

Exercise 2: Launching a Spear Phishing Campaign

In this exercise, you will execute a spear phishing campaign against an employee of ACME Corp., using the information that you gathered in the previous exercise.

Execute the Spear Phishing Attack

You will execute an SMTP user enumeration attack using third-party tools.

To emulate the attack

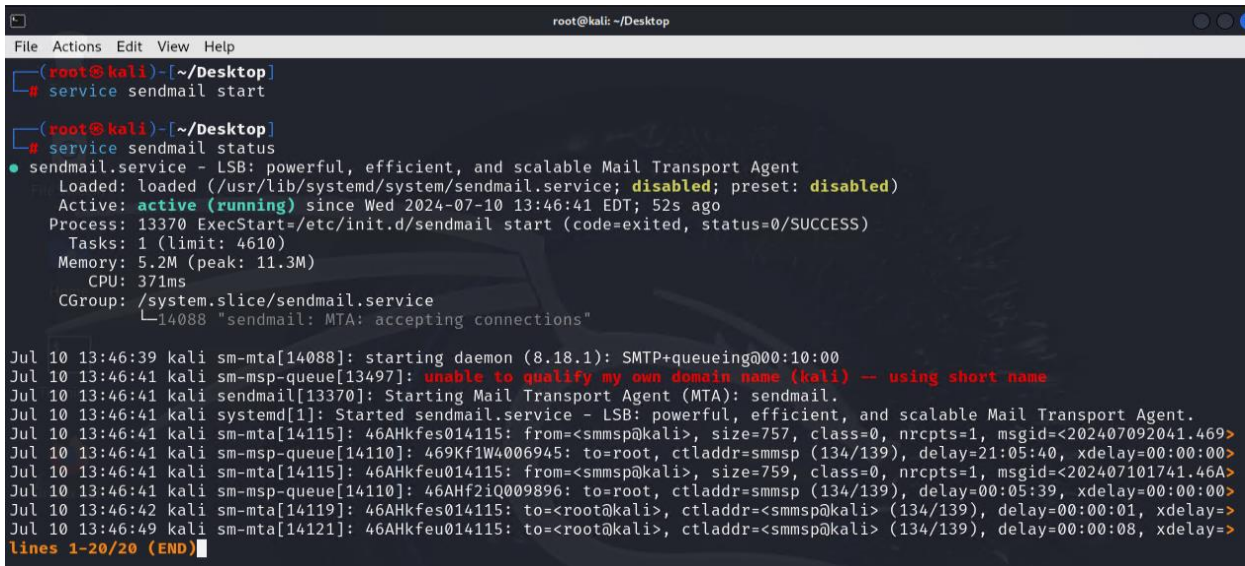
1. On the bastion host, on the desktop, double-click the **Kali Linux** RDP shortcut.
2. Log in with the following credentials:
 - Username: root
 - Password: Passw0rd
3. On the Kali Linux VM, on the desktop, double-click the **Terminal** shortcut to open two terminal windows.
4. In the first terminal window, enter the following command to start your local sendmail server:

service sendmail start

You will use this SMTP server later in this exercise as your relay to send the spear phishing email. It may take a while for the sendmail server to start.

