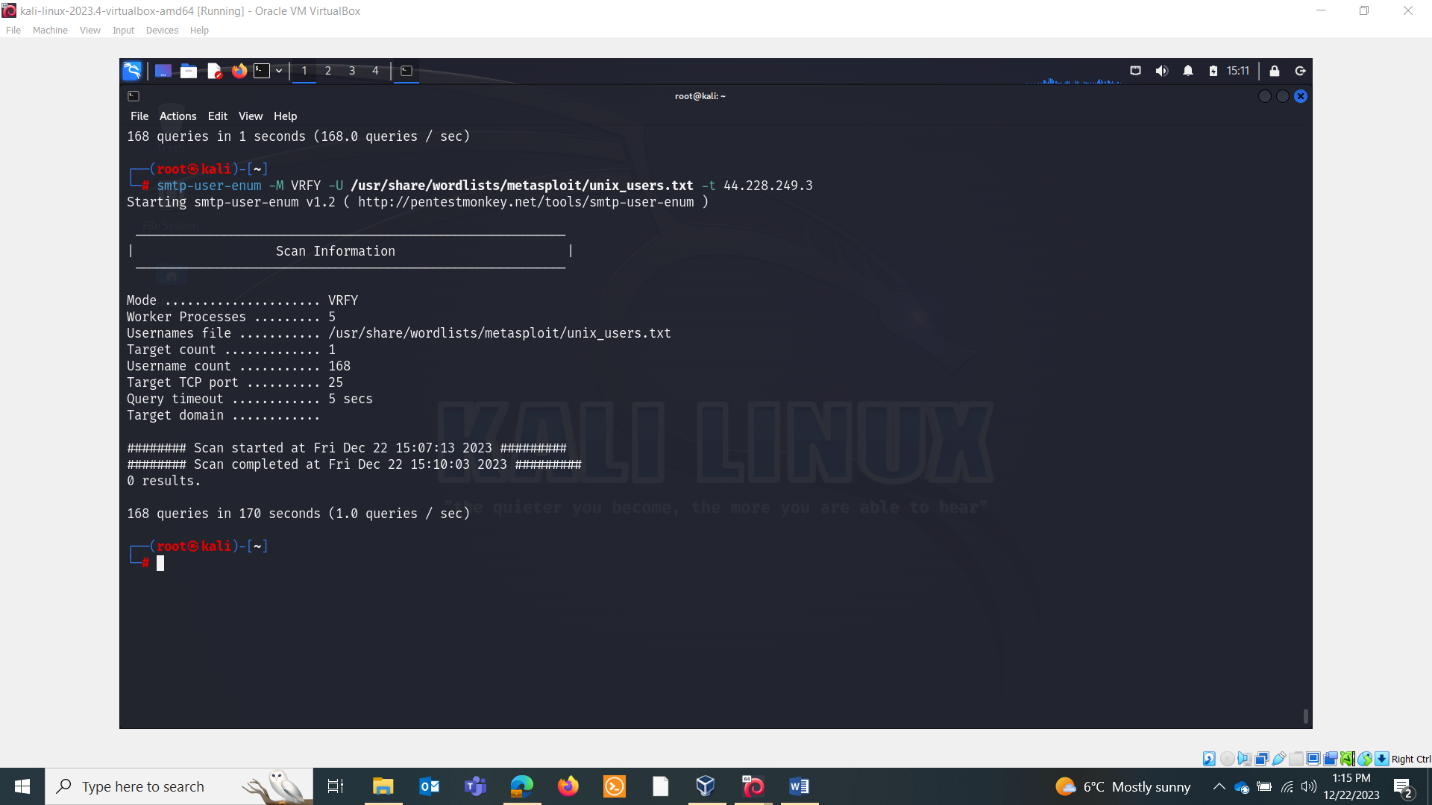
