Module 13
(Fierce and CeWL)

• At the end of this module, you should have an idea why the Fierce domain scanner can identify hostnames when zone transfer is unavailable. You should also know how to use CeWL to mine a web site for a list of names to be used for host, password, account, or other identification.
Fierce Domain Scanner
From the Applications Menu

- Try to run the fierce domain scanner in kali

- Select from the menu:
  Applications–>
  Kali Linux–>
    Information Gathering–>
      DNS Analysis–>
        fierce

- This prints the fierce help message in a terminal, which says to run it as follows:
  perl fierce.pl ...

- Let's try that by typing `perl fierce.pl` in that terminal
Try Running Fierce

root@kali:~# perl fierce.pl
Can't open perl script "fierce.pl": No such file or directory

• That's no fun at all. What happened?
• The default message is bogus. Fierce isn't installed as a perl script.
• How do I find out where fierce is in Kali?
A Little Bit about Navigating Linux

- The shell is the program that listens to the commands you type in a terminal window.
- The user manual can be accessed by executing the command `man` with a program name following it, presents the manual entry for that program.
- In theory, typing `man man` should tell you everything you need to know (almost).
- A very useful program on most Linux systems to find out about installed software, etc. is `locate`.
- Execute `man locate` to find out about it.
What's a Terminal? (VT-100)
Ancient Terminal – TTY 33.
What about Locating Fierce?

root@kali:~# locate fierce.pl
root@kali:~# locate fierce
/usr/bin/fierce
/usr/share/applications/kali-fierce.desktop
/usr/share/doc/fierce
/usr/share/doc/fierce/changelog.Debian.gz
/usr/share/doc/fierce/copyright
/usr/share/kali-menu/applications/kali-fierce.desktop
/var/lib/dpkg/info/fierce.list
/var/lib/dpkg/info/fierce.md5sums

• Hmmm. It looks like fierce is installed as fierce, not fierce.pl. How can we make sure?
Linux `file` command

- What does it do? `man file`

- Let's find out about `fierce`. It's in `/usr/bin/fierce`. That means that from the root directory, we traverse into the `usr` subdirectory, then to the `bin` subdirectory of that, then we find the file `fierce`.

- What file type is it?
  
  `root@kali:~# file /usr/bin/fierce`
  `/usr/bin/fierce: Perl script, ASCII text executable`
So Let's Try to Run Fierce Again

root@kali:~# fierce -dns cise.ufl.edu
DNS Servers for cise.ufl.edu:
ns0.cise.ufl.edu
...
Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the default wordlist
Exiting...

- Whoa! What happened?
- Fierce needs a hosts.txt file or a default wordlist. Let's check the source code
How do I check the source file?

- I use less. To find out: `man less` (of course)
- Start up less
  
  `less /usr/bin/fierce`

- Then search for hosts.txt by typing
  `/hosts.txt`

- Then see some wonderful perl code to see what the program tried to do.
What Did Fierce Do?

- What did less show me?

```perl
output("Okay, trying the good old fashioned way... brute force");
$wordlist = $wordlist || 'hosts.txt';
if (-e $wordlist) {
    # user provided or default
    open (WORDLIST, '<', $wordlist) or
    open (WORDLIST, '<', 'hosts.txt') or
    quit_early("Can't open $wordlist or the default wordlist");
```

- The red portion tries to open the file `hosts.txt` in the current directory. Hackers don't always write the best code, but it usually works.

- This is something we can handle if we can find the hosts.txt file. Where should we look?
The Internets!

- Searching for *fierce hosts.txt* we get luck: http://ha.ckers.org/fierce/hosts.txt

- That is a list of 2280 common host names. Fierce uses those to look up specific host names within the domain. It then looks up and down the IP address range doing reverse lookups of nearby (+-5) IP addresses.

- Copy the hosts.txt file into your current directory (~, i.e, the root's home directory) and run again.
How Did Fierce Do?

- It found 175 host names in cise.ufl.edu
- Can we do better? What if we have a better wordlist?
- We can get one using CeWL from Robin Wood (digininja). CeWL scans a web site looking for words to be used in a password, account name, etc. It is useful for generating custom word lists for a site.
- CeWL can be found in the Kali menu:

  Applications->
  Kali Linux->
  Password Attacks->
  Online Attacks->
  cewl
What Does CeWL Buy Us?

- First run CeWL
  
  cewl http://cise.ufl.edu -w cise-wordlist

- This looks 2 pages deep and grabs all strings 3 characters or longer. It finds 12,492 words. 10,362 are unique up to case.

- Adding these to the 2,280 words in hosts.txt yields 12,160 unique words.

- Running fierce with these words takes much longer, but yields 77 undiscovered hosts such as acm.cise.ufl.edu and various skypephones. It found 11 extra hosts with 10.227.xxx.xxx addresses.