5. When the shell prompt reappears, enter the following command to verify that the sendmail server is running correctly:

service sendmail status



```
root@kali: ~/Desktop
File Actions Edit View Help
(root@kali)~[~/Desktop]
# service sendmail start

(root@kali)~[~/Desktop]
# service sendmail status
sendmail.service - LSB: powerful, efficient, and scalable Mail Transport Agent
Loaded: loaded (/usr/lib/systemd/system/sendmail.service; disabled; preset: disabled)
Active: active (running) since Wed 2024-07-10 13:46:41 EDT; 52s ago
Process: 13370 ExecStart=/etc/init.d/sendmail start (code=exited, status=0/SUCCESS)
Tasks: 1 (limit: 4610)
Memory: 5.2M (peak: 11.3M)
CPU: 371ms
CGroup: /system.slice/sendmail.service
└─14088 "sendmail: MTA: accepting connections"

Jul 10 13:46:39 kali sm-mta[14088]: starting daemon (8.18.1): SMTP+queueing@00:10:00
Jul 10 13:46:41 kali sm-msp-queue[13497]: unable to qualify my own domain name (kali) -- using short name
Jul 10 13:46:41 kali sendmail[13370]: Starting Mail Transport Agent (MTA): sendmail.
Jul 10 13:46:41 kali systemd[1]: Started sendmail.service - LSB: powerful, efficient, and scalable Mail Transport Agent.
Jul 10 13:46:41 kali sm-mta[14115]: 46AHkfes014115: from=<smmsp@kali>, size=757, class=0, nrcpts=1, msgid=<202407092041.469>
Jul 10 13:46:41 kali sm-msp-queue[14110]: 469Kf1W4006945: to=root, ctladdr=smmsp (134/139), delay=21:05:40, xdelay=00:00:00>
Jul 10 13:46:41 kali sm-mta[14115]: 46AHkfeu014115: from=<smmsp@kali>, size=759, class=0, nrcpts=1, msgid=<202407101741.46A>
Jul 10 13:46:41 kali sm-msp-queue[14110]: 46AHf2iQ009896: to=root, ctladdr=smmsp (134/139), delay=00:05:39, xdelay=00:00:00>
Jul 10 13:46:42 kali sm-mta[14119]: 46AHkfes014115: to=<root@kali>, ctladdr=<smmsp@kali> (134/139), delay=00:00:01, xdelay=>
Jul 10 13:46:49 kali sm-mta[14121]: 46AHkfeu014115: to=<root@kali>, ctladdr=<smmsp@kali> (134/139), delay=00:00:08, xdelay=>
lines 1-20/20 (END)
```

6. Type q to exit the status command.
7. In the second terminal window, enter the following commands to change the directory and list the files:

cd /root/CyberSecurity/phishing

ls

```
root@kali: ~/CyberSecurity/phishing
File Actions Edit View Help
(root@kali)-[/]
# cd /root/CyberSecurity/phishing
(root@kali)-[~/CyberSecurity/phishing]
# ls
email-users.txt
(root@kali)-[~/CyberSecurity/phishing]
#
```

8. Enter the following command to list the contents of the email-users.txt file in that directory:

cat email-users.txt

```
root@kali: ~/CyberSecurity/phishing
File Actions Edit View Help
yaco
yang
yellowstone
yolanda
yosemite
zap
zimmerman
zipfiles
zips
zmodem
(root@kali)-[~/CyberSecurity/phishing]
#
```

The email-users.txt file contains a list of common usernames. You will use this file with SMTP enumeration to find valid email accounts on the acmecorp.net email server.



In the previous exercise, you noted some employee names of the target. An attacker would typically add names gathered from reconnaissance to an enumeration file to increase their chances of finding a match.

9. Enter the following command to see how many users are in the list:

wc -l email-users.txt

```
root@kali: ~/CyberSecurity/phishing
File Actions Edit View Help
yellowstone
yolanda
yosemite
zap
zimmerman
zipfiles
zips
zmodem
(root@kali)-[~/CyberSecurity/phishing]
# wc -l email-users.txt
1659 email-users.txt
```



