This site is dedicated to sharing information about the practice, ideas, concepts and patterns regarding computer security.

How to securely isolate and execute the Social-Engineer Toolkit from Kali Linux

Version 0.1, Last Updated: July 24

Table of Contents

Chapter 1. Introduction

The motivation behind this paper is to explore using the tool Social-Engineer Toolkit (SET) that comes with Kali Linux.

Chapter 2. Requirements

2.1. Writing Conventions

If you see the following $ symbol on a command line to execute, what that means is that the command is executed as a regular user; meaning an account that does not have administrative privileges. Ignore the leading $ and execute the rest of the command.

```
$ command to execute as a regular user
```

If you see a command line lead with the # symbol, then that means that the command is executed as the root user. This implies you need to elevate to the root user before running the command, e.g. with: `sudo su — root`.

```
# command to execute as the root user
```

2.2. VirtualBox

Go to: https://www.virtualbox.org/wiki/Downloads and download VirtualBox.

The author is running on Ubuntu 18.04, so following to this URL: https://www.virtualbox.org/wiki/Linux_Downloads

For Ubuntu, double click on the .deb file, i.e. virtualbox-5.2_5.2.0-118431-Ubuntu-zesty_amd64.deb, and install VirtualBox on your local workstation.

2.2.1. Clean VirtualBox Networking

This section is here in case you already had virtualbox installed from before. The intent is to clean up the previous networking. If you do not need to do this, skip to Add VirtualBox Networking

Run these two commands from a Terminal:

```
$ VBoxManage list natnetworks
$ VBoxManage list dhcpservers
```

Output (example):

```
NetworkName:    192.168.139-NAT
IP:             192.168.139.1
Network:        192.168.139.0/24
IPv6 Enabled:   No
IPv6 Prefix:    fd17:625c:f037:2::/64
DHCP Enabled:   Yes
```

```
Enabled:        Yes
loopback mappings (ipv4)
        127.0.0.1=2


NetworkName:    192.168.139-NAT
Dhcpd IP:       192.168.139.3
LowerIPAddress: 192.168.139.101
UpperIPAddress: 192.168.139.254
NetworkMask:    255.255.255.0
Enabled:        Yes
Global Configuration:
    minLeaseTime:     default
    defaultLeaseTime: default
    maxLeaseTime:     default
    Forced options:   None
    Suppressed opts.: None
        1/legacy: 255.255.255.0
Groups:               None
Individual Configs:   None

NetworkName:    HostInterfaceNetworking-vboxnet0
Dhcpd IP:       172.20.0.3
LowerIPAddress: 172.20.0.101
UpperIPAddress: 172.20.0.254
NetworkMask:    255.255.255.0
Enabled:        Yes
Global Configuration:
    minLeaseTime:     default
    defaultLeaseTime: default
    maxLeaseTime:     default
    Forced options:   None
    Suppressed opts.: None
        1/legacy: 255.255.255.0
Groups:               None
Individual Configs:   None
```

Now, delete ALL of the pre-installed VirtualBox networks (one at a time following the syntax below):

```
VBoxManage natnetwork remove --netname <NetworkName_from_above>
VBoxManage natnetwork remove --netname 192.168.139-NAT
```

Repeat as many times as necessary to delete all of them.

Now, delete ALL of the pre-installed DHCP services:

```
VBoxManage dhcpserver remove --netname <DHCP_Server_NetworkName_from_above>
VBoxManage dhcpserver remove --netname 192.168.139-NAT
```

Repeat as many times as necessary to delete all of them.

2.2.2. Add VirtualBox Networking

Now, add the new VirtualBox networks so the Kali Linux guides work.

```
VBoxManage natnetwork add \
    --netname 192.168.139-NAT \
    --network "192.168.139.0/24" \
    --enable --dhcp on

VBoxManage dhcpserver add \
    --netname 192.168.139-NAT \
    --ip 192.168.139.3 \
    --lowerip 192.168.139.101 \
    --upperip 192.168.139.254 \
    --netmask 255.255.255.0 \
    --enable

VBoxManage hostonlyif create

VBoxManage hostonlyif ipconfig vboxnet0 \
    --ip 172.20.0.1 \
    --netmask 255.255.255.0

VBoxManage dhcpserver add \
    --ifname vboxnet0 \
    --ip 172.20.0.3 \
    --lowerip 172.20.0.101 \
    --upperip 172.20.0.254 \
    --netmask 255.255.255.0

VBoxManage dhcpserver modify \
    --ifname vboxnet0 \
    --enable
```

VirtualBox install complete.

2.3. Vagrant

Go to: https://www.vagrantup.com/downloads.html, follow the appropriate link to your OS and 32 or 64 bit version representing your local workstation. Download.

For Ubuntu, double click on the .deb file, i.e. vagrant_2.0.1_x86_64.deb, and install Vagrant on your local system.

NOTE Update vagrant vm: `vagrant box update`

2.4. Kali Linux and Damn Vulnerable Web Application (DVWA)

The author highly recommends to create a directory structure that is easy to navigate and find your code. As an example, you could use something similar to:

```
${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

Go ahead and make this structure with the following command (inside a Terminal):

```
$ mkdir –p ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

From a Terminal, change directory to:

```
$ cd ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

2.4.1. Vagrantfile

Inside of the kali-linux-vm directory, populate a new file with the exact name, “Vagrantfile”. Case matters, uppercase the “V”. This file will contain both virtual machines for Kali Linux as well as setting up the DVWA virtual machine. Aggregating both virtual machines into one file has saved the author a lot of time. The coolness here is setting up the variables at the top of the Vagrantfile mimicing shell scripting inside of a virtual machine (passed in with provision: shell). I tested using: `apt-get update && apt-get upgrade -y`, but opted to take it out since it took over 45 minutes on my slower (old) hardware. See comment about downloading this file immediately preceding the code block.

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

$os_update = <<SCRIPT
apt-get update
SCRIPT

VAGRANTFILE_API_VERSION = "2"


Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
    config.vm.define "kali-linux-vagrant" do |conf|
        conf.vm.box = "kalilinux/rolling"

        # For Linux systems with the Wireless network, uncomment the line:
```

```
        conf.vm.network "public_network", bridge: "wlo1", auto_config: true

        # For macbook/OSx systems, uncomment the line and comment out the Linux
Wireless network:
        #conf.vm.network "public_network", bridge: "en0: Wi-Fi (AirPort)",
auto_config: true

        conf.vm.hostname = "kali-linux-vagrant"
        conf.vm.provider "virtualbox" do |vb|
            vb.gui = true
            vb.memory = "4096"
            vb.cpus = "2"
            vb.customize ["modifyvm", :id, "--vram", "32"]
            vb.customize ["modifyvm", :id, "--accelerate3d", "off"]
            vb.customize ["modifyvm", :id, "--ostype", "Debian_64"]
            vb.customize ["modifyvm", :id, "--boot1", "dvd"]
            vb.customize ["modifyvm", :id, "--boot2", "disk"]
            vb.customize ["modifyvm", :id, "--audio", "none"]
            vb.customize ["modifyvm", :id, "--clipboard", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--paravirtprovider", "kvm"]
        end
        conf.vm.provision "shell", inline: $os_update
    end

    config.vm.define "dvwa-vagrant" do |conf|

        conf.vm.box = "ubuntu/xenial64"

        conf.vm.hostname = "dvwa-vagrant"

        # For Linux systems with the Wireless network, uncomment the line:
        conf.vm.network "public_network", bridge: "wlo1", auto_config: true

        # For macbook/OSx systems, uncomment the line and comment out the Linux
Wireless network:
        #conf.vm.network "public_network", bridge: "en0: Wi-Fi (AirPort)",
auto_config: true

        config.vm.network "forwarded_port", guest: 80, host: 8080, auto_correct: true
        config.vm.network "forwarded_port", guest: 3306, host: 3306, auto_correct:
true

        conf.vm.provider "virtualbox" do |vb|
            vb.memory = "1024"
            vb.cpus = "2"
            vb.gui = false
            vb.customize ["modifyvm", :id, "--vram", "32"]
            vb.customize ["modifyvm", :id, "--accelerate3d", "off"]
            vb.customize ["modifyvm", :id, "--ostype", "Ubuntu_64"]
            vb.customize ["modifyvm", :id, "--boot1", "dvd"]
            vb.customize ["modifyvm", :id, "--boot2", "disk"]
            vb.customize ["modifyvm", :id, "--audio", "none"]
            vb.customize ["modifyvm", :id, "--clipboard", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--paravirtprovider", "kvm"]
        end
        conf.vm.provision "shell", inline: $os_update
        conf.vm.provision :shell, path: "bootstrap.sh"
    end
end
```

Save and write this file.

You can also download from:

```
$ curl -o Vagrantfile  http://securityhardening.com/files/Vagrantfile_20200928.txt
```

2.4.2. bootstrap.sh

Inside of the kali-linux-vm directory, populate a new file with the exact name, `bootstrap.sh`. Case matters, all lowercase. See comment about downloading this file immediately preceding the code block. `bootstrap.sh` (include the shebang in your file: the first line with `#!/usr/bin/env bash`):

```
#!/usr/bin/env bash
PHP_FPM_PATH_INI='/etc/php/7.0/fpm/php.ini'
PHP_FPM_POOL_CONF='/etc/php/7.0/fpm/pool.d/www.conf'
MYSQL_ROOT_PW='Assword12345'
MYSQL_dvwa_user='dvwa'
MYSQL_dvwa_password='sunshine'
DVWA_admin_password='admin'
recaptcha_public_key='u8392ihj32kl8hujalkshuil32'
recaptcha_private_key='89ry8932873832lih32ilj32'


install_base() {
    add-apt-repository -y ppa:nginx/stable
    sudo apt-get update
    sudo apt-get dist-upgrade -y
    sudo apt-get install -y \
        nginx \
        mariadb-server \
        mariadb-client \
        php \
        php-common \
        php-cgi \
        php-fpm \
        php-gd \
        php-cli \
        php-pear \
        php-mcrypt \
        php-mysql \
        php-gd \
        git \
        vim
}

config_mysql(){
    mysqladmin -u root password "${MYSQL_ROOT_PW}"
## Config the mysql config file for root so it doesn't prompt for password.
## Also sets pw in plain text for easy access.
## Don't forget to change the password here!!

cat <<EOF > /root/.my.cnf
[client]
user="root"
password="${MYSQL_ROOT_PW}"
EOF
    mysql -BNe "drop database if exists dvwa;"
    mysql -BNe "CREATE DATABASE dvwa;"
    mysql -BNe "GRANT ALL ON *.* TO '"${MYSQL_dvwa_user}"'@'localhost' IDENTIFIED BY
'"${MYSQL_dvwa_password}"';"

    systemctl enable mysql
    systemctl restart mysql
    sleep 2
}



config_php(){
    ## Config PHP FPM INI to disable some security settings:

    sed -i 's/^;cgi.fix_pathinfo.*$/cgi.fix_pathinfo = 0/g' ${PHP_FPM_PATH_INI}
    sed -i 's/allow_url_include = Off/allow_url_include = On/g' ${PHP_FPM_PATH_INI}
    sed -i 's/allow_url_fopen = Off/allow_url_fopen = On/g' ${PHP_FPM_PATH_INI}
    sed -i 's/safe_mode = On/safe_mode = Off/g' ${PHP_FPM_PATH_INI}
    echo "magic_quotes_gpc = Off" >> ${PHP_FPM_PATH_INI}
    sed -i 's/display_errors = Off/display_errors = On/g' ${PHP_FPM_PATH_INI}

    ## explicitly set pool options
    ## (these are defaults in ubuntu 16.04 so i'm commenting them out.
    ## If they are not defaults for you try uncommenting these)
    #sed -i 's/^;security.limit_extensions.*$/security.limit_extensions = \
    #.php .php3 .php4 .php5 .php7/g' /etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^listen.owner.*$/listen.owner = www-data/g'
/etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^listen.group.*$/listen.group = www-data/g'
/etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^;listen.mode.*$/listen.mode = 0660/g' /etc/php/7.0/fpm/pool.d/www.conf
    systemctl restart php7.0-fpm
}


config_nginx(){

cat << 'EOF' > /etc/nginx/sites-enabled/default
server
{
    listen  80;
    root /var/www/html;
    index index.php index.html index.htm;
    #server_name localhost
    location "/"
    {
        index index.php index.html index.htm;
        #try_files $uri $uri/ =404;
    }

    location ~ \.php$
    {
        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/var/run/php/php7.0-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $request_filename;
    }
}
EOF

    systemctl restart nginx
}


install_dvwa(){

    if [[ ! -d "/var/www/html" ]];
    then
          mkdir -p /var/www;
          ln -s /usr/share/nginx/html /var/www/html;
          chown -R www-data. /var/www/html;
    fi

    cd /var/www/html
    rm -rf /var/www/html/.[!.]*
    rm -rf /var/www/html/*
    git clone https://github.com/ethicalhack3r/DVWA.git ./
    chown -R www-data. ./
    cp config/config.inc.php.dist config/config.inc.php

    ### chmod uploads and log file to be writable by nobody
    chmod 777 ./hackable/uploads/
    chmod 777 ./external/phpids/0.6/lib/IDS/tmp/phpids_log.txt

    ## change the values in the config to match our setup (these are what you need to
update!
    sed -i '/db_user/ s/root/'${MYSQL_dvwa_user}'/'
/var/www/html/config/config.inc.php
    sed -i '/db_password/ s/p@ssw0rd/'${MYSQL_dvwa_password}'/'
/var/www/html/config/config.inc.php
    sed -i "/recaptcha_public_key/ s/''/'"${recaptcha_public_key}"'/"
/var/www/html/config/config.inc.php
    sed -i "/recaptcha_private_key/ s/''/'"${recaptcha_private_key}"'/"
/var/www/html/config/config.inc.php

}



update_mysql_user_pws(){
## The mysql passwords are set via /usr/share/nginx/html/dvwa/includes/DBMS/MySQL.php.
#  If you edit this every time they are reset it will reset to those.
#  Otherwise you can do a sql update statement to update them all (they are just md5's
of the string.
#  The issue is the users table doesn't get created until you click that button T_T to
init.

#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'admin';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'gordonb';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'1337';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'pablo';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'smithy';"

sed -i '/admin/ s/password/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/gordonb/ s/abc123/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/1337/ s/charley/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/pablo/ s/letmein/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/smithy/ s/password/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
}



install_base
config_mysql
```

```
install_dvwa
update_mysql_user_pws
config_php
config_nginx
```

Save and write this file.

