Assignment – 3

SOCIAL ENGINEERING

- Social engineering attacks exploit human psychology rather than technical hacking techniques to gain access to systems, data, or personal information.
- These attacks often involve manipulating individuals into breaking normal security procedures. Here's a summarized overview of how a social engineering attack might unfold to breach security.
- After deciding on a target company, the attacker begins to collect data. This can entail looking for the names, responsibilities, and contact details of staff members on public platforms like social media and business websites.
- Finding possible human weaknesses in the company, such as staff members who could have access to private data but are not aware of cybersecurity issues.
- Attackers often employ sophisticated methods to appear credible and trustworthy, thereby lowering the victim's guard and making them more likely to comply with malicious requests.
- This could be someone from within the victim's own organization, such as an IT staff member, or external entities like a wellknown company, government agency, or tech support.
- The attacker creates a context or scenario that seems familiar or plausible to the victim.
- Social proof involves making the victim believe that other trustworthy individuals or groups are also complying with or endorsing a request.
- For instance, mentioning that "most team members have already completed this step" can pressure the victim into acting without wanting to appear noncompliant or out of the loop.
- In more targeted attacks, such as spear phishing or pretexting, attackers might engage in conversation with their target to build rapport. This could involve discussing common interests, mutual connections, or any number of topics that would make the victim feel a personal connection to the attacker, thus lowering their defences.
- Attackers may offer assistance with an issue the victim is facing or promise some form of reward for compliance.
- For example, they might offer a free security scan or a financial incentive for filling out a survey. The offer of help or reward can make the victim feel indebted to the attacker, increasing the likelihood of trust.
- The visual and linguistic quality of the communication plays a significant role in establishing trust. Using professional language, correct grammar, highquality logos, and clean, welldesigned websites can make fraudulent requests appear legitimate.
- Creating a sense of urgency or invoking fear can make victims act impulsively, bypassing their usual scepticism. By suggesting that immediate action is required to

prevent a negative outcome (e.g., account closure, loss of service, or legal action), attackers can push victims to act quickly, with the implied trust that the urgency is real.

- Making the victim feel as though they must act immediately without sufficient substantiation by arousing anxiety or a sense of urgency. Saying there was a security breach, for instance, necessitates a quick password reset.
- Posing as a person in a position of authority or power in order to dissuade people from asking questions. Asserting that, in order to normalize the activity, other colleagues have already complied with a request.
- Identifying vulnerabilities within an organization's security posture is crucial for preventing social engineering attacks and other cybersecurity threats.
- Three primary areas often exploited by attackers due to their inherent weaknesses include lack of employee awareness training, inadequate authentication measures, and poor email security protocols. Here's a breakdown of these vulnerabilities:

Lack of Employee Awareness Training:

- A lack of regular, comprehensive training on recognizing and responding to these threats leaves employees vulnerable to manipulation.
- Employees are often the first line of defence against social engineering attacks. Without awareness, employees are more likely to fall for phishing scams, pretexting, baiting, and other tactics used by attackers.
- The direct consequence is an increased likelihood of successful breaches, leading to data loss, financial damage, and reputational harm. Employees unaware of the threats and the importance of their role in the organization's security are less vigilant and more prone to making mistakes.

Inadequate Authentication Measures

- Weak authentication processes, such as relying solely on passwords, not implementing multifactor authentication (MFA), or using easily guessable passwords, significantly increase an organization's risk profile.
- Social engineering attacks often target these weak points, with attackers seeking to steal or guess credentials.
- Inadequate authentication measures make it easier for attackers to gain unauthorized access to sensitive systems and data once they have obtained or cracked an employee's credentials.
- The lack of robust authentication mechanisms allows attackers to move laterally within the network, potentially causing significant damage.

Poor Email Security Protocols

- Email is a common vector for social engineering attacks. Poor email security protocols, such as the absence of spam filters, lack of domainbased message authentication, reporting, and conformance (DMARC) policies, or failure to implement email authentication methods like Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), leave organizations susceptible to phishing and other emailbased attacks. Without strong email security protocols, malicious emails are more likely to reach employees, increasing the risk of successful social engineering attacks. This can lead to malware infections, data breaches, and financial fraud.