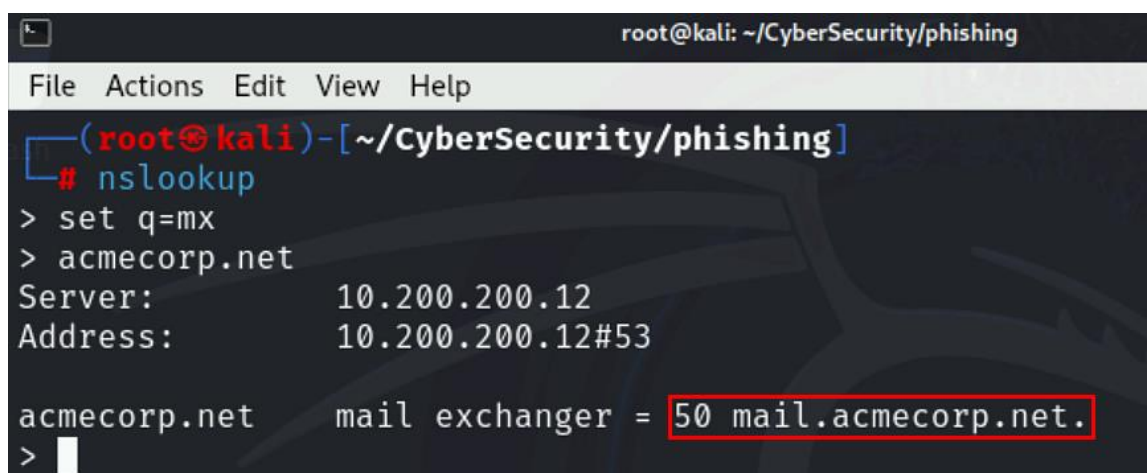
The file contains 1659 usernames, so the output in the image above is truncated.

10. Enter the following commands to identify the MX record for the acmecorp.net email server:

nslookup

set q=mx

acmecorp.net

A terminal window titled 'root@kali: ~/CyberSecurity/phishing' showing the nslookup command being used. The user sets the query type to 'mx' and queries 'acmecorp.net'. The output shows the server as 10.200.200.12 and the address as 10.200.200.12#53. Below this, it shows 'acmecorp.net mail exchanger = 50 mail.acmecorp.net.', where '50 mail.acmecorp.net.' is highlighted with a red box.

```
root@kali: ~/CyberSecurity/phishing
File Actions Edit View Help
(root@kali)-[~/CyberSecurity/phishing]
# nslookup
> set q=mx
> acmecorp.net
Server:      10.200.200.12
Address:     10.200.200.12#53

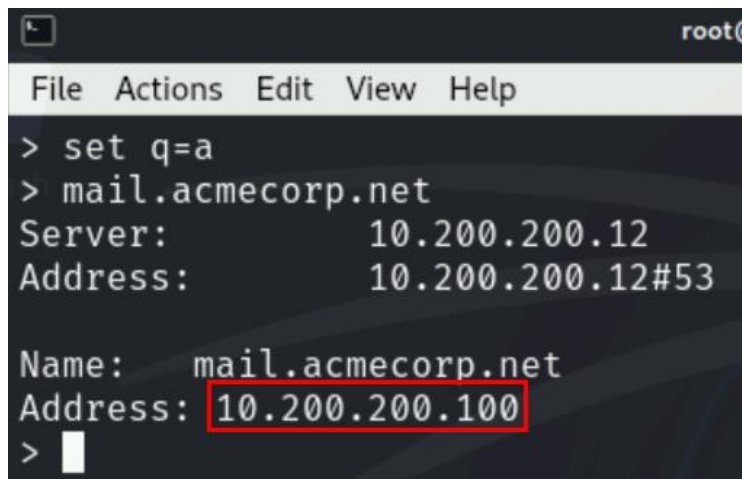
acmecorp.net mail exchanger = 50 mail.acmecorp.net.
>
```

According to the DNS server response, the mail server for acmecorp.net resolves to mail.acmecorp.net.

11. Continuing at the nslookup prompt, enter the following commands to identify the IP address of the FQDN mail.acmecorp.net:

set q=a

mail.acmecorp.net

A terminal window titled 'root@kali: ~/CyberSecurity/phishing' showing the nslookup command being used. The user sets the query type to 'a' and queries 'mail.acmecorp.net'. The output shows the server as 10.200.200.12 and the address as 10.200.200.12#53. Below this, it shows 'Name: mail.acmecorp.net' and 'Address: 10.200.200.100', where '10.200.200.100' is highlighted with a red box.

```
root@kali: ~/CyberSecurity/phishing
File Actions Edit View Help
> set q=a
> mail.acmecorp.net
Server:      10.200.200.12
Address:     10.200.200.12#53

Name: mail.acmecorp.net
Address: 10.200.200.100
>
```

According to the DNS server response, the mail.acmecorp.net FQDN resolves to 10.200.200.100.