If you have issues with copying and pasting the above file because code blocks in PDFs always copy correctly [NOT!], you could use curl, i.e. Make sure the bootstrap.sh file ends up in the same directory as the Vagrantfile.

```
$ curl -o bootstrap.sh  http://securityhardening.com/files/bootstrap_sh_20200928.txt
```

From a Terminal, change directory to:

```
$ cd ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

Then run (inside the directory kali-linux-vm):

```
$ vagrant up
```

This will download the appropriate images and start the virtual machines. Once running, through the VirtuaBox GUI, login as root. Password is “toor”, root backwards. Edit the following file: `/etc/ssh/sshd_config`

And change the line: `#PermitRootLogin prothibit-password` To: `PermitRootLogin yes` Meaning strip the comment out on the beginning of the line and alter `prohibit-password` to `yes`.

Then restart the ssh daemon:

```
# kill □HUP $(pgrep sshd)
```

Notice, you are on a Bridged adapter, this will open the instance to allow root to ssh in with the most unsecure password in the world. Only make this change (allowing root to login via SSH) if you require root SSH access. You can change the root user’s password, which is highly recommended.

For the DVWA instance, I would first run ‘vagrant status’ to capture the name that vagrant is using for the running instance.

```
# vagrant status
```

Choose

```
Current machine states:
```

```
kali-linux-vagrant running (virtualbox)
dvwa-vagrant running (virtualbox)
```

This environment represents multiple VMs. The VMs are all listed above with their current state. For more information about a specific VM, run `vagrant status NAME`.

From there, log into the DVWA instance with:

```
$ vagrant ssh dvwa-vagrant
```

And then get the current IP address.

```
$ ip a
```

Choose the second network adapter, it should look like:

```
ubuntu@dvwa:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 02:53:17:3c:de:80 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::53:17ff:fe3c:de80/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 08:00:27:f0:77:2d brd ff:ff:ff:ff:ff:ff
    inet 172.20.156.76/24 brd 172.20.156.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef0:772d/64 scope link
        valid_lft forever preferred_lft forever
```

The test network used for this paper uses 172.20.156.0/24 as the network range [shown here in section 3]. Therefore, the adapter, enp0s8 is what he is looking for. The IP to use as a target is 172.20.156.76. Write down your value.

Chapter 3. Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python software pacakge aimed at penetration testing using Social Engineering.

Leveraged by security researchers, penetration testers, blue and purple teams globally, SET targets humans as the weakest link in the chain as its primary attack technique.

The main features of SET are:

- Allows multiple tweaks from the configuration menu.
- Includes access to the Fast-Track Penetration Testing platform
- Multi-platform: It can run on Linux, and Windows.
- Supports integration with third party modules.
- Social engineering attack options such as:
    - Arduino-Based Attack
    - Infection Media Generator
    - Mass Mailing
    - Powershell Attack Vectors
    - QRCode Attacks
    - Spear-Phishing Attacks
    - Website Attacks
    - and many more

Chapter 4. Main Attacks with the Social-Engineer Toolkit

4.1. Phishing Attacks

What they are:

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, phishing is by far the most common attack performed by cybercriminals, the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.

4.2. Web Application Attack

What they are:

To understand this, we need to know what a Web Application does. A web application or web app is a software program that runs on a server and is accessed usually with the same means of accessing a website. Most modern websites consist of two different components: a web browser [on the client side] and at least one web application [on the server side].

A web application attack targets a web application. The web application is frequently the front end between the web servers and backend end servers, e.g. database servers. When a web application is compromised, typically both the front end servers and backend servers [e.g. database] might also be compromised.

4.3. Infectious Media Generator

What this is:

This feature enables you to create an infected media device (USB/CD/DVD) with an autorun.inf file. Said device(s) can then be left in a busy area, or given to a targetted person to insert into any PC and will automatically run a chosen Metasploit payload if the autorun is enabled on the device this media was inserted into.

4.4. Create a Payload and Listener

What this is:

A payload is the carrying capacity of a packet or other transmission data unit. The term has its roots in the military and is often associated with the capacity of executable malicious code. Payload in this context has two meanings: data payload, which is related to the transport of data across a network, and malware payload, which refers to malicious code used to exploit and compromise IT networks and systems.

From the User Manual, "The create payload and listener is an extremely simple wrapper around Metasploit to create a payload, export the exe[cutable] for you and generate a listener. You would need to transfer the exe [file] onto the victim machine and execute it in order for it to properly work."

4.5. Mass Mailer Attack

What this is:

A Mass Mailer Attack is a type of social engineering attack in which large amount of mails is sent to the victim to fill his or her email inbox and crash said.

This type of attack can be performed against one or multiple individuals; letting you import users lists to send to any people you wish. It also lets you use a Gmail account for your email attack, or use your own server or open relay for mass delivery.

4.6. Wireless Access Point

From the User Manual, "Welcome to the Wireless Attack Vector, this will create an access point leveraging your wireless card and redirect all DNS queries to you. The concept is fairly simple, SET will create a wireless access point, dhcp server, and spoof DNS to redirect traffic to the attacker machine. It will then exit out of that menu with everything running as a child process. You can then launch any SET attack vector you want, for example the Java Applet attack and when a victim joins your access point and tries going to a website, will be redirected to your attacker machine. This attack vector uses AirBase-NG, AirMon-NG, DNSSpoof, and dhcpd3 to work properly."

4.7. QR Code Generator

What is a QR code:

A machine-readable code consisting of an array of black and white squares; typically used for storing URLs or other information by reading from a camera on a smartphone.

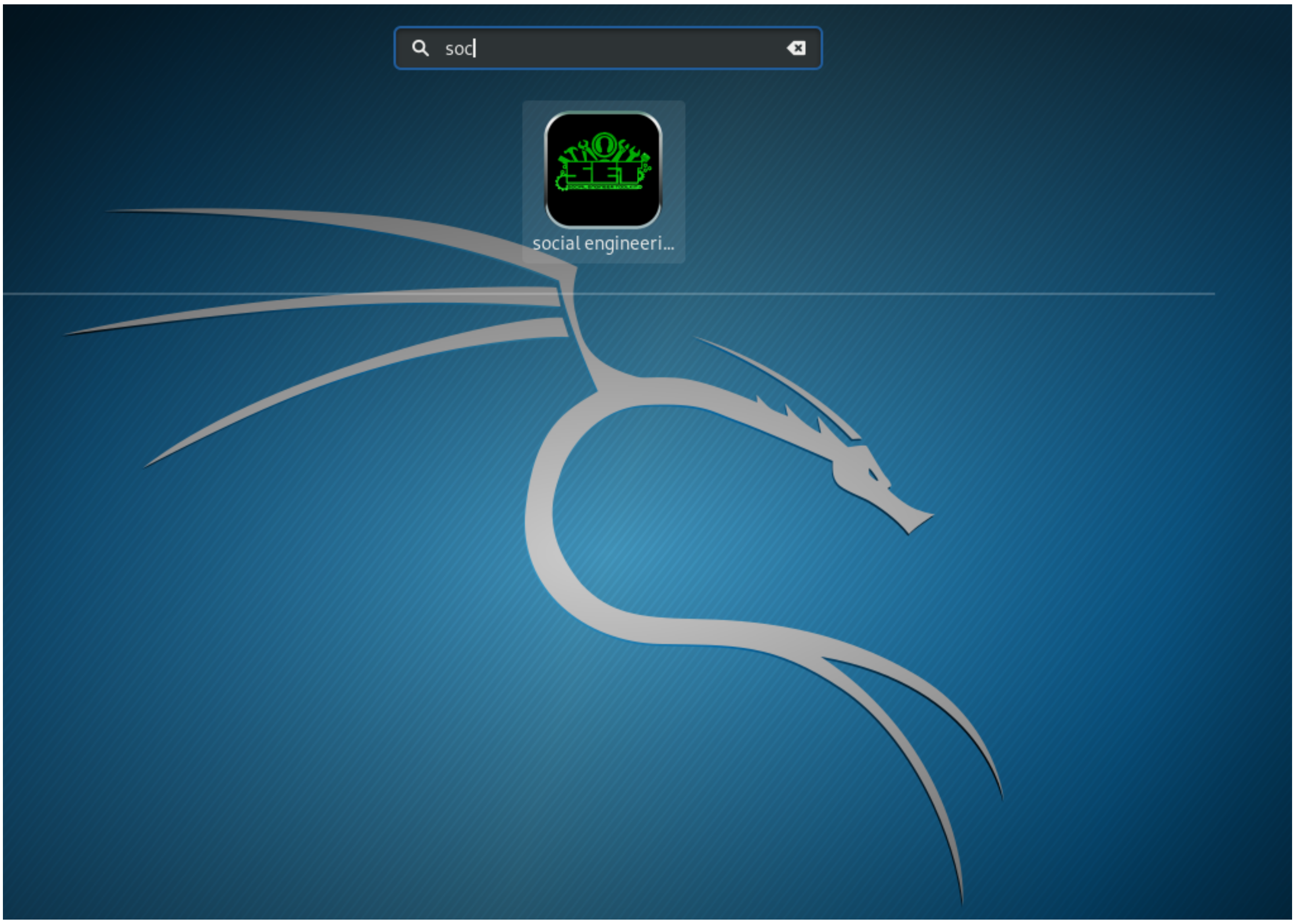
From the User Manual: "The QRCode Attack Vector will create a QRCode for you with whatever URL you want. When you have the QRCode Generated, select an additional attack vector within SET and deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet and send the QRCode via a mailer."

4.8. Powershell Attack Vectors

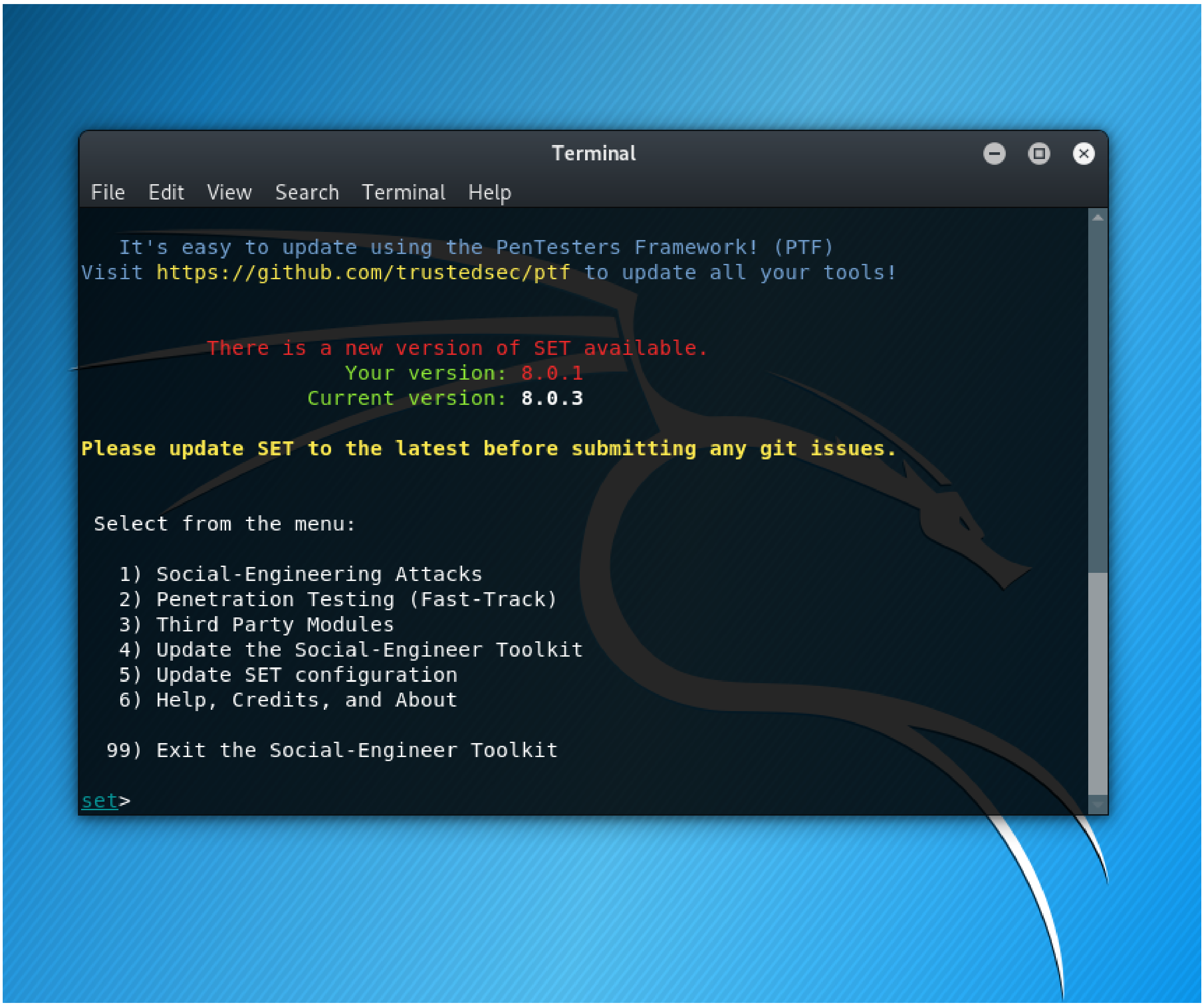
Advanced Volatile Threats (AVT), better known as fileless malware. This kind of threat is designed specifically not to write onto the storage device. Instead, it works from the memory of the target system. The absence of files on the storage device makes it impossible for traditional protection systems [that ONLY scan the filesystem] to detect the threat.

PowerShell, the Windows system console (CLI), is a great attack vector for fileless malware. PowerShell allows systems administrators to fully automate tasks on servers and computers.

Chapter 5. A deeper look at the available commands with SET

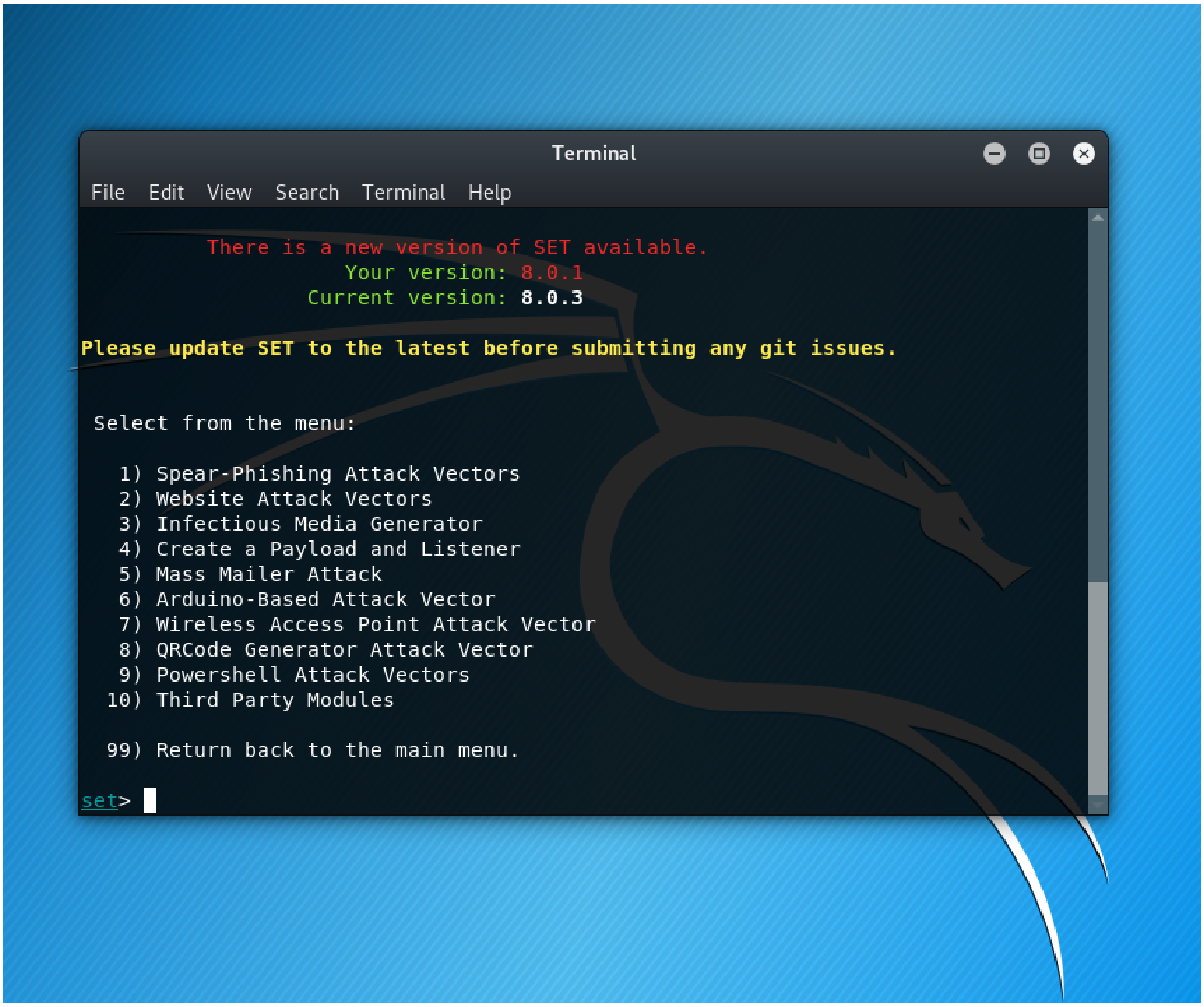


Here the author normally depresses the Windows or Command key and this opens a Window with all Applications. Use the search box at the top of the screen to search for the keyword, "social". Once SET is displayed, double click on the icon to launch SET.



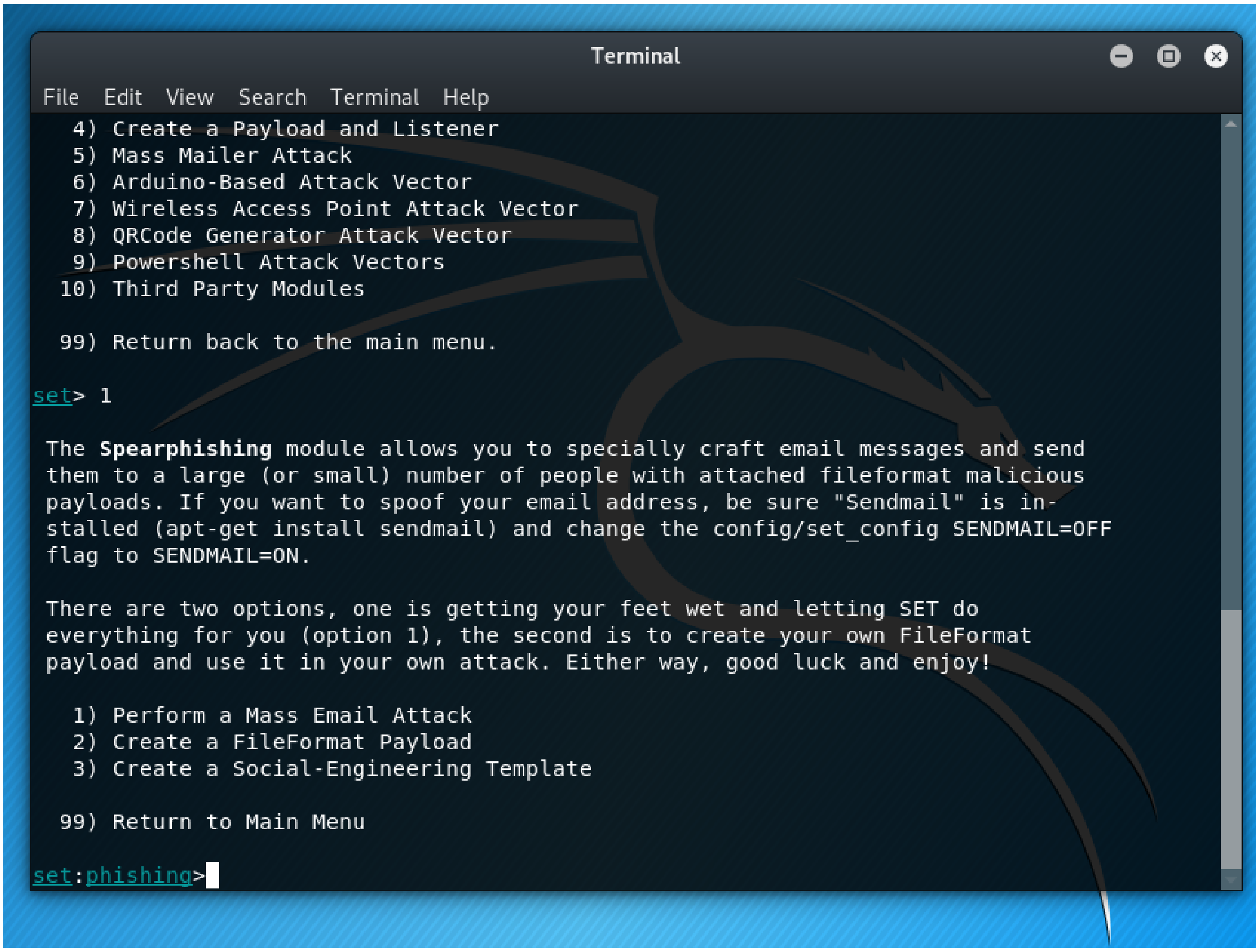
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


          There is a new version of SET available.
                     Your version: 8.0.1
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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>
```

