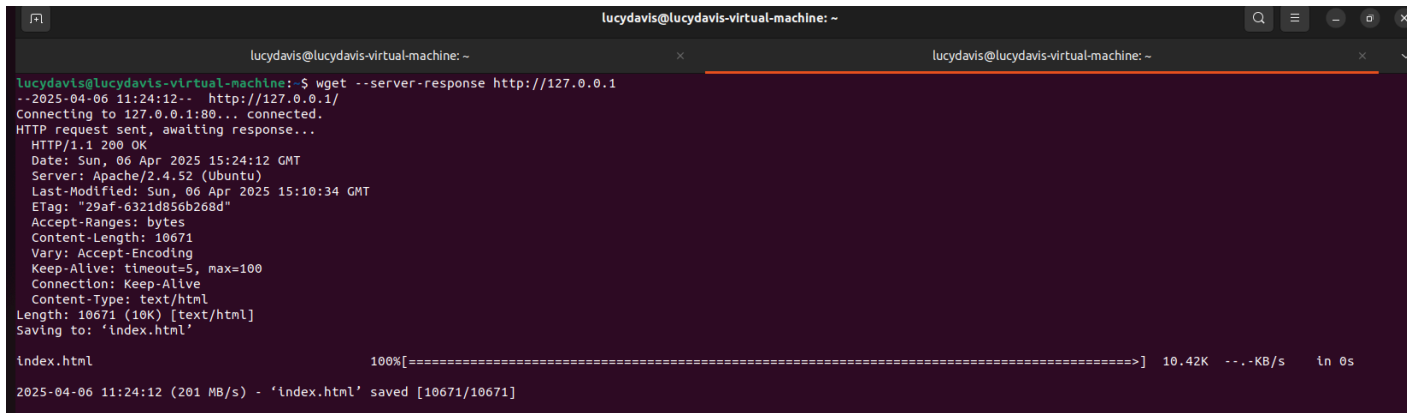


Lucy Njuguna

Network Banner Grabbing Project

1. Apache Banner Grabbing Result (Using wget)



```
lucydavis@lucydavis-virtual-machine: ~  
lucydavis@lucydavis-virtual-machine:~$ wget --server-response http://127.0.0.1  
--2025-04-06 11:24:12-- http://127.0.0.1/  
Connecting to 127.0.0.1:80... connected.  
HTTP request sent, awaiting response...  
HTTP/1.1 200 OK  
Date: Sun, 06 Apr 2025 15:24:12 GMT  
Server: Apache/2.4.52 (Ubuntu)  
Last-Modified: Sun, 06 Apr 2025 15:10:34 GMT  
ETag: "29af-6321d856b268d"  
Accept-Ranges: bytes  
Content-Length: 10671  
Vary: Accept-Encoding  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html  
Length: 10671 (10K) [text/html]  
Saving to: 'index.html'  
  
index.html      100%[=====] 10.42K  --.-KB/s  in 0s  
2025-04-06 11:24:12 (201 MB/s) - 'index.html' saved [10671/10671]
```

Command Used:

wget --server-response http://127.0.0.1

Tool: wget

Target: Apache Web Server (Port 80)

Result:

The wget tool was used to retrieve the HTTP response from the Apache web server running on port 80. The server returned the following banner:

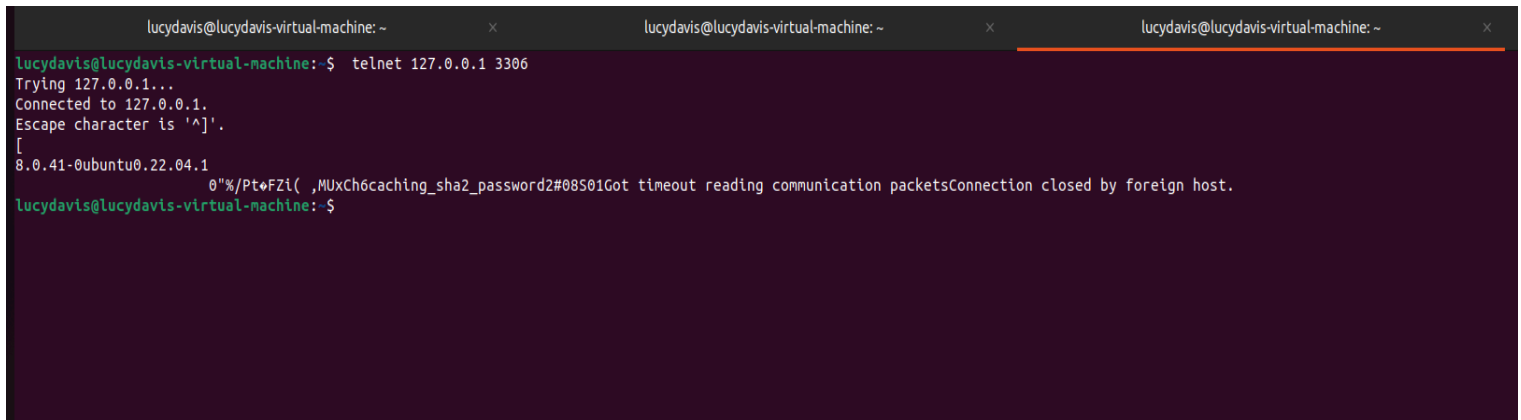
Server: Apache/2.4.52 (Ubuntu)

