**Laboratory Exercise X – SET Malicious Website Template**

Due Date: Date

Points Possible: 10% of the course grade.

**1. Overview**

Students will obtain hands-on experience creating a malicious website using SET in Kali by completing the following:

* Setting up and configuring penetration testing software;
* At the application level, understanding how a malicious website is created; and,
* Running simulation case scenarios to detect suspicious sites.

**2. Resources required**

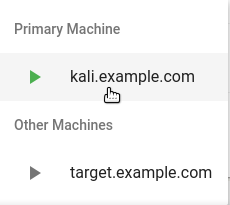
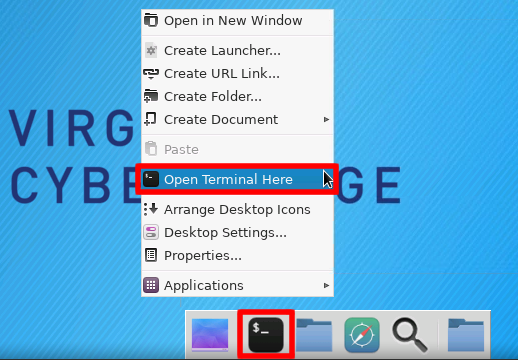
Virtual Machines (VMs) Needed: Windows 7 and Kali Linux. The Windows 7 VM is the victim machine while the Kali VM is the attacker machine. If you do not have a Cyber Range account, see your instructor for an invite or access code.

[**NOTE to Instructors**: Use the Cyber Range Environment: Kali Linux and Vulnerable Windows 7(64bit) VMs for this lab exercise.]

**3. Initial Setup**

The attacker VM (kali.example.com) and target VM (target.example.com) are on the same virtual network in the cloud network, so that they can ping each other and access all each other's ports; however, you may want to examine/record each VM’s IP address. In real hacking, attackers utilize a variety of techniques (e.g., social engineering) and security tools to get onto the victim’s network.  
  
You will be opening up two remote desktop sessions within your browser (once logged into the cyber range). Your Kali Linux desktop VM in one browser tab, and your target Windows desktop VM in another.

*NOTE: This is a good opportunity to refresh your knowledge of network fundamentals. A good way to do this is perform a network scan or vulnerability assessment/hardening procedures or comparing the target system before vs. after hardening.*

1.  **Log into the Cyber Range:** To log into the range for the first time, either click on the email invite sent to you by your instructor, or if you were provided an “invitation code” then point your browser to the link provided by your instructor to use it. At the Range Login window, select the “Have an invitation code?” link, paste in your invitation code and then select your preferred authentication provider Facebook, Google, or Microsoft.
2. **Log into Kali Linux VM:** Once logged into your instructor's course, click on the exercise as directed by your instructor, and click the start button (power icon) for your VM if not already started (could take a couple of minutes if it has never been started before). Once it comes up, the Join (play icon) will appear. Click on it and select the Primary Machine to log into, the “kali.example.com” desktop VM. This will pop open another browser tab.
3. Once your Kali Linux VM CyberRange console login pops up, log into the primary Kali desktop by using the **username=student** and **password=student**, which should place you at the Kali Linux VM's desktop. Your VM desktop may launch automatically without having to log in.
4. Once logged in to the Kali desktop, open a terminal window by either right-clicking on the desktop and selecting **Open Terminal Here**, by clicking on the black terminal icon in the **Launch Bar** at the bottom of the desktop, or through the **Applications** menu at the top left (not shown). See image on the right.
5. Your Kali Linux desktop should have the host name kali.example.com. In the Linux terminal, type:

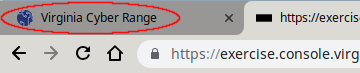
**host kali.example.com**

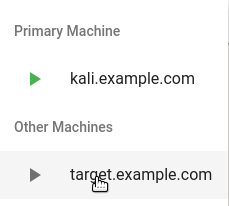
to see your Kali Linux machine's IP address. Write down this IP. Similarly, discover the IP of the target Windows VM by typing:

**host target.example.com** (from the Kali VM)

and see what that IP is. Record these two IP addresses below.  
  