Once the user [you] have accepted the license agreement, you will be presented with the main menu.



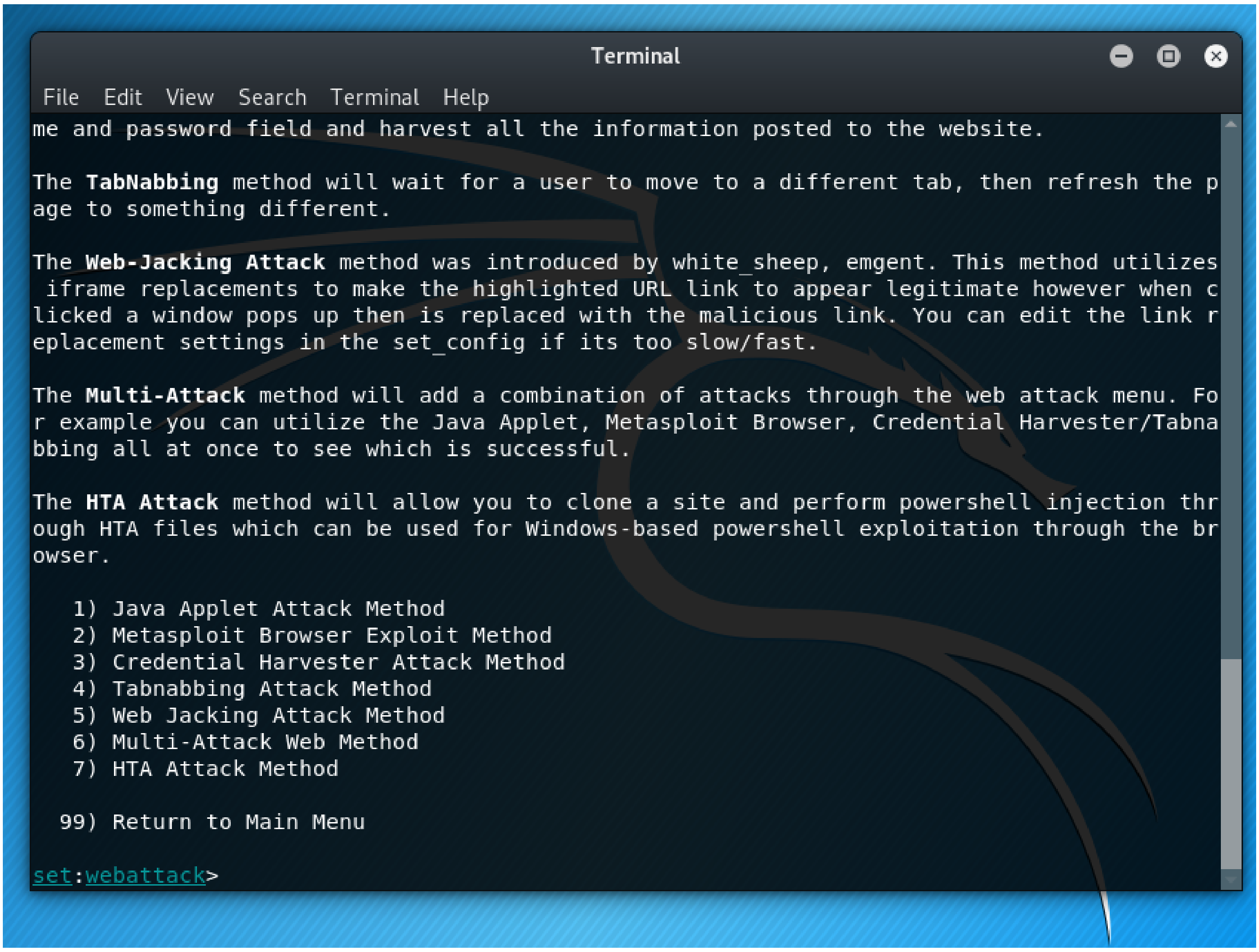
```
          There is a new version of SET available.
                     Your version: 8.0.1
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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>
```

This was from choosing the Social Engineering Attacks link (1). As you can observe, there are ten attack types to choose from on this menu.