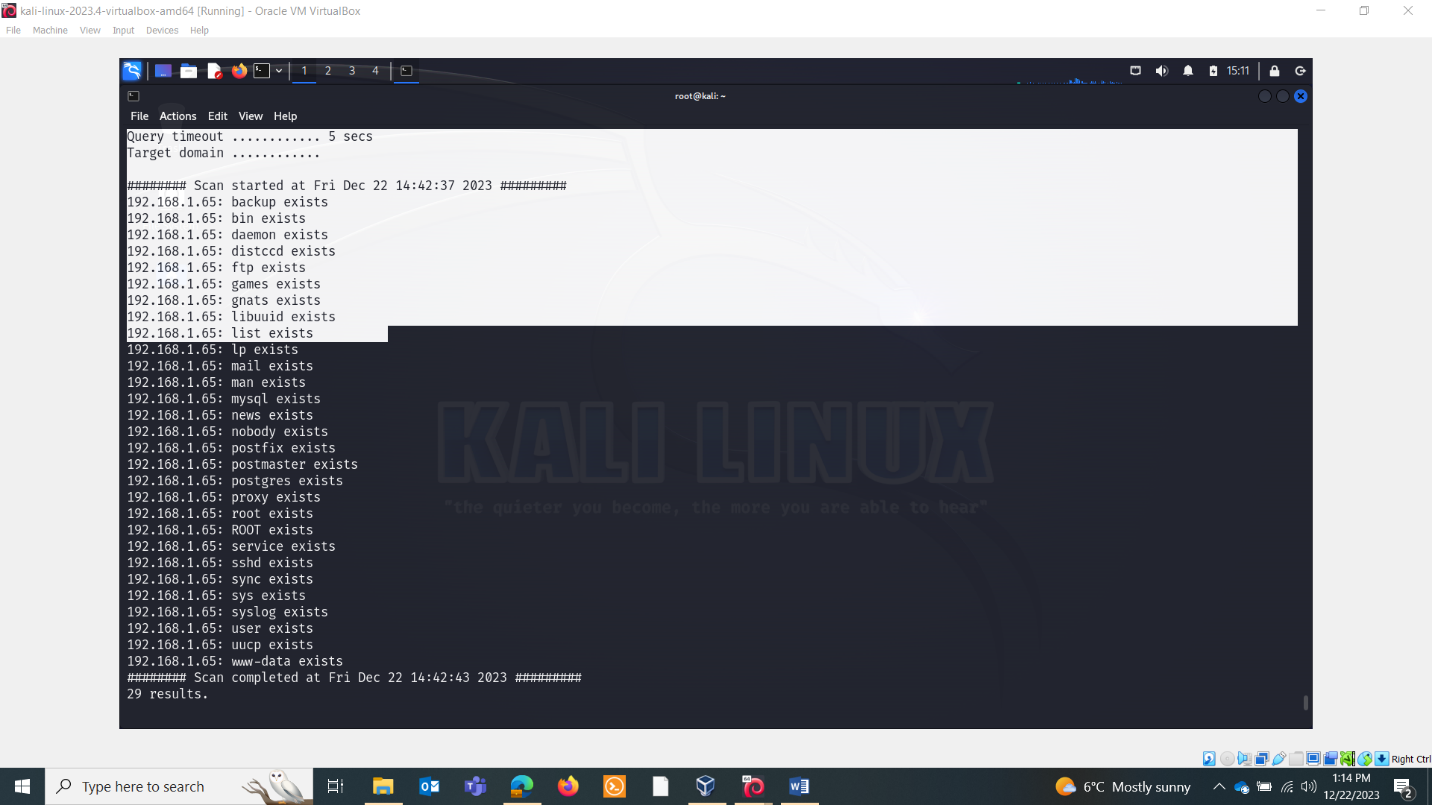