Your Kali Linux Desktop's IP address:

Your Target Windows's IP address:



1. **Log into Target Windows VM:** In your browser's tabs at the very top of your screen, click back on the Cyber Range tab to access the console of your target Windows VM.
2. Again, click on the Join (play) icon, but this time select the login for the target.example.com machine. When the familiar Window login pops up for that VM, click on the **student** button, and then enter **password=student**. Your VM desktop may launch automatically without having to log in.
3. Once logged into the Windows desktop, a one-time “Windows Activation” window may pop up. If it does, just bypass this by selecting “Ask Me Later” (we're not registering this OS since this is for temporary, educational use).   
   ***NOTE****: On the “Windows Activation” requester, DO NOT select “Activate Now” or this will cause problems for you and you'll have to ask your instructor or TA to reset your VM environment.*
4. **Set Windows Network Location:** If you have never booted this VM before, you may also get this one-time network security check the first time this windows system comes on line and sees a new network. If you get this “Set Network Location” requester, you will get three options, “Home Network” (trusted), “Work Network” (trusted), or “Public Network” (untrusted). Select either Home or Work so that the Windows firewall will be disabled and you will be able to attack this target system from the Kali VM.

**4. Tasks**

**PART I – Verify/Install SET on Kali:**

1. **Verify Your SET Install:** If you're running the Cyber Range's Kali Linux VM, you already have SET installed. Verify it is working by opening a Kali Linux terminal and typing **sudo setoolkit**. (NOTE: The first time you execute this command, you may get a question asking you: “**Do you agree to the terms of service [y/n]:**” type **y** and hit enter.) Once the SET console comes up, it will look something like this:



The color text-graphics logo looks different each time you start setoolkit.

*NOTE: If you are not running Kali Linux or your VM does not have setoolkit, it can be manually installed from* [*https://github.com/trustedsec/social-engineer-toolkit/*](https://github.com/trustedsec/social-engineer-toolkit/) *.*

**Part II - Launch Exploit using SET**

* 1. **Configuring SET for Malicious Credential Harvest Attack**  
     In order to configure SET to launch the malicious credential harvester web attack, first ensure you have used the Cyber Range to log into both the attacker (Kali) and target (Windows) virtual machines.

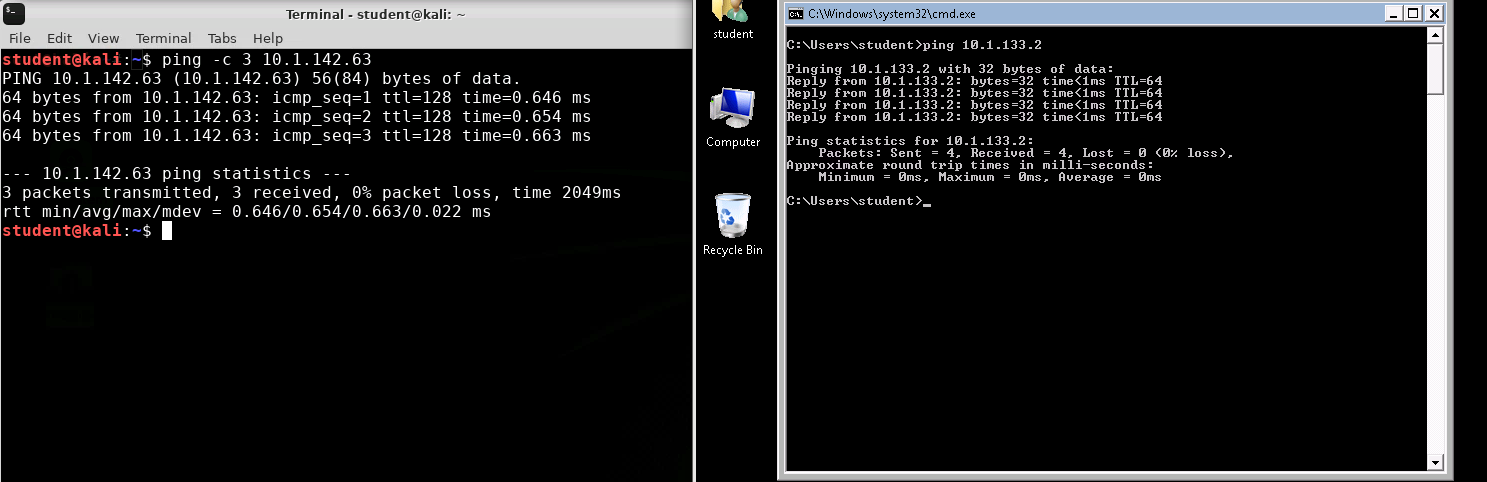
*NOTE: If your Windows VM has either the Windows firewall system or Windows Updates running, disable these. More information on this can be found here:* [*https://www.lifewire.com/2624505*](https://www.lifewire.com/2624505)

