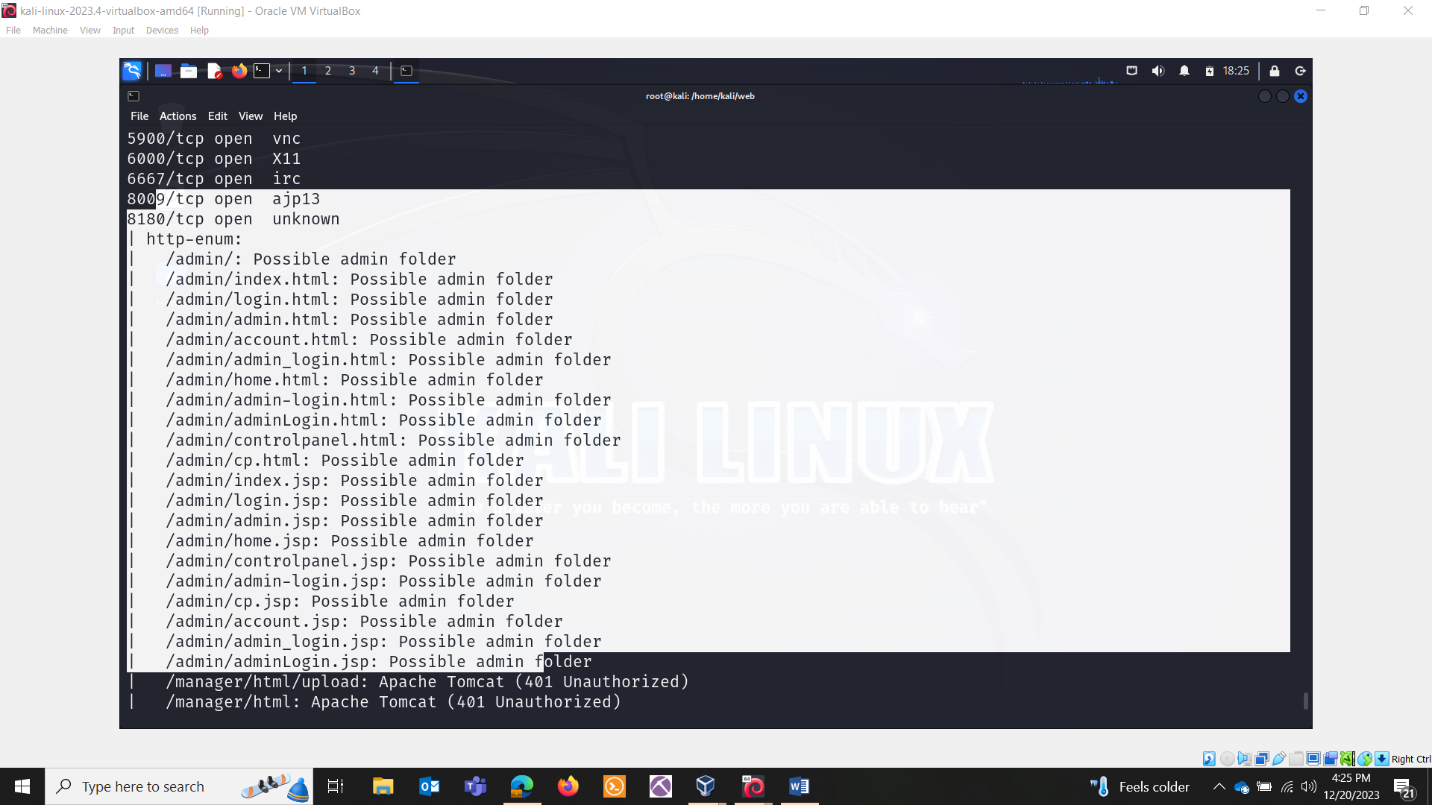
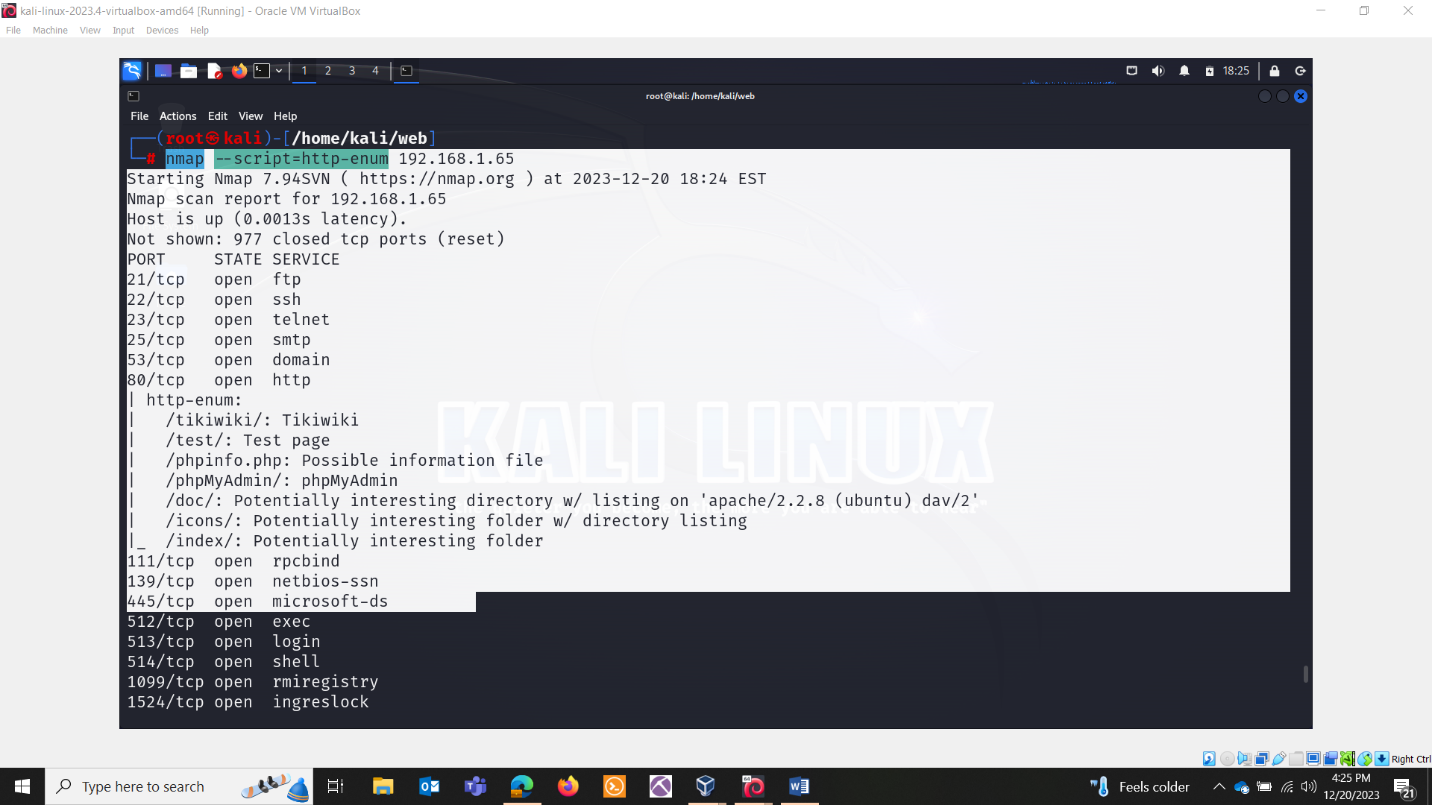