Addressing the Vulnerabilities

- Regular, engaging training sessions that include realworld examples, simulations, and tests can significantly improve employees' ability to recognize and respond to social engineering tactics.
- Adopting multifactor authentication, enforcing strong password policies, and considering biometric or behavioural authentication methods can drastically reduce the risk of unauthorized access.
- Implementing advanced spam filters, adopting DMARC policies, and ensuring SPF and DKIM are set up correctly can help authenticate email communications and reduce the risk of phishing attacks.
- By addressing these vulnerabilities, organizations can significantly enhance their security posture and resilience against social engineering and other cyber threats.

The consequences of a successful social engineering attack can be farreaching and devastating for an organization. Beyond the immediate disruption and data loss, the longerterm impacts on reputation, financial health, and customer trust can be even more challenging to recover from. Here's a detailed look at these aspects:

1. Reputation Damage:

   News of a security breach can spread rapidly, especially through social media and news outlets. The perception that the organization failed to protect sensitive data can lead to a loss of public confidence. Rebuilding a reputation after a breach can be a lengthy and costly process. Potential partners may be wary of associating with a company perceived as insecure, and attracting top talent can become more difficult if the organization is seen as careless with data security.

2. Financial Losses:

   The immediate aftermath of an attack often involves significant financial expenditure, including forensic investigations, legal fees, and costs associated with notifying affected individuals. In cases where regulatory fines are imposed (such as GDPR penalties for data breaches involving EU citizens), these can be substantial. There are also longerterm financial impacts to consider, such as the cost of implementing new security measures, increased insurance premiums, and potential loss of revenue due to downtime. Businesses may also face lawsuits from affected parties and have to compensate customers for their losses.

3. Customer Trust:

Trust is the foundation of customer relationships, and once it's broken, it can be extremely difficult to rebuild. Customers entrust companies with their personal and financial information with the expectation that it will be protected.Restoring trust requires transparent communication, demonstrable improvements in security practices, and often, incentives to affected customers.

Recommendations align with best practices in cybersecurity and can significantly enhance an organization's resilience against various cyber threats, including social engineering attacks. Here's a detailed breakdown of each recommendation:

- Regular Security Training for Employees
- Adopting MultiFactor Authentication (MFA)
- Improving Email Filtering Systems
- Additional Recommendations
- Incident Response Plan
- Regular Security Audits
- Employee Reporting Mechanisms
- Vendor Security Assessment
- Continuous Monitoring

Social engineering is a type of manipulation that exploits human psychology to gain access to sensitive information, systems, or resources. Attackers use various tactics to deceive individuals and manipulate them into divulging confidential information or taking actions that may compromise security. Here are some common social engineering tactics, including authority exploitation, urgency, and familiarity:

1. Authority Exploitation:

Impersonation: Attackers may pose as someone with authority, such as a supervisor, IT administrator, or executive, to gain trust and access to sensitive information.

False Credentials: Creating fake identification or using officialsounding titles to give the impression of authority.

2. Urgency:

Creating a Crisis: Attackers often fabricate emergencies or crises, claiming that quick action is necessary to resolve the issue. This sense of urgency can lead individuals to make hasty decisions without thoroughly verifying the situation.

Deadline Pressure: Attackers may impose artificial deadlines, pressuring individuals to act quickly and without proper consideration.

3. Familiarity:

Pretexting: Crafting a fabricated scenario or pretext to establish a sense of familiarity. For example, an attacker might claim to be from the same organization or project to gain trust.

Name Dropping: Mentioning names of colleagues, superiors, or friends to create a sense of familiarity and trust.

4. Phishing:

Emails: Sending deceptive emails that appear legitimate, often with urgent or alarming messages, to trick individuals into clicking on malicious links or providing sensitive information.

Website Spoofing: Creating fake websites that mimic legitimate ones to trick users into entering confidential information.

5. Baiting:

Physical Media: Leaving infected USB drives, CDs, or other physical media in places where the target is likely to find them, relying on curiosity to prompt the individual to use the media.

Online Baiting: Offering tempting downloads, links, or content to lure individuals into clicking and unknowingly installing malware.

6. Scare Tactics:

Threats and Intimidation: Using threats or intimidation to create fear, such as claiming legal action, loss of job, or other severe consequences if the individual does not comply.

7. Trust Exploitation:

Building Rapport: Establishing a relationship and gaining the trust of individuals through social interactions, either in person or online, before exploiting that trust for malicious purposes.

8. Reverse Social Engineering:

Pretending Helplessness: Making the target believe that the attacker is in a vulnerable position, appealing to their empathy and encouraging them to provide assistance.

