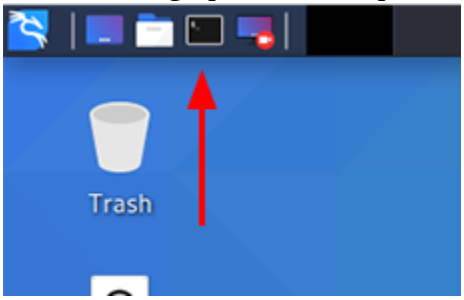
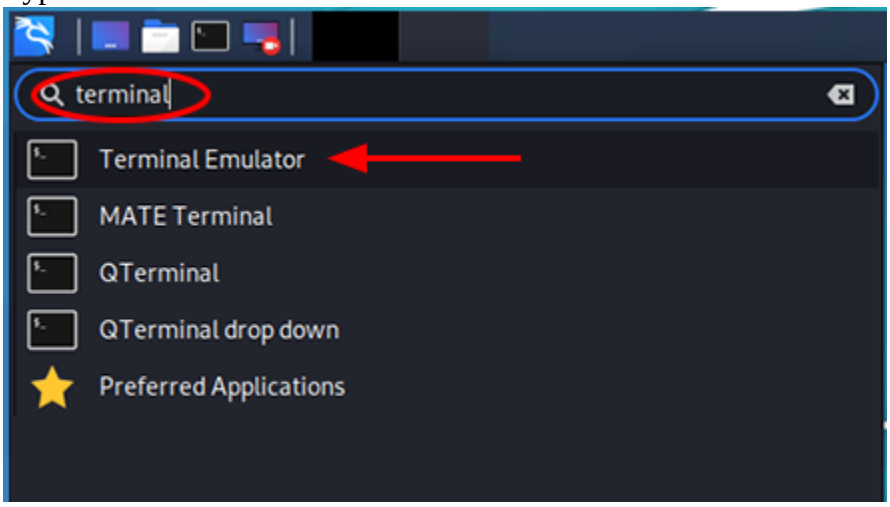
In this laboratory exercise, we are going to explore the different command line tool in Kali Linux Virtual Machine. Instructions in this exercise were excerpts from the book, *Penetration Testing – A Hands-on Introduction to Hacking by Georgia Weidman*.

Opening the Kali Linux Command Line

1. Click on the graphical desktop session.



2. Type "terminal" and select the *Terminal Emulator*.



The Whois Lookups

All domain registrars keep records of the domains they host. These records contain information about the owner, including contact information. To see an example, we are going to run the Whois command line tool on the Kali Linux to query information about *bulbsecurity.com*. If it's a private registration, we won't learn much.

```
root@kali:~# whois bulbsecurity.com
 Registered through: GoDaddy.com, LLC (http://www.godaddy.com)
 Domain Name: BULBSECURITY.COM
 Created on: 21-Dec-11
 Expires on: 21-Dec-12
```

```
Last Updated on: 21-Dec-11

Registrant:
Domains By Proxy, LLC
DomainsByProxy.com
14747 N Northsight Blvd Suite 111, PMB 309
Scottsdale, Arizona 85260
United States

Technical Contact:
Private, Registration BULBSECURITY.COM@domainsbyproxy.com
Domains By Proxy, LLC
DomainsByProxy.com
14747 N Northsight Blvd Suite 111, PMB 309
Scottsdale, Arizona 85260
United States
(480) 624-2599 Fax -- (480) 624-2598

Domain servers in listed order:
NS65.DOMAINCONTROL.COM w
NS66.DOMAINCONTROL.COM
```

The site *bulbsecurity.com* has a private registration, so both the registrant and the technical contact are domains by proxy. Domains by proxy offer private registration, hiding the personal details in the Whois information for the domains of your own. However, we do see the domain servers for this site.

Running Whois queries against other domains will show more interesting results. For example, if you do a Whois lookup on *georgiaweidman.com*, you might get an interesting blast from the past, including the college phone number.

Nslookup

For DNS Reconnaissance, DNS (Domain Name System) servers can be used to learn more about a domain. DNS servers translate the human-readable URL *www.bulbsecurity.com* into an IP address.

Type the command `nslookup www.bulbsecurity.com` on the Kali Linux Command Line.

```
root@Kali:~# nslookup www.bulbsecurity.com
Server: 75.75.75.75
Address: 75.75.75.75#53

Non-authoritative answer:
www.bulbsecurity.com canonical name = bulbsecurity.com.
Name: bulbsecurity.com
Address: 50.63.212.1
```

Nslookup returned the IP address of the *www.bulbsecurity.com*. We can also tell Nslookup to find the mail servers for the same website by looking for MX records (DNS speak for email).

```
root@kali:~# nslookup
> set type=mx
> bulbsecurity.com
Server: 75.75.75.75
Address: 75.75.75.75#53
Non-authoritative answer:
bulbsecurity.com mail exchanger = 40 ASPMX2.GOOGLEMAIL.com.
bulbsecurity.com mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.
bulbsecurity.com mail exchanger = 50 ASPMX3.GOOGLEMAIL.com.
bulbsecurity.com mail exchanger = 30 ALT2.ASPMX.L.GOOGLE.com.
bulbsecurity.com mail exchanger = 10 ASPMX.L.GOOGLE.com.
```

Nslookup says *bulbsecurity.com* is using Google Mail for its email servers.

Host

Another utility for DNS queries is Host. We can ask Host for the name servers for a domain with the command host `-t ns domain`. A good example for domain queries is *zoneedit.com*, a domain set up to demonstrate transfer vulnerabilities, as shown here.

```
root@kali:~# host -t ns zoneedit.com
zoneedit.com name server ns4.zoneedit.com.
zoneedit.com name server ns3.zoneedit.com.
--snip—
```

Searching for Email Addresses

External penetration tests often find fewer services exposed than internal ones do. One excellent way to find usernames is by looking for email address on the Internet. You might be surprised to find corporate email addresses publicly listed on parent-teacher association contact information, sports team roster, and social media.

You can use a Python tool called theHarvester to quickly scour thousands of search engine results for possible email addresses. theHarvester can automate searching Google, Bing, PGP, LinkedIn, and others for email addresses. For example, we'll look at the first 500 results in all search engines for *bulbsecurity.com.*

Type in the command line, `theharvester -d bulbsecurity.com -l 500 -b all`

```
root@kali:~# theharvester -d bulbsecurity.com -l 500 -b all

*******************************************************************
* *
* | |_| |__ ___       /\ /\__ _ _      ____ _____ ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* |  |_| | | | __/ / __ /  (_| | |    \ V /  __/\__ \  || __/ | *
* \__|_| |_|\___|  \/ /_/ \__,_|_|     \_/ \___||___/\__\___|_| *
* *
* TheHarvester Ver. 2.2a *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*******************************************************************

Full harvest..
[-] Searching in Google..
 Searching 0 results...
 Searching 100 results...
 Searching 200 results...
 Searching 300 results...
--snip—

[+] Emails found:
------------------
georgia@bulbsecurity.com

[+] Hosts found in search engines:
-----------------------------------
50.63.212.1:www.bulbsecurity.com

--snip—
```

There’s not too much to be found for *bulbsecurity.com*, but theHarvester found the email address, *georgia@bulbsecurity.com*, and the website *www.bulbsecurity.com*, as well as other websites shared for virtual hosting with. More results can be found if theHarvester is ran against your organization.