This indicates that the web server is running **Apache version 2.4.52** on an **Ubuntu** operating system. The version number is critical because attackers can cross-reference it with known vulnerability databases to identify potential exploits for that version of Apache. The server also returned the **index.html** page, which was saved locally.

Potential Risk:

Knowing the version of Apache running on the server can be a security risk. If the version is outdated or has known vulnerabilities, attackers could exploit those weaknesses. This shows the importance of keeping software up to date to avoid unnecessary security risks.

B. MySQL Server- telnet Banner Grabbing



```
lucydavis@lucydavis-virtual-machine: ~  
lucydavis@lucydavis-virtual-machine: ~  
lucydavis@lucydavis-virtual-machine: ~  
lucydavis@lucydavis-virtual-machine:~$ telnet 127.0.0.1 3306  
Trying 127.0.0.1...  
Connected to 127.0.0.1.  
Escape character is '^]'.  
[  
8.0.41-0ubuntu0.22.04.1  
0"%/PtoFZi( ,MUXCh6caching_sha2_password2#08S01Got timeout reading communication packetsConnection closed by foreign host.  
lucydavis@lucydavis-virtual-machine:~$
```

Command Used:

telnet 127.0.0.1 3306

Tool: telnet

Target: MySQL Server (Port 3306)

Findings:

The telnet tool was used to connect to MySQL running on port 3306. The server returned the following banner: **8.0.41-0ubuntu0.22.04.1**.

This banner revealed that the MySQL server is running version 8.0.41. The banner confirms that MySQL is operational and responding on port 3306.

Potential risk:

The banner reveals the version of MySQL in use, which can be valuable information for both system administrators and attackers. Knowing the version can help determine if the system is vulnerable to known exploits specific to that version. For instance, certain vulnerabilities are associated with older versions of MySQL, and attackers can use this information to tailor their attacks.

Banner grabbing using telnet successfully identified that MySQL is running on port 3306 and revealed its version number, 8.0.41. This information could potentially expose the server to security risks if left unprotected, as attackers could use it to exploit vulnerabilities tied to this version.

C. Django App (Port 8000)

```
lucydavis@lucydavis-virtual-machine:~/Downloads/djangotutorial$ wget --server-response http://127.0.0.1:8000/admin/login/?next=/admin/
--2025-04-06 13:57:00-- http://127.0.0.1:8000/admin/login/?next=/admin/
Connecting to 127.0.0.1:8000... connected.
HTTP request sent, awaiting response...
HTTP/1.1 200 OK
Date: Sun, 06 Apr 2025 17:57:00 GMT
Server: WSGIServer/0.2 CPython/3.10.12
Content-Type: text/html; charset=utf-8
Expires: Sun, 06 Apr 2025 17:57:00 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate, private
X-Frame-Options: DENY
Content-Length: 710
Vary: Cookie
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Length: 710 [text/html]
Saving to: 'index.html?next=%2Fadmin%2F'

index.html?next=%2Fadmin%2F          100%[=====] 710 --.-KB/s  in 0s

2025-04-06 13:57:00 (83.6 MB/s) - 'index.html?next=%2Fadmin%2F' saved [710/710]
```

Command used:

wget --server-response http://127.0.0.1:8000/admin/login/?next=/admin/

Findings:

The wget tool was used to send an HTTP request to the Django application. The banner revealed that the server is running WSGIServer/0.2 with CPython/3.10.12 as the Python runtime. This indicates that the Django application is hosted using WSGI and is running on Python 3.10.12. The server successfully served the request with an HTTP 200 OK status, confirming that the Django application is operational and accessible via HTTP on the specified port (8000).

Potential Risks

Server Disclosure: The banner discloses the WSGI server and Python version(**WSGIServer/0.2** and **CPython/3.10.12**). This could potentially help attackers pinpoint known vulnerabilities associated with the server or Python version.



Key Takeaways

- Banner grabbing is a simple but powerful reconnaissance technique.
- Exposed software versions can significantly increase an organization's attack surface.
- Masking server banners or using reverse proxies/firewalls can mitigate these risks.