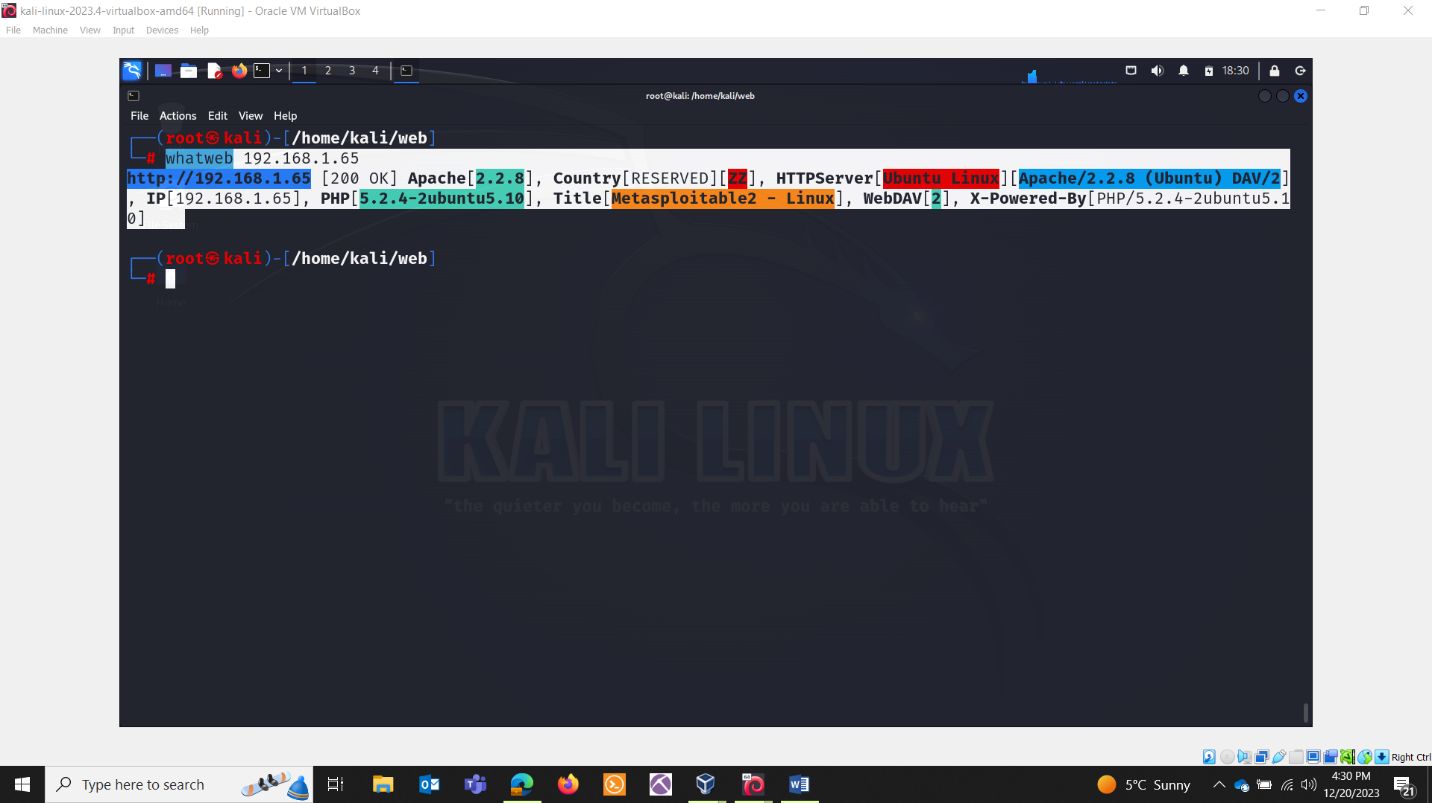
HTTP