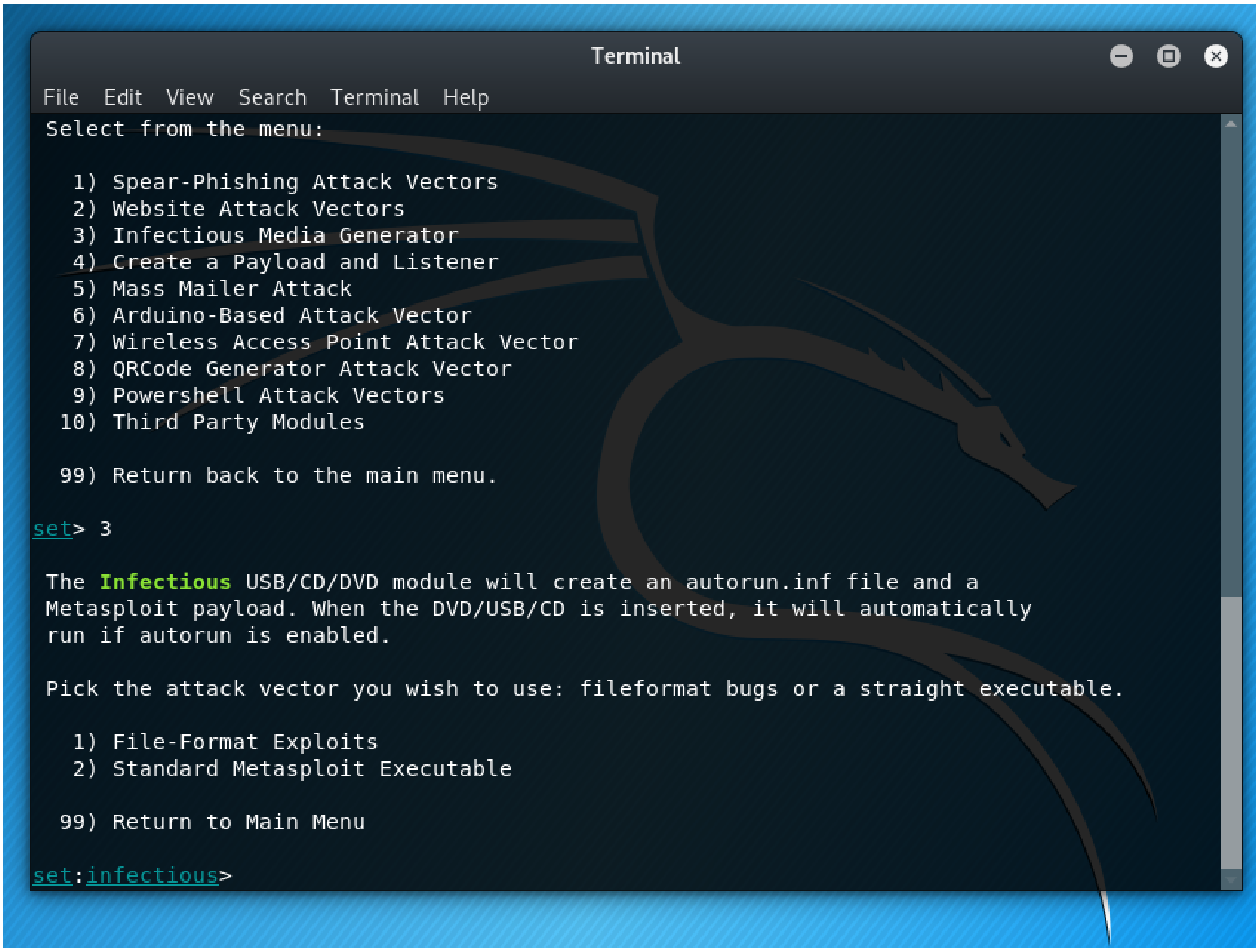
```
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

The Spear-Phishing Attack Vectors.



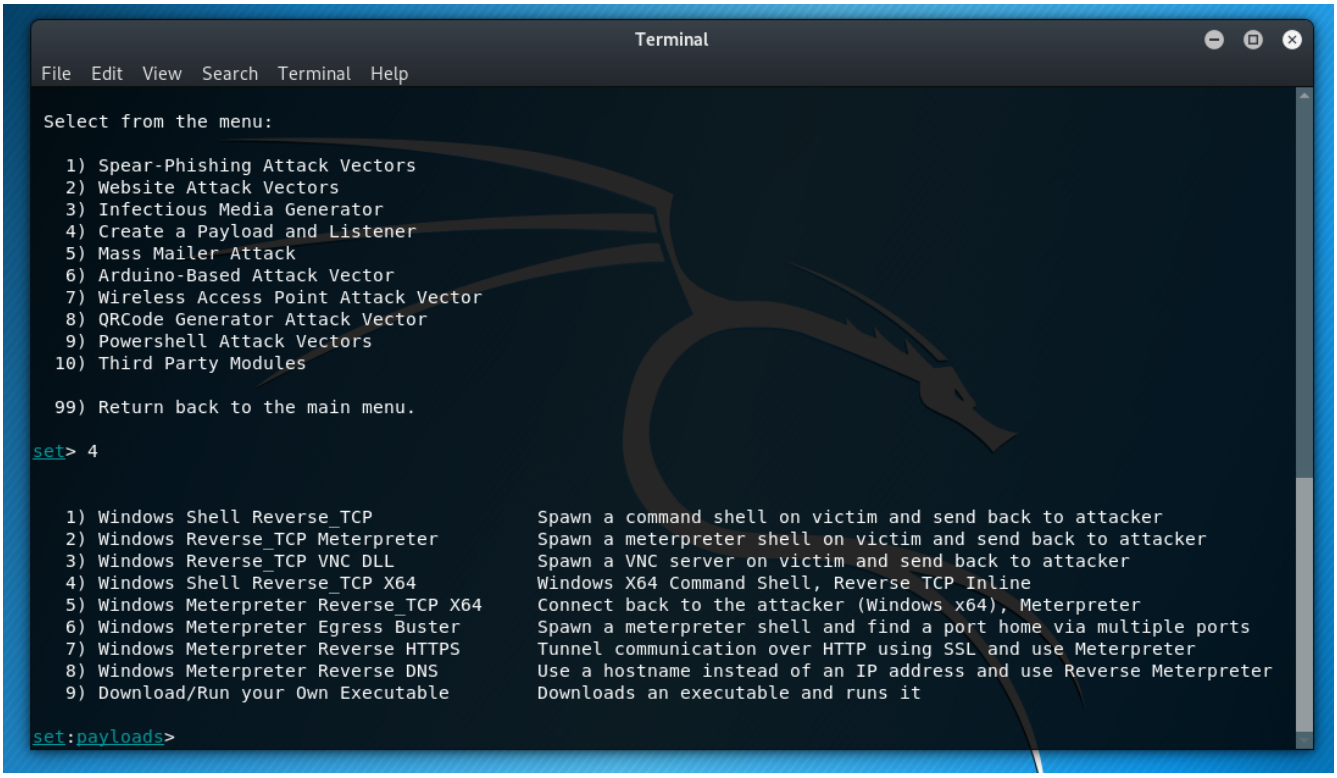
```
me and password field and harvest all the information posted to the website.

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

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes
 iframe replacements to make the highlighted URL link to appear legitimate however when c
licked a window pops up then is replaced with the malicious link. You can edit the link r
eplacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. Fo
r example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabna
bbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection thr
ough HTA files which can be used for Windows-based powershell exploitation through the br
owser.

   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>
```

The Website Attack Vectors.



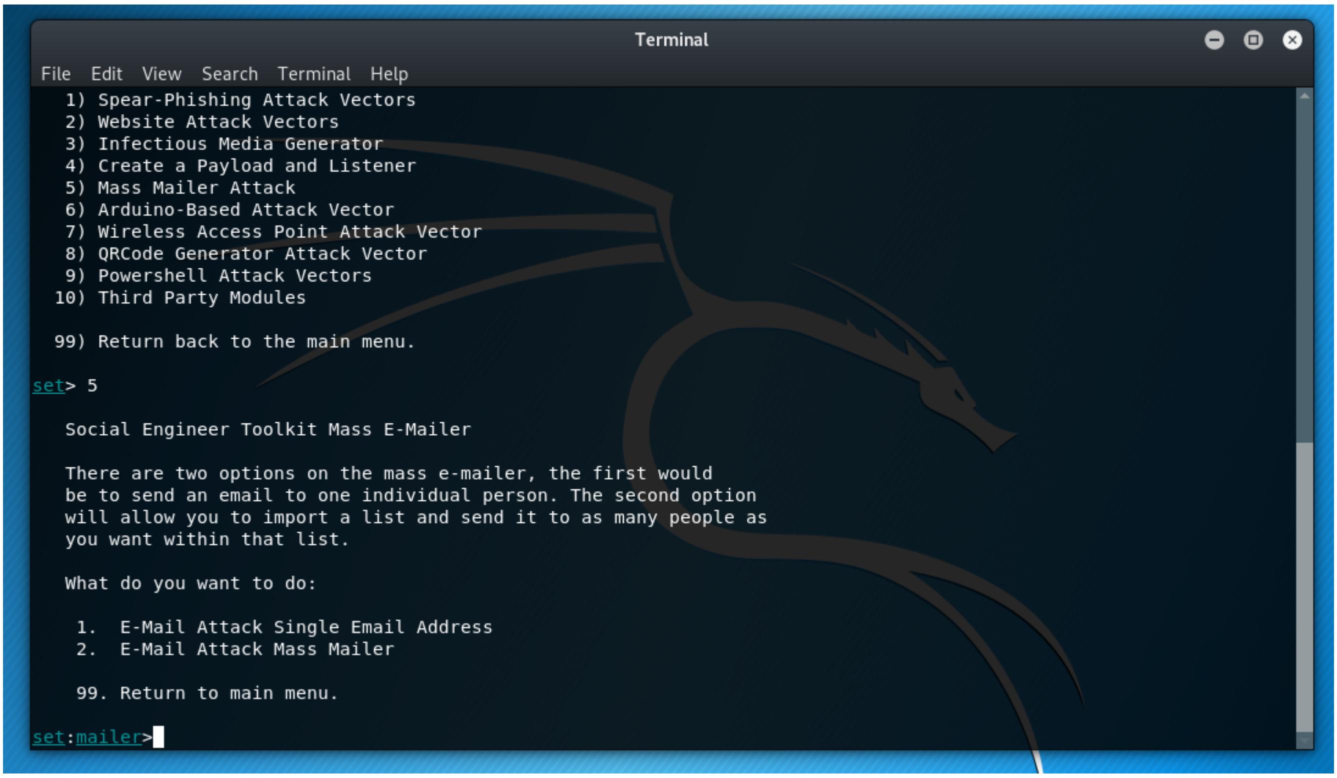
```
Select from the menu:

   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> 3

 The Infectious USB/CD/DVD module will create an autorun.inf file and a
 Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
 run if autorun is enabled.

 Pick the attack vector you wish to use: fileformat bugs or a straight executable.

   1) File-Format Exploits
   2) Standard Metasploit Executable

  99) Return to Main Menu

set:infectious>
```

The Infectious Media Generator.



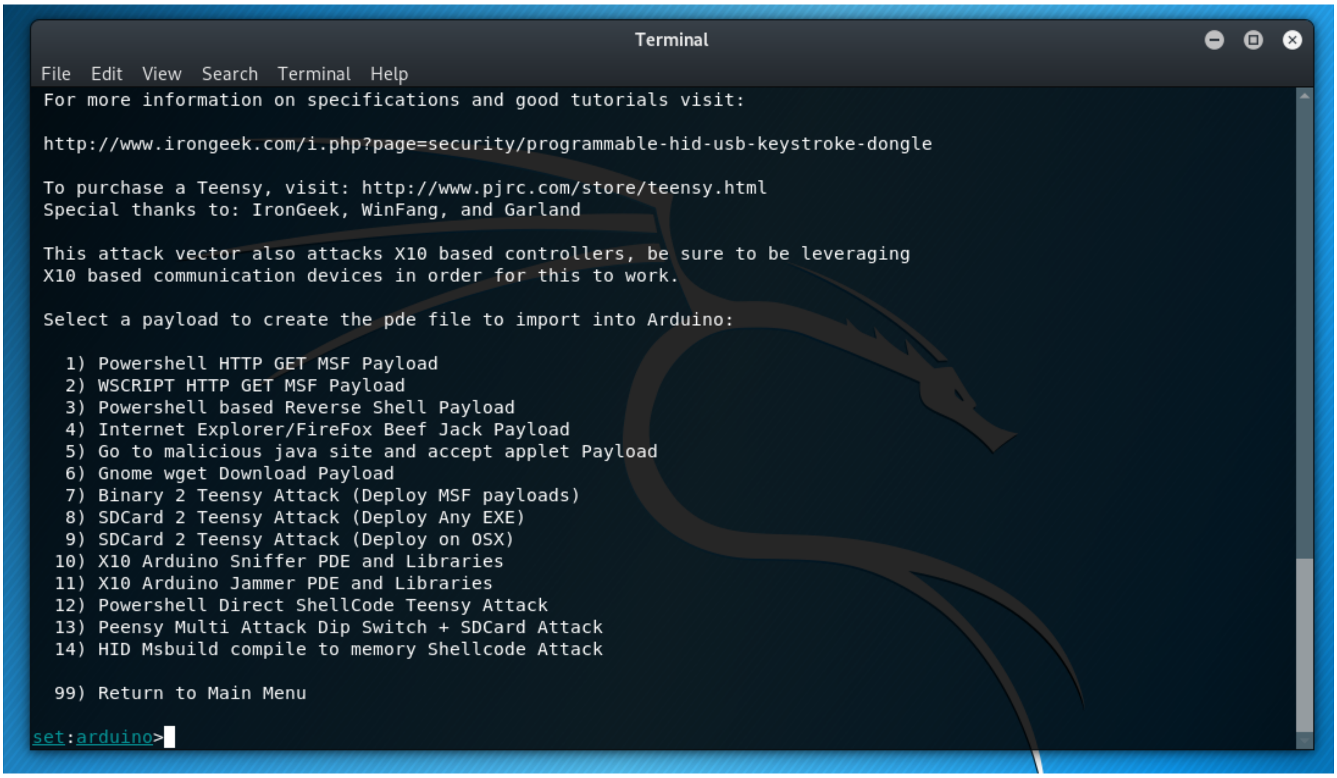
```
 Select from the menu:

   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> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>
```

The Create a Payload and Listener.



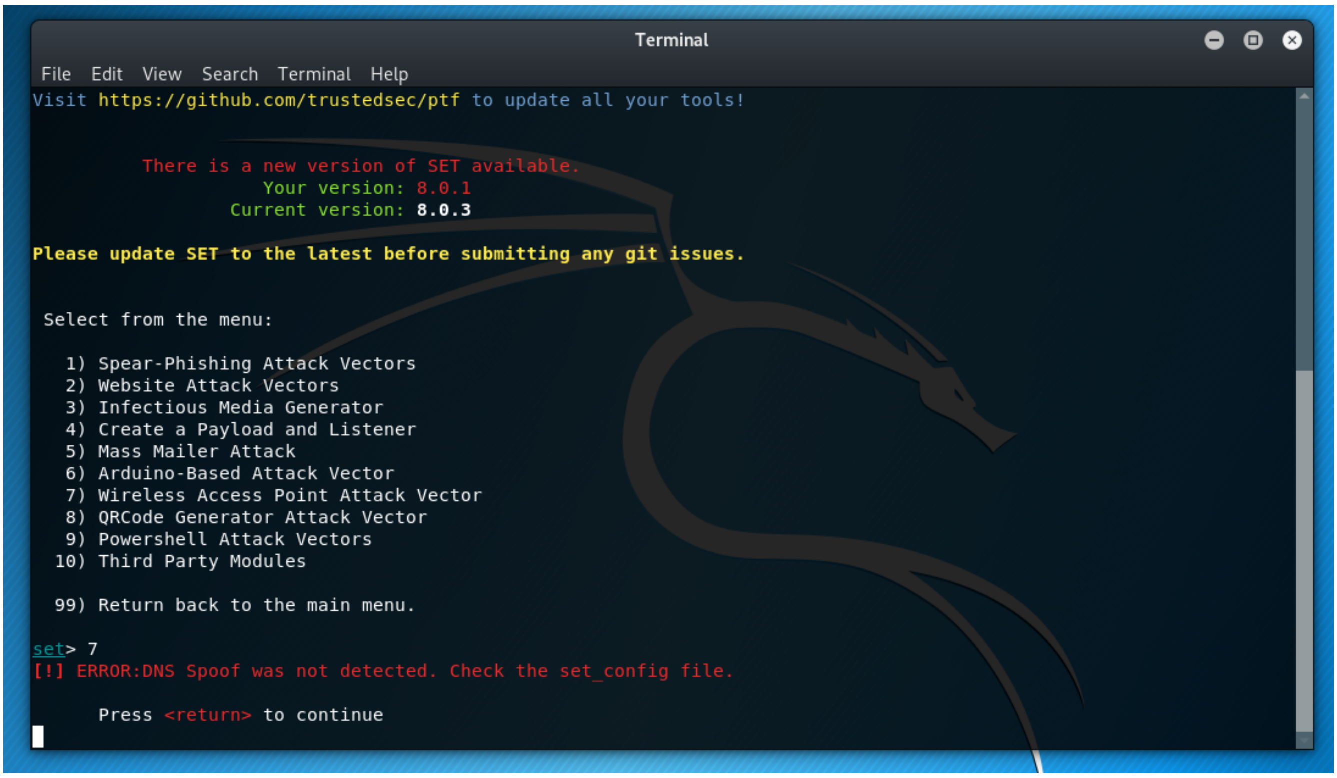
```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  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>
```

The Mass Mailer Attack.



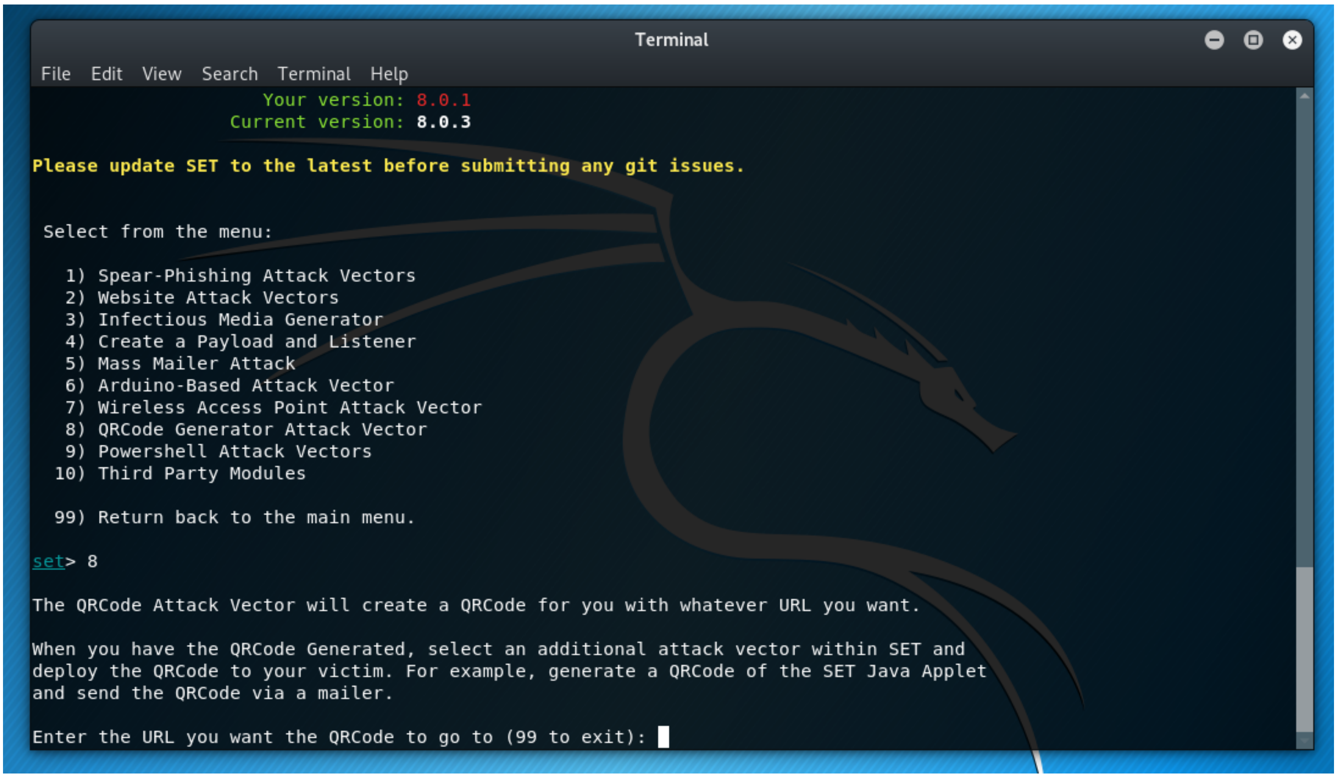
```
 For more information on specifications and good tutorials visit:

 http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle

 To purchase a Teensy, visit: http://www.pjrc.com/store/teensy.html
 Special thanks to: IronGeek, WinFang, and Garland

 This attack vector also attacks X10 based controllers, be sure to be leveraging
 X10 based communication devices in order for this to work.

 Select a payload to create the pde file to import into Arduino:

   1) Powershell HTTP GET MSF Payload
   2) WSCRIPT HTTP GET MSF Payload
   3) Powershell based Reverse Shell Payload
   4) Internet Explorer/FireFox Beef Jack Payload
   5) Go to malicious java site and accept applet Payload
   6) Gnome wget Download Payload
   7) Binary 2 Teensy Attack (Deploy MSF payloads)
   8) SDCard 2 Teensy Attack (Deploy Any EXE)
   9) SDCard 2 Teensy Attack (Deploy on OSX)
  10) X10 Arduino Sniffer PDE and Libraries
  11) X10 Arduino Jammer PDE and Libraries
  12) Powershell Direct ShellCode Teensy Attack
  13) Peensy Multi Attack Dip Switch + SDCard Attack
  14) HID Msbuild compile to memory Shellcode Attack

  99) Return to Main Menu

set:arduino>
```

The Arduino-Based Attack Vector.



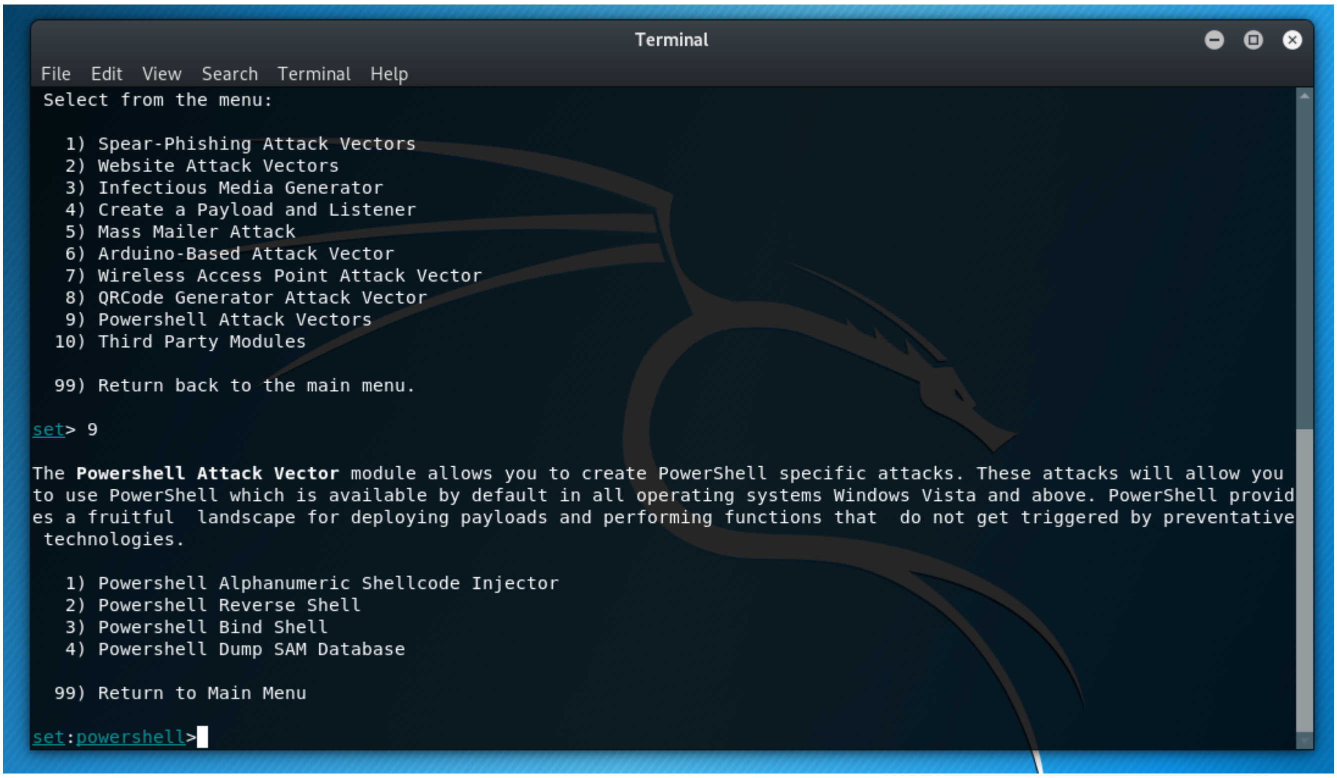
```
Visit https://github.com/trustedsec/ptf to update all your tools!


          There is a new version of SET available.
                     Your version: 8.0.1
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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> 7
[!] ERROR:DNS Spoof was not detected. Check the set_config file.

      Press <return> to continue
```

The Wireless Access Point Attack Vector.



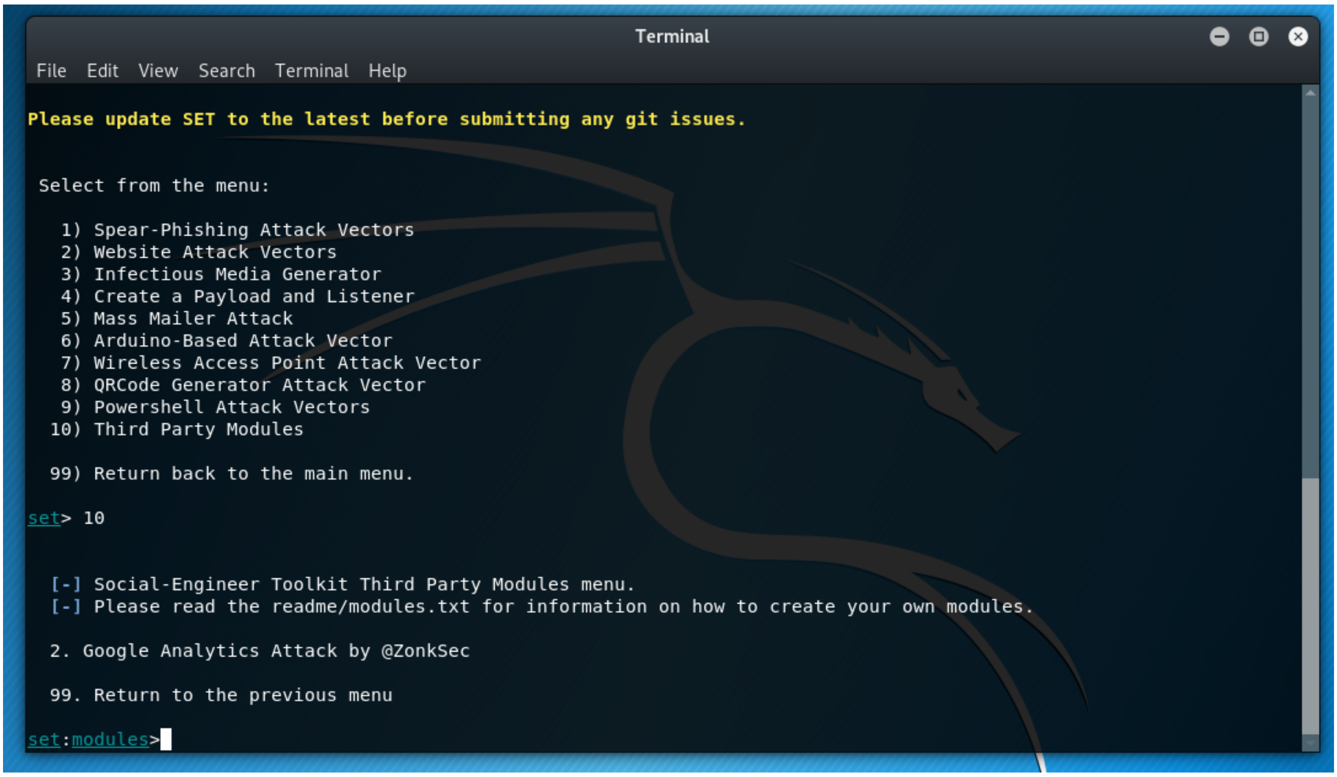
```
                     Your version: 8.0.1
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit):
```

The QRCode Generator Attack Vector.



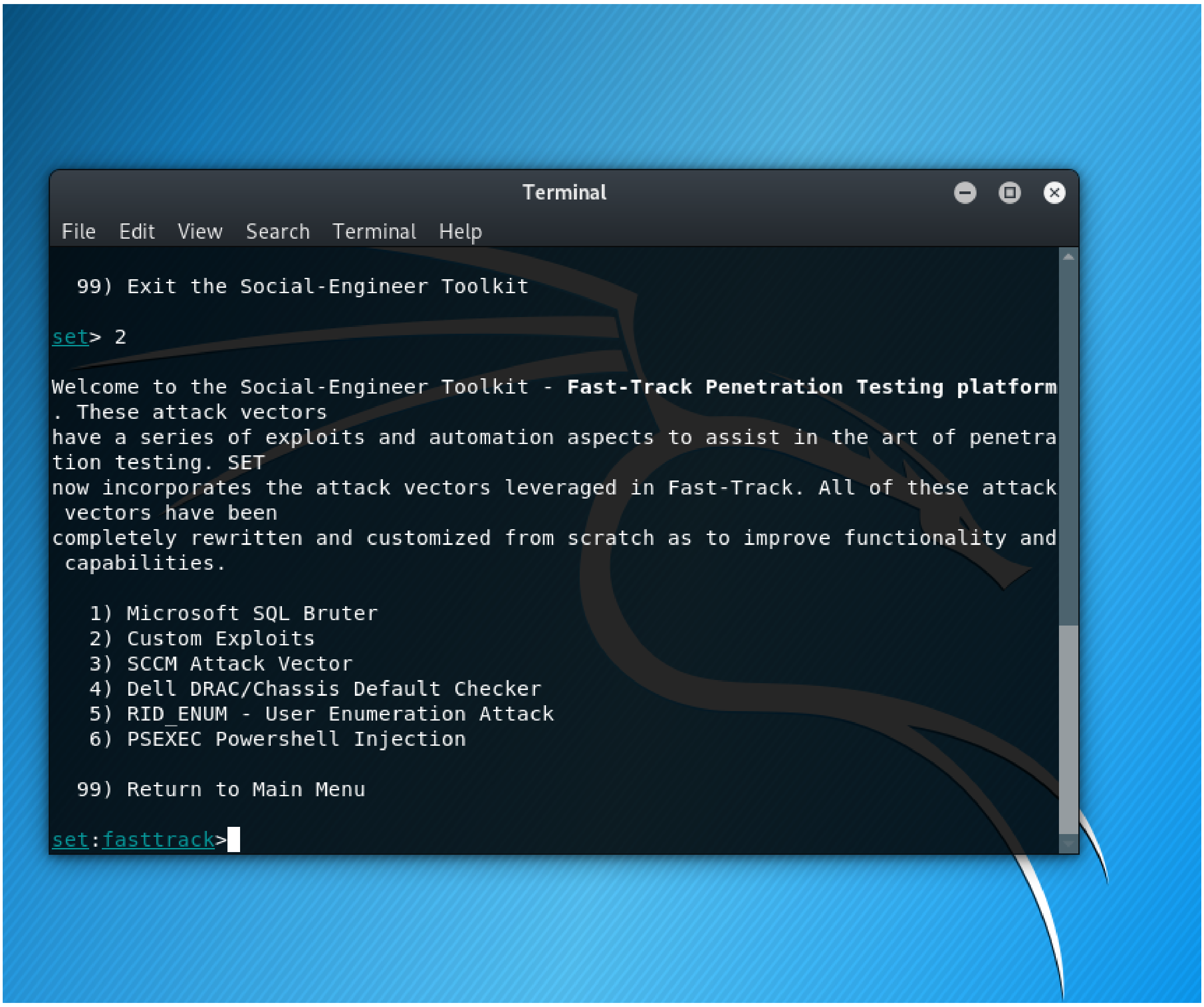
```
 Select from the menu:

   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> 9

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you
to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provid
es a fruitful  landscape for deploying payloads and performing functions that  do not get triggered by preventative
 technologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu

set:powershell>
```

The Powershell Attack Vectors.



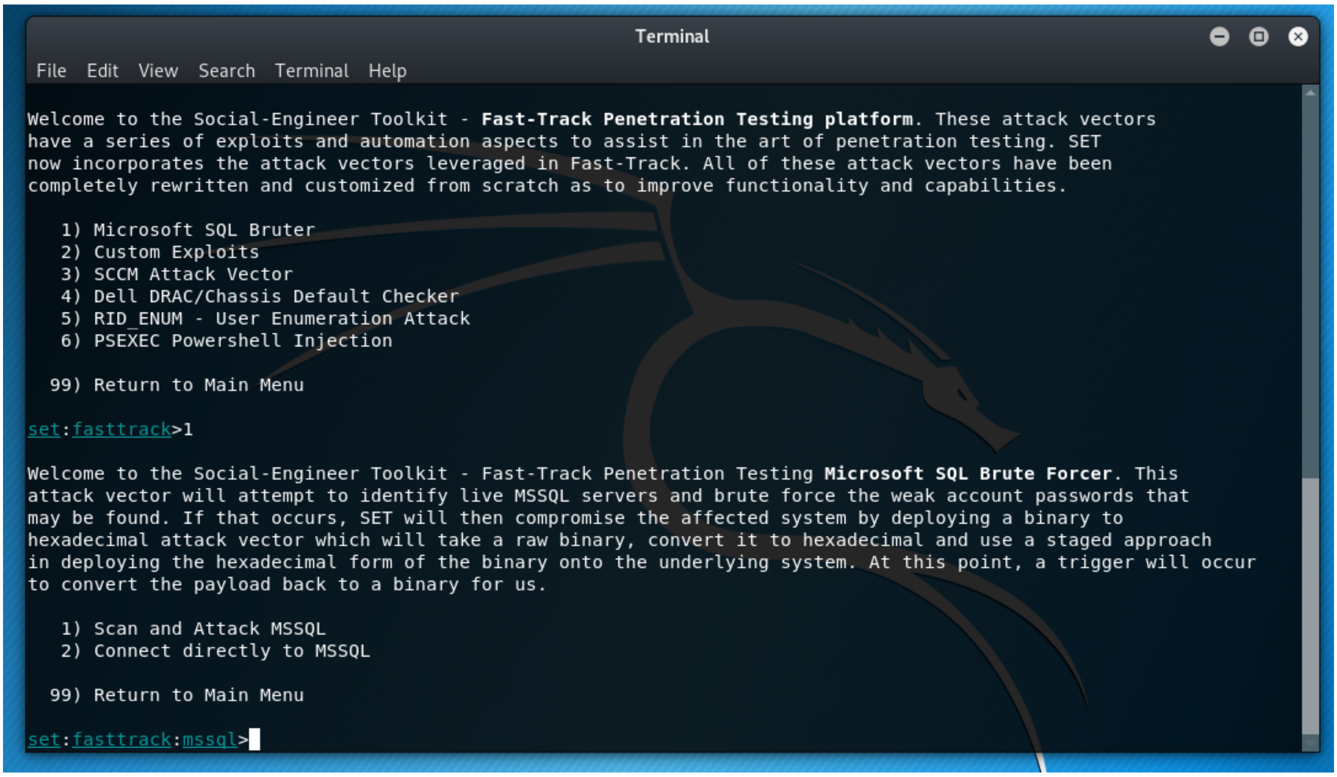
```
Please update SET to the latest before submitting any git issues.


 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> 10


  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your own modules.

  2. Google Analytics Attack by @ZonkSec

  99. Return to the previous menu

set:modules>
```

The Third Party Modules.



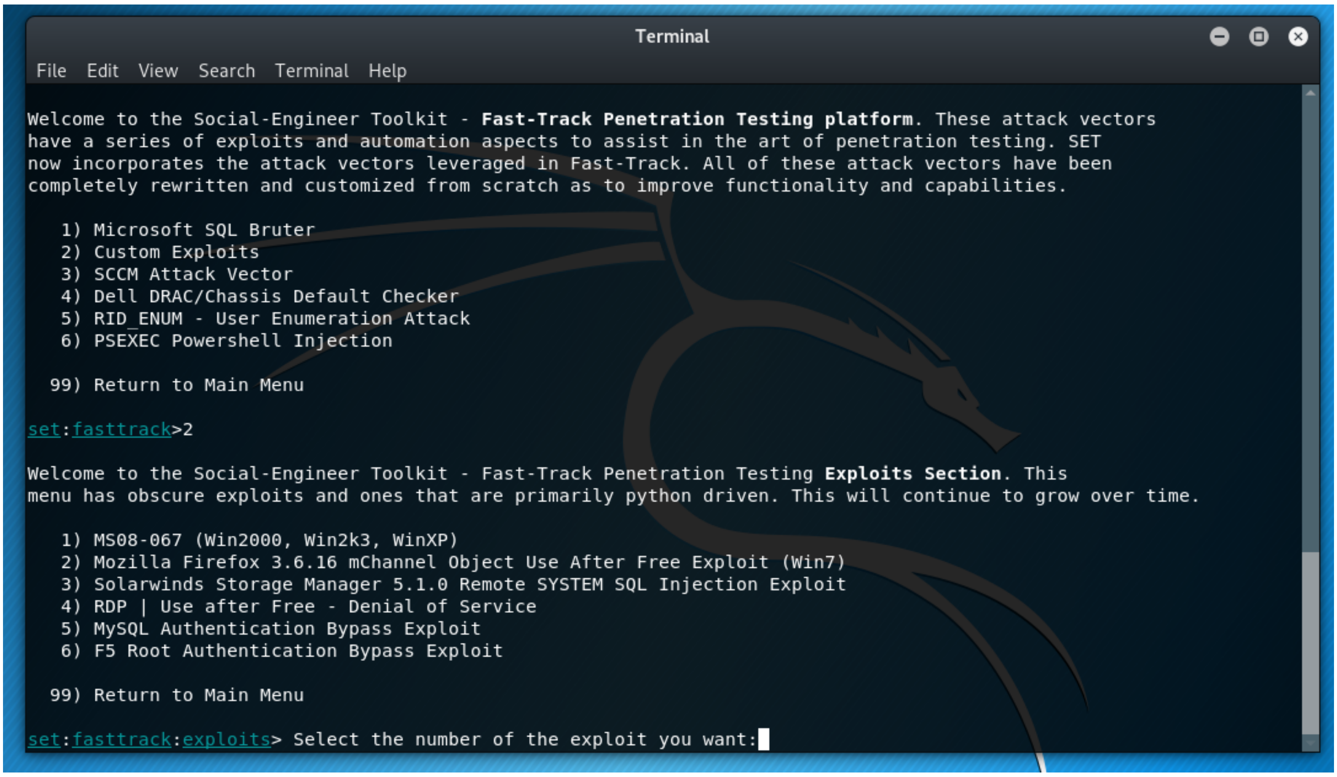
```
  99) Exit the Social-Engineer Toolkit

set> 2

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform
. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetra
tion testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack
 vectors have been
completely rewritten and customized from scratch as to improve functionality and
 capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>
```

The Sub-Menu for the Fast-Track Penetration Testing Platform.



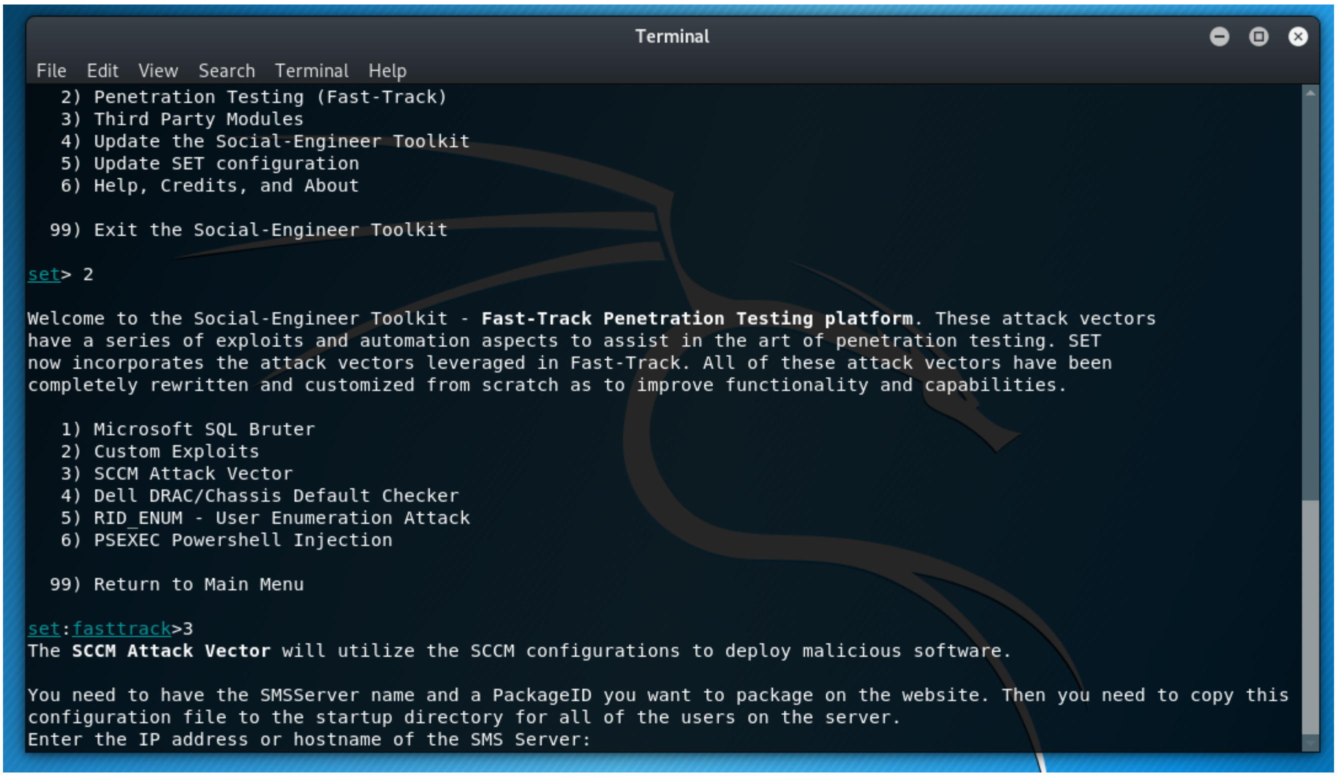
```
Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetration testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack vectors have been
completely rewritten and customized from scratch as to improve functionality and capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>1

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing Microsoft SQL Brute Forcer. This
attack vector will attempt to identify live MSSQL servers and brute force the weak account passwords that
may be found. If that occurs, SET will then compromise the affected system by deploying a binary to
hexadecimal attack vector which will take a raw binary, convert it to hexadecimal and use a staged approach
in deploying the hexadecimal form of the binary onto the underlying system. At this point, a trigger will occur
to convert the payload back to a binary for us.

   1) Scan and Attack MSSQL
   2) Connect directly to MSSQL

  99) Return to Main Menu

set:fasttrack:mssql>
```

The Microsoft SQL Bruter attack tool.



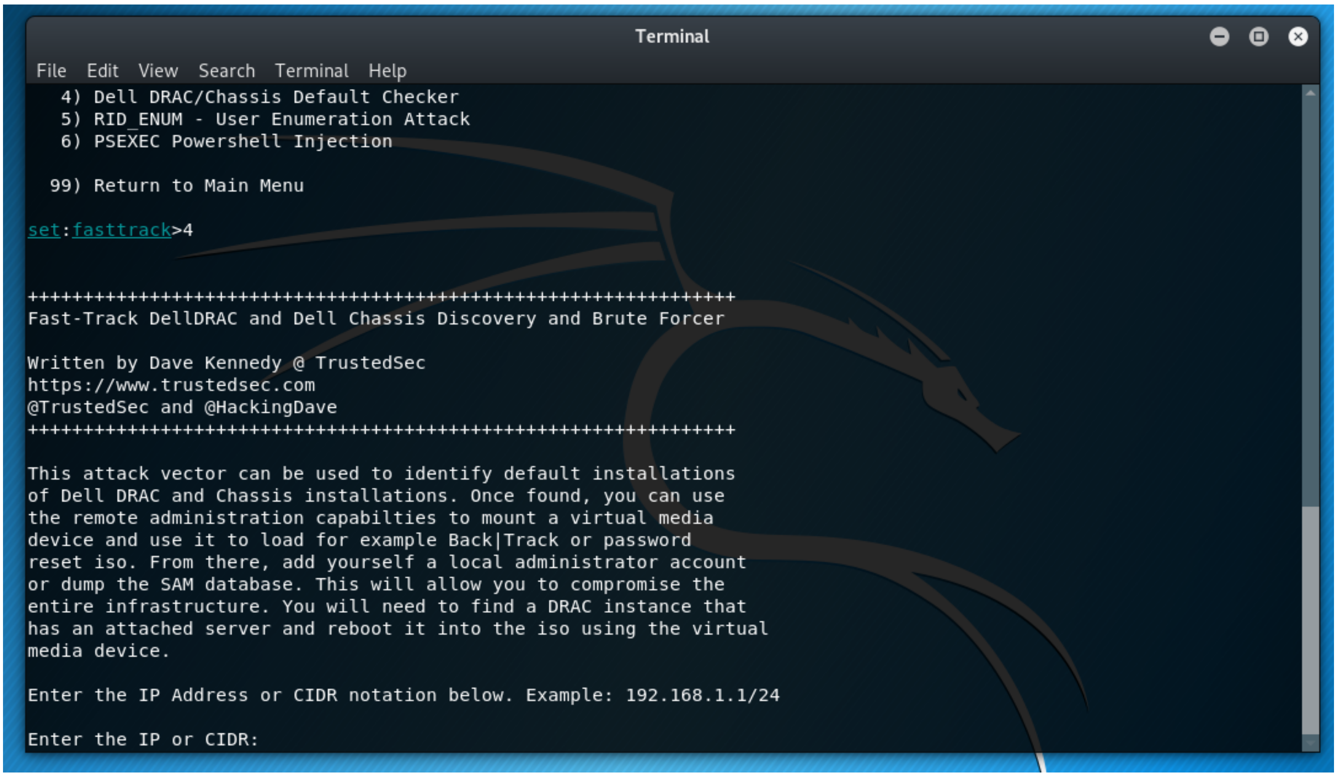
```
Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetration testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack vectors have been
completely rewritten and customized from scratch as to improve functionality and capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>2

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing Exploits Section. This
menu has obscure exploits and ones that are primarily python driven. This will continue to grow over time.

   1) MS08-067 (Win2000, Win2k3, WinXP)
   2) Mozilla Firefox 3.6.16 mChannel Object Use After Free Exploit (Win7)
   3) Solarwinds Storage Manager 5.1.0 Remote SYSTEM SQL Injection Exploit
   4) RDP | Use after Free - Denial of Service
   5) MySQL Authentication Bypass Exploit
   6) F5 Root Authentication Bypass Exploit

  99) Return to Main Menu

set:fasttrack:exploits> Select the number of the exploit you want:
```

The Custom Exploits tool.



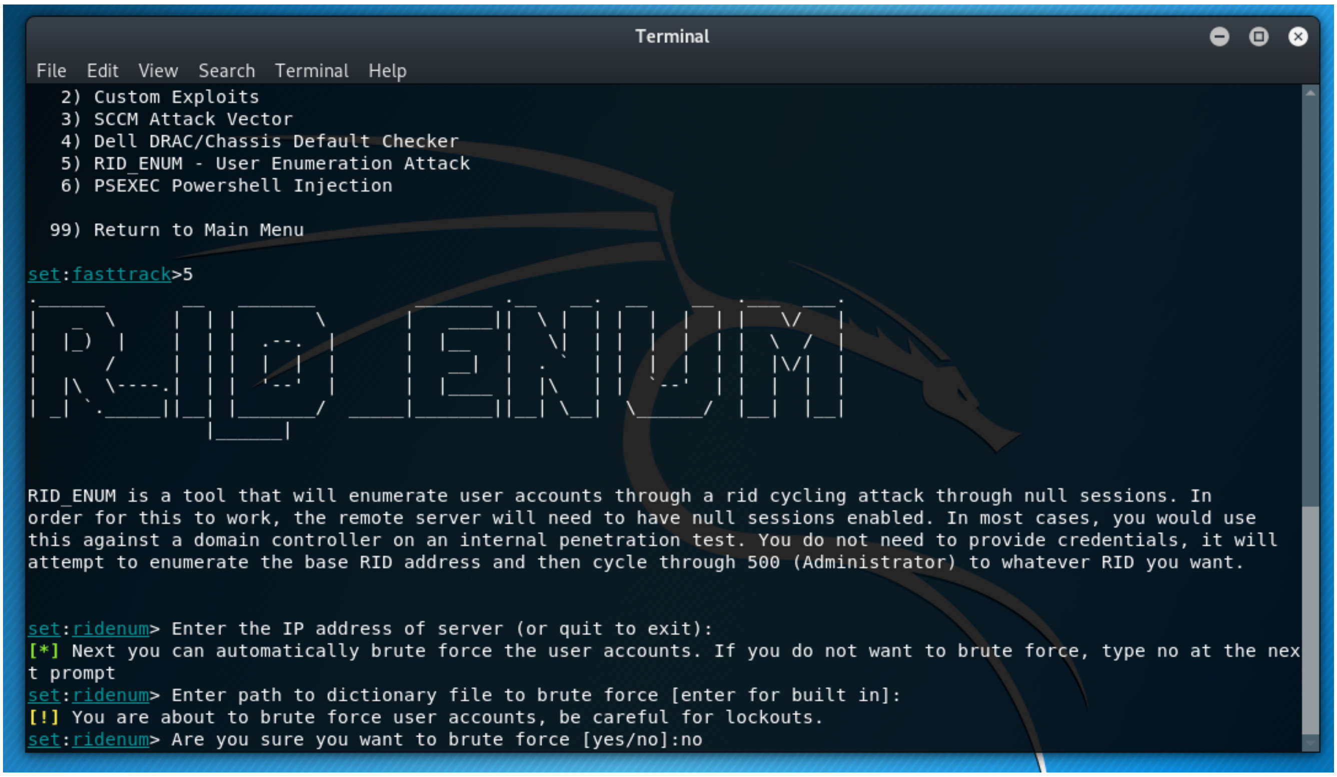
```
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 2

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetration testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack vectors have been
completely rewritten and customized from scratch as to improve functionality and capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>3
The SCCM Attack Vector will utilize the SCCM configurations to deploy malicious software.

You need to have the SMSServer name and a PackageID you want to package on the website. Then you need to copy this
configuration file to the startup directory for all of the users on the server.
Enter the IP address or hostname of the SMS Server:
```

The SCCM attack tool.



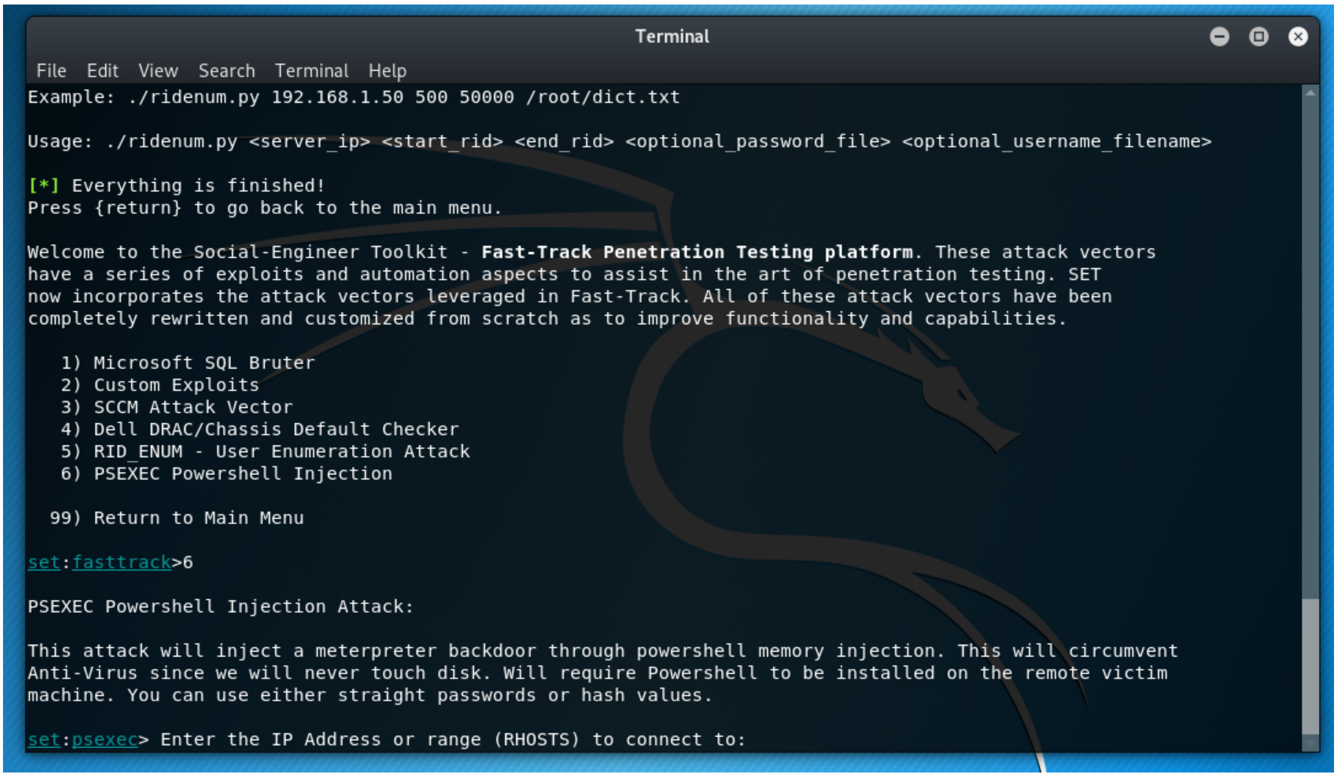
```
    4) Dell DRAC/Chassis Default Checker
    5) RID_ENUM - User Enumeration Attack
    6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>4


+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Fast-Track DellDRAC and Dell Chassis Discovery and Brute Forcer

Written by Dave Kennedy @ TrustedSec
https://www.trustedsec.com
@TrustedSec and @HackingDave
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

This attack vector can be used to identify default installations
of Dell DRAC and Chassis installations. Once found, you can use
the remote administration capabilties to mount a virtual media
device and use it to load for example Back|Track or password
reset iso. From there, add yourself a local administrator account
or dump the SAM database. This will allow you to compromise the
entire infrastructure. You will need to find a DRAC instance that
has an attached server and reboot it into the iso using the virtual
media device.

Enter the IP Address or CIDR notation below. Example: 192.168.1.1/24

Enter the IP or CIDR:
```

The Dell DRAC/Chassis Default Checker tool.



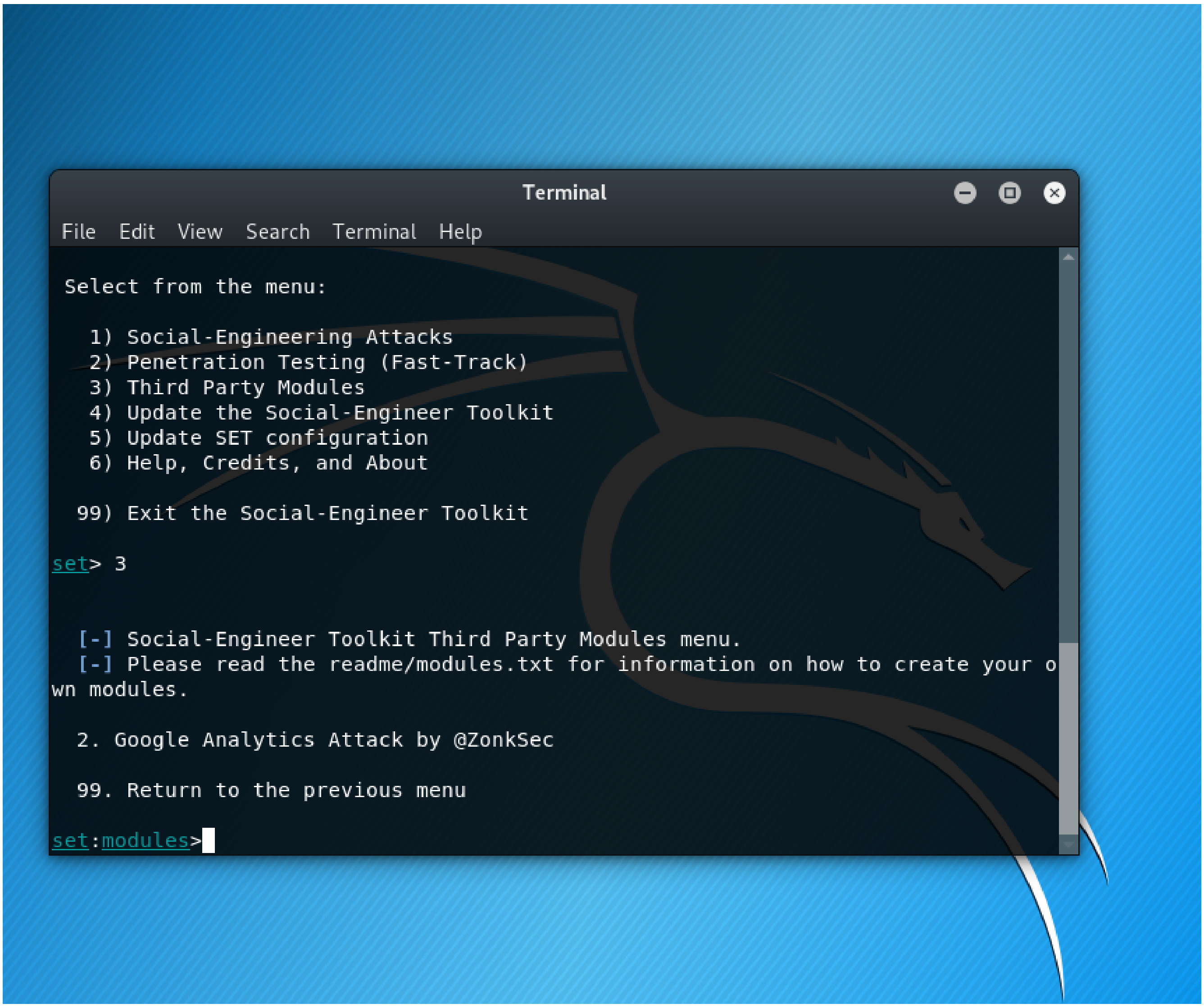
```
    2) Custom Exploits
    3) SCCM Attack Vector
    4) Dell DRAC/Chassis Default Checker
    5) RID_ENUM - User Enumeration Attack
    6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>5
.______       __   _______         _______ .__   __.  __    __  .___  ___.
|   _  \     |  | |       \       |   ____||  \ |  | |  |  |  | |   \/   |
|  |_)  |    |  | |  .--.  |      |  |__   |   \|  | |  |  |  | |  \  /  |
|      /     |  | |  |  |  |      |   __|  |  . `  | |  |  |  | |  |\/|  |
|  |\  \----.|  | |  '--'  |      |  |____ |  |\   | |  `--'  | |  |  |  |
| _| `._____||__| |_______/  _____|_______||__| \__|  \______/  |__|  |__|
                |______|


RID_ENUM is a tool that will enumerate user accounts through a rid cycling attack through null sessions. In
order for this to work, the remote server will need to have null sessions enabled. In most cases, you would use
this against a domain controller on an internal penetration test. You do not need to provide credentials, it will
attempt to enumerate the base RID address and then cycle through 500 (Administrator) to whatever RID you want.


set:ridenum> Enter the IP address of server (or quit to exit):
[*] Next you can automatically brute force the user accounts. If you do not want to brute force, type no at the nex
t prompt
set:ridenum> Enter path to dictionary file to brute force [enter for built in]:
[!] You are about to brute force user accounts, be careful for lockouts.
set:ridenum> Are you sure you want to brute force [yes/no]:no
```

The RID_ENUM [User Enumeration Attack] tool.



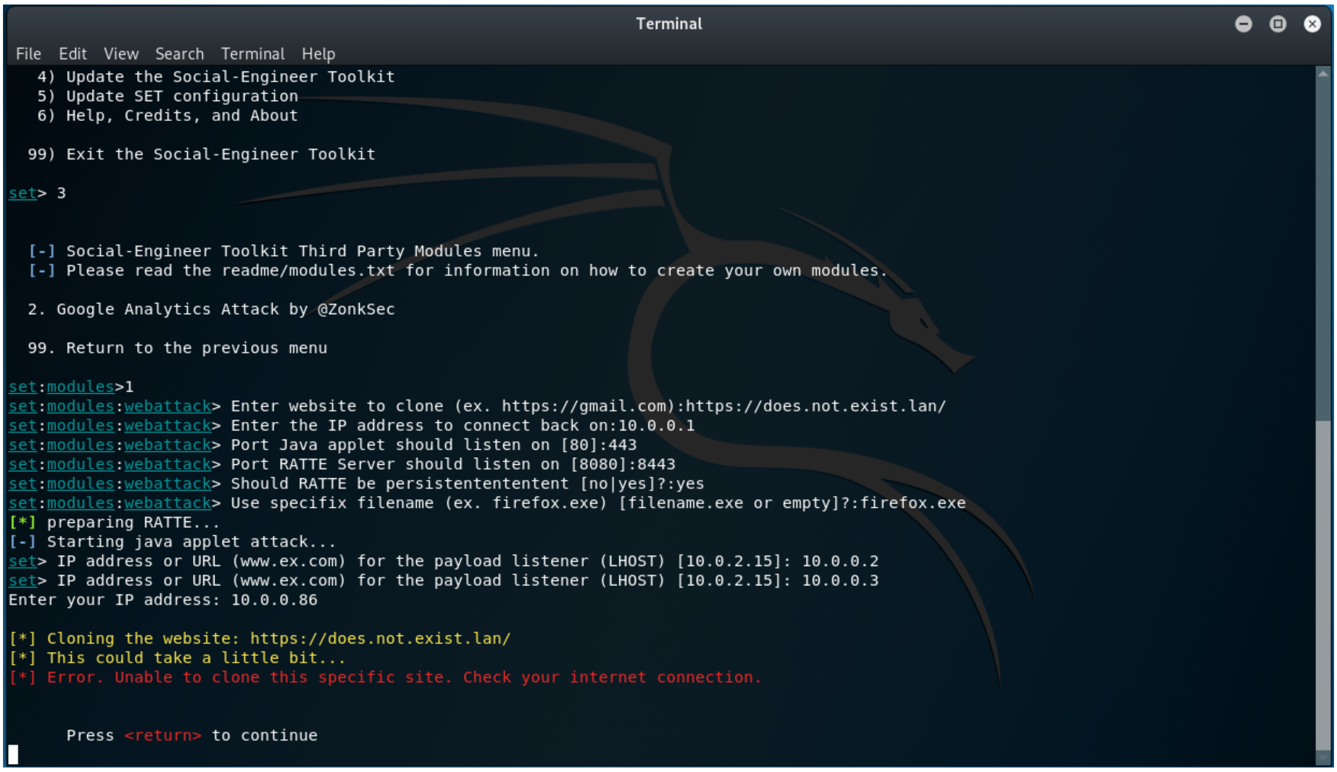
```
Example: ./ridenum.py 192.168.1.50 500 50000 /root/dict.txt

Usage: ./ridenum.py <server_ip> <start_rid> <end_rid> <optional_password_file> <optional_username_filename>

[*] Everything is finished!
Press {return} to go back to the main menu.

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetration testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack vectors have been
completely rewritten and customized from scratch as to improve functionality and capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>6

PSEXEC Powershell Injection Attack:

This attack will inject a meterpreter backdoor through powershell memory injection. This will circumvent
Anti-Virus since we will never touch disk. Will require Powershell to be installed on the remote victim
machine. You can use either straight passwords or hash values.

set:psexec> Enter the IP Address or range (RHOSTS) to connect to:
```

The PSEXEC Powershell Injection attack tool.



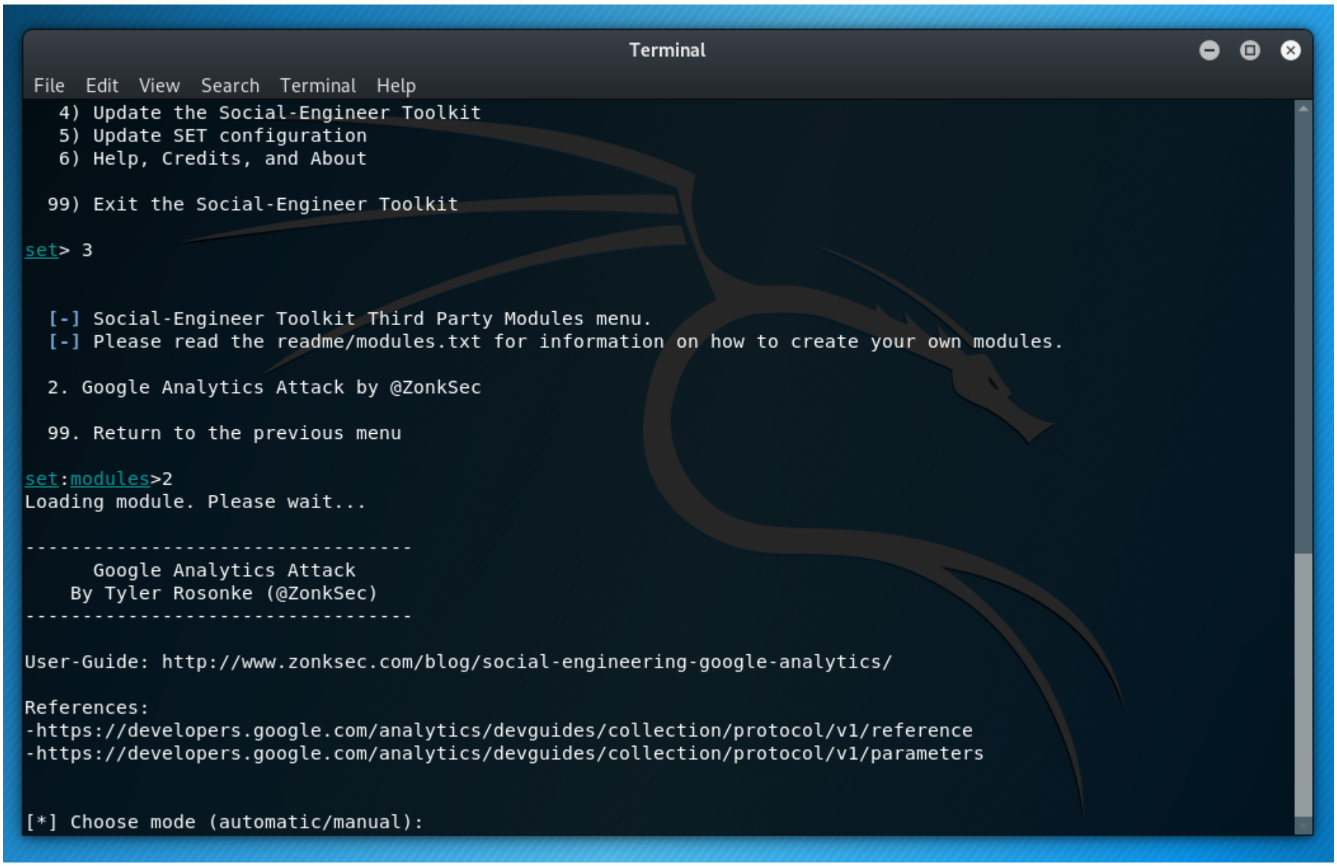
```
 Select from the menu:

   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> 3


  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your o
wn modules.

  2. Google Analytics Attack by @ZonkSec

  99. Return to the previous menu

set:modules>
```

The Third Party Modules menu.



```
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 3


 [-] Social-Engineer Toolkit Third Party Modules menu.
 [-] Please read the readme/modules.txt for information on how to create your own modules.

 2. Google Analytics Attack by @ZonkSec

 99. Return to the previous menu

set:modules>1
set:modules:webattack> Enter website to clone (ex. https://gmail.com):https://does.not.exist.lan/
set:modules:webattack> Enter the IP address to connect back on:10.0.0.1
set:modules:webattack> Port Java applet should listen on [80]:443
set:modules:webattack> Port RATTE Server should listen on [8080]:8443
set:modules:webattack> Should RATTE be persistententent [no|yes]?:yes
set:modules:webattack> Use specifix filename (ex. firefox.exe) [filename.exe or empty]?:firefox.exe
[*] preparing RATTE...
[-] Starting java applet attack...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.0.2.15]: 10.0.0.2
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.0.2.15]: 10.0.0.3
Enter your IP address: 10.0.0.86

[*] Cloning the website: https://does.not.exist.lan/
[*] This could take a little bit...
[*] Error. Unable to clone this specific site. Check your internet connection.


      Press <return> to continue
```

The demo this, the author had to drill into the tool a bit. Of course, providing dummy values here.



```
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 3


  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your own modules.

  2. Google Analytics Attack by @ZonkSec

  99. Return to the previous menu

set:modules>2
Loading module. Please wait...

----------------------------------
      Google Analytics Attack
    By Tyler Rosonke (@ZonkSec)
----------------------------------

User-Guide: http://www.zonksec.com/blog/social-engineering-google-analytics/

References:
-https://developers.google.com/analytics/devguides/collection/protocol/v1/reference
-https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters


[*] Choose mode (automatic/manual):
```

The Help section.

Chapter 6. Conclusion

This review of the Social Engineering Toolkit has taught us about:

- Phishing Attacks
- Website Attacks
- Infection Media Generation
- Creating Payloads and Listeners
- Mass Mail Attacks
- Attacking Wireless Access Points
- QRCode Generation for Attacks
- Powershell Attack Vectors

There are roughly 17 tools designed to attack users presented in this toolkit.

For a Corporation, or a local, state, or Federal Government, this high level examination of this toolkit is one reason that end-user security training is so important in regards to user awareness of where these attacks are coming for them [in the context of what generates an attack]. Their annual security awareness training needs to look at tools like this to demonstrate what attackers are going to be leveraging against them. When walking through a large parking lot and a user finds a thumb-drive; absolutely pick it up and then walk over and insert it into the trash to prevent another less-than suave computer user from doing the unthinkable and inserting it into a computer [preferably crushing it with your heel before you pick it up to render the device defeated]. If someone sends you an email with an attachment, `anything.exe`; delete it and report said to security.

The beauty of tools like this is that it showcases the imagination of the attacker(s) in their craftiness of the messaging to lure human targets into doing something that they should know better not-to-do in the first place. For Companies and Governments, continue to educate your workforce on old and new attack vectors and how to handle said.

Until next time, Secure the System, Live your Life!

Chapter 7. Appendix

References

User Manual:

https://github.com/trustedsec/social-engineer-toolkit/blob/master/readme/User_Manual.pdf

Source code:

https://github.com/trustedsec/social-engineer-toolkit