12. Enter exit to exit the nslookup prompt.
13. Enter the following command to enumerate valid SMTP users on the target mail server, based on the list of common usernames you have:

smtp-user-enum -M RCPT -D acmecorp.net -U email-users.txt -t 10.200.200.100 -f email@mail.com

```
(root@kali)~[~/CyberSecurity/phishing]
# smtp-user-enum -M RCPT -D acmecorp.net -U email-users.txt -t 10.200.200.100 -f email@mail.com
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )


|-----|
| Proxy C200 | Scan Information |
|-----|

Mode ..... RCPT
Worker Processes ..... 5
Usernames file ..... email-users.txt
Target count ..... 1
Username count ..... 1659
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain ..... acmecorp.net

##### Scan started at Wed Jul 10 14:31:27 2024 #####
10.200.200.100: admin@acmecorp.net exists
10.200.200.100: alice@acmecorp.net exists
10.200.200.100: bob@acmecorp.net exists
10.200.200.100: student@acmecorp.net exists
##### Scan completed at Wed Jul 10 14:31:56 2024 #####
4 results.

1659 queries in 29 seconds (57.2 queries / sec)
```

The results of this command should show four email accounts, including two previously seen addresses from the website, and two usernames that match the employee profiles.

 FortiMail can block this enumeration based on the volume and rate of requests from the same client in a short amount of time. In your lab, these limits have been removed to emulate a mail server without any restrictions to this operation. This is also because you are using FortiMail as the email server itself. In most real-world organization scenarios, there would be dedicated email servers, with FortiMail working only as a gateway. For this type of proof-of-concept scenarios, this setup will work, but you should take notice that the FortiMail configurations have been purposely *weakened* to allow the enumeration to work seamlessly and quickly.

Verify Incidents

You will verify, on FortiAnalyzer, that the event handler rule matched and generated the correct incident.


To verify that the custom event handler matched and generated the correct event

1. On the bastion host, in Chrome, log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:
 - Username: admin
 - Password: Fortinet1!
2. Click **Incidents & Events > Event Monitor**.

It may take some time for the event to appear. You can also filter the results to **Last 5 Minutes** to reduce the number of events.

3. On the **All Events** tab, beside **FortiMail**, click **+**.

All Events	By Endpoint	By Threat	System Events	Toggle Views			
	All Devices	Last 5 Minutes	2024-07-10 11:06:59 - 2024-07-10 11:11:59	<input type="checkbox"/> Show Acknowledged		Expand All	Refresh
Search or type filters...							
<input type="checkbox"/> Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
<input type="checkbox"/> FortiMail (1)	Unhandled	Email Filter	1647	High	7 minutes ago	5 minutes ago	SOC SMTP Enumeration Data Handler

 Do not proceed if FortiAnalyzer does not generate the correct event. Ask your instructor to help you troubleshoot your environment. The cause of FortiAnalyzer not generating the event is most likely a misconfiguration of the FortiAnalyzer basic event handler or an error when executing the attacker behavior.

4. Click **SOC SMTP Enumeration Data Handler**.

All Events	By Endpoint	By Threat	System Events	Toggle Views			
	All Devices	Last 5 Minutes	2024-07-10 11:06:59 - 2024-07-10 11:11:59	<input type="checkbox"/> Show Acknowledged		Expand All	Refresh
Search or type filters...							
<input type="checkbox"/> Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
<input type="checkbox"/> FortiMail (1)	Unhandled	Email Filter	1647	High	7 minutes ago	5 minutes ago	SOC SMTP Enumeration Data Handler
<input checked="" type="checkbox"/> devname:FortiMail from:user	Unhandled	Email Filter	1647	High	2024-07-10 11:08:35	2024-07-10 11:09:58	SOC SMTP Enumeration Data Handler

The **Edit Basic Event Handler** page opens. The event handler rule that was triggered is highlighted.

