Cybersecurity Update

Charlie Hernandez

PROJECT?

Learning the tools of the trade

Network Fundamentals

Being able to apply these skills

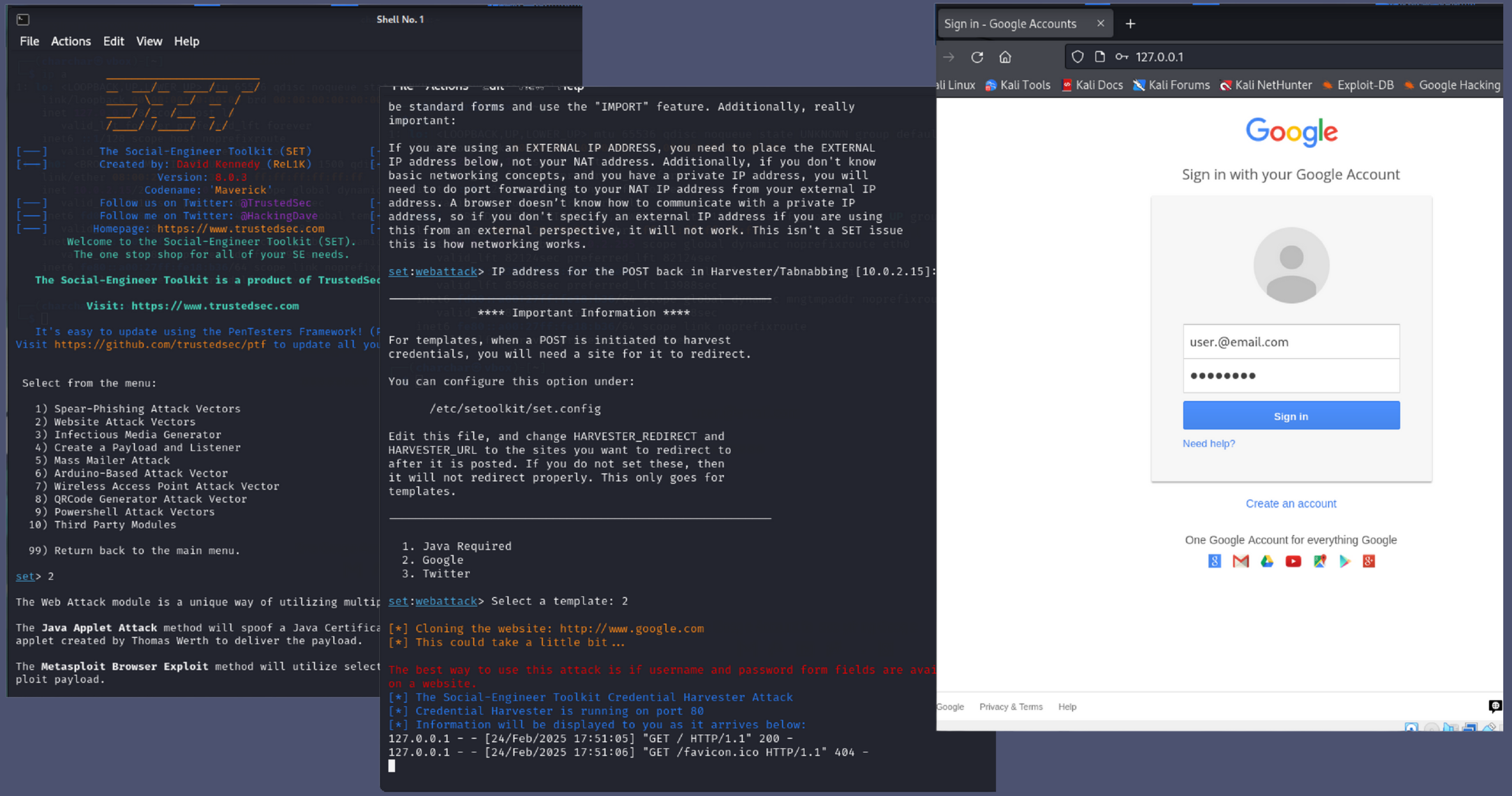
STUFF I'VE LEARNED

- NMAP
- Virtual Machines
- SET (Social Engineering Toolkit)
- Linux Console

```
[➜  ~ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-16 12:59 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.081s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    open     domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds
```

VirtualBox


Shell No. 1
File Actions Edit View Help
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! (P
Visit https://github.com/trustedsec/ptf to update all you
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
The Web Attack module is a unique way of utilizing multip
The Java Applet Attack method will spoof a Java Certifica
applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select
ploit payload.
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.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
**** 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 avai
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:
127.0.0.1 - - [24/Feb/2025 17:51:05] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [24/Feb/2025 17:51:06] "GET /favicon.ico HTTP/1.1" 404 -
Sign in - Google Accounts
127.0.0.1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking
Google
Sign in with your Google Account
user.@email.com
Sign in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help