* 1. **Testing Connectivity Between Kali and Target (Windows):**   
     Open a new terminal on your Kali VM (leaving your setoolkit terminal alone), and then over on the Windows VM, open a command prompt by clicking the Windows menu and typing cmd.exe to pop open a command prompt window:
  2. Using the IP addresses for your Kali (kali.example.com) and Windows (target.example.com) VMs you retrieved via host/DNS in step 3.5, ping each machine from the other to verify accessible network connectivity between them.

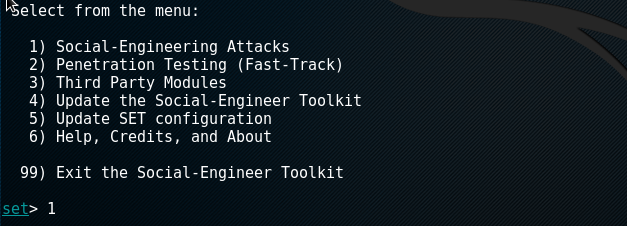
On Kali Linux terminal, type: **ping -c 3 *windows-IP***

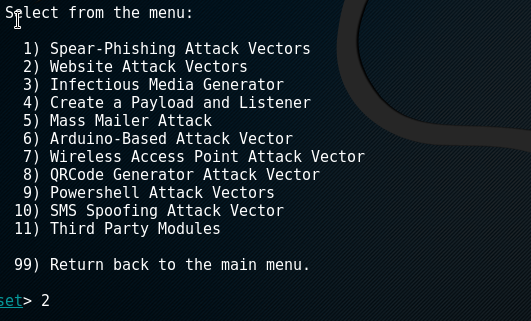
On the Windows cmd.exe window, type: **ping *kali-IP***

Here's an image of the kali (left) and windows/cmd.exe (right) terminals pinging each other. Use the IPs from step 3.5:

**

***NOTE:*** *If you cannot ping the Windows system from the Linux system, Google how to check and turn off, or disable the Windows firewall.*

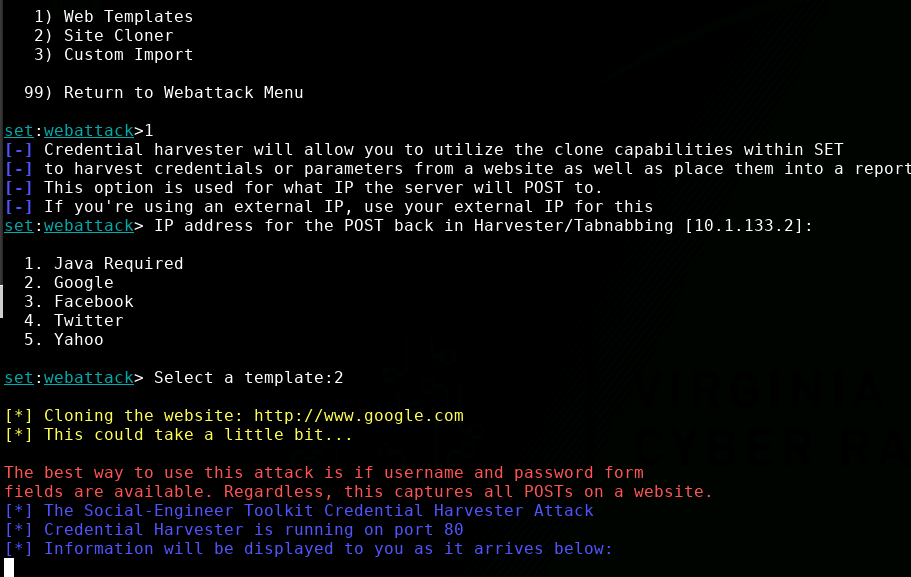
* 1. Once each machine can ping the other, go to the Kali terminal where you're running the SET (setoolkit) app, or if not already running SET, type **sudo setoolkit** to begin configuring the malicious website exploit.
  2. On the Kali machine, once you can see the SET configuration menu, begin configuring this exploit.   
       