Edit Basic Event Handler

Status

Name

SOC SMTP Enumeration Data Handler

Description

Handler for checking adversaries that are looking to gather email addresses

MITRE Domain

N/A Enterprise ICS

MITRE Tech ID

T1589 Gather Victim Identity Information

T1589.002 Email Addresses

2 entries selected

Data Selector

SOC SMTP Enumeration Data Selector

Automation Stitch

Rules

SOC Antispam Rule 1

Add New Rule

Handler Settings

Notifications

SOC SMTP Enumeration Alert

5. Close the **Edit Basic Event Handler** page.
6. Click **Log View > FortiMail > Email Filter**.
7. View the FortiMail enumeration logs that generated this event.

History

Event▼

Email Filter

All Devices▼

Last 5 Minutes▼

11:27:31 - 11:32:31

Create Custom View

Refresh

More Colur

#	↓ Date/Time	Device ID	Session ID	Client Name	Destination I	From	To	Subject	Message
1	2024-07-10 11:31:56	FEVMSLTM22000	46AIVvG2012		10.200.200.1	email@mail.co	zmodem@acrn		<zmodem@acmecorp.net>... User unknown
2	2024-07-10 11:31:56	FEVMSLTM22000	46AIVv8Q012		10.200.200.1	email@mail.co	zap@acmecor		<zap@acmecorp.net>... User unknown
3	2024-07-10 11:31:56	FEVMSLTM22000	46AIVvap012		10.200.200.1	email@mail.co	zips@acmecor		<zips@acmecorp.net>... User unknown
4	2024-07-10 11:31:56	FEVMSLTM22000	46AIVu1A012		10.200.200.1	email@mail.co	yolanda@acm		<yolanda@acmecorp.net>... User unknown
5	2024-07-10 11:31:56	FEVMSLTM22000	46AIVvZd012		10.200.200.1	email@mail.co	zipfiles@acme		<zipfiles@acmecorp.net>... User unknown
6	2024-07-10 11:31:56	FEVMSLTM22000	46AIVvtN012		10.200.200.1	email@mail.co	zimmerman@		<zimmerman@acmecorp.net>... User unknown
7	2024-07-10 11:31:56	FEVMSLTM22000	46AIVuec012		10.200.200.1	email@mail.co	yosemite@acr		<yosemite@acmecorp.net>... User unknown
8	2024-07-10 11:31:56	FEVMSLTM22000	46AIVuHJ012		10.200.200.1	email@mail.co	yang@acmecc		<yang@acmecorp.net>... User unknown

8. In Chrome, open a new tab, and then log in to the FortiMail (webmail) GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
9. Open the notification email.

CloseReplyReply AllForwardMoveMore

Subject: Adversaries are scanning for email accounts (high spam alert devname:FortiMail from:email@mail.com device_id:FEVMSLTM22000111 FortiMail)

From: admin@acmecorp.net
To: admin@acmecorp.net
Date: Jul 10, 2024 2:31:46 PM

DeviceFortiMail
Severityhigh
FromFAZ-SiteB(FAZ-VMTM24000908)
TriggerSOC SMTP Enumeration Data Handler
Tag
Alertid202407101000000740

Log Details:

Device ID	FEVMSLTM22000111	Virtual Domain	root
Time Stamp	2024-07-10 11:31:27	idseq	164156720619192368
Date	2024-07-10	Time	14:31:28.384
Device ID	FEVMSLTM22000111	ID	0300009570
Type	spam	Sub Type	default
Level	information	Session ID	46AIVSKo009567-46AIVSKp009567
Client Name		client_ip	100.64.1.21
Destination IP	10.200.200.100	From	email@mail.com
To	20@acmecorp.net	Subject	
Message	<20@acmecorp.net>... User unknown		

FortiAnalyzer generated this alert email when it detected attempts to gather victim identity information.