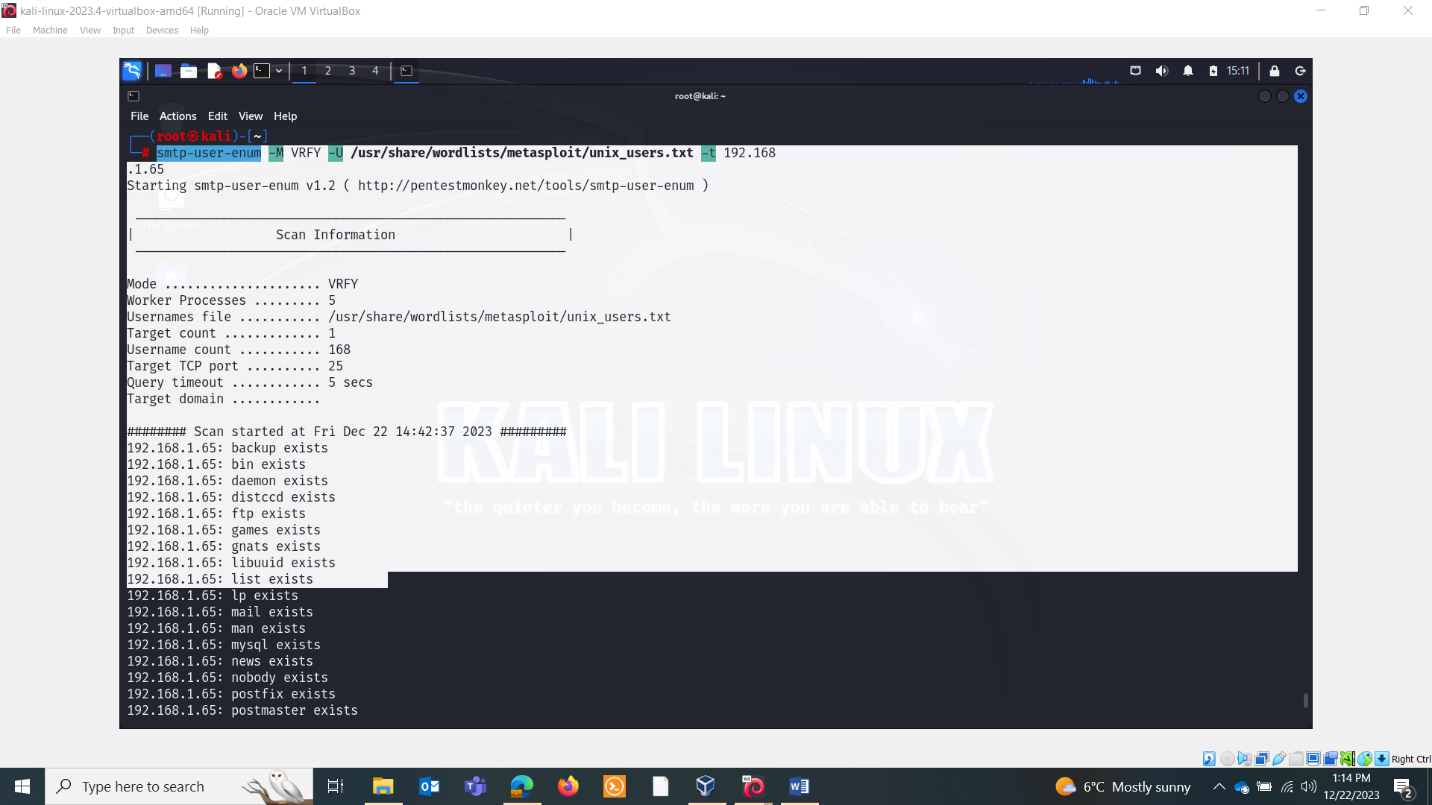