Nmap script:

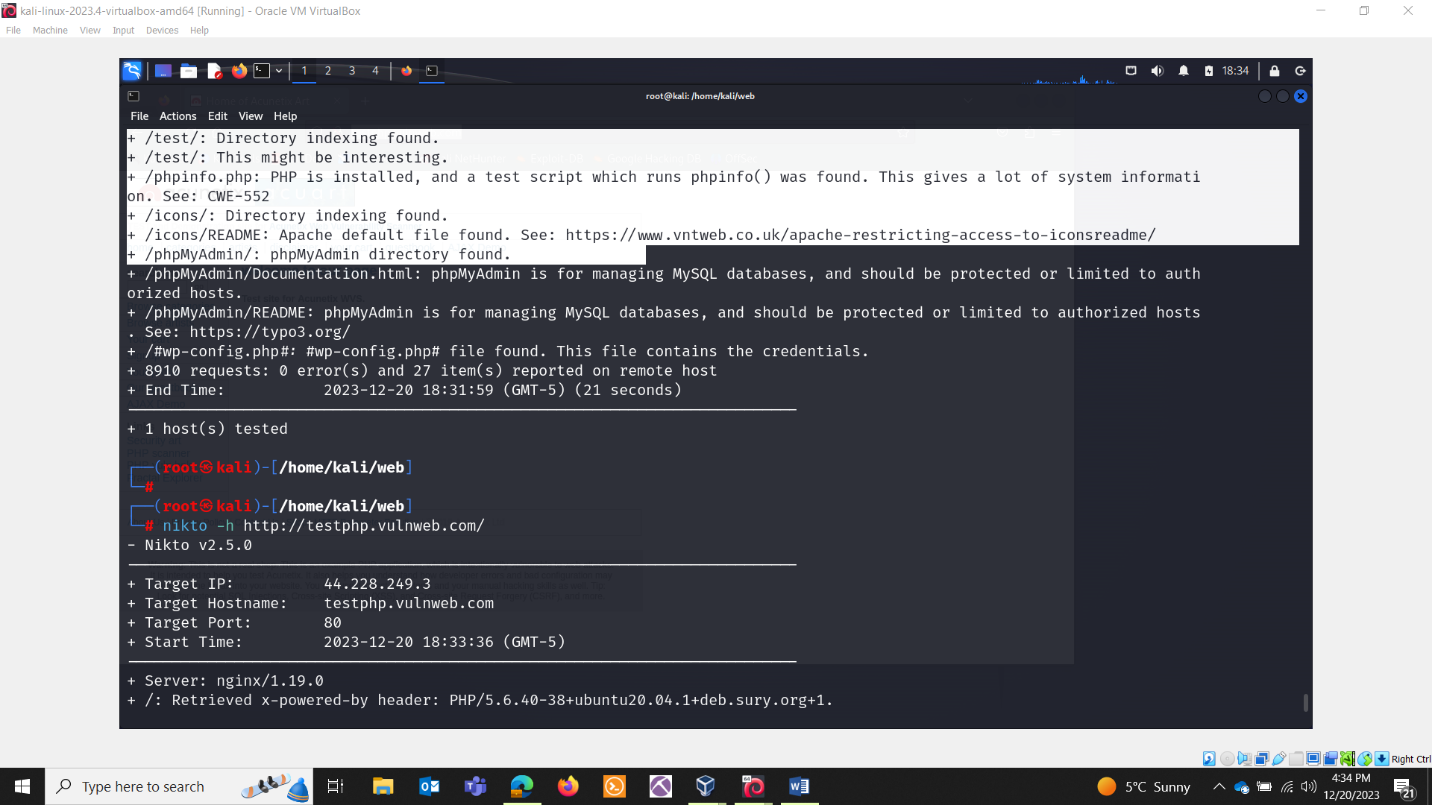