Identifying red flags in emails can help you spot phishing attempts and other types of email scams. Here are key red flags to watch for:

Suspicious Sender Address:

The email comes from a public domain (e.g., @gmail.com) instead of a corporate domain.

The sender's email address is misspelled or varies slightly from the legitimate organization's email format.

Urgent or Threatening Language:

The email creates a sense of urgency, pressuring you to act quickly.

Messages threaten negative consequences, such as account closure, if you do not respond.

Generic Greetings:

The email uses generic greetings like "Dear Customer" instead of your name, which legitimate organizations usually use if they have your information.

Spelling and Grammar Mistakes:

Phishing emails often contain typos, grammatical errors, and awkward language, indicating that the message may not be from a professional source.

Mismatched URLs:

Hovering over any links shows a URL that does not match the context of the email or the supposed sender’s official website.

The use of shortened URLs or URLs with subtle misspellings.

Requests for Personal Information:

The email asks for sensitive information such as passwords, credit card numbers, or Social Security numbers, which legitimate organizations typically do not request via email.

Unexpected Attachments:

The presence of attachments that you were not expecting, especially if they have a strange file name or an unusual file extension (e.g., .exe, .zip).

Too Good to Be True Offers:

Promises of rewards, money, or gifts that seem too good to be true are common in phishing scams designed to lure recipients.

Unusual Email Content:

The email content is not relevant to you or is unexpected, such as an invoice for a purchase you did not make or a job offer without application.

Lack of Customization:

The email lacks personalized information that a legitimate sender would have, making it applicable to anyone.

Inconsistencies in Email Design:

The email's design looks unprofessional, uses low quality images, or has a layout that does not match the organization's standard branding.

Security and Privacy Disclaimers Missing:

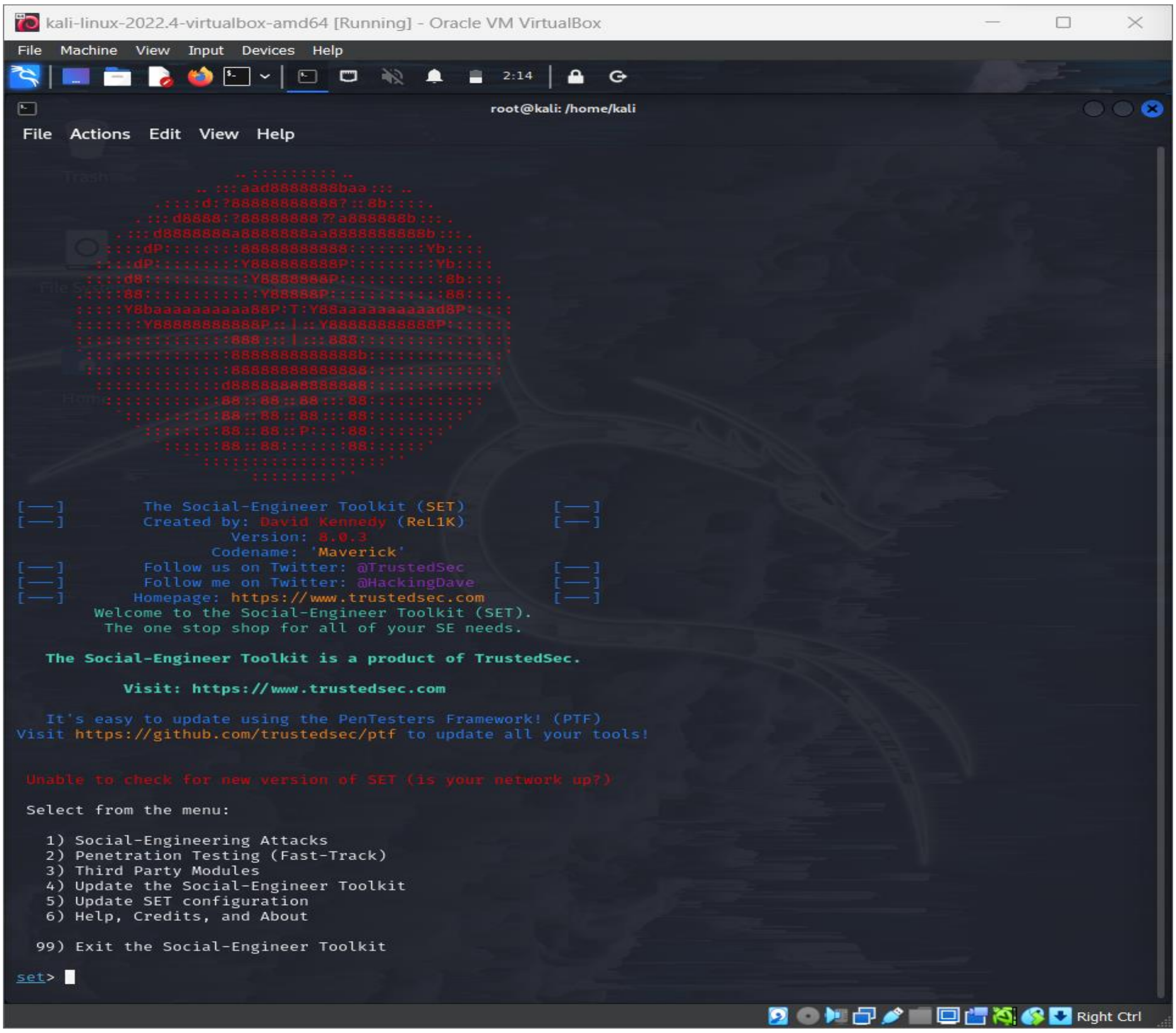
Legitimate emails from companies often include privacy information or disclaimers at the bottom, which phishing attempts might omit.