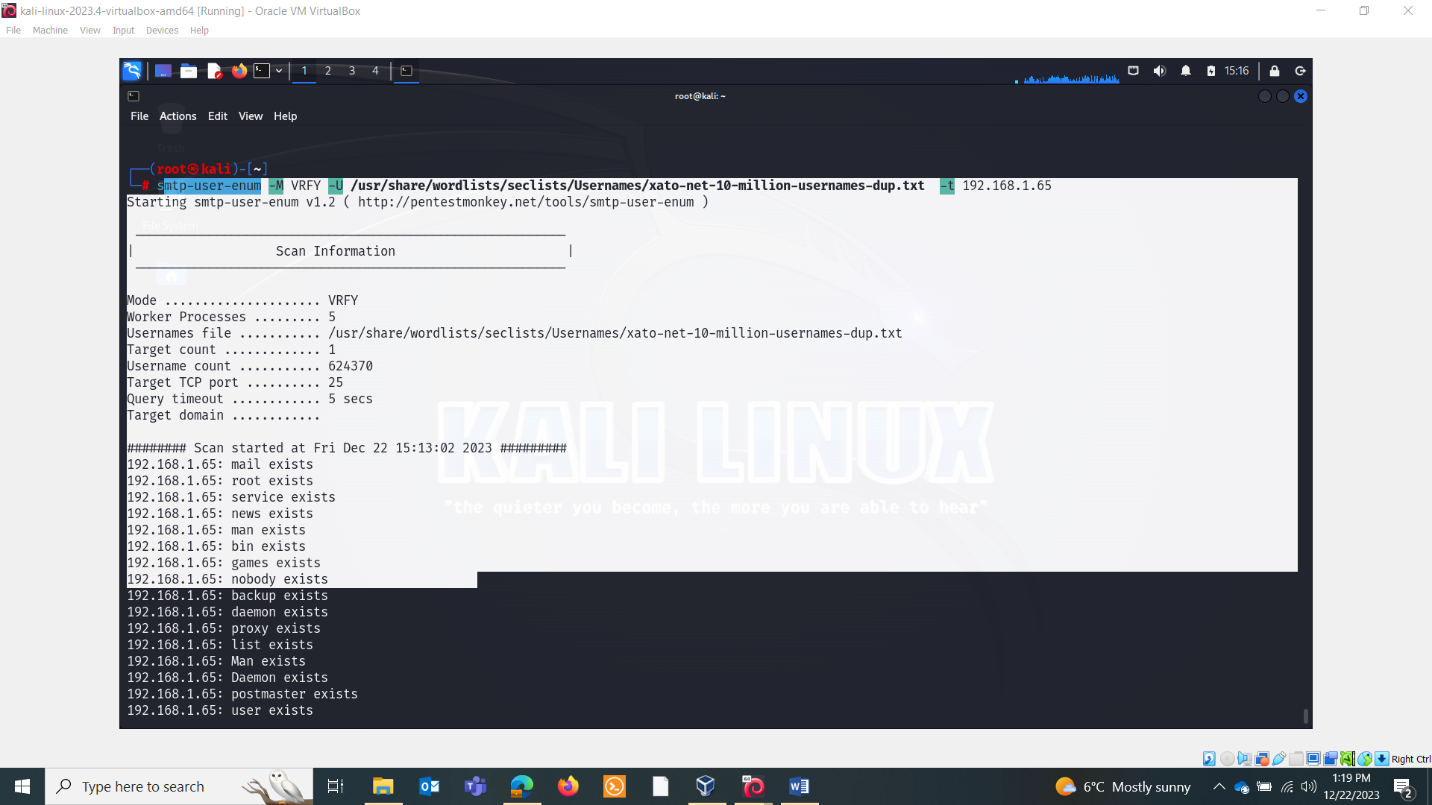
**SMTP**