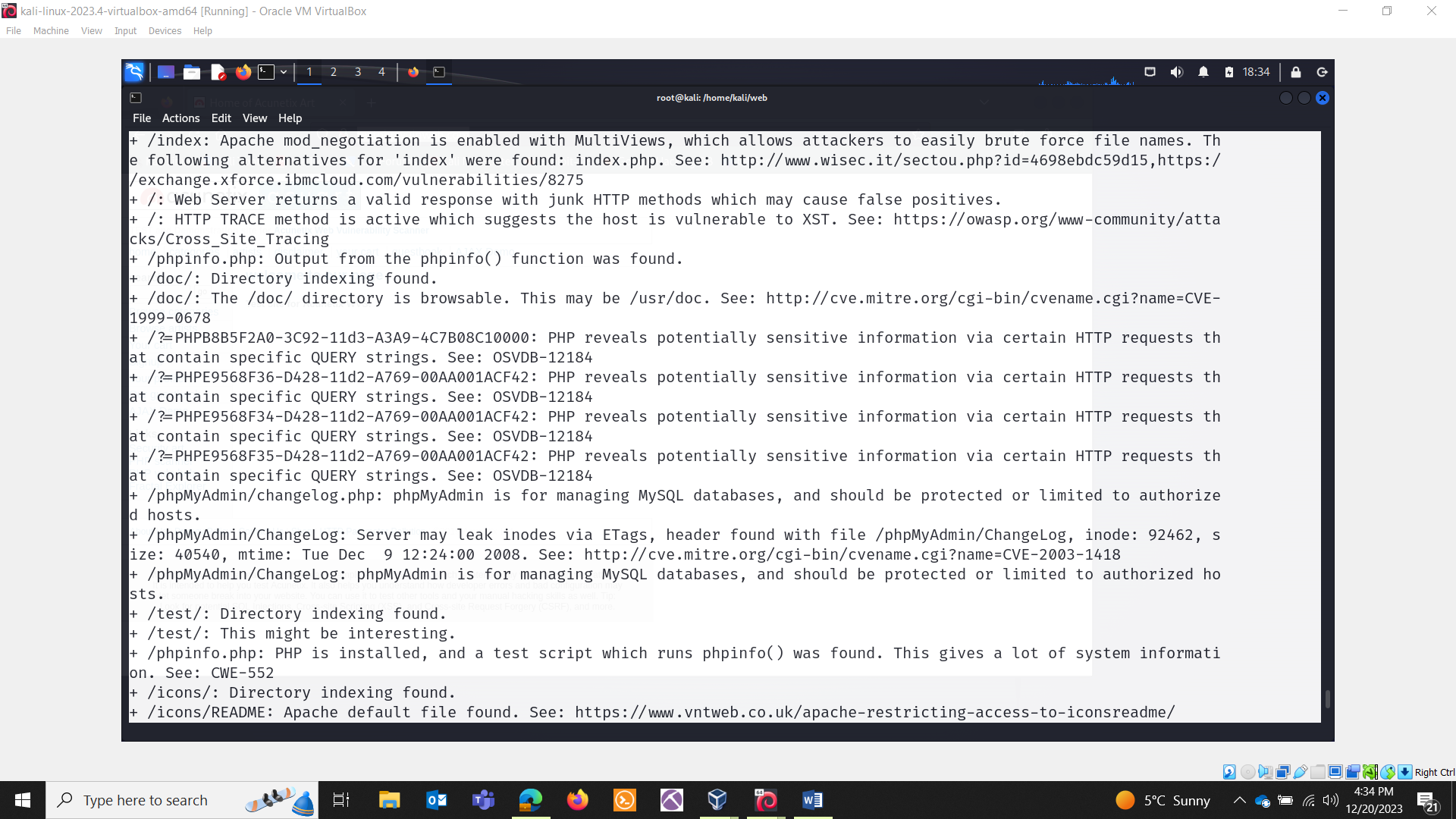
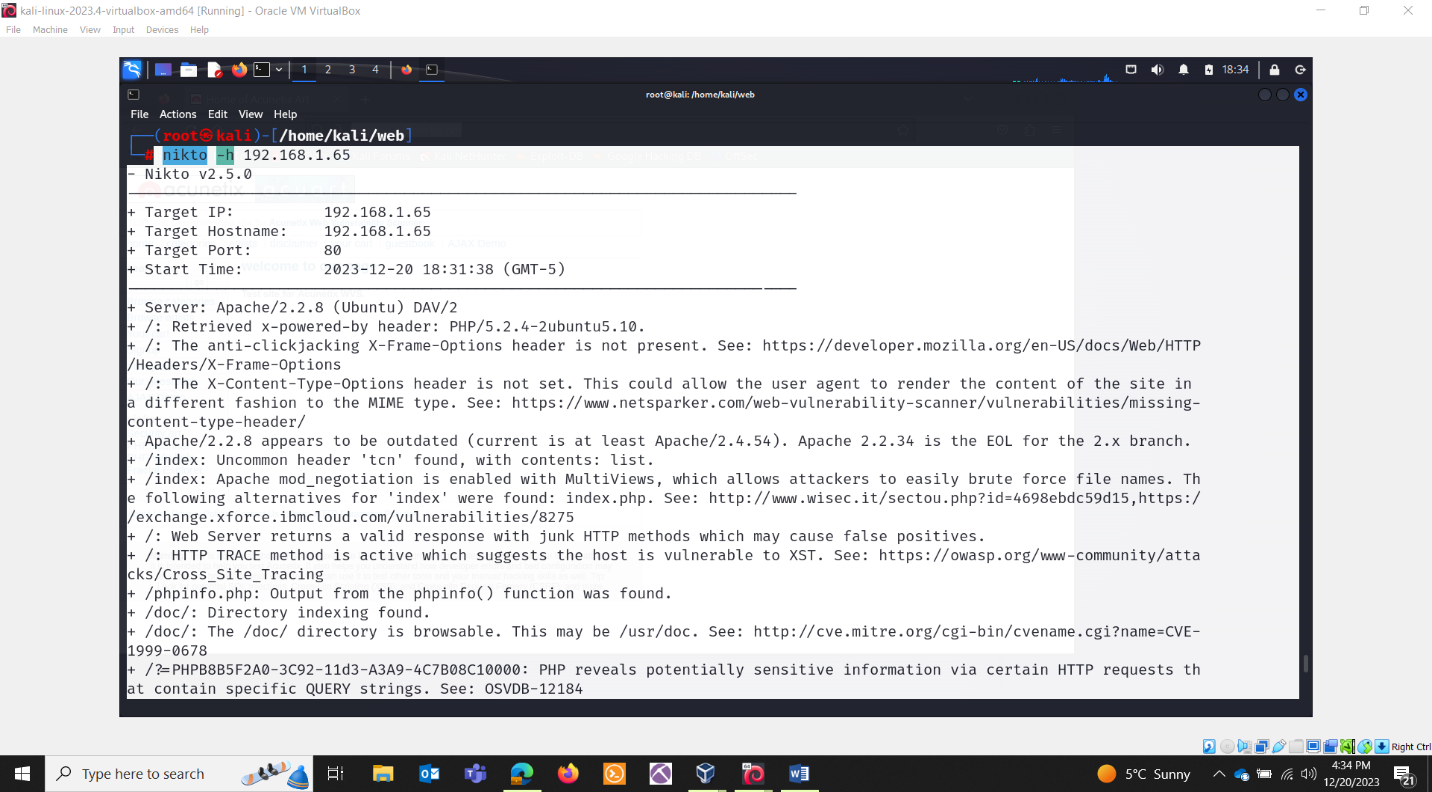