Demo of Mass mailer attack.

Use command:

>setoolkit

Press enter you will get the following interface.



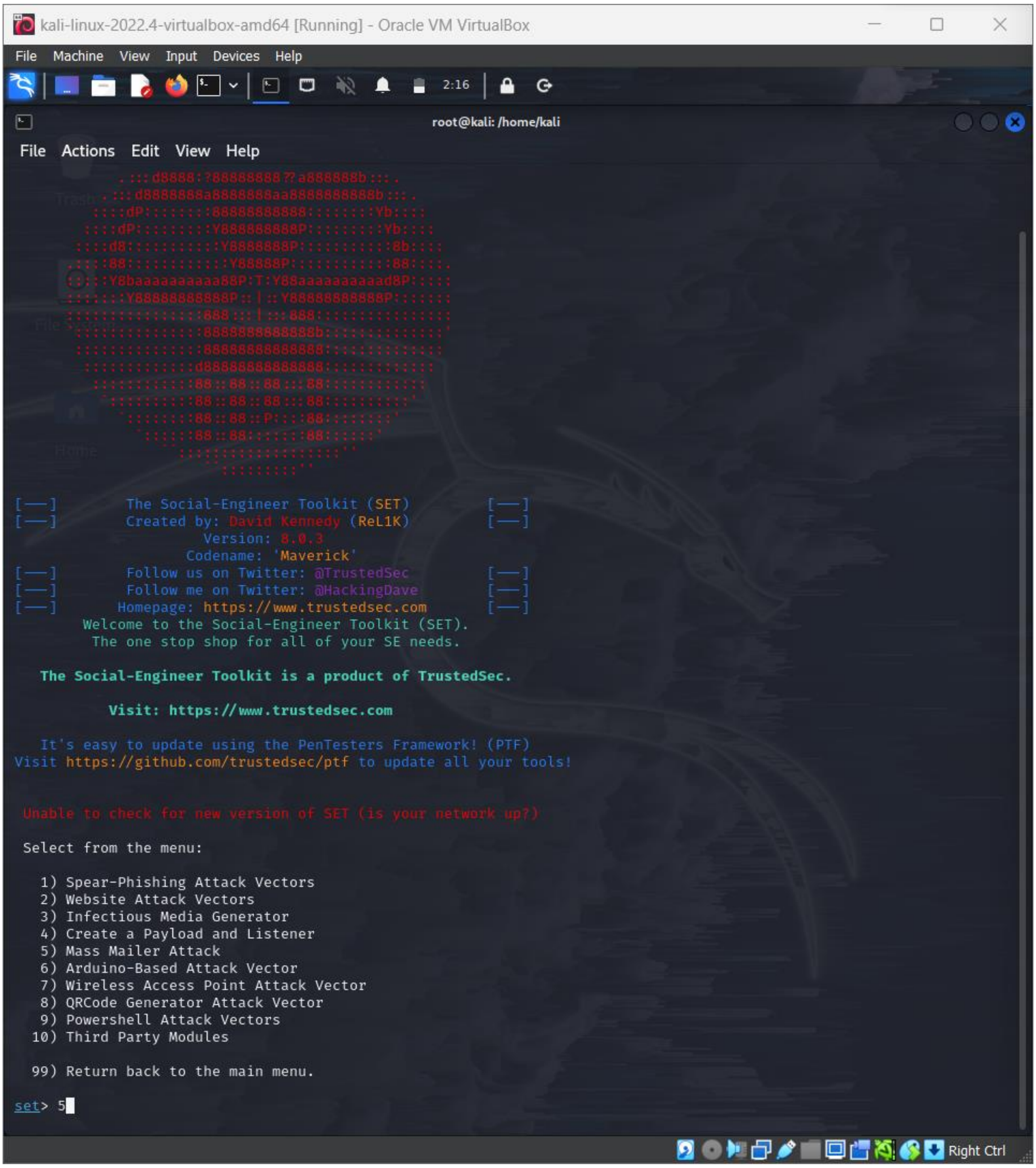
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
2:14
root@kali: /home/kali
File Actions Edit View Help
Right Ctrl

```
[---]        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!


 Unable to check for new version of SET (is your network up?)

 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> 
```