User enumeration:



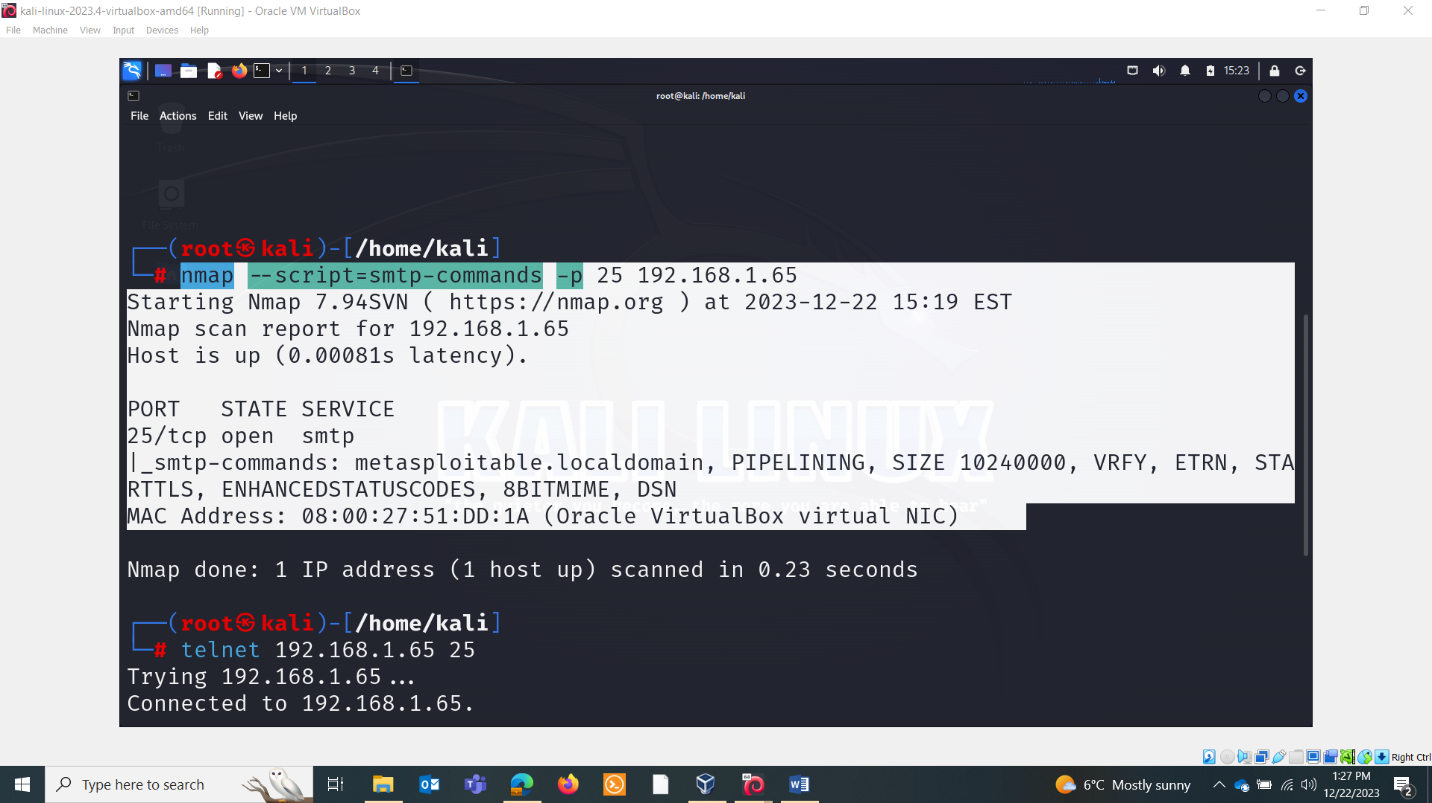


* telnet ip 25

ENUM & VULN SCANNING:

nmap --script=smtp-commands,smtp-enum-users,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 -p 25 $ip

script=smtp-commands



Telnet commands:

HELO metasploitable.localdomain: This command initiates the SMTP session and identifies the client to the server. In this case, the client claims to be the machine with the domain name "metasploitable.localdomain."

PIPELINING: This command indicates that the client supports command pipelining. Command pipelining is an optimization technique that allows the client to send multiple commands to the server without waiting for each response individually.

SIZE 10240000: This command informs the server about the maximum size of messages that the client is willing to accept. In this example, the maximum message size is set to 10,240,000 bytes (10 MB).

VRFY: This command is used to request verification of a specific email address or username. However, due to security concerns (potential for user enumeration), many modern mail servers disable or restrict the use of the VRFY command.