WHATWEB:

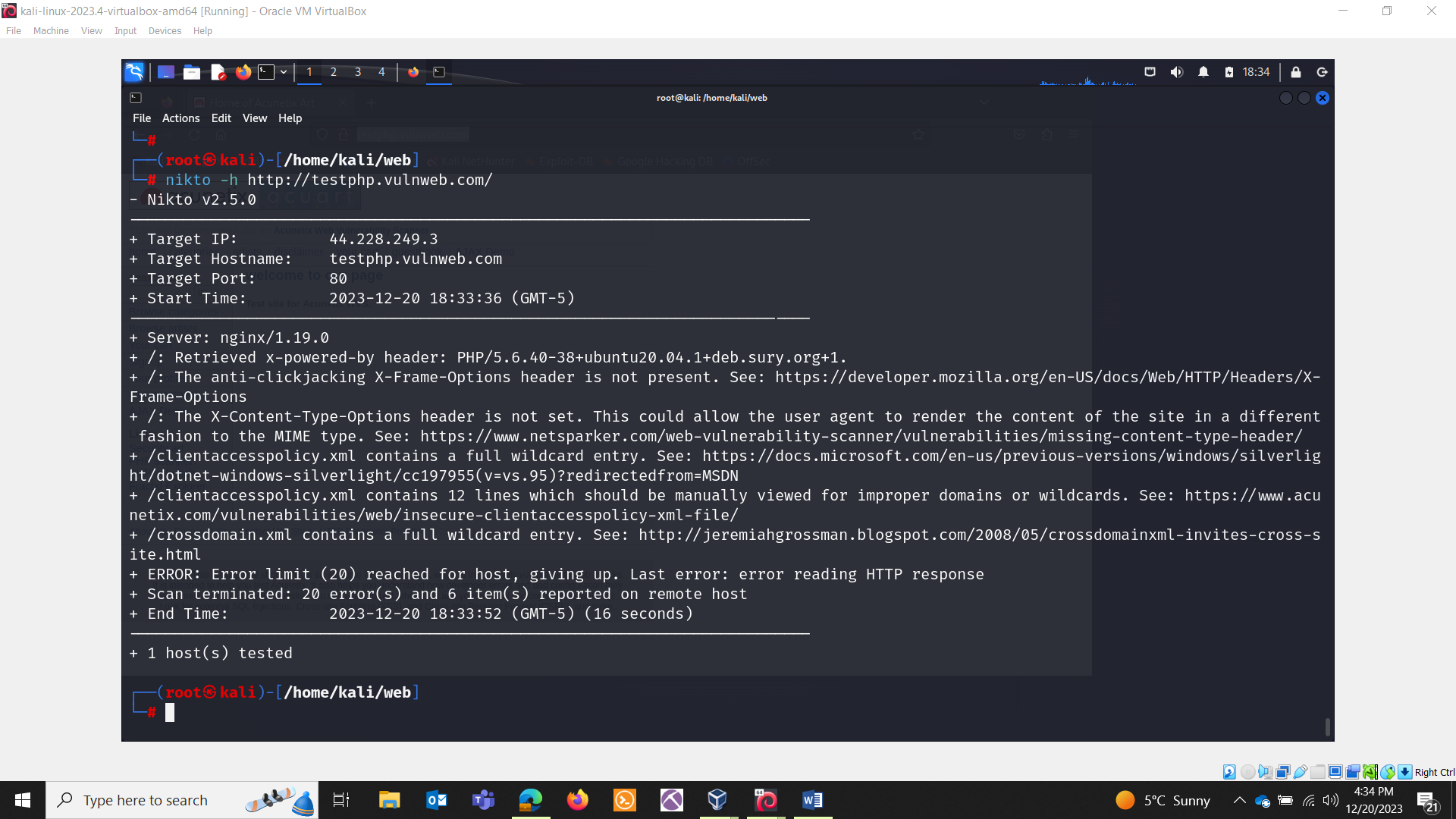


NIKTO :

On meta machine:



On testphp.vulnweb:



* The anti-clickjacking X-Frame-Options header is not present:

Explanation: The X-Frame-Options header is missing, which can leave the website vulnerable to clickjacking attacks. Clickjacking involves tricking a user into clicking on something different from what the user perceives, potentially leading to malicious actions.

Recommendation: Implement the X-Frame-Options header to mitigate clickjacking. This header tells the browser whether the site can be framed and helps prevent attacks.

* The X-Content-Type-Options header is not set:

Explanation: The X-Content-Type-Options header is missing, which could allow the user agent to render content in a different fashion than the declared MIME type. This may expose the site to MIME-sniffing attacks.

Recommendation: Set the X-Content-Type-Options header to "nosniff" to prevent browsers from interpreting files as a different MIME type.

* Apache/2.2.8 appears to be outdated:

Explanation: The web server is running an outdated version of Apache (2.2.8). The current recommended version is at least Apache/2.4.54. Apache 2.2.34 is the End-of-Life (EOL) for the 2.x branch.

Recommendation: Update the Apache server to a more recent version to address known vulnerabilities and benefit from security updates.

* Uncommon header 'tcn' found:

Explanation: The 'tcn' header is an uncommon header found in the response, with contents: "list."

Recommendation: Investigate the presence and significance of the 'tcn' header. It may be necessary to review server configurations and headers.

* Apache mod\_negotiation is enabled with MultiViews:

Explanation: Apache mod\_negotiation is enabled with MultiViews, allowing attackers to easily brute force file names. Alternatives for 'index' were found, such as 'index.php.'