     From the first config menu, choose 1 (Social-Engineering Attacks):   
     
  3. Then select 2 (Website Attack Vectors):

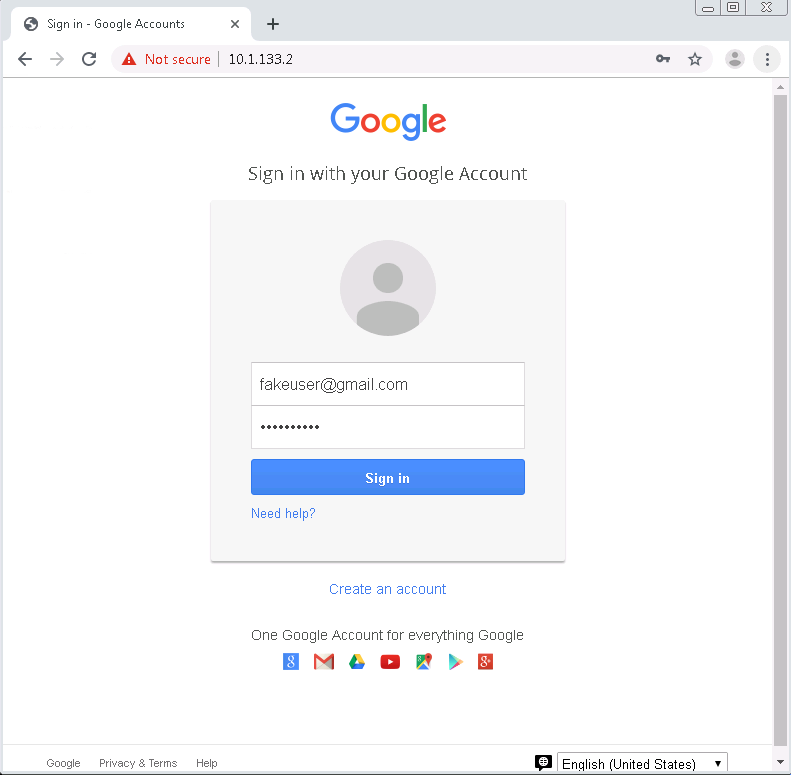


* 1. Then choose option 3 (Credential Harvester Attack Method):

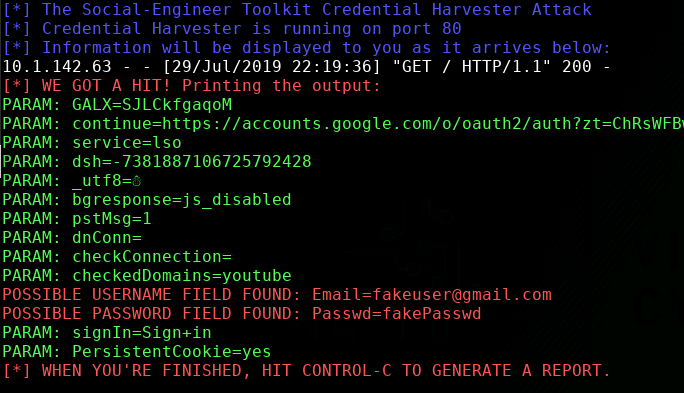


* 1. Then select 1 (Web Templates):

  
When prompted for an IP address to serve the webattack fake login server on, SET should default to your VM’s default IP address. Just hit enter to use [your-kali-IP], and then choose 2, which tells SET to use the Google login credential template.