You will find the options as shown above and select ‘1’ which is Social engineering attack.

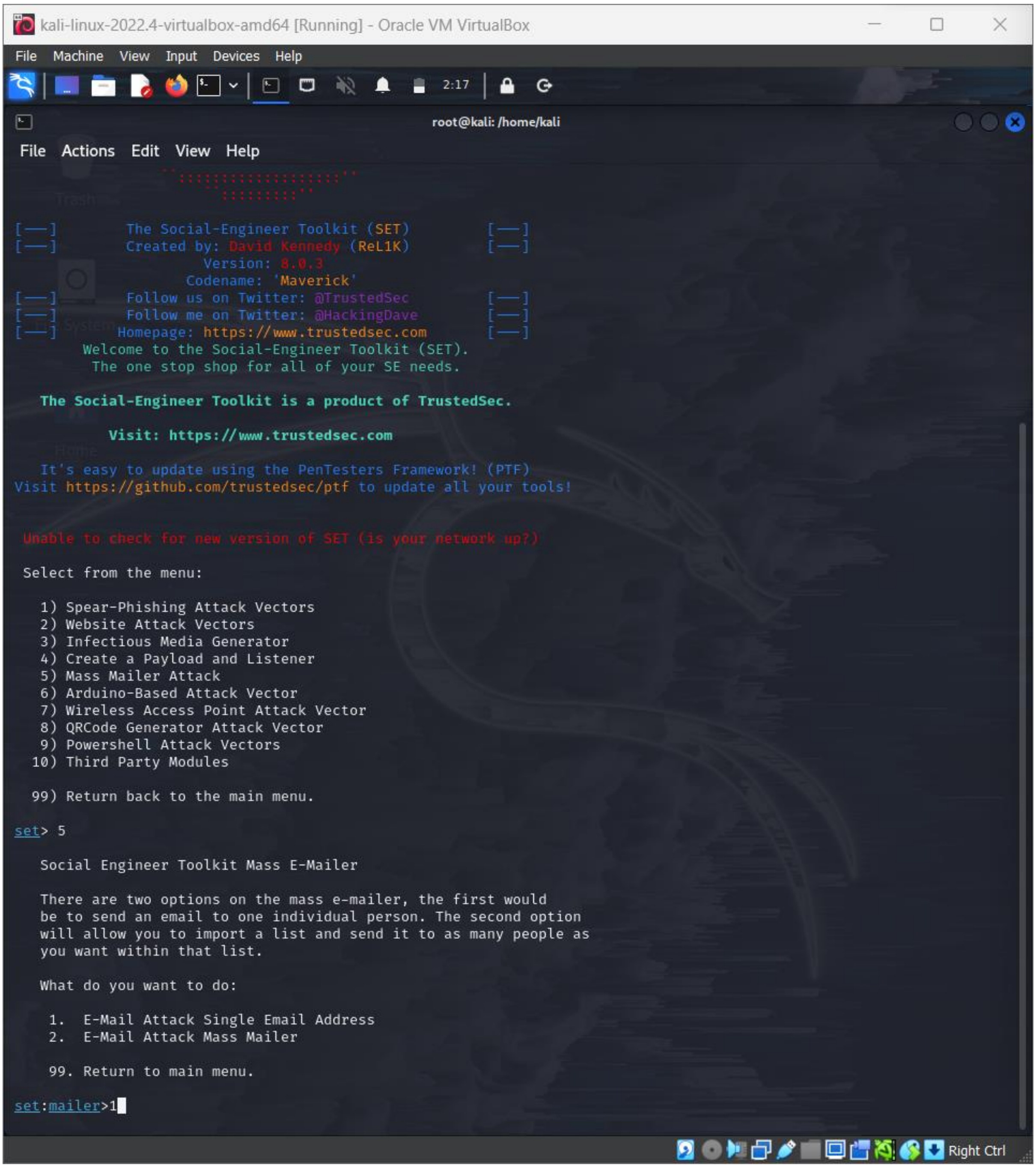
After entering it, we get to another interface which has some more options like mass mailer, spear phishing etc.

From that select ‘5’ which is mass mailer attack.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
2:16
root@kali: /home/kali
File Actions Edit View Help
Right Ctrl

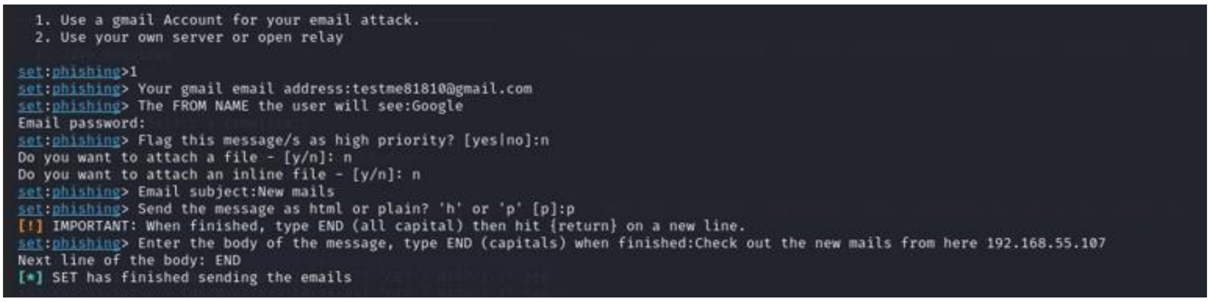
```
              .:::d8888:?88888888??a888888b:::.
            .:::d8888888a8888888aa8888888888b:::.
           ::::dP::::::::88888888888::::::::Yb::::
          ::::dP:::::::::Y888888888P:::::::::Yb::::
         ::::d8:::::::::::Y8888888P:::::::::::8b::::
        .::::88::::::::::::Y88888P::::::::::::88::::.
        :::::Y8baaaaaaaaaa88P:T:Y88aaaaaaaaaad8P:::::
        :::::::Y88888888888P::|::Y88888888888P:::::::
        ::::::::::::::::888:::|:::888::::::::::::::::
        `:::::::::::::::8888888888888b::::::::::::::'
         :::::::::::::::88888888888888::::::::::::::
          ::::::::::::::d88888888888888:::::::::::::
           ::::::::::::::88::88::88:::88::::::::::::
            `::::::::::::88::88::88:::88::::::::::'
              `::::::::::88::88::P::::88:::::::::'
                `::::::::88::88:::::::88::::::::'
                   ``::::::::::::::::::::::''
                        ``:::::::::''

[---]        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!


 Unable to check for new version of SET (is your network up?)

 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> 5
```

Under mass mailer attack, we would see 2 options as shown in below image select which ever you want. Here I am selecting option ‘1’ which is “Email attack single Email address”.



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
2:17
root@kali: /home/kali
File Actions Edit View Help
Right Ctrl

```
[—]         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!


 Unable to check for new version of SET (is your network up?)

 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> 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>1
```



```
   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:testme81810@gmail.com
set:phishing> The FROM NAME the user will see:Google
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:n
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:New mails
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] 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:Check out the new mails from here 192.168.55.107
Next line of the body: END
[*] SET has finished sending the emails
```

As shown above enter the mail id of the target and the mail id which you want to send from.

Enter Name which you want to display on target’s mail.

Now Enter Subject of the mail and body of the mail, in the body enter the phishing link you want to send to the target.

Whenever the target clicks on the phishing link, the targets details will be displayed on our (attacker's) device.