Recommendation: Disable MultiViews and review server configurations to enhance security against brute force attacks.

* Web Server returns a valid response with junk HTTP methods:

Explanation: The web server responds with valid responses to non-standard HTTP methods, which may cause false positives in security testing.

Recommendation: Configure the server to respond appropriately to standard HTTP methods and restrict responses to unknown or unnecessary methods.

* HTTP TRACE method is active:

Explanation: The HTTP TRACE method is active, suggesting a potential vulnerability to Cross-Site Tracing (XST).

Recommendation: Disable the TRACE method to mitigate the risk of XST attacks.

* Output from the phpinfo() function was found:

Explanation: Information from the phpinfo() function is exposed, providing detailed system information.

Recommendation: Remove or restrict access to the phpinfo.php script to prevent the disclosure of sensitive information.

* Directory indexing found in /doc/ and /test/:

Explanation: Directory indexing is enabled in the '/doc/' and '/test/' directories, allowing the contents of these directories to be browsed.

Recommendation: Disable directory indexing to enhance security and privacy.

* PHP reveals potentially sensitive information via certain QUERY strings:

Explanation: PHP reveals potentially sensitive information through specific QUERY strings.

Recommendation: Review and secure the PHP configurations to prevent the disclosure of sensitive information.

* phpMyAdmin is for managing MySQL databases:

Explanation: phpMyAdmin directories and files are found, and some may be accessible without proper protection.

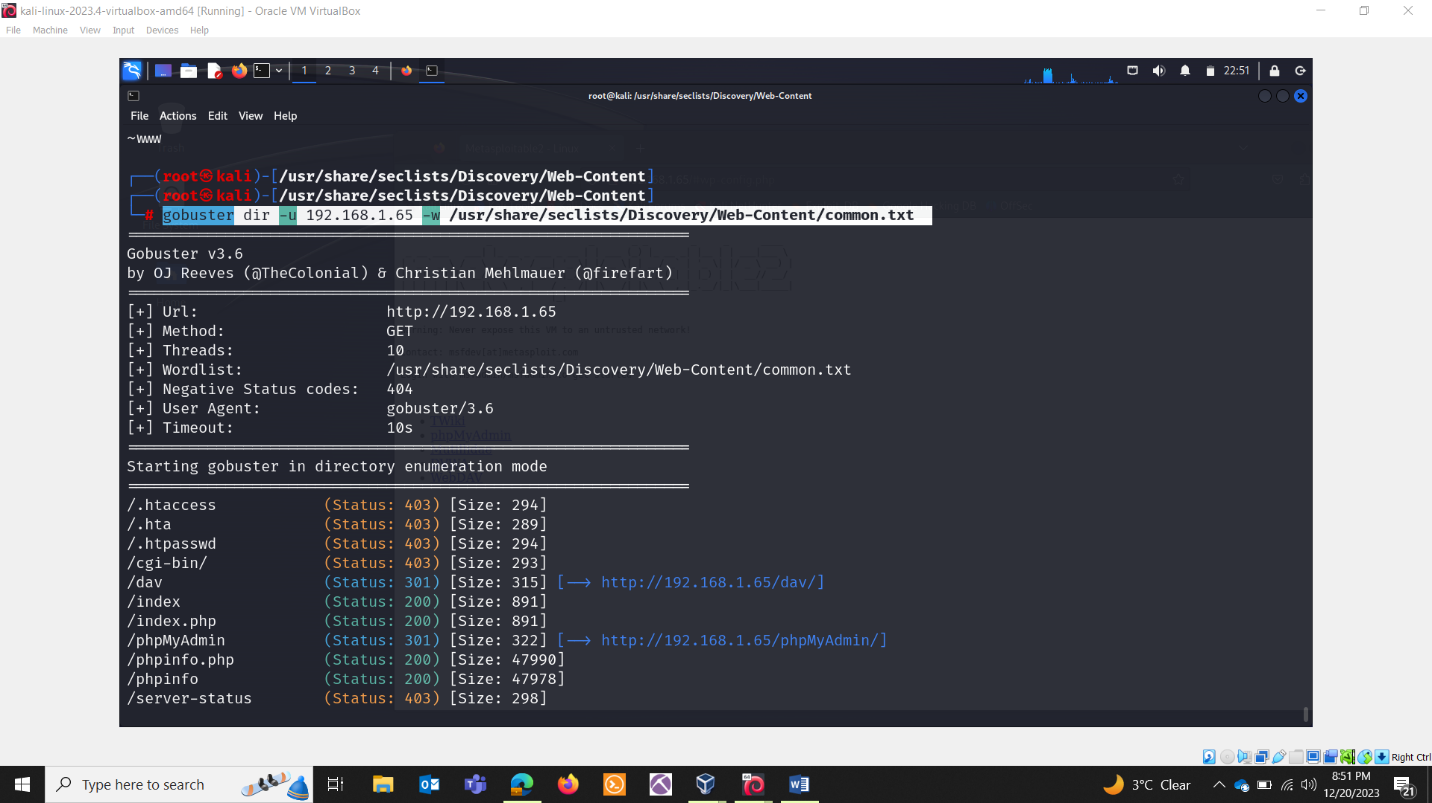
Recommendation: Secure the phpMyAdmin installation, restrict access to authorized hosts, and apply necessary security measures.