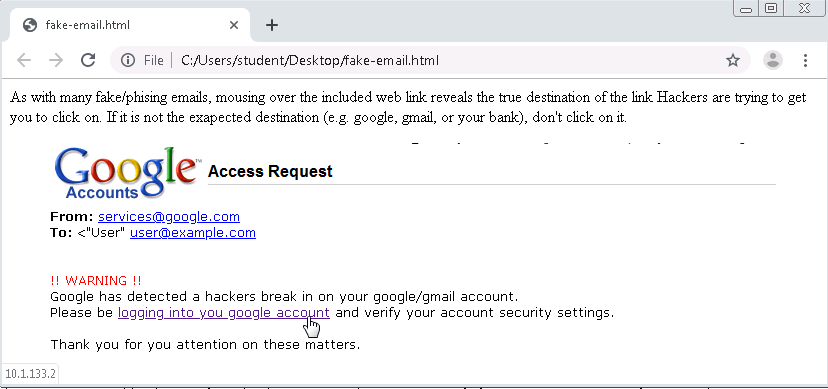
* 1. After choosing the option 2 (for Google), the webattack SET module will start running the Man-in-the-Middle credential harvester server and be ready to use once the final blue colored lines appear as seen below here:  
       
     At this point, the SET webattack Credential Harvester is up and running on your Kali machine's IP address, and your target(s) can be sent to that IP to start harvesting Google username/password credentials.
  2. **Harvesting Google Usernames and Passwords:** Switch over to the Windows/Target VM session, open a Chrome browser, and in the URL address field type the attacker (Kali) IP address (from step 3.5) to get to the fake google login page:  
       
     Finally, enter a test or fake username/password and click “Sign In.”

* 1. Back on the Kali attack system, you will see the SET terminal has collected the user's Google username and password as seen on the two red lines below:



**Class Discussion**

This type of attack is often delivered via email. Look at the following fake phishing/password harvesting email and discuss how you can be diligent in detecting and avoiding such scams:

 **CLASS DISCUSSION QUESTION:** How many questionable “red flags” can you detect in the above scammer phishing email?

**5. References**

* **Kali Linux -** [http://www.kali.org](http://www.kali.org/)
* **Website Phishing Scams** - <https://www.phishing.org/common-phishing-scams>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[This portion of the lab exercise template is provided for instructors that will be using this lab in a class they are teaching.]

**[CLASS DISCUSSION INSTRUCTOR NOTES]**  
  
From <https://www.phishing.org/common-phishing-scams>, the common signs of website phishing scams are:

* **“Unusual Urgency –** A legitimate website for a bank, credit card company or other organization isn’t going to have an air of desperation about it. You aren’t going to find urgent messages sprawling across such sites. Phishers rely on this type of urgency to increase the odds that people will quickly and willingly disclose sensitive information. If you land on a site [ore read an email that] seems to include a lot of [urgent messages], you should double-check [or mouse over] the URL and make sure that you’re [not going to a scammer site].
* **Poor Design –** The websites of professional businesses and organizations are generally sleek and stylish. If you visit one that seems to look a little ramshackle [or even if the fonts looks a little off], there’s a very good chance that you’ve stumbled upon a spoofed or cloned site. [...] If things look sloppy, take the time to do a little investigating before you proceed.
* **Misspellings –** Business websites typically written by professionals. They are not going to be riddled with misspellings and glaring grammatical errors. Scan through a site before you proceed. Does it seem to be well-written and professional? Has anything changed since your last visit? If it looks or sounds unprofessional or poorly written, don't click on anything before looking deeper.
* **Pop-Up Windows –** Legitimate sites are not going to bombard you with pop-up windows the second you land on them. Use a browser that allows you to block pop-ups. If one slips through, you should consider it to be a major red flag.”

The cyber range should be providing all the necessary platforms and software needed to complete this lab. Make sure both VMs can ping each other. This lab should be individual-based instead of group-based.

Course instructor can design follow-up exercises including the latest developments in malicious website attacks, especially in conjunction with Social Engineering.

**KSAs from NIST SP 800-181:** <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>

* S0016 Skill in configuring and optimizing software.
* S0044 Skill in mimicking threat behaviors.
* S0051 Skill in the use of penetration testing tools and techniques.
* S0078 Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
* A0093 Ability to identify/describe techniques/methods for conducting technical exploitation of the target.

**NSA/DHS CAE Knowledge Units:** <https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf>

(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

* Cyber Threats (CTH)