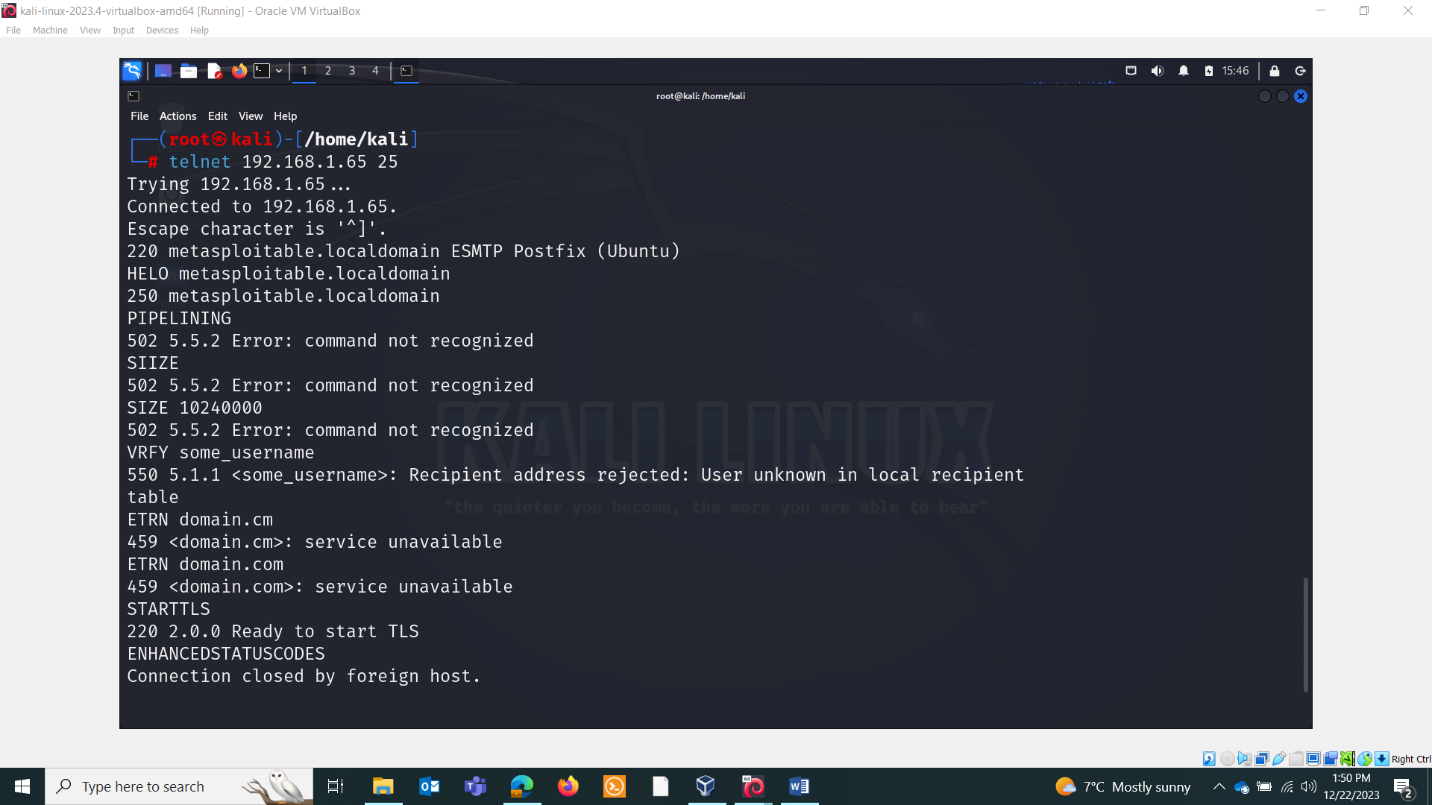
ETRN: This command is used to request the immediate delivery of queued messages for a specific domain. It's not commonly used in modern email systems.

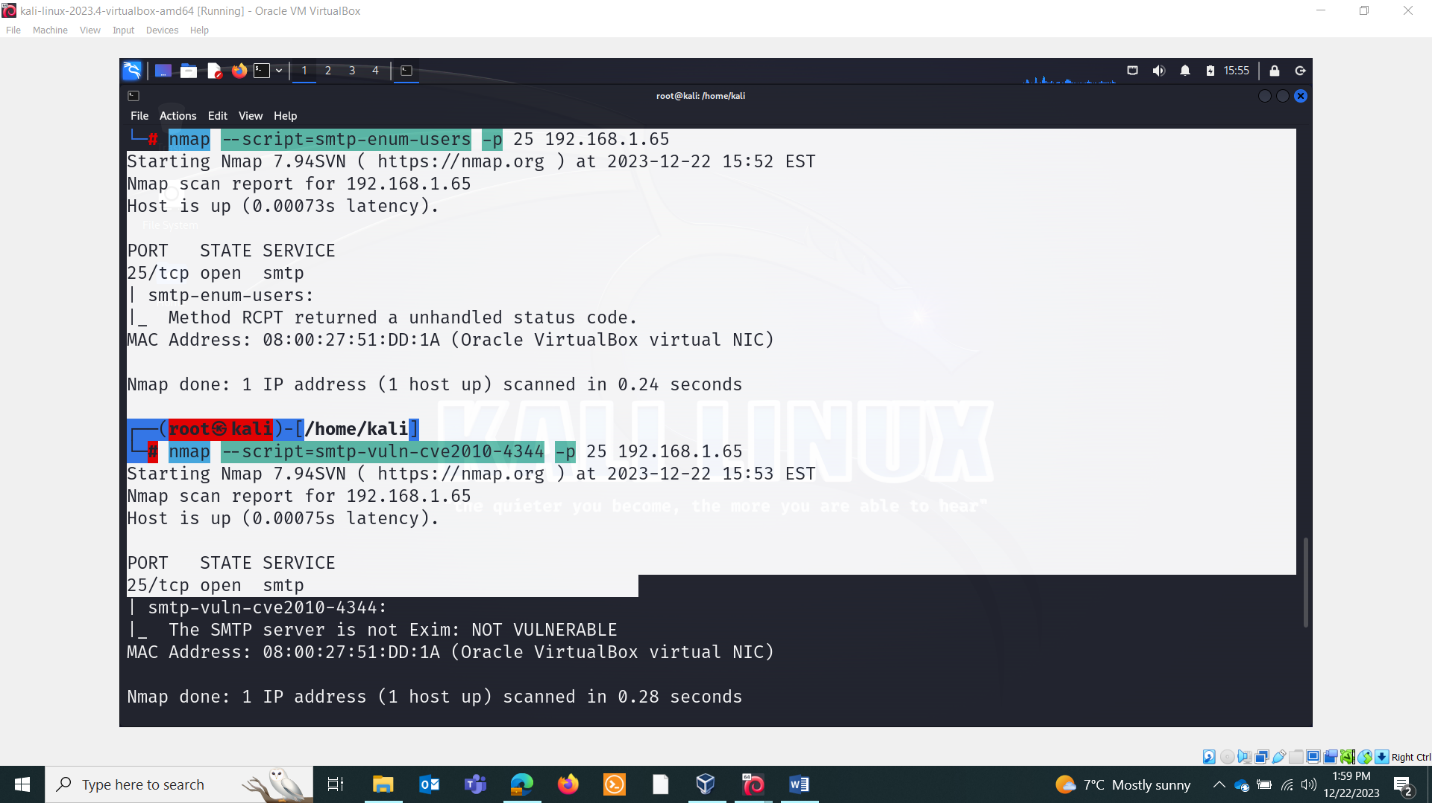
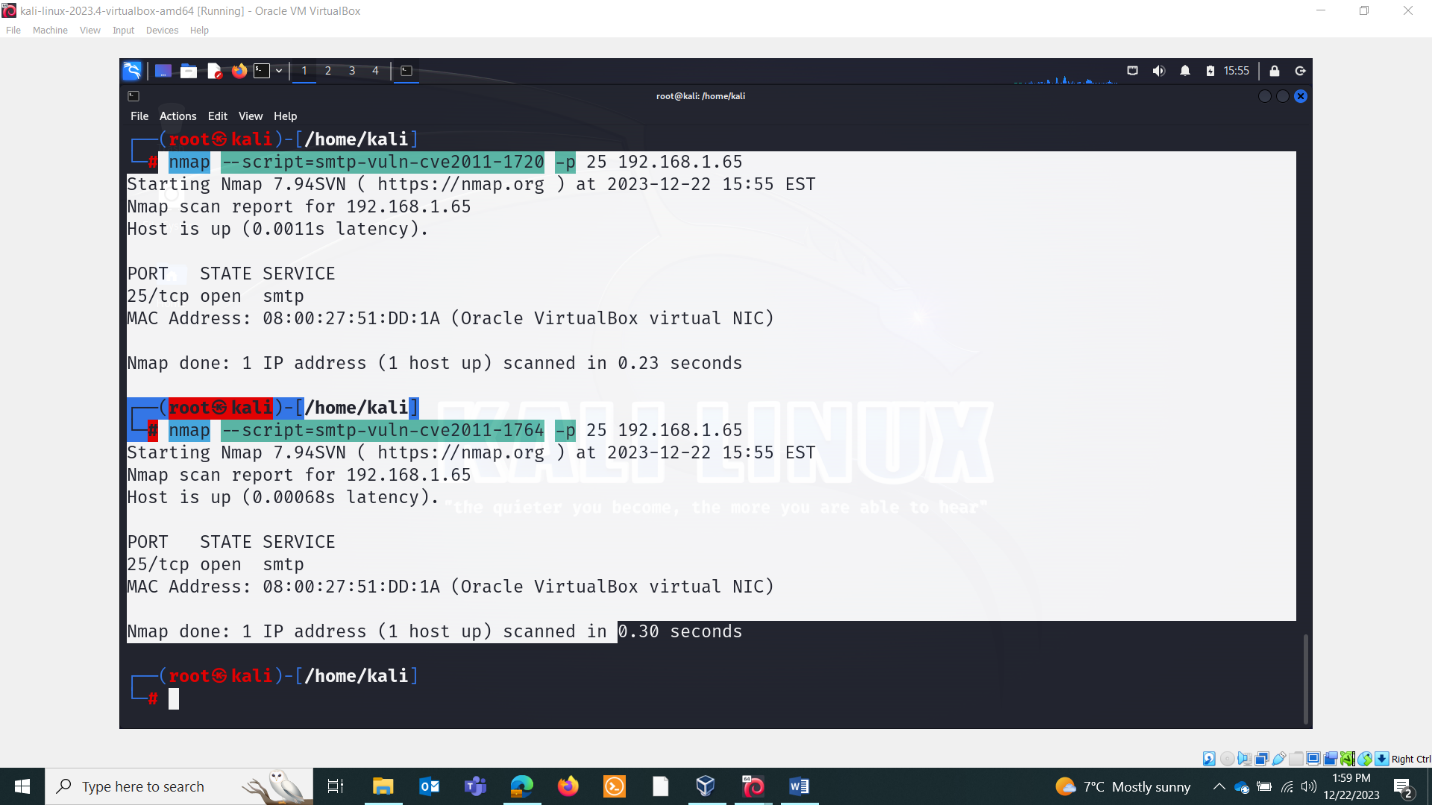
STARTTLS: This command is used to request a secure connection using the Transport Layer Security (TLS) protocol. It initiates the process of upgrading the connection to an encrypted and secure channel.

ENHANCEDSTATUSCODES: This command requests that the server provide enhanced status codes in its responses. Enhanced status codes provide more detailed information about the status of a message delivery.

8BITMIME: This command indicates that the client supports the transmission of 8-bit MIME (Multipurpose Internet Mail Extensions) data. It allows for the encoding of characters with values greater than 127.

DSN: This command is used to request delivery status notifications. It enables the sender to receive notifications about the delivery status of messages.





Brute force