* #wp-config.php# file found:

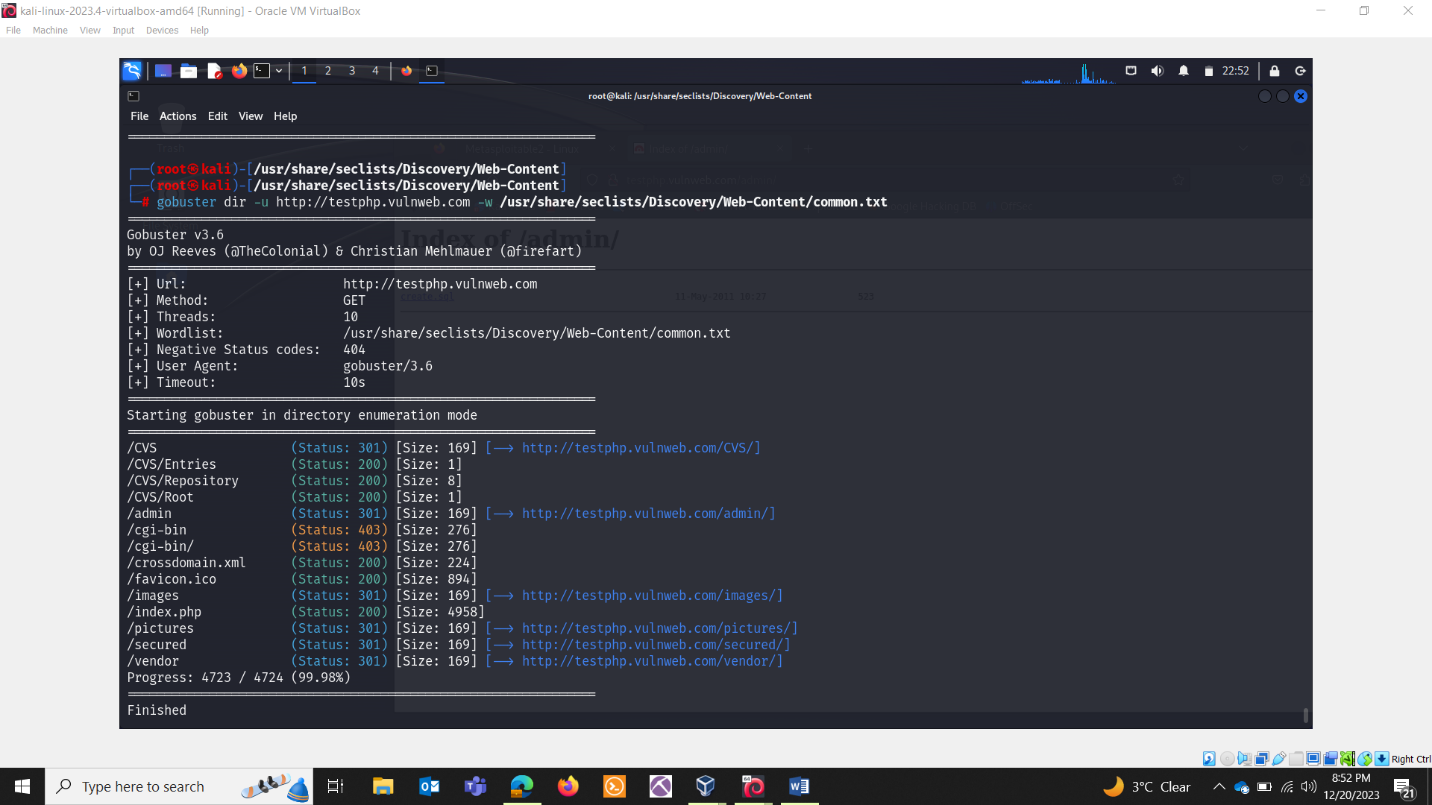
Explanation: A potentially sensitive file, '#wp-config.php#,' is discovered. This file may contain credentials.

Recommendation: Remove or secure the '#wp-config.php#' file to prevent unauthorized access to sensitive information.

GOBUSTER



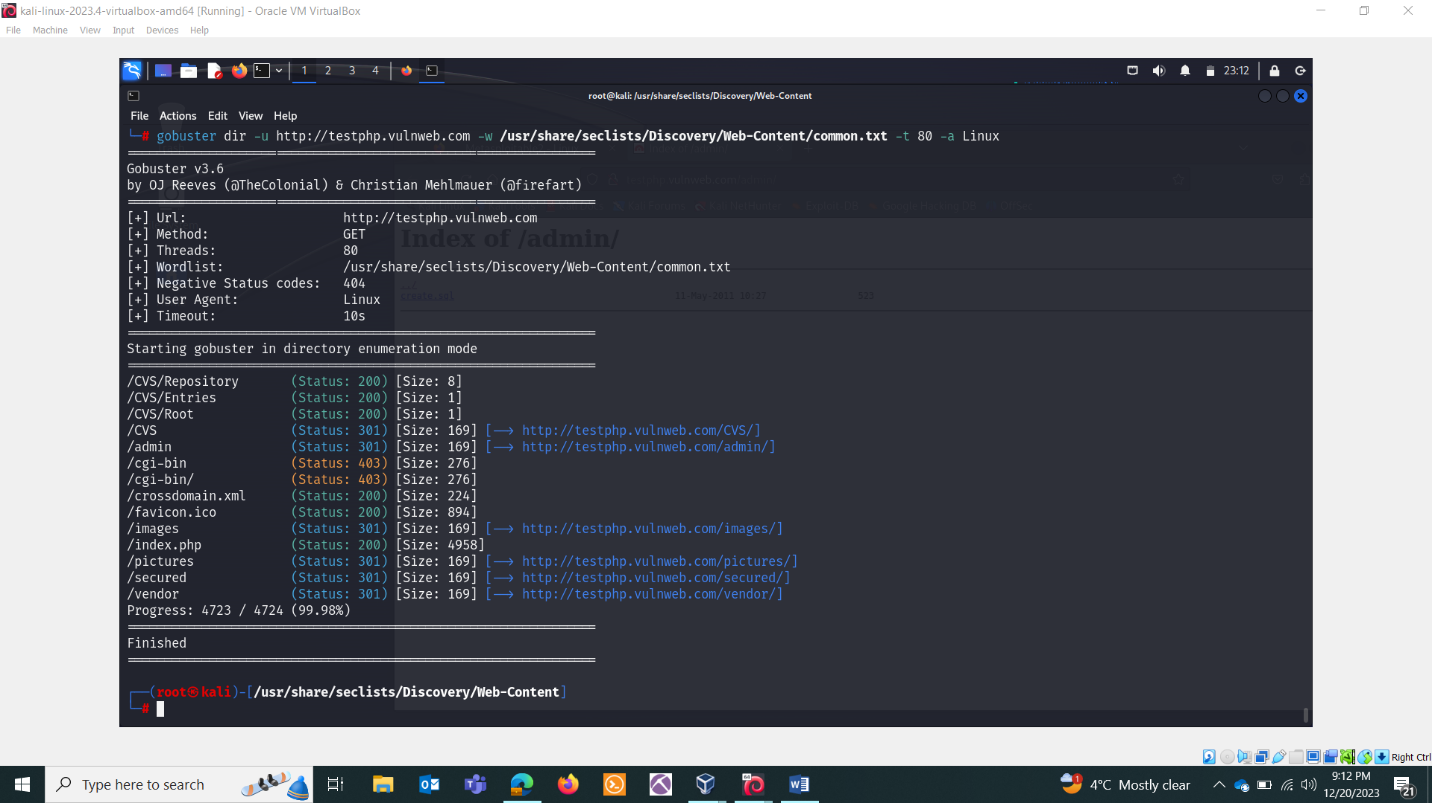
Testphp:

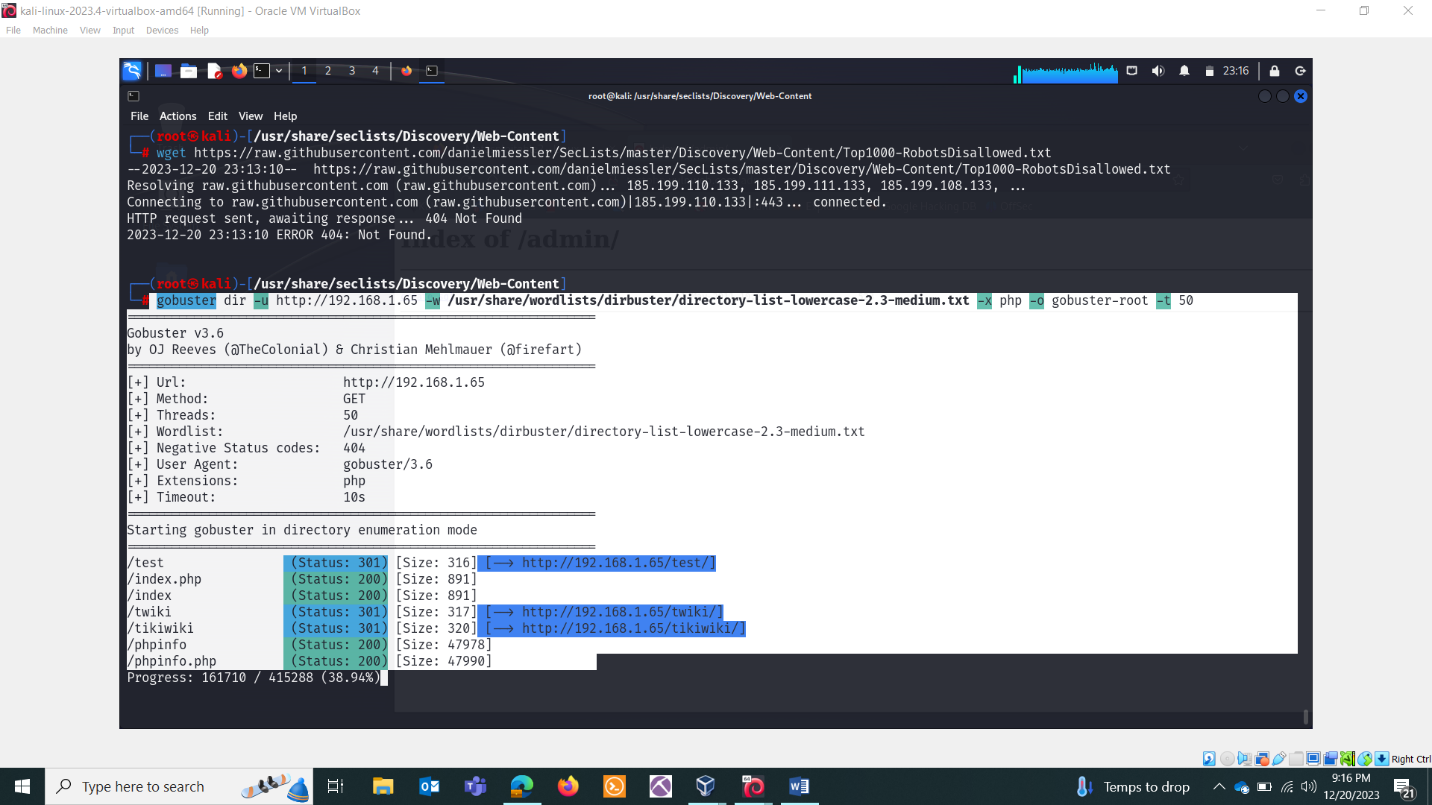


Gobuster quick:

-t 80: the number of concurrent threads.

-a Linux: This flag specifies the user-agent string to be used in HTTP requests.





-x .txt, .php