To verify that the **playbook** ran and generated the correct incident

1. Return to the FAZ-SiteB GUI, and then click **Fabric View > Automation**.
2. Click the **Playbook Monitor** tab.
3. Notice the **SOC SMTP Enumeration Playbook** that ran successfully.

Summary	Connectors	Playbook	Playbook Monitor				
Refresh		Delete		Search...			
<input type="checkbox"/>	Job ID	Playbook	Trigger	Start Time	End Time	Status	
<input type="checkbox"/>	2024-07-10 11:32:28.234644-07	SOC SMTP Enumeration Playbook	event(202407101000	2024-07-10 11:32:29-0700	2024-07-10 11:32:33-0700	success(Scheduled:0/Running:0)	
<input type="checkbox"/>	2024-07-10 11:09:27.770054-07	SOC SMTP Enumeration Playbook	event(202407101000	2024-07-10 11:09:28-0700	2024-07-10 11:09:32-0700	success(Scheduled:0/Running:0)	

4. Click **SOC SMTP Enumeration Playbook**.

The following three tasks ran successfully:

- Attach the data to the incident
- Create an incident for SMTP enumeration
- Get events from the SMTP logs

Playbook Tasks					
RefreshView Raw Log		Search...@*			
<input type="checkbox"/>	Task ID	Task	Start Time	End Time	Status
<input type="checkbox"/>	placeholder_62ba2832_adf2_4be3_a9a1_e2	Attach_Data_To_Incident	2024-07-10 11:32:31-0700	2024-07-10 11:32:32-0700	success
<input type="checkbox"/>	placeholder_1ff2289f_7353_4b1a_9e4f_7c6	Create_SMTp_Enumeration_Incident	2024-07-10 11:32:30-0700	2024-07-10 11:32:31-0700	success
<input type="checkbox"/>	placeholder_ddd198b7_a596_4b5f_b5b6_95	Get_Events	2024-07-10 11:32:30-0700	2024-07-10 11:32:31-0700	success

5. Close the **Playbook Tasks** window.

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 FAZ-SiteB GUI, click **Incidents & Events**.
2. Click the **MITRE ATT&CK** tab, and then select **Attack**.
3. In the **Reconnaissance** column, verify that the **Gather Victim Identity Information** tactic is covered by an event handler.

Attack

Coverage

Refresh

Last 1 Week

2024-02-09 09:14:53 - 2024-02-16 09:14:53

Reconnaissance

10 techniques

Active Scanning

2

Gather Victim Host Information

Covered

Gather Victim Identity Information

2 1

Resource Development

8 techniques

Acquire Access

Acquire Infrastructure

Covered

Compromise Accounts

Compromise Infrastructure

Covered

Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

Covered

External Remote Services

Covered

Hardware

Execution

14 techniques

Cloud Administration Command

Command and Scripting Interpreter

Covered

Container Administration Command

Persistence

19 techniques

Account Manipulation

BITS Jobs

Covered

Boot or Logon Autostart Execution

Covered

Boot or Logon

4. Click the **Gather Victim Identity Information** block.
5. View the generated events that matched this tactic.

T1589 Gather Victim Identity Information

Events

Incidents

Search...

Event Handler	Severity	Technique	Affected Endpoints	Event Count
SOC SMTP Enumeration Data Handler	High	T1589 Gather Victim Identity Information	no enough info	1

Execute a Spear Phishing Attack

One behavior of Group ABC is that, after they enumerate valid accounts, they analyze the results and try to establish hierarchical and/or power relationships between users, in order to leverage this in the social engineering aspects of their **Spearphishing Attachment** execution. This is a clear example of an adversary procedure—Group ABC executes a subtechnique in this way to try to lure the target user to open the malicious attachment.

You will now emulate this social engineering aspect by using admin@acmecorp.net as the sender. You will create a message that looks like it was sent by the office administrator, and that includes a plausible reason for